ЛЬВІВСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
БЕЗПЕКИ ЖИТТЄДІЯЛЬНОСТІ

Р. Л. Ткачук
Н. О. Маслова
А. І. Івануса

ОСНОВИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ та КІБЕРЗАХИСТУ

НАВЧАЛЬНИЙ ПОСІБНИК

Львів
2025

УДК 004.056(075.8)

Рекомендовано рішенням Вченої ради
Львівського державного університету
безпеки життєдіяльності
(Протокол від 04.06.2025 № 10)

Рецензенти:

Людмила КОВАЛЬЧУК, д-р техн. наук, професор, провідний науковий співробітник відділу математичного та комп'ютерного моделювання Інституту проблем моделювання в енергетиці ім. Г.Є.Пухова НАН України

Євген МАРТИН, доктор технічних наук, професор, прфесор кафедри інформаційних технологій та систем електронних комунікацій Львівського державного університету безпеки життєдіяльності

Т45 Ткачук Р. Л., Маслова Н. О., Івануса А. І. *Основи інформаційної безпеки та кіберзахисту: навч. посібник / Р. Л. Ткачук, Н. О. Маслова, А. І. Івануса.* — Львів: ЛДУБЖД", 2025. — 271 с

ISBN 978-617-8654-19-1

Навчальний посібник висвітлює ключові аспекти інформаційної безпеки, актуальні для сучасного цифрового середовища. У ньому розглянуто принципи захисту інформації, методи виявлення загроз і вразливостей, шифрування даних, формування цифрових підписів, стратегії протидії зловмисникам і принципи побудови систем безпеки. Особливу увагу зосереджено на питаннях захисту даних у повсякденній діяльності та в умовах війни, а також на типах шкідливого програмного забезпечення, кіберзлочинності й кібервійні.

Матеріал подано у доступній формі з використанням прикладів та ілюстрацій, що сприяє легкому засвоєнню матеріалів. Завдання для самоперевірки та практичні вправи допоможуть закріпити знання та розвинути навички у сфері кібербезпеки.

Посібник стане корисним для студентів спеціальностей 125 "Кібербезпека" та 122 "Комп'ютерні науки", а також для всіх, хто цікавиться питаннями захисту інформації і прагне набути практичних навичок протидії кіберзагрозам та кіберзлочинності.

УДК 004.056(075.8)

ЗМІСТ

ТЕМА 1. ВСТУП ДО КІБЕРБЕЗПЕКИ

Курс «Основи інформаційної безпеки» призначений для ознайомлення та вивчення кібербезпеки з точки зору перспективної спеціалізації в IT-кар'єрі.

Матеріали цього курсу допоможуть розвинути навички, необхідні для:

- *розуміння важливості безпечної поведінки в Інтернеті;*
- *опису різних типів шкідливого програмного забезпечення та атак;*
- *опису стратегій, які використовують організації для захисту від атак.*

У цій темі пояснюється, що таке кібербезпека і чому попит на фахівців з кібербезпеки продовжує зростати. Пояснюється, що таке онлайн-ідентифікація, що таке дані, де вони знаходяться в мережі і чому так цікавлять кіберзлочинців.

У цій темі також пояснюється, що таке дані організації та чому їх важливо захищати. Ви дізнаєтесь, хто такі кіберзловмисники і що їм потрібно. Фахівці з кібербезпеки повинні мати такі самі навички, що й кібернападники, але повинні працювати в межах місцевого, національного та міжнародного законодавства. Професіонали з кібербезпеки також мають використовувати свої навички, не порушуючи етичних норм.

Також ця тема містить матеріали, в яких коротко пояснюється що таке кібервійна та чому країнам та урядам потрібні фахівці з кібербезпеки для захисту громадян та інфраструктури.

1.1. ПОТРЕБА У КІБЕРБЕЗПЕЦІ

Існує велика кількість груп даних, які утворюють різні домени «кіберсвіту». Якщо групи можуть збирати і обробляти велику кількість даних, вони починають накопичувати силу і вплив. Ці дані можуть бути у вигляді чисел, зображень, відео, аудіо або у вигляді будь-якого типу даних, який може бути поданий у цифровій формі. Групи можуть стати настільки потужними, щоб діяти як окремі сили, створюючи окремі області кібербезпеки.

Слово «domain» (домен) має велику кількість значень. У технічному значенні домен — це унікальне ім'я, яке ідентифікує вебсайт або сервер в Інтернеті. У контексті кібербезпеки "домен" використовується метафорично, щоб описати сукупність пов'язаних систем, даних і операцій, які потрібно захищати. Будь-яку область, де існує контроль, авторизація або захист, можна вважати доменом. В цьому сенсі домен розглядається як область, яка підлягає захисту. Вона може бути обмежена логічною або фізичною межею. Це буде залежати від розміру задіяної системи. У багатьох аспектах, експерти в області кібербезпеки, повинні захищати свої домени відповідно до законів своєї країни.

Такі компанії, як Google, Facebook і LinkedIn, можуть вважатися доменами даних в нашому кіберсвіті. Розвиваючи цю аналогію далі – люди, які працюють в цих компаніях, можуть вважатися експертами з кібербезпеки.

Експерти Google створили один з перших і найпотужніших доменів у відкритому кіберсвіті Інтернету (Додаток 1). Мільярди людей щоденно використовують Google для пошуку в Інтернеті. Ймовірно Google, створив найбільшу в світі інфраструктуру збору даних**.** ***Google*** розробив Android – операційну систему, встановлену на більше, ніж 80% всіх мобільних пристроїв, підключених до Інтернету. Кожен пристрій вимагає від користувачів створення облікових записів Google. За допомогою облікового запису Google можна відстежувати історію пошуку, зберігати закладки та інформацію про обліковий запис. Крім того, можна знаходити свої пристрої, синхронізувати дані між ними, що спрощує доступ і керування особистим контентом і налаштуваннями.

Пошукові машини Google дають змогу шукати не тільки серед вебсайтів, але й в більш вузьких джерелах інформації.

Коли Google проіндексував більше HTML-сторінок в Інтернеті, ніж будь-який інший пошуковик, інженери компанії звернулися до інших, менш доступних джерел інформації. Так з'явилися функції пошуку по телефонним номерам, адресам, словникам і довідникам. Пізніше Google пішов ще далі. І тепер ми можемо шукати на Google новини, патенти, статті в журналах, картинки, книги, відеоролики і багато чого іншого (Таблиця 1). І це далеко не повний перелік !

Таблиця 1. Окремі Сервіси Google та їх статус

Назва	URL	стан	сфера
Google Картинки (Google Images)	https://www.google.com.ua/imghp?hl=uk	працює	зображення
Google відео (Google Video)	https://www.google.com/videohp?hl=uk	закритий	пошук і скачування відео
Google Авіабілети (Google Flights)	https://www.google.com/travel/flights/	працює	авіабілети
Google Блоги	https://blogsearch.google.com/	працює	блоги
Google Коди (Google Codes)	http://www.google.com/codesearch	закритий	вихідні коди
Google Академія (Google Scholar)	https://scholar.google.com.ua/	працює	наукові статті, публікації
Google Shopping	https://shopping.google.com/	працює	товари в інтернет-магазинах
Google Карти (Google Maps)	https://www.google.com/maps	працює	географічні карти, маршрути

Масштаб і значення зібраних Google даних, включаючи інформацію про пошукові запити, пристрої користувачів та їхню активність, роблять компанію критично важливою в екосистемі Інтернету, але водночас підвищують її вразливість до кібератак, таких як викрадення персональних даних, зловживання інформацією через соціальну інженерію чи компрометація хмарних сервісів.

Повернемось до згаданих вище Facebook і LinkedIn.

Facebook є одним з основних і найбільш впливових онлайн-ресурсів в Інтернеті, що забезпечує доступ до широкого спектру можливостей для користувачів по всьому світу. Експерти в Facebook виявили, що люди щодня створюють персональні облікові записи для спілкування з родиною та друзями. Роблячи це, вони добровільно надають значний обсяг особистих даних. Facebook щоденно впливає на мільйони людей і дає змогу компаніям та організаціям спілкуватися з людьми персоналізовано і цілеспрямовано. З точки зору кібербезпеки, Facebook є важливим доменом через величезну кількість користувачів і даних, що зберігаються на платформі. Це робить Facebook привабливою ціллю для кіберзагроз, таких як фішинг, шахрайство, зломи акаунтів та порушення конфіденційності. Для запобігання таким загрозам важливо застосовувати заходи на кшталт автентифікації, регулярного оновлення паролів і активного відстеження підозрілих дій на облікових записах.

LinkedIn – це ще один домен зберігання даних в Інтернеті. Експерти LinkedIn підтверджують, що учасники цієї мережі діляться інформацією про свої досягнення з метою створення мережі професійних контактів. Користувачі LinkedIn надають інформацію для створення онлайн-профілів і контактів з іншими учасниками цієї соціальної мережі. LinkedIn сприяє зв’язкам працівників з роботодавцями, а компаніям з іншими компаніями у всьому світі.

Для LinkedIn, як і для інших соціальних мереж, необхідно впроваджувати суворі заходи безпеки. Платформа, орієнтована на професіоналів, зберігає значний обсяг персональної та корпоративної інформації, що робить її мішенню для фішингу, атак на акаунти та витоків даних. Використання двофакторної автентифікації, перевірка налаштувань конфіденційності та обережність у взаємодії з підозрілими контактами є важливими заходами для захисту облікових записів і збереження особистих даних.

LinkedIn і Facebook мають багато схожих рис. На базовому рівні ці домени є потужними через здатність збирати дані, які надаються самими користувачами. Ці дані часто включають в себе біографічні дані користувачів, їх коментарі, симпатії, місця, що були відвідані, подорожі, інтереси, друзів і членів сім’ї, професію, хобі, а також робочий і особистий графік. Для організацій, що зацікавлені у використанні цих даних для кращого розуміння і спілкування з своїми клієнтами та співробітниками, така інформація має велику цінність.

Для порушників кібербезпеки інформація з LinkedIn і Facebook може мати високу цінність. Так, інформація, розміщена на LinkedIn, дає змогу здійснювати цільові атаки, такі як фішинг чи атаки з використанням соціальної інженерії. Facebook містить багатий обсяг особистої інформації, що може бути використано для зловмисних цілей, таких як ідентифікація жертв або створення фальшивих профілів. Обидві платформи є потенційними джерелами для кіберзлочинців.

Що таке кібербезпека?

Під'єднання до електронної інформаційної мережі стало невід'ємною частиною нашого повсякденного життя. Усі види організацій, такі як медичні, фінансові та навчальні заклади, використовують цю мережу для ефективного функціонування. Вони використовують мережу для збору, обробки, зберігання та обміну великою кількістю цифрової інформації. Чим більше цифрової інформації збирається і чим частіше вона спільно використовується, тим важливішим стає захист цієї інформації забезпечення національної безпеки та економічної стабільності.

Рис. 1.1. Кібербезпека[1]

Кібербезпека – це безпека IT систем (обладнання та програм).

Інформаційна безпека – це безпека інформації, зазвичай організацій чи компаній, у тому числі в IT системах. Кібербезпека є частиною Інформаційної безпеки будь-якої організації (рис. 1.1).

Приклади.

Наскільки захищений ваш домашній комп'ютер чи ваш вебсайт від зламу хакерами – це питання кібербезпеки. Але чи кріпите ви стікер із записаним паролем від комп'ютера чи профайлу у соцмережі на екран свого монітора – це вже питання вашої Інформаційної безпеки.

Кібербезпека включає в себе не тільки захист інформації, а й захист від різноманітних кіберзагроз, таких як хакерські атаки, віруси, шкідливе програмне забезпечення та інші загрози, які можуть вплинути на цифрові системи та мережі. На рівні підприємств та урядів кібербезпека стає критично важливою для захисту комунікацій, фінансових даних, інфраструктури та для запобігання кібертероризму.

[1] - https://www.researchgate.net/publication/317646127_Analiza_e_sulmeve_kibernetike_ne_ambientin_DVWA/figures?lo=1

Кібербезпека – це постійні зусилля спрямовані на захист мережевих систем та усіх видів даних від несанкціонованого використання або пошкодження. На особистому рівні вам необхідно захищати свій обліковий запис, дані та електронні пристрої. На корпоративному рівні відповідальність кожного співробітника полягає в захисті репутації організації, її даних та клієнтів. На державному рівні – це питання національної безпеки, а також безпеки та добробуту громадян.

1.2. ВАША ОНЛАЙН ТА ОФЛАЙН - ІДЕНТИФІКАЦІЯ

Рис. 1.2. Онлайн ідентичність[2]

Чим більше часу ви проводите в Інтернеті, тим сильніше на ваше життя може вплинути ваша ідентичність як в Інтернеті, так і в офлайні (рис. 1.2). Ваша офлайн-ідентичність – це ви самі, особа, з якою ваші друзі та сім'я взаємодіють щодня вдома, у школі чи на роботі. Оточуючі знають ваші персональні дані, а саме ваше ім'я, вік або місце проживання. Ваша ідентичність в Інтернеті – це ви у кіберпросторі. Ваша онлайн-ідентичність – це те, як ви представляєте себе іншим в Інтернеті. Ця онлайн-ідентичність має розкривати лише мінімум інформації про вас.

Будьте обачні, обираючи ім'я користувача або псевдонім для себе в Інтернеті. Ім'я користувача не повинно містити жодної особистої інформації. Це має бути щось доречне і прийнятне. Ім'я користувача не повинно давати привід стороннім людям подумати, що ви є легкою ціллю для кіберзлочинців або хочете привернути небажану увагу.

Ваші дані

Будь-яка інформація про вас може вважатися вашими персональними даними. Персональна інформація може однозначно ідентифікувати вас як особистість. Ці дані включають фотографії та повідомлення, якими ви обмінюєтесь з родичами та друзями в Інтернеті. Інша інформація, така як ім'я, номер соціального страхування, дата і місце народження або дівоче прізвище матері, відома лише вам і використовується для встановлення вашої особистості.

[2] - https://thumbs.dreamstime.com/z/%D0%BE%D0%BD-%D0%B0%D0%B9%D0%BD-%D0%B8-%D0%B5%D0%BD%D1%82%D0%B8%D1%87%D0%BD%D0%BE%D1%81%D1%82%D1%8C-32032778.jpg?w=768

Такі відомості, як медична, освітня, фінансова інформація та дані про працевлаштування також можуть бути використані для ідентифікації вас в Інтернеті (рис.1.3).

Медичні записи (медична карта пацієнта)

Щоразу, коли ви відвідуєте кабінет лікаря, до вашої електронної медичної картки (electronic health records, EHR) додається ще більше інформації. Рекомендації сімейного лікаря також вносяться до вашої картки. Вона містить інформацію про ваше фізичне і психічне здоров'я та інші особисті дані, які можуть бути не пов'язані зі здоров'ям.

Рис. 1.3 Відомості про особу[3]

Наприклад, якщо ви в дитинстві отримували консультації психолога в період серйозних змін у родині, це буде зафіксовано у вашій медичній картці. Окрім відомостей про перенесені захворювання та особистої інформації, картка може містити інформацію про вашу сім'ю.

Медичні пристрої, такі як фітнес-браслети, використовують хмарну платформу для забезпечення бездротового передавання, зберігання та відображення таких клінічних показників, як частота серцевих скорочень, артеріальний тиск і рівень цукру в крові. Ці пристрої здатні генерувати величезну кількість клінічних даних, які можуть стати частиною вашої медичної картки.

Записи про освіту

Коли ви здобуваєте освіту, інформація про ваші оцінки та результати тестування, відвідування занять, курси, нагороди та присвоєні ступені, а також будь-які записи про дисциплінарні порушення можуть бути відображені у цих записах. Крім того, записи можуть містити контактну інформацію, про стан здоров'я та вакцинації, а також відомості про спеціальну освіту, включно з індивідуальними освітніми програмами (individualized education programs, IEП).

Записи про працевлаштування та фінансова документація

Ваші фінансові записи можуть містити інформацію про ваші доходи та витрати. Податкові записи можуть містити інформацію про заробітну плату, виписки з кредитної картки, кредитний рейтинг та іншу банківську інформацію.

Інформація про працевлаштування може містити відомості про ваші попередні місця роботи та результати діяльності.

[3] - https://encrypted-tbn2.gstatic.com/images?q=tbn:ANd9GcR94KX8uqLOXGrGQirYcWmP3d5G6gFKpTwJ36rRc8gqq5WNfEBz

Де зберігаються ваші дані?

В кожній країні діють свої закони, які захищають вашу конфіденційність та дані. Але чи знаєте ви, де саме знаходяться ваші дані (рис.1.4)?

Кожного дня ви залишаєте цифровий слід, використовуючи онлайн-сервіси, соціальні мережі чи мобільні додатки.

Коли ви перебуваєте в кабінеті лікаря, ваша розмова записується до вашої медичної картки. Для покриття страхових витрат ці відомості можуть надсилатись до страхової компанії, щоб забезпечити виставлення правильних рахунків та якість послуг. Тепер частина ваших медичних записів, які стосуються цього візиту, також зберігаються у страховій компанії.

Рис.1.4. Розміщення даних[4]

Картки постійних покупців магазинів можуть бути зручним способом заощадити кошти на покупках. Однак магазин складає профіль ваших покупок і використовує цю інформацію для власних цілей. У профілі відображено, що покупець регулярно купує зубну пасту певної марки та типу. Магазин використовує цю інформацію, щоб відправити покупцю спеціальні пропозиції від маркетингового партнера. Використовуючи картки постійних покупців, магазин та його маркетинговий партнер отримують профілі покупців для передбачення поведінки клієнтів.

Коли ділитесь з друзями своїми фото в Інтернеті, чи знаєте ви, хто може мати копії цих фотографій? Копії фотографій містяться на ваших власних пристроях. Ваші друзі можуть мати копії фотографій, завантажені на їхні пристрої.

Якщо фотографії публікуються як загальнодоступні, незнайомці також можуть їх скопіювати. Вони можуть завантажувати ці фотографії або робити з них скріншоти. Оскільки зображення були розміщені в мережі, вони також зберігаються на серверах, розташованих у різних частинах світу. Отже, тепер ці фотографії можна знайти не лише на ваших пристроях.

Ваші дані можуть переміщуватися між країнами та зберігатися на серверах, які підпорядковуються законам інших держав, і це може впливати на рівень їхнього захисту та вашу конфіденційність.

[4] - https://zn.ua/img/article/5335/5_main-v1677912216.jpg

Ваші комп’ютерні пристрої

Рис. 1.5. Генерація даних[5]

Комп’ютерні пристрої виконують не лише функцію збереження ваших даних, але й стали інструментом доступу до них, водночас генеруючи інформацію про вас (рис.1.5).

Якщо ви не зберігаєте всю особисту інформацію на папері, то використовуєте комп’ютери для доступу до даних.

Наприклад, щоб отримати цифрову копію виписки з кредитної картки, ви заходите на сайт емітента. Для оплати рахунку онлайн — звертаєтеся до вебсайту свого банку через комп’ютер. Окрім забезпечення доступу до даних, ці пристрої створюють нову інформацію про вас.

Ці дані, наявні в Інтернеті, можуть зацікавити хакерів. Тож зручність доступу до інформації супроводжується ризиками, оскільки дані, доступні в Інтернеті, можуть зацікавити хакерів. Зокрема, паролі, як один із факторів доступу, потребують надійного захисту. У розділі 4 ви знайдете поради щодо захисту паролів, які є одним із ключових засобів доступу до ваших даних.

Вони хочуть ваші гроші

Якщо у вас є дещо цінне, то злочинці захочуть це викрасти. Ваші мережеві облікові дані є цінними. Вони надають злодіям доступ до ваших рахунків. Можливо, ви думаєте, що преміальні милі авіакомпаній, які ви заробили, не є цінними для кіберзлочинців. Подумайте ще раз. Після зламу близько 10 000 облікових записів авіакомпаній American Airlines та United Airlines, кіберзлочинці отримали можливість безкоштовно бронювати авіаквитки та підвищувати клас обслуговування, використовуючи викрадені дані. пристрої. Незважаючи на те, що авіакомпанії повернули преміальні бонуси своїм клієнтам, цей випадок демонструє цінність реєстраційних облікових даних.

Злочинці можуть також скористатися інформацією про ваші родинні відносини. Вони можуть отримати доступ до ваших облікових записів в Інтернеті, щоб змусити вас передати гроші вашим друзям або родичам. Злочинець може надсилати повідомлення про те, що ваша сім’я або друзі потребують допомоги у вигляді грошового переказу для повернення додому з-за кордону після втрати гаманця.

[5] – https://www.associes-gouvernance.com/wp-content/uploads/2022/09/entreprise-numerique-320x213.jpg

Злочинці дуже вигадливі, коли намагаються змусити вас віддати гроші. Вони не просто викрадають ваші гроші (рис.1.6). Вони можуть також вкрасти ваші ідентифікаційні дані та зруйнувати ваше життя..

Їм потрібні ваші ідентифікаційні дані

Зловмисникам недостатньо крадіжки ваших грошей для короткострокової грошової вигоди, вони хочуть отримати довгостроковий прибуток, викрадаючи ваші ідентифікаційні дані.

Рис. 1.6. Доступ до фінансів[6]

Оскільки вартість медичних послуг зростає, крадіжки медичних страхових полісів також частішають. Злочинець може викрасти ваш медичний страховий поліс та скористатися медичним обслуговуванням замість вас, а ці медичні процедури відобразяться у вашій карті.

Щорічні процедури подання податкової декларації різняться залежно від країни, проте для кіберзлочинців – це час для нових можливостей (рис.1.7). Наприклад, у Сполучених Штатах громадяни мають подати свої податкові декларації до 15 квітня щорічно. Федеральне податкове управління (The Internal Revenue Service, IRS) не перевіряє податкову декларацію та інформацію від роботодавця до липня. Зловмисник, який викрав ідентифікаційні дані, може подати підроблену податкову декларацію та одержати відшкодування. Реальні декларанти помітять це, коли їхні декларації про доходи будуть повернуті податковою. За допомогою викрадених ідентифікаційних даних особи, вони також можуть відкривати кредитні рахунки та накопичувати борги на ваше ім’я. Це зашкодить вашому кредитному рейтингу і ускладнить отримання кредитів. Компрометація персональних облікових даних відкриває доступ до корпоративних даних або навіть до державної таємниці.

Рис.1.7. Збережені дані[7]

[6] - https://delo.ua/static/content/thumbs/850x550/0/d9/citt5f---c17x11x50px50p-c17x11x50px50p--42055bf4fa3e4ba195933b5a4abccd90.jpeg
[7] - https://encrypted-tbn3.gstatic.com/images?q=tbn:ANd9GcQ73c-BOYz3g4eWD0P9jf-LvR-nweV7K6RsiVzdAb18R8KYvm3J

1.3. ТИПИ КОРПОРАТИВНИХ ДАНИХ

Корпоративні дані — це інформація, яка створюється, зберігається або використовується організацією для підтримки її бізнес-операцій. Вони є основою для прийняття рішень, планування, аналізу та інших бізнес-процесів (рис.1.8). Корпоративні дані є стратегічним активом, тому важливо забезпечити їх безпеку, точність і своєчасний доступ. Захист корпоративних даних є критично важливим, оскільки їх компрометація може призвести до фінансових втрат, репутаційних ризиків та юридичних наслідків.

Рис. 1.8. Корпоративні дані[8]

Традиційні дані

Корпоративні дані містять інформацію про персонал, інтелектуальну власність та фінансові дані. Інформація про персонал включає заяви претендентів на посади, нарахування заробітної плати, листи з пропозиціями роботи, контракти співробітників та будь-яку інформацію, яка використовується для прийняття рішень про працевлаштування. Інтелектуальна власність, така як патенти, торгові марки та плани випуску нових продуктів, дає змогу підприємству отримувати економічні переваги над своїми конкурентами. Інтелектуальна власність може вважатися комерційною таємницею; втрата цієї інформації може бути катастрофічною для майбутнього компанії. Фінансові дані, такі як декларації про доходи, балансові звіти та звіти про рух грошових коштів, надають уявлення про фінансовий стан компанії.

Інтернет речей та великі дані

З появою Інтернету речей (Internet of Things, IoT) з'явилося значно більше даних, які потребують керування та захисту. IoT – це велика мережа фізичних об'єктів, таких як сенсори та пристрої, які виходять за межі традиційної комп'ютерної мережі. Технології IoT дають змогу людям підключати до Інтернету мільярди пристроїв. Всі ці зв'язки, а також зростання обсягів і послуг зберігання завдяки хмарним технологіям і віртуалізації призводять до експоненційного збільшення даних.

Ці дані створили нову область технологій та бізнесу під назвою "Великі дані" (Big Data). Поява Big Data є наслідком появи великих наборів даних складної структури й вимагає розробки нових алгоритмів обробки даних.

[8] – https://iotbusinessnews.com/WordPress/wp-content/uploads/market-data-report-forecasts.jpg

Big Data створює як проблеми так і можливості, що базуються на трьох аспектах:

- Обсяг або кількість даних.
- Швидкість приросту та обробки даних.
- Різноманітність типів даних та їх джерел.

В новинах є багато прикладів хакерських атак на великі корпорації. Такі компанії, як Target, Home Depot і PayPal, стали об'єктами атак, які отримали широкий розголос. Як наслідок, корпоративні системи потребують суттєвих змін у розробці продуктів безпеки та ґрунтовної модернізації їх технологій та методів. Крім того, уряд та промисловість впроваджують нові правила та інструкції, які потребують більш якісного захисту даних і контролю безпеки, щоб допомогти захистити Big Data.

Завдяки швидкості, обсягу та різноманітності даних, що генеруються IoT та щоденними бізнес-операціями, конфіденційність, цілісність і доступність цих даних є життєво важливими для організації. Ці виклики потребують впровадження передових технологій штучного інтелекту та машинного навчання для аналізу та забезпечення безпеки даних у реальному часі.

Конфіденційність, цілісність та доступність

Три основні принципи інформаційної безпеки -конфіденційність, цілісність та доступність, відомі як тріада КЦД (рис. 1.9), є керівним принципом безпеки інформації для організації. У світовій практиці цей концепт широко відомий як **CIA Triad** (Confidentiality, Integrity, Availability). Конфіденційність гарантує нерозголошення даних, обмежуючи доступ до них через механізми автентифікації і шифрування. Цілісність гарантує точність і достовірність інформації. Доступність гарантує, що інформація доступна для авторизованих користувачів.

Рис. 1.9. Тріада КЦД

Конфіденційність (Confidentiality)

Синонімом до терміну конфіденційність є приватність. Політики компанії мають обмежувати доступ до інформації колом авторизованих користувачів та гарантувати, що тільки ці особи бачать ці дані. Доступ до даних надається відповідно до політики безпеки або рівня секретності інформації. Наприклад,

розробник Java-програми не повинен мати доступу до персональних даних усіх співробітників. Крім того, працівники мають проходити навчання, щоб ознайомитись з найкращими рекомендаціями щодо убезпечення конфіденційної інформації, аби захистити себе і компанію від атак. Методи забезпечення конфіденційності передбачають шифрування даних, ідентифікацію по імені користувача та пароля, двофакторну автентифікацію та мінімізацію розголошення конфіденційної інформації.

Цілісність (Integrity)

Цілісність – точність, узгодженість і достовірність даних впродовж всього їх життєвого циклу. Дані повинні залишатися незмінними в процесі передачі, а також недоступними для змін неавторизованими суб'єктами. Дозволи на використання файлів та контроль доступу користувачів можуть запобігти неавторизованому доступу. Контроль версій може використовуватися для запобігання випадковим змінам авторизованими користувачами. Резервні копії повинні бути доступні для відновлення будь-яких пошкоджених даних, а хеш (контрольна сума) може бути використаний для перевірки цілісності даних під час передавання.

Контрольна сума використовується для перевірки цілісності файлів або рядків символів після перенесення їх з одного пристрою на інший через локальну мережу або Інтернет. Контрольна сума розраховується за допомогою хеш-функцій. Деякі популярні функції обчислення контрольних сум: MD5, SHA-1, SHA-256 та SHA-512. Хеш-функція використовує математичний алгоритм для перетворення даних у значення фіксованої довжини, що представляє ці дані, як зображено на рисунку 1.10. Значення хешу наведено тут просто для прикладу. Вихідні дані не можуть бути отримані безпосередньо з хеш-значення. Наприклад, якщо ви забули свій пароль, він не може бути відновлений з хеш-значення. Доведеться встановити новий пароль.

Рис. 1.10. Створення хешу[9]

[9] – https://encrypted-tbn1.gstatic.com/images?q=tbn:ANd9GcQdx1lhKqei2QDFyg1XXKV99X1oRZ_-Jt26GPFCJbQv60UROQV7

Після завантаження файлу ви можете перевірити його цілісність, порівнявши значення хешу, що обчислений джерелом, з тим, який ви розрахували, використовуючи будь-який хеш-калькулятор. Порівнявши значення хешу, ви можете переконатися, що під час передавання файл не був підроблений або пошкоджений.

Доступність (Availability)

Обслуговування обладнання, проведення ремонту апаратного забезпечення, оновлення операційних систем та програмного забезпечення і створення резервних копій забезпечують доступність мережі та даних для авторизованих користувачів. Має бути план швидкого відновлення систем після природних катаклізмів або техногенних катастроф. Апаратні та програмні засоби безпеки, як наприклад, фаєрволи, захищають систему від простоїв через такі атаки, як Відмова в обслуговуванні (Denial of Service, DoS). Відмова в обслуговуванні виникає, коли зловмисник намагається надмірно завантажити ресурси системи, щоб унеможливити доступ користувачів до потрібних сервісів.

Для забезпечення безперервної доступності слід також регулярно проводити тестування резервних копій і відновлення, щоб переконатися у їхній працездатності.

1.4. КОНЦЕПТУАЛЬНА МОДЕЛЬ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Концептуальна модель інформаційної безпеки пояснює, як захищати комп’ютери, дані та мережі від загроз.

Джерелами інформації є персонал і пам’ять людей, які володіють знаннями та кваліфікацією в різних галузях науки і техніки; документи всіх видів і публікації на будь-яких носіях; технічні носії інформації, що використовуються в обчислювальній техніці для збирання, зберігання, обробки та передачі даних, а також засоби зв’язку, необхідні для цього; технічні засоби забезпечення виробничої та трудової діяльності; науковий інструментарій, включно з автоматизованими системами, робочими місцями науковців і проєктувальників, експертними системами та базами знань; продукція, відходи виробництва, промислові зразки, рецептури, технології та програмні засоби, які є результатом діяльності людей.

Концептуальна модель інформаційної безпеки — це структурний підхід до захисту інформаційних систем та даних від кіберзагроз, за яким визначаються основні принципи, механізми та процеси, які забезпечують захист конфіденційності, цілісності та доступності даних.

Конфіденційність (Confidentiality) гарантує, що доступ до інформації мають лише авторизовані користувачі. Це досягається через шифрування, контроль доступу та застосувананя політик безпеки.

Цілісність (Integrity) забезпечує точність і повноту даних, запобігаючи їхній несанкціонованій зміні чи пошкодженню. Використовуються хешування, цифрові підписи та контроль версій.

Доступність (Availability) потребує, щоб дані та сервіси бути доступні для авторизованих користувачів у потрібний час. Методи забезпечення включають резервне копіювання, захист від атак типу DDoS та надійну інфраструктуру.

Виділяють п’ять основних складових концептуальної моделі інформаційної безпеки, які формують основу для оцінки та побудови ефективної системи захисту. Це активи, загрози, вразливості, механізми захисту, контроль і моніторинг (рис.1.11).

Рис. 1.11. Концептуальна модель інформаційної безпеки

Під об'єктами захисту розуміють дані, програмне та апаратне забезпечення, мережі, інфраструктуру, персонал та користувачів.

Власниками активів для захисту, можуть бути держава та її структури (органи), підприємства, акціонерні товариства, громадські організації та громадяни.

Засоби захисту — це сукупність методів, інструментів, технологій та процедур, спрямованих на забезпечення безпеки інформації, збереження її конфіденційності, цілісності та доступності. Засоби захисту поділяються на кілька категорій залежно від їхнього призначення, сфери застосування та принципів дії.

Загрозами є можливі події або дії, що можуть завдати шкоди системі. Загрози реалізуються в конкретний момент часу за допомогою певних способів доступу, але їм перешкоджає захист інформації.

Вразливостями є слабкі місця системи, які можуть бути використані порушниками для реалізації загроз. Наприклад, застаріле програмне забезпечення, недостатній контроль доступу, відсутність оновлень.

Модель використовується для створення політик, стандартів та протоколів безпеки в організаціях і є основою для розробки та впровадження систем захисту інформації. Вона допомагає зрозуміти, що треба робити, щоб інформація була захищеною.

Розвиток концептуальної моделі інформаційної безпеки

Сучасні підходи до забезпечення інформаційної безпеки включають інтеграцію новітніх технологій, таких як штучний інтелект, машинне навчання та блокчейн. Штучний інтелект (рис.1.12) та машинне навчання дають змогу аналізувати великі обсяги даних у реальному часі, виявляти аномалії та кіберзагрози. Блокчейн, у свою чергу, забезпечує підвищену прозорість і захист даних завдяки своїй децентралізованій природі.

Рис.1.12. Штучний інтелект в інформаційній безпеці[10]

Крім того, зростає роль автоматизації у процесах моніторингу та реагування на інциденти безпеки. Використання автоматизованих систем знижує ризик людських помилок і підвищує швидкість виявлення загроз. Організації також усе частіше впроваджують багатофакторну автентифікацію для захисту доступу до критичних даних і систем. Використання сучасних методів мінімізує ризики несанкціонованого доступу.

Навчання персоналу також залишається ключовим елементом забезпечення інформаційної безпеки. Регулярні тренінги з кібергігієни, симуляція фішингових атак і роз'яснення основних принципів захисту допомагають уникнути людського фактору як причини компрометації систем.

Не менш важливим є використання сучасних криптографічних протоколів для забезпечення безпеки передачі даних у мережах. Технології, такі як TLS 1.3, забезпечують високий рівень захисту комунікацій між пристроями.

Сьогодні зростає потреба в інтеграції засобів безпеки безпосередньо у фази розробки програмного забезпечення. Підхід DevSecOps сприяє створенню більш захищених продуктів завдяки тестуванню безпеки на кожному етапі розробки.

Уряди й міжнародні організації відіграють значну роль у розвитку нормативної бази інформаційної безпеки. Зокрема, такі акти, як GDPR у ЄС та закони про захист персональних даних, встановлюють стандарти для обробки й захисту даних, що стимулює організації до вдосконалення своїх систем захисту.

[10] - https://news.ztu.edu.ua/wp-content/uploads/2024/05/00-1-825x510.jpg

1.5. ВНУТРІШНІ ТА ЗОВНІШНІ ЗАГРОЗИ У КІБЕРБЕЗПЕЦІ

Як було сказано раніше, експерти мають бути новаторами і провидцями. Вони будують різноманітні кібердомени в Інтернеті. Вони мають здатність розпізнавати потужність даних і використовувати їх. Надалі вони створюють свої організації та забезпечують захист життєво важливих інтересів людини, суспільства й держави від усіх видів сучасних кіберзагроз.

Загрози і вразливості є основним предметом діяльності фахівців з кібербезпеки. Головним чином вирішальними є дві ситуації:

- Коли загроза відкриває ймовірність того, що станеться негативна подія, наприклад, відбудеться атака.
- Коли вразливість робить ціль сприйнятливою до атаки.

Наприклад, дані в руках зловмисників можуть привести до втрати конфіденційності для власників, можуть вплинути на їх фінансове становище або поставити під загрозу їх кар'єру чи особисті відносини. *Крадіжка особистих даних* – великий бізнес. Проте, Google і Facebook не обов'язково є найбільшим ризиком. Школи, лікарні, фінансові установи, державні установи, звичайні робочі місця і електронна комерція можуть становити ще більшу небезпеку. Такі організації, як Google і Facebook, мають у своєму розпорядженні ресурси для найму дуже талановитих кіберспеціалістів для захисту своїх доменів. Оскільки все більше організацій створюють великі бази даних, що містять всю нашу персональну інформацію, потреба в професіоналах з кібербезпеки зростає. Тому для менших підприємств та організацій залишається конкурувати за решту кіберспеціалістів. Кіберзагрози особливо небезпечні для певних галузей і даних, які вони використовують.

Наступні приклади – це всього лише кілька джерел даних, які можуть бути отримані від існуючих організацій:

- *медичні записи;*
- *дані про освіту;*
- *зайнятість і фінансовий стан*.

Загрозам у кібербезпеці можуть піддаватися і ключові галузі промисловості (мережеві інфраструктурні системи), такі як виробництво, енергетика, зв'язок та транспорт. Наприклад, розумна мережа електропостачання (smart grid) – це удосконалена система генерації та розподілу електроенергії. Мережа електропостачання передає електроенергію від центральних генераторів до великої кількості клієнтів. Розумна мережа використовує інформацію для створення сучасної автоматизованої системи постачання електроенергії. Світові лідери визнають, що захист цієї інфраструктури є критичним для захисту економіки.

Першою зафіксованою кібератакою, яку назвали формою "кіберзброї" вважається атака Stuxnet, яка сталася у 2010 році. Stuxnet був спеціально

спрямований на інфраструктуру Ірану, зокрема на ядерну програму країни, з метою зупинити роботу центрифуг збагачення урану. Після атаки стало зрозуміло, що критична інфраструктура, як-от енергетичні мережі, ядерні об'єкти та інші стратегічно важливі системи, можуть бути вразливими до таких атак. Це призвело до зростання інвестицій у кібербезпеку в урядах та корпораціях й мало значний вплив на міжнародну політику та розвиток кібербезпеки.

За останнє десятиліття кібератаки, подібні Stuxnet, довели, що кібератаки можуть успішно знищити або перервати роботу критичних інфраструктур. Зокрема, атака Stuxnet була націлена на систему контролю і збору даних (Supervisory Control and Data Acquisition, SCADA), яка використовувалась для контролю і моніторингу промислових процесів. SCADA може бути частиною різних технічних процесів у промисловості, виробничих, енергетичних і комунікаційних системах.

Кібератака може привести до знищення або зупинки таких галузей, як телекомунікації, транспорт, виробництво електроенергії та системи її розподілу. Це може також порушити роботу сектору фінансових послуг. Однією з проблем в середовищах, де використовується SCADA, є той факт, що розробники не підключали SCADA до традиційного IT-середовища та Інтернету. Тому вони не врахували питання кібербезпеки на етапі розробки цих систем. Як і в інших галузях, організації, що використовують системи SCADA, визнають цінність збору даних для покращення виробництва і зниження витрат. Загальна тенденція полягає в тому, щоб підключити SCADA-системи до традиційних IT-систем. Однак це підвищує вразливість підприємств, що використовують системи SCADA.

Після Stuxnet було значно посилено увагу до питань кібербезпеки в міжнародних організаціях, таких як ООН та НАТО. Розпочалися дебати щодо встановлення міжнародних норм і правил для кіберпростору, зокрема щодо визначення "кібертероризму" і допустимих меж використання кіберзброї. Виникли нові ініціативи для співпраці між державами у боротьбі з кіберзагрозами, зокрема через обмін розвідданими та розвиток спільних засобів для запобігання та реагування на кібернапади.

Просунутий потенціал загроз, який існує сьогодні, потребує спеціально навчених експертів з кібербезпеки.

Кібербезпека – це постійна робота щодо захисту мережевих систем і даних від несанкціонованого доступу.

На особистому рівні, кожен повинен захищати свою конфіденційність, свої дані і комп’ютерні пристрої.

На корпоративному рівні обов’язок працівників захищати репутацію організації, дані та клієнтів.

На державному рівні на карту поставлена національна безпека і благополуччя громадян.

Фахівці з кібербезпеки часто беруть участь у роботі державних органів в процесах ідентифікації і збору даних.

У США Агентство національної безпеки (National Security Agency, NSA) відповідає за збір і контроль даних. NSA заснувало новий дата-центр обробки даних для обробки зростаючого обсягу інформації. У 2015 році Конгрес США прийняв закон Про свободу слова (Freedom Act), який припинив практику загального запису телефонних розмов громадян США. Ця програма забезпечувала метадані, які надали NSA інформацію про відправлені та отримані повідомлення.

Зусилля щодо захисту життя людей часто суперечать їх праву на недоторканність приватного життя. Буде цікаво подивитися, що відбуватиметься з балансом між цими правами і безпекою користувачів Інтернету.

Внутрішні загрози безпеки

Як показано на рисунку, атаки можуть організовуватись як зсередини організації, так і ззовні. Внутрішній користувач, наприклад працівник або бізнес-партнер, може випадково чи навмисно:

- Неправильно поводитися з конфіденційною інформацією.
- Загрожувати роботі внутрішніх серверів або пристроїв мережевої інфраструктури.
- Сприяти зовнішнім атакам, підключивши заражений USB-носій до корпоративної комп'ютерної системи.
- Випадково завантажити шкідливе програмне забезпечення у мережу через шкідливі електронні листи або вебсайти.

Внутрішні загрози потенційно можуть спричинити більший збиток, ніж зовнішні, оскільки внутрішні користувачі мають прямий доступ до приміщень та інфраструктурних пристроїв. Працівники до того ж знають структуру корпоративної мережі, її ресурси та конфіденційні дані, а також мають різні рівні користувацьких або адміністративних привілеїв (рис. 1.13).

Зовнішні загрози безпеці

Зовнішні загрози від аматорів або досвідчених нападників можуть використовувати вразливі місця в мережевих або комп'ютерних пристроях або застосовувати соціальну інженерію для отримання доступу шляхом обману. Зовнішні атаки використовують слабкі сторони або вразливі місця для доступу до внутрішніх ресурсів.

Корпоративні дані включають інформацію про персонал, інтелектуальну власність і фінансові дані.

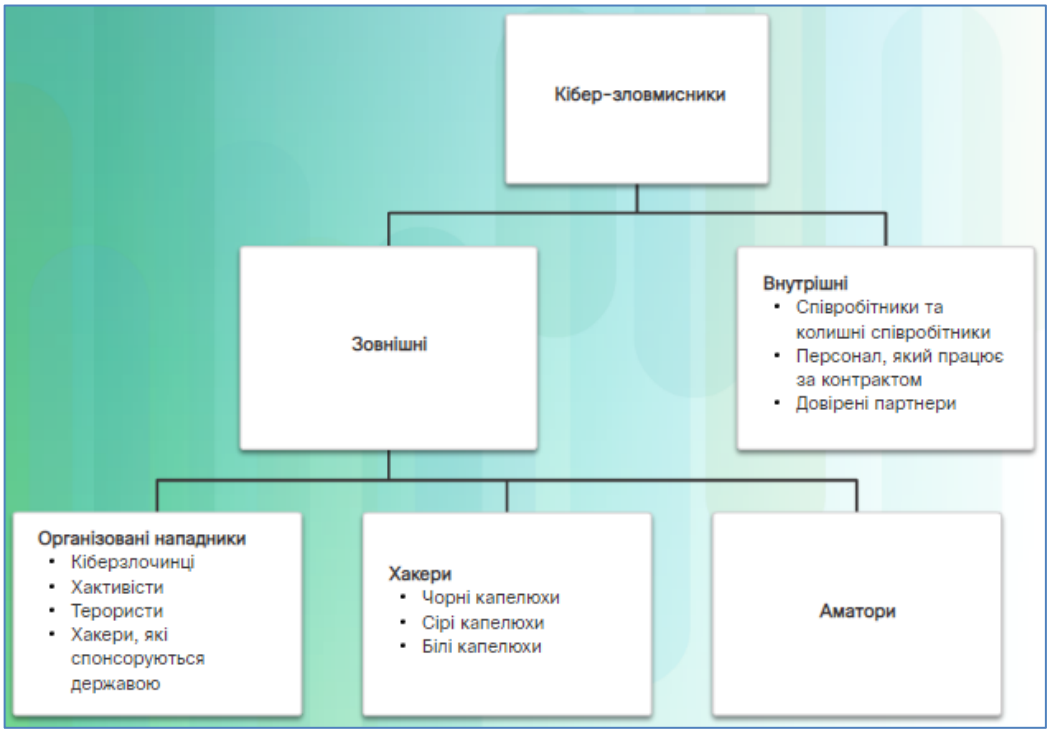


Рис. 1.13. Внутрішні та зовнішні загрози безпеці

Інформація про персонал включає заяви про влаштування на роботу, відомості про зарплату, оголошення про вакансії, контракти співробітників і будь-яку інформацію, яка використовується для прийняття рішень про працевлаштування.

Інтелектуальна власність, така як патенти, торговельні марки і плани випуску нових продуктів, дає змогу бізнесу отримати економічну перевагу над конкурентами. Розглянемо цю інтелектуальну власність як комерційну таємницю; втрата цієї інформації може бути катастрофічною для майбутнього компанії.

Фінансові дані, такі як звіти про доходи, балансові звіти та інформація про рух грошових коштів, дають уявлення про фінансовий стан компанії.

Раніше співробітники зазвичай використовували комп'ютери компанії, які були підключені до корпоративної локальної мережі. Адміністратори постійно контролюють і оновлюють ці комп'ютери відповідно до вимог безпеки. Сьогодні мобільні пристрої, такі як iPhone, смартфони, планшети і тисячі інших пристроїв, стають потужними замінниками або доповненням до традиційного ПК. Все більше і більше людей використовують ці пристрої для доступу до корпоративної інформації. Принести свій власний пристрій (Bring Your Own Device, BYOD) є зростаючою тенденцією. Неможливість централізованого керування і оновлення мобільних пристроїв створює зростаючу загрозу для організацій, які дають змогу мобільним пристроям співробітників доступ до мереж підприємства.

1.6. КІБЕРЗЛОЧИНЦІ І ФАХІВЦІ З КІБЕРБЕЗПЕКИ

У 60-ті роки, коли у світі з'явились перші хакери, серед них було багато аматорів, програмістів та студентів. Спочатку термін **хакер** описував людей з хорошими навичками програмування. Хакери використовували ці навички, щоб перевірити можливості та обмеження існуючих тоді систем. Перші хакери також брали участь в розробці комп'ютерних ігор. У багатьох іграх того часу були чарівники та використовувалась магія.

З розвитком культури хакерства, до неї додавалась лексика цих ігор. Навіть зовнішній світ почав проектувати образи могутніх чарівників та незрозумілу хакерську культуру. Книги, такі як *Там, де чарівники лягають пізно спати: витоки Інтернету (Where Wizards Stay up Late: The Origins of The Internet),* яка опублікована у 1996 році, додали містики до хакерської культури. Ці образи та термінологія закріпились. Багато хакерських угрупувань у наш час використовують саме цей імідж. Одна з найбільш сумновідомих хакерських груп має назву Легіон долі (Legion of Doom). Важливо знати кіберкультуру, щоб зрозуміти злочинців кіберсвіту та їх мотивацію.

Китайський філософ і воїн Сунь-Цзи, що жив у шостому столітті до нашої ери, написав книгу під назвою *Мистецтво війни (The Art of War)*, що є класичною роботою про стратегії перемоги над ворогом. Ця книга століттями використовувалась як рекомендації з тактики та стратегії. Знати ворога – один з основних принципів Сунь-Цзи. Хоча він посилався саме на війну, більша частина його рекомендацій підходить і для інших аспектів життя, включаючи проблеми кібербезпеки.

У перші роки існування світу кібербезпеки типовими кіберзлочинцями були підлітки або аматори, які працювали на домашньому ПК, і атаки в основному обмежувалися пустощами або вандалізмом. Сьогодні світ кіберзлочинців став більш небезпечнішим. Нападники – це окремі особи або групи, які намагаються використати кібервразливість для особистої або фінансової вигоди Вони зацікавлені в усьому: від кредитних карток до дизайну продукту, та будь-чого, що має цінність.

Аматори (Amateurs), таких людей іноді називають скріпт-дітьми (Script Kiddies). Зазвичай це зловмисники, які практично не мають навичок і часто для запуску атак використовують існуючі інструменти або вказівки, знайдені в Інтернеті. Деякі з них роблять це просто з цікавості, а інші намагаються продемонструвати свою майстерність і заподіяти шкоду. Навіть якщо вони використовують прості інструменти, наслідки таких атак можуть бути руйнівними.

Хакери (Hackers) – це група зловмисників, яка зламує комп'ютери або мережі з метою отримання доступу.

Залежно від наміру вторгнення ці зловмисники класифікуються як Білі, Сірі чи Чорні капелюхи (рис.1.14). Білі капелюхи входять в мережі або комп'ютерні системи, щоб виявити слабкі місця та покращити безпеку цих систем. Такі вторгнення виконуються за попереднім дозволом і всі результати повідомляються власнику. З іншого боку, Чорні капелюхи використовують будь-яку вразливість для отримання незаконної особистої, фінансової або політичної користі. Сірі капелюхи знаходяться десь посередині між Білими та Чорними. Сірі капелюхи можуть виявити вразливість у системі та повідомити про неї власників системи, якщо це збігається з їхніми планами. (Таблиця 2). Деякі Сірі капелюхи публікують факти про вразливість в Інтернеті, щоб інші нападники могли нею скористатися.

Рис. 1.14. Хакер[11]

Таблиця 2. Характерні дії хакерів

Опис дій	Білий капелюх	Сірий капелюх	Чорний капелюх
1. За допомогою ноутбука мені вдалося виконати віддалений злам банкомату, але потім почав співпрацювати з виробниками банкоматів для виправлення вразливостей		V	
2. Відслідковував введення даних й параметри входу користувачів, а потім застосував номери рахунків і пін-коди жертв й зі свого ноутбука, переказав 10 мільйонів доларів на свій банківський рахунок.			V
3. Працюю з технологічними компаніями для виправлення дефектів в системі DNS	V		
4. Моя діяльність полягає у виявленні слабких місць у комп'ютерній системі компанії, в якій працюю	V		
5. Застосовував шкідливе програмне забезпечення для зламу кількох корпоративних систем і викрадення даних про кредитні картки, які потім продавав тому, хто запропонував найкращу ціну.			V
6. Під час перевірки слабких місць у системі безпеки корпоративної мережі, до якої маю доступ, знайшов вразливість.	V		

Організовані хакери (Organized Hackers) – до таких хакерів належать організації кіберзлочинців, хактивісти, терористи та хакери, що фінансуються державами-нападниками.

[11] - www.programacionparatodos.com

Кіберзлочинці – це, зазвичай, групи професійних злочинців, орієнтовані на контроль, владу та збагачення. Ці злочинці висококваліфіковані та організовані і навіть можуть надавати кіберзлочинність, як сервіс іншим злочинцям. Хактивісти роблять політичні заяви, щоб привернути увагу до важливих для них проблем. Нападники, які фінансуються державою, здійснюють розвідку або диверсії від імені свого уряду. Ці нападники зазвичай якісно підготовлені та добре фінансуються, а їх атаки зосереджені на корисних для їхнього уряду конкретних цілях. Деякі хакери, які фінансуються державою, перебувають на службі у збройних силах своєї держави (рис. 1.15).

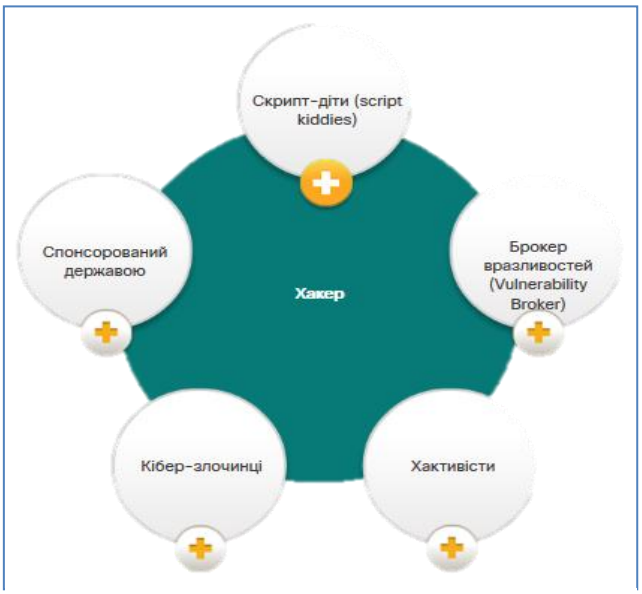


Рис. 1.15. Основні групи хакерів

Профілі та мотиви кіберзлочинців змінювалися з роками. Хакінг почався в 60-ті роки з телефонного фрікінгу (phone freaking або phreaking), що полягав у використанні різних звукових частот для маніпулювання телефонними системами.

Приклад: у 1971 році Джон Дрейпер першим здійснив міжміський дзвінок за допомогою свистка, який дістався йому як подарунок прикріплений до акційної пачки з печивом. Співпала тональність дзвінка та міжміського сигналу за допомогою якого здійснювалося переключення.

У середині 80-х років злочинці використовували комп'ютерні модеми для комутованих ліній для підключення комп'ютерів до мереж і застосовували програми для зламу паролів, щоб отримати доступ до даних. В наш час злочинці виходять за рамки банальної крадіжки інформації. Сьогодні злочинці можуть використовувати шкідливе програмне забезпечення і віруси як високотехнологічну зброю. Однак, найбільша мотивація для більшості кіберзлочинців – фінансова. Кіберзлочинність стала більш прибутковою, ніж нелегальна торгівля наркотиками.

Хакерам протидіють не тільки Білі Хакери (White Hats), які також знаходять вразливі місця в наших IT системах, але роблять це відкрито, аби допомогти нам закрити наявні проблемні місця, але й спеціалісти з інформаційної безпеки, тому що для проникнення в ту чи іншу організацію можуть використовуватись не тільки прямі методи зламу, але також і прості людські слабкості – збережені паролі у відкритих місцях, зайва балакучість співробітників, фішинг, спам, прийоми соціальної інженерії по телефону, відкриття поштових емейл від незнайомих адресатів і т.п.

Попит на фахівців в області кібербезпеки виріс більше, ніж попит на інші IT-спеціальності. Усі технології, які змінюють світ та покращують спосіб життя людей, також роблять їх більш вразливими для атак. Сама технологія не може запобігати, виявляти, реагувати і відновлюватися після кібератак. Слід взяти до уваги такі тенденції:

- Рівень кваліфікації, необхідний для ефективної роботи фахівця з кібербезпеки, і нестача кваліфікованих фахівців у цій галузі веде до високого рівня зарплат.
- Інформаційні технології постійно змінюються. Це також справедливо і для кібербезпеки. Через високу динамічність сфери кібербезпеки, вона може бути складною і захопливою.
- Кар'єра фахівця з кібербезпеки також є дуже мобільною. Робочі місця існують практично у кожній географічній точці.
- Фахівці з кібербезпеки надають необхідні послуги організаціям, країнам та суспільству аналогічно, як співробітники правоохоронних органів або міністерства з надзвичайних ситуацій.

Як відрізнити спеціаліста кібербезпеки від спеціаліста з ІБ?

Найпростіший і найочевидніший спосіб – по сертифікації. Сертифікацій на тему кібербезпеки та ІБ у світі величезна кількість, але є декілька найпоширеніших та найбільш популярних.

Спеціалісти з Кібербезпеки:

- CEH (Certified Ethical Hacker) – сертифіковані етичні хакери;
- CISSP (Certified Information System Security Professional) – сертифікований професіонал із забезпечення безпеки;
- CCSP (Cisco Certified Security Professional) – сертифікований фахівець з безпеки інформаційних систем;
- Спеціалісти з Інформаційної безпеки:
- CISM (Certified Information Security Manager) – сертифікований менеджер з інформаційної безпеки;
- CISA (Certified Information Systems Auditor) – сертифікований аудитор з інформаційної безпеки;
- ISO 27001 Lead Implementer – головний розробник;
- ISO 27001 Lead Auditor – ведучий аудитор.

З IT аудиторами також часто виникає плутанина. Класичний IT аудитор чітко знає набір процедур і методологічних практик, які потрібно пройти, аби проаналізувати будь-які IT систему згідно з поставленими цілями. Також є Пентестери, які інколи позиціонують себе як IT аудитори, але виконують зовсім інші задачі. Задача Пентестера – зламати систему, у той час як задача IT аудитора

проаналізувати систему, наприклад, на відповідність налаштувань до рекомендацій постачальника.

Стати фахівцем з кібербезпеки – це хороша можливість побудувати кар'єру.

Запобігання кіберзлочинам – це складне завдання і такої універсальної речі, як «срібна куля» немає. Однак компанії, уряди і міжнародні організації почали здійснювати скоординовані дії спрямовані на те, щоб обмежити або захиститись від кіберзлочинців. Скоординовані дії включають в себе перелічені нижче заходи.

- Створення комплексних баз даних відомих системних вразливостей і сигнатур атак (унікальні домовленості щодо зберігання інформації, яка використовується для ідентифікації спроб зловмисників експлуатувати відомі вразливості). Організації по всьому світу діляться цими базами даних, щоб допомогти підготуватись та відбити велику кількість поширених атак.
- Встановлення сенсорів раннього попередження та мереж оповіщення. Через високу вартість і неможливість моніторингу кожної мережі, організації контролюють важливі об'єкти або створюють пастки, які виглядають як важливі об'єкти. Оскільки на ці псевдоважливі цілі найчастіше здійснюються атаки, вони дають змогу попередити інших про потенційні напади.
- Обмін інформацією в кіберрозвідці. На сьогодні бізнес, урядові організації та країни співпрацюють в обміні критичною інформацією про напади на найважливіші цілі, щоб запобігти подібним атакам в інших місцях. Багато країн створили агентства кіберрозвідки для міжнародної співпраці у боротьбі з великими кібератаками.
- Створення стандартів керування інформаційною безпекою серед національних і міжнародних організацій. ISO 27000 є одним з найбільш відомих стандартів в рамках цих міжнародних зусиль.
- Прийняття нових законів про запобігання кібератак і порушення безпеки даних. Ці закони передбачають суворі покарання для кіберзлочинців, які здійснили незаконні дії.

1.7. КІБЕРВІЙНА ТА ЇЇ АСПЕКТИ

Кіберпростір став ще одним важливим аспектом війни, де країни можуть конфліктувати без зіткнення традиційних військ та техніки й вести війну, використовуючи інтернет-атаки для пошкодження критичної інфраструктури. Це дає змогу країнам з мінімальними військовими силами бути такими ж сильними, як і інші країни в кіберпросторі. Кібервійна – це Інтернет-конфлікт, який передбачає проникнення у комп'ютерні системи та мережі інших країн.

Нападники мають ресурси та спеціальні знання, щоб започатковувати масштабні інтернет-атаки проти інших країн, завдаючи збитків або порушуючи роботу сервісів, наприклад припинення роботи енергосистеми (Рис.1.16).

Новини про безпеку завжди викликають занепокоєння, але часто залишаються поза увагою, якщо тільки не йдеться про щось справді значуще. Загрози в цій сфері мають постійний характер, однак тільки серйозні інциденти привертають суспільний інтерес. Прикладом атаки, що фінансується державою, була загроза зловмисного програмного забезпечення Stuxnet, яке було розроблене для того, щоб завдати шкоди фабриці зі збагачення урану в Ірані. Шкідливе програмне забезпечення Stuxnet не зламувало цільові комп'ютери, щоб викрасти інформацію. Stuxnet був розроблений для пошкодження фізичного обладнання, яке контролювалося комп'ютерами. Він використовував програмні модулі, які були націлені на виконання певного завдання шкідли вого програмного забезпечення, застосовував вкрадені цифрові сертифікати, завдяки чому для системи атака здавалася легальною дією.

Рис.1.16. Небезпека енергосистеми[12]

Ця атака мала всі необхідні елементи для створення резонансу: комп'ютерні атаки, ядерна енергетика, участь іноземних урядів і саботаж. Це виглядає як сюжет шпигунського фільму, але є реальним прикладом загроз сучасного світу.

Розглядаючи розвиток потужних кіберзагроз, можна виділити п'ять ключових аспектів.

Перший з яких, *нетривіальний розподіл*. Його особливістю є спосіб поширення кіберзагроз, який відбувається, головним чином через, USB-флеш-накопичувачі. Цей метод дає змогу атакувати системи, які ізольовані від Інтернету, що значно ускладнює їхній захист.

Другий – *вишуканість атаки*. Це розумний черв'як. Stuxnet демонструє високий рівень складності. Він орієнтований на системи Windows, де встановлював власні драйвери, використовуючи викрадені, але легітимні сертифікати. Навіть після скасування одного сертифіката зловмисники швидко заміняли його новим, забезпечуючи безперервність роботи протягом 24 годин.

[12] - https://encrypted-tbn0.gstatic.com/images?q=tbn:ANd9GcSNZ-ZI5V18PgE87sBEwGPVH2WarnOJA3vXNS6mAxTb7ImqQDIj

Третій – *модульне кодування та гнучкість*. Stuxnet має модульну структуру, що дає змогу оновлювати його навіть під час поширення. Черв'як взаємодіє через велику кількість керуючих серверів, які змінюють своє розташування: спочатку в Малайзії, потім у Данії, а тепер і через однорангові мережі. У разі зустрічі двох копій вони порівнюють версії та синхронізують оновлення.

Четвертим пунктом є *унікальне націлювання*. Stuxnet не атакує хаотично, а націлений на конкретну модель програмованих логічних контролерів (PLC). Ці пристрої, які керують промисловими процесами, використовуються на фабриках, нафтопереробних заводах та атомних електростанціях. Зловмисне програмне забезпечення експлуатує вразливість контролера, щоб змінити специфічні дані, уникаючи при цьому тривожних сигналів. Для такої атаки потрібні унікальні знання, значні навички програмування та серйозне фінансування.

Наша остання точка, *мотив*. Stuxnet не орієнтований на злочинну діяльність, як-от крадіжка даних чи формування ботнетів. Його метою є саботаж інфраструктури, зокрема енергетики, водопостачання та інших критичних галузей. Він атакує старі, зазвичай не оновлювані системи, які часто не отримують належного технічного обслуговування.

Тож Stuxnet є унікальним прикладом сучасної кіберзагрози, що демонструє новий рівень складності та цілеспрямованості. Це не лише виклик для безпеки, а й урок, який має навчити нас бути готовими до подібних загроз у майбутньому.

Мета кібервійни

Основна мета кібервійни – отримати перевагу над супротивниками, незалежно від того, чи є вони державами або конкурентами.

Держава може постійно втручатися в інфраструктуру іншої країни, викрадати військові секрети та збирати інформацію про технології, щоб скоротити відставання у галузях промисловості та військовій сфері. Окрім промислового та військового шпигунства, під час кібервійни можуть здійснюватися диверсії на інфраструктурі інших країн і це може коштувати людських життів в країнах-цілях. Наприклад, атака може зруйнувати енергосистему великого міста. Дорожній рух буде порушено. Обмін товарами та послугами зупинено. Пацієнти не зможуть отримати невідкладну допомогу. Доступ до Інтернету також може бути порушено. Пошкодивши енергосистему, напад може вплинути на повсякденне життя простих громадян.

Крім того, скомпрометовані конфіденційні дані надають нападникам можливість шантажу членів уряді.

Інформація може дати змогу зловмиснику видати себе за авторизованого користувача для доступу до конфіденційної інформації або обладнання.

Якщо уряд не може захистити громадян від кібератак, то вони можуть втратити довіру до здатності уряду захищати їх взагалі. Кібервійна може дестабілізувати державу, зруйнувати торгівлю та впливати на довіру громадян до їхнього уряду, навіть коли немає фізичного вторгнення до країни-жертви.

1.8. НАСЛІДКИ ПОРУШЕННЯ БЕЗПЕКИ

Захистити організацію від усіх можливих кібератак неможливо з кількох причин. Знання та досвід, необхідні для налаштування та підтримки безпечної роботи мережі, можуть мати високу вартість. Зловмисники завжди будуть шукати нові способи атак на мережі. Згодом цілеспрямована кібератака підвищеної складності досягне своєї мети. У такому випадку пріоритетним буде те, наскільки швидко ваша команда безпеки може відреагувати на атаку, щоб мінімізувати втрати даних, час простою та втрати прибутку (рис. 1.17).

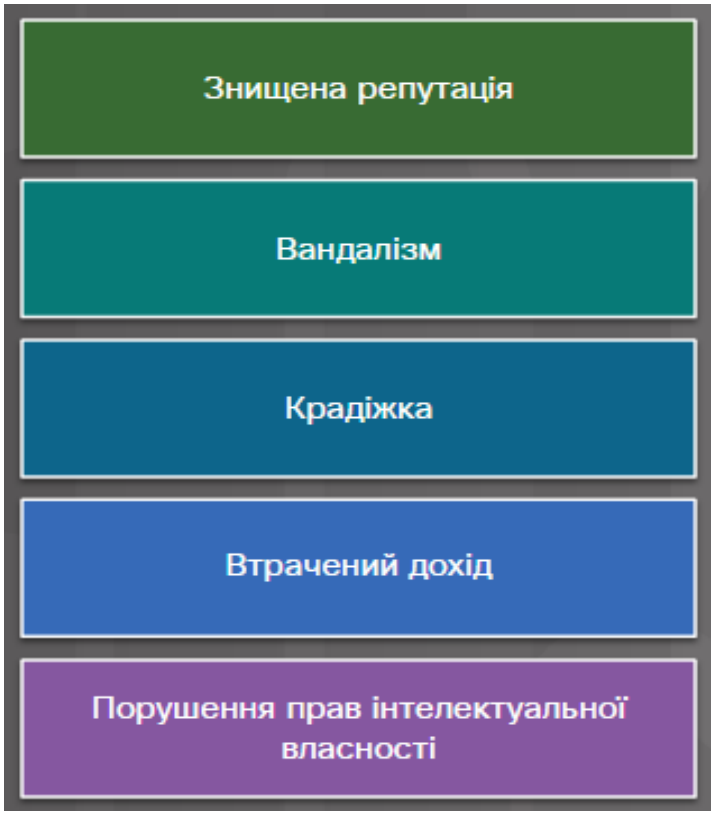


Рис. 1.17. Наслідки порушення безпеки

Як ви вже знаєте, будь-що розміщене в Інтернеті може залишатись там назавжди, навіть якщо ви змогли видалити усі копії, що є у вашому розпорядженні. В разі зламу ваших серверів, конфіденційна інформація про персонал може бути оприлюднена. Хакер (або хакерська група) може пошкодити вебсайт компанії, розмістивши на ньому неправдиву інформацію та зруйнувати репутацію компанії, вибудовану роками. Хакери також можуть вивести з ладу вебсайт компанії, через що компанія втратить дохід. Якщо вебсайт не працює тривалий період часу, компанія може видатися клієнтам ненадійною і втратити їхню довіру. Злам вебсайту або мережі компанії може призвести до витоку конфіденційних документів, розкриття комерційних таємниць та викрадення інтелектуальної власності. Втрата всієї цієї інформації може ускладнити зростання та розвиток компанії.

Грошова вартість збитків набагато вища, ніж просто заміна будь-яких пошкоджених або викрадених пристроїв, інвестування в існуючу систему безпеки та зміцнення фізичного захисту будівлі. Компанія повинна повідомити

про злам клієнтів, на яких це може вплинути, та бути готовою до судових позовів. Через усі ці потрясіння співробітники можуть звільнитися з компанії. Компанії, можливо, буде потрібно більше зосередитись на відновленні своєї репутації, а не на зростанні.

Порушення безпеки. Приклад 1

Онлайн-менеджер паролів LastPass зафіксував незвичну активність у своїй мережі в липні 2015 року. Виявилося, що хакери викрали електронні адреси користувачів, нагадування про паролі та хеші автентифікації. На щастя для користувачів, хакери не змогли отримати доступ до сховищ зашифрованих паролів користувачів (рис.1.18).

Рисунок 1.18. Безпека паролів[13]

Навіть незважаючи на порушення безпеки, LastPass все ще може захистити інформацію облікових записів користувачів. LastPass потребує підтвердження через електронну пошту або використовує багатофакторну автентифікацію, завжди під час нового входу з невідомого пристрою або IP-адреси. Хакерам також потрібно мати майстер-пароль для доступу до облікового запису.

Користувачі LastPass також несуть певну відповідальність за захист своїх власних облікових записів. Користувачі мають завжди використовувати складні майстер-паролі та регулярно їх змінювати. Користувачі завжди мають остерігатися фішингових атак. Прикладом атаки з фішингу може бути ситуація, коли зловмисник надсилає підроблені електронні листи, у яких вказується, що вони надіслані компанією LastPass. Електронні листи закликають користувачів натиснути на вбудоване посилання та змінити пароль.

Посилання в електронному листі переадресовує на шахрайську версію вебсайту, що використовується для викрадання майстер-паролів. Користувачі мають знати, що не можна натискати вбудовані посилання в електронному листі. Користувачі також повинні бути обережні з текстом нагадування пароля. Нагадування пароля не має дозволити вгадати ваш пароль. Найголовніше, коли є можливість, користувачам слід вмикати багатофакторну автентифікацію для будь-якого вебсайту, який це пропонує.

[13] - https://encrypted-tbn1.gstatic.com/images?q=tbn:ANd9GcTE24XGzv38hXtPu5L4GfChbISkqcPKx9Y1-8cnRVQ-GgqnjAsq

Якщо користувачі та постачальники послуг використовують належні інструменти та процедури для захисту інформації користувачів, то є більше шансів захистити їхні дані, навіть у випадку порушення безпеки.

Порушення безпеки. Приклад 2

Виробник високотехнологічних іграшок для дітей, компанія Vtech, зазнала втручання у систему безпеки своєї бази даних в листопаді 2015 року. Це втручання могло вплинути на мільйони клієнтів по всьому світу, включаючи дітей. Злам даних розкрив таку конфіденційну інформацію, як імена клієнтів, адреси електронної пошти, паролі, фотографії та журнали чату (рис.1.19).

Рис.1.19. Проблеми Vtech[14]

Новою ціллю для хакерів став дитячий планшет. Клієнти ділилися фотографіями та використовували функції чату на цих планшетах. Інформація не була належним чином захищена, а вебсайт компанії не підтримував безпечне SSL-з'єднання. Навіть незважаючи на те, що під час зламу не була розкрита інформація про кредитні картки та персональні ідентифікаційні дані, діяльність компанії на фондовій біржі була тимчасово припинена, настільки великим було занепокоєння з приводу хакерського втручання. Vtech не змогла забезпечити захист даних клієнтів належним чином, що і виявилось під час зламу. Навіть незважаючи на те, що компанія інформувала своїх клієнтів про те, що їхні паролі були хешовані, ймовірність того, що хакери їх розшифрують, залишається. Паролі в базі даних були зашифровані за допомогою хеш-функції MD5, але секретні питання та відповіді на них зберігалися у відкритому вигляді.

На жаль, функція хешування MD5 має відомі вразливості. Хакери можуть визначити вихідні паролі, порівнюючи мільйони попередньо розрахованих значень хешу.

Інформацію, розкриту під час цього зламу, кіберзлочинці могли використовувати для створення облікових записів електронної пошти, подання заявок на отримання кредитів та вчинення інших злочинів.

Порушення безпеки не лише вплинуло на конфіденційність споживачів, але й знищило репутацію компанії, коли її усунули з фондової біржі.

[14] – https://encrypted-tbn3.gstatic.com/images?q=tbn:ANd9GcQ9EDFtYzn6arzJy3zBLCG0VFNfkeKAB1USibYIy-xUK_-6iWj0

Для батьків – це попередження бути пильними та дбати про захищеність своїх дітей в Інтернеті та вимагати кращого захисту для дитячих товарів. Виробникам товарів, що під'єднуються до мережі, варто бути більш активними у захисті даних клієнтів та конфіденційності, як зараз так і в майбутньому, оскільки ландшафт кіберзагроз еволюціонує.

Порушення безпеки. Приклад 3

Equifax Inc. – одне із загальнонаціональних агенств зі звітності про споживачів кредитів у Сполучених Штатах. Ця компанія збирає інформацію про мільйони користувачів та комерційних підприємств по всьому світу. На основі отриманої інформації, створюються кредитні бали та кредитні звіти користувачів. Ця інформація може вплинути на користувачів при отриманні позик та у пошуку працевлаштування (рис.1.20).

Рис. 1.20. Доступ до даних[15]

У вересні 2017 року Equifax публічно повідомив про порушення доступу до даних. Нападники використали вразливість у програмному вебзастосунку Apache Struts. Компанія вважає, що важливі дані мільйонів американських користувачів стали доступні кіберзлочинцям з травня по липень 2017 р. Персональні дані містили повні імена клієнтів, номери соціального страхування, дати народження, адреси та іншу особисту інформацію. Існують докази, що цей злам міг вплинути на користувачів з Великобританії та Канади.

Equifax створив окремий вебсайт, який дозволяв клієнтам визначити чи були їх дані скомпрометовані і підключитися до кредитного моніторингу та захисту від крадіжки особистих даних. Використання нового доменного імені замість піддомена equifax.com дозволило зловмісникам створювати неавторизовані вебсайти з подібними назвами. Ці вебсайти можуть використовуватися як частина фішингової схеми, щоб змусити користувачів до надання персональної інформації. Більше того, працівник Equifax надав неправильне вебпосилання у соціальних мережах для стурбованих клієнтів. На щастя, цей вебсайт було деактивовано протягом доби. Він був створений особою, яка використовувала його як можливість навчитися виявленню вразливостей, що існують на сторінці відповідей Equifax.

[15] – https://encrypted-tbn0.gstatic.com/images?q=tbn:ANd9GcTmpH0p77-de096mMPVBmqhsJc2y6yd3cm1LfI6MsdZz-m9VxP7

На жаль, реальними жертвами нападу є особи, чиї дані могли бути скомпрометовані. У цьому випадку Equifax несе відповідальність за захист зібраних даних при проведенні кредитних перевірок, оскільки клієнти не обирали використання послуг, наданих Equifax.

Клієнт повинен довіряти компанії захист зібраної інформації. Більше того, нападники можуть використовувати ці дані від вашого імені, що дуже важко заперечити, оскільки і нападник і жертва знають однакову інформацію. У таких ситуаціях, найбільше, що ви можете зробити – це не втрачати пильність при наданні персональної інформації через Інтернет. Регулярно перевіряйте ваші звіти по кредитах (раз на місяць або раз на квартал). Негайно повідомляйте про будь-яку невідповідну інформацію, наприклад, заявки на кредити, які ви не ініціювали або покупки з вашою кредитною карткою, які ви не робили.

ВИСНОВКИ

У цій темі було показано особливості та характеристики кібербезпеки. Пояснено, чому попит на фахівців з кібербезпеки буде зростати. Чому ваші персональні ідентифікаційні дані в мережі та будь-які ваші дані є вразливими для кіберзлочинців. Щоб уникнути випадків компрометації даних, важливо обережно ставитись до надання персональної інформації.

У цій темі також обговорювалися що таке корпоративні дані, де вони знаходяться і чому важливо їх захищати. Компанії несуть відповідальність за захист інформації від несанкціонованого доступу. Вони повинні регулярно оновлювати програмне забезпечення для усунення відомих вразливостей, а їхні працівники мають проходити навчання з процедур захисту інформації та реагування на випадки зламу

Концептуальна модель інформаційної безпеки допомагає організаціям створювати політики, стандарти і протоколи безпеки, а також розробляти та впроваджувати механізми захисту для запобігання втратам або порушенням інформаційної безпеки.

Ви також дізналися, хто такі кіберзловмисники та чого вони хочуть. Експерти з кібербезпеки повинні мати такі ж навички, як і кіберзловмисники. Експерти з кібербезпеки повинні працювати в межах місцевого, національного та міжнародного права. Фахівці з кібербезпеки також мають використовувати свої навички, не порушуючи етичних норм.

Нарешті, тут коротко пояснюється, що таке кібервійна і чому країни та уряди потребують фахівців з кібербезпеки, й як захищають дані своїх громадян та інфраструктуру.

ТЕРМІНИ І КОНЦЕПЦІЇ

Ця вправа призначена для того, щоб ви могли практикувати важливі терміни та концепції, викладені у цій темі.

1. ***Аматори***

- зловмисники, які практично не мають навичок і часто для запуску атак використовують існуючі інструменти або вказівки, знайдені в Інтернеті.

2***. Білі капелюхи***

– особи або організації, які працюють з мережами або комп'ютерними системама, щоб виявити недоліки з метою підвищення безпеки цих систем.

3. Внутрішні загрози безпеці

– атаки, які зароджуються всередині організації.

4. Доступність

– термін, який описує послуги та дані, які перебувають в належному стані та можуть бути доступні в будь-який час.

5. Зовнішні загрози безпеці

– кіберзагрози або атаки, які надходять ззовні організації чи системи. Потребують використання різних методів захисту, таких як фаєрволи, антивірусні програми, шифрування даних і постійний моніторинг безпеки..

6. Кібербезпека

– постійні зусилля щодо захисту мережевих систем, підключених до Інтернету, і захист усіх даних від несанкціонованого використання або пошкодження.

7. Кібервійна

– Інтернет-конфлікт, який включає в себе проникнення в комп'ютерні системи і мережі інших країн.

8. Компоненти тріади CIA (КЦД)

– конфіденційність, цілісність та доступність.

9. Конфіденційність

– так звана приватність, означає, що доступ до даних обмежений колом уповноваженого персоналу.

10. ***Концептуальна модель інформаційної безпеки***

— теоретична структура, яка описує основні принципи та підходи до захисту інформаційних систем, даних і мереж від кіберзагроз.

10. Методи забезпечення конфіденційності

– шифрування даних, ідентифікація користувача та парольний захист, двофакторна автентифікація тощо.

11. Методи забезпечення цілісності

– дозволи файлів, контроль доступу користувачів, контроль версій і контрольні суми.

12. Міжнародне багатостороннє партнерство проти кіберзагроз (IMPACT)

– глобальне партнерство світових урядів, галузей і наукових кіл, що займаються покращенням глобальних можливостей протистояння кіберзагрозам.

13. Організовані нападники

– спільноти кіберзлочинців, хактивістів, терористів і фінансованих державами-нападниками хакерів.

14. Сірі капелюхи

- здійснюють хакерські атаки з метою виявлення вразливостей і повідомлення про них відповідним органам чи організаціям, вони діють не зовсім законно, але і без мети завдання шкоди.

15. Цілісність

– принцип, який гарантує точність, узгодженість та достовірність даних протягом їх життєвого циклу.

16. Чорні капелюхи

– особи або організації, які використовують будь-яку вразливість для незаконної особистої, фінансової або політичної вигоди.

17. Етика

– кодекси поведінки, які іноді, але не завжди, підкріплюються законами.

18. IoT (Інтернет речей)

- концепція, що описує мережу фізичних об'єктів, які оснащені датчиками, програмним забезпеченням та іншими технологіями для збору, обміну та обробки даних через Інтернет..

19. ***DevSecOps***

— підхід до розробки програмного забезпечення, що інтегрує безпеку на кожному етапі процесу розробки.

20. ***GDPR*** *(General Data Protection Regulation)*

— загальний регламент захисту даних Європейського Союзу, що встановлює стандарти обробки та захисту персональних даних.

21. Stuxnet

– зловмисна програма, що була призначена щоб завдати шкоду збагачувальному ядерному заводу в Ірані, програма, яка є прикладом атаки, що спонсорувалася державою.

ПРАКТИЧНЕ ЗАВДАННЯ 1.1. ХТО ВОЛОДІЄ ВАШИМИ ДАНИМИ?

Цілі завдання

Дослідіть яким є право власності на Ваші дані, якщо вони зберігаються не в локальній системі.

Частина 1: Знайомимося з правилами надання послуг

Частина 2: Чи знаєте Ви під чим підписуєтесь?

Довідкова інформація/Сценарій

Соціальні медіа та онлайн-сховища стали невід'ємною частиною життя багатьох людей. Файли, фотографії та відео використовуються разом з друзями та рідними. Співпраця онлайн та онлайн-наради проводяться на робочих місцях людьми, які знаходяться за багато миль один від одного. Можливості зберігання даних більше не обмежуються пристроями, доступними локально. Географічне положення пристроїв зберігання даних більше не є обмеженням для зберігання або резервного копіювання даних у віддалених сховищах.

В цій роботі Ви маєте дослідити правові угоди, необхідні для використання різних онлайн-сервісів. Ви також дізнаєтеся про деякі способи захисту Ваших даних.

Необхідні ресурси

ПК або мобільний пристрій з доступом до Інтернету.

ХІД ВИКОНАННЯ

Частина 1: Знайомимося з правилами надання послуг

Якщо Ви використовуєте онлайн-сервіси для зберігання даних або спілкування з друзями чи родиною, напевно Ви уклали угоду з провайдером цих сервісів. Умови надання послуг, також відомі як "Умови використання" або "Загальні положення та умови", є юридично обов'язковим контрактом, який регулює правила взаємовідносин між Вами, Вашим провайдером та іншими особами, які користуються сервісом.

Перейдіть на вебсайт онлайн-сервісу, який Ви використовуєте та знайдіть Угоду про умови надання послуг. Нижче наведено список найбільш популярних соціальних мереж та сервісів для онлайн-зберігання даних.

Соціальні мережі

Facebook: https://www.facebook.com/policies

Instagram: http://instagram.com/legal/terms/

Twitter: https://twitter.com/tos

Pinterest: https://about.pinterest.com/en/terms-service

Сервіси для онлайн-зберігання даних

iCloud: https://www.apple.com/legal/internet-services/icloud/en/terms.html

Dropbox: https://www.dropbox.com/

OneDrive: https://www.microsoft.com/uk-ua/microsoft-365/onedrive/online-cloud-storage

Ще раз перегляньте терміни і дайте відповіді на наступні запитання.

a. Чи маєте Ви обліковий запис у постачальника онлайн-послуг? Якщо так, чи ознайомилися Ви з Угодою про надання послуг?

_____

_____

b. Що таке політика використання даних?

_____

_____

c. Що таке налаштування конфіденційності?

_____

_____

d. Що таке політика безпеки?

_____

_____

e. Які права Ви маєте щодо своїх даних? Чи можете Ви запросити копію Ваших даних?

_____

_____

_____

f. Що може робити постачальник послуг із даними, які Ви завантажили?

_____

_____

_____

g. Що відбувається з вашими даними, коли Ви закриваєте свій обліковий запис?

_____

_____

_____

Частина 2: Чи знаєте Ви під чим підписалися?

Після того, як Ви створили обліковий запис і погодились з Умовами надання послуг, чи дійсно ви знаєте, під чим підписалися?

В Частині 2 Ви дізнаєтеся, як Умови надання послуг можуть бути інтерпретовані та використані постачальниками сервісів.

Використовуйте Інтернет для пошуку інформації щодо інтерпретації Умов надання послуг.

Нижче наведено кілька прикладів статей, які допоможуть Вам розпочати роботу.

Facebook:

https://about.fb.com/news/2022/05/metas-updated-privacy-policy/

iCloud:

https://bigmag.ua/ua/kak-i-zachem-sozdavat-uchetnuy-zapis-icloud.html

https://support.apple.com/uk-ua/guide/iphone/iphde0f868fd/ios

Dropbox:

https://www.dropbox.com/uk_UA/terms

Перегляньте статті та дайте відповіді на такі запитання.

h. Що Ви можете зробити щоб захистити себе?

_____

_____

_____

i. Що Ви можете зробити, щоб захистити свій обліковий запис і свої дані?

_____

_____

_____

ПРАКТИЧНЕ ЗАВДАННЯ 1.2. РИЗИКИ ПОВЕДІНКИ В ІНТЕРНЕТІ

Цілі завдання

Дослідити дії в Інтернеті, що можуть скомпрометувати вашу безпеку чи конфіденційність.

Довідкова інформація/Сценарій

Інтернет – це вороже середовище, і ви повинні бути пильними, щоб ваші дані не були скомпрометовані. Зловмисники креативні і будуть використовувати різні методи, щоб обдурити користувачів. Ця робота допоможе визначити ризики своєї поведінки в Інтернеті та надати поради щодо безпечного використання Інтернету.

ХІД ВИКОНАННЯ

Частина 1: Знайомимося з правилами надання послуг

Відповідайте на питання, наведені нижче, чесно та зверніть увагу, скільки балів дає кожна відповідь. Додайте всі очки до загального балу та перейдіть до Частини 2 для аналізу вашої поведінки в Інтернеті.

Текст опитувальника

a. Якою інформацією ви ділитеся на сайтах соціальних мереж? _____

1) Всією; покладаюся на соціальні мережі, щоб підтримувати зв'язок з друзями та родиною. (3 бали)

2) Статті та новини, які знаходжу чи читаю (2 бали)

3) Це залежить від того чим і з ким ділюся. Я відфільтровую. (1 бал)

4) Нічим. Не використовую соціальні мережі. (0 балів)

b. Коли ви створюєте новий обліковий запис в онлайн-службі, ви: _____

1) Повторно використовуйте той самий пароль, який використовується в інших службах, щоб полегшити його запам'ятовування. (3 бали)

2) Створюєте пароль, який є максимально простим, щоб ви могли його запам'ятати. (3 бали)

3) Створюєте дуже складний пароль і зберігаєте його в службі керування паролями. (1 бал)

4) Створюєте новий пароль, який схожий, але відрізняється від пароля, який використовується в іншій службі. (1 бал)

5) Створюєте абсолютно новий надійний пароль. (0 балів)

c. Коли ви отримуєте електронне повідомлення з посиланнями на інші сайти: _____

1) Ви не натискаєте на посилання, тому що ви ніколи не переходите за посиланнями, що приходять вам в електронних повідомленнях. (0 балів)

2) Ви переходите за посиланням, тому що поштовий сервер вже просканував це повідомлення. (3 бали)

3) Ви переходите за всіма посиланнями, якщо повідомлення надійшло від людини, яку ви знаєте. (2 бали)

4) Ви наводите курсор миші на посилання, щоб перевірити кінцеву URL адресу перед тим як натиснути. (1 бал)

d. Під час відвідування вебсайту відображається спливаюче вікно. У ньому говориться, що ваш комп'ютер перебуває під загрозою і ви повинні завантажити та встановити діагностичну програму, щоб убезпечити свій комп'ютер: _____

1) Ви натискаєте, завантажуєте та встановлюєте програму, щоб захистити ваш комп'ютер. (3 бали)

2) Ви перевіряєте спливаючі вікна та наводите курсор на посилання, щоб перевірити його безпеку. (3 бали)

3) Ігноруєте повідомлення, переконавшись, що ви не натиснули на нього, не завантажуєте програму та закриваєте вебсайт. (0 балів)

e. Коли вам потрібно ввійти на вебсайт своєї фінансової установи, щоб виконати щось, ви: _____

1) Вводите свою реєстраційну інформацію негайно. (3 бали)

2) Ви перевіряєте URL, щоб переконатися, що це заклад, який вам потрібен, перед введенням будь-якої інформації. (0 балів)

3) Ви не використовуєте онлайн-банкінг або будь-які онлайн-фінансові послуги. (0 балів)

f. Ви прочитали про програму і вирішите спробувати її. Ви шукаєте в Інтернеті та знаходите пробну версію на невідомому сайті, ви: _____

1) Негайно завантажуєте та встановлюєте програму. (3 бали)

2) Шукайте більше інформації про автора програми, перш ніж завантажувати її. (1 бал)

3) Не завантажуєте та не встановлюєте програму. (0 балів)

g. Ви знаходите USB-флешдиск на шляху до роботи, ви: _____

1) Берете його та підключаєте до комп'ютера, щоб переглянути його вміст. (3 бали)

2) Берете його та підключаєте до комп'ютера, щоб стерти його вміст перед використанням. (3 бали)

3) Берете його та підключаєте до комп’ютера, щоб запустити антивірусне сканування, перш ніж повторно використовувати його для власних файлів (3 бали)

4) Не піднімаєте його. (0 балів)

h. Вам потрібно підключитися до Інтернету, і ви знаходите відкриту точку доступу Wi-Fi. Ви: _____

1) Підключаєтеся до неї та користуєтеся Інтернетом. (3 бали)

2) Не підключаєтеся до неї та чекаєте на появу надійного з’єднання з Інтернетом. (0 балів)

3) Підключаєтеся до неї та встановлюєте VPN на надійний сервер перед надсиланням будь-якої інформації. (0 балів)

Частина 2: Проаналізуйте свою поведінку в Інтернеті

Чим більша ваша сума балів, тим менш безпечною є ваша поведінка в Інтернеті. Вашою метою має бути досягнення максимальної, 100% безпеки в Інтернеті, якої ви зможете досягти, звертаючи увагу на всі свої дії онлайн. Це дуже важливо, оскільки лише одна помилка може поставити під загрозу ваш комп’ютер та дані.

Інтерпретація отриманих результатів

Додайте бали з Частини 1. Запишіть свою суму балів. _____

0: Ви дуже безпечно поводите себе в Інтернеті.

0-3: Ви частково безпечно поводите себе в Інтернеті, але все одно повинні трохи змінити свою поведінку, щоб вона була повністю безпечною.

3-17: Ваша поведінка у Інтернеті небезпечна і ви ризикуєте поставити себе під загрозу.

18 і більше: Ваша поведінка в Інтернеті дуже небезпечна і ваші дані будуть скомпрометовані.

Декілька важливих порад щодо безпеки онлайн

Чим більшою кількістю інформації ви ділитеся в соціальних мережах, тим більше ви даєте змогуте зловмисникові дізнатись про вас. Маючи більше знань про вас, зловмисник може створити набагато більш спрямовану атаку. Наприклад, якщо ви поділитеся з світом інформацією про те, що ви були на автомобільних перегонах, зловмисник зможе надіслати вам електронного листа від імені компанії, що відповідальна за продаж квитків на перегони. Оскільки ви нещодавно були на цьому заході, повідомлення буде виглядати більш надійним.

Повторне використання паролів – це погана практика. Якщо ви повторно використовуєте пароль у службі, що перебуває під контролем зловмисників,

вони можуть успішно спробувати увійти під вашим обліковим записом у інші служби.

Електронні листи можуть легко підробити, щоб вони виглядали надійно. Підроблені електронні листи часто містять посилання на шкідливі сайти або шкідливе програмне забезпечення. Візьміть за правило не натискати на вкладенні посилання з листів, отриманих електронною поштою.

Не погоджуйтесь на встановлення небажаного програмного забезпечення, особливо якщо його пропонують вам на вебсторінці. Дуже малоймовірно, що ця вебсторінка матиме для вас законне та безпечне програмне забезпечення. Настійно рекомендується закрити браузер та використати інструменти операційної системи, щоб перевірити наявність оновлень.

Шкідливі вебсторінки легко можна зробити схожими на вебсайт банку або фінансової установи. Перш ніж натискати посилання або надавати будь-яку інформацію, двічі перевірте URL-адресу, щоб переконатися, що це правильна вебсторінка.

Коли ви даєте змогуте програмі запускатись на вашому комп'ютері, ви даєте їй багато можливостей. Добре подумайте перш ніж запускати програму. Проведіть невелике дослідження, щоб переконатися, що компанія або особа, відповідальна за програму, є серйозним та законним автором. Завантажуйте цю програму лише з офіційного вебсайту компанії чи особи.

USB-накопичувачі та флешки містять мініатюрний контролер, що дає змогу комп'ютерам з ними спілкуватися. Цей контролер можна заразити і навчити встановлювати шкідливе програмне забезпечення на комп'ютер. Оскільки шкідливе програмне забезпечення розміщується безпосередньо в контролері USB, а не в області даних, то видалення даних або антивірусне сканування не виявить зловмисного програмного забезпечення.

Зловмисники часто розгортають підроблені точки доступу Wi-Fi, щоб заманити користувачів. Оскільки атакуючий має доступ до всієї інформації, переданої через скомпрометовану точку доступу, користувачі, підключені до цієї точки доступу, піддаються ризику. Ніколи не використовуйте невідомі точки Wi-Fi, не шифруючи трафік через VPN. Ніколи не передавайте конфіденційні дані, такі як номери кредитних карток, під час використання невідомої мережі (дротова або бездротова).

Міркування

Проаналізувавши свою поведінку в Інтернеті, які зміни ви б зробили, щоб захистити себе в Інтернеті?

_____

_____

ДОДАТКОВІ РЕСУРСИ ТА ЗАВДАННЯ

Розуміння проблем у банківській галузі

На сайті організації Tapestry Network можна знайти звіти членів мережі фінансових послуг, в яких розглядаються проблеми, з якими стикаються фінансові установи. Перейдіть за цим посиланням і дізнайтеся про проблеми, які виникають під час надання банківських послуг:

http://www.tapestrynetworks.com/issues/financial-services/

Управління ризиками ланцюга поставок

Це посилання вказує на документ, який пояснює, як постачальник може поставити під загрозу безпеку мережі і надає інші ресурси щодо управління ризиками ланцюга поставок:

http://measurablesecurity.mitre.org/directory/areas/supplychainrisk.html

Кіберзлочинність чи кібервійна?

Кіберзлочинність – це акт скоєння злочину в кіберсередовищі; проте кіберзлочинність не обов'язково є актом кібервійни. Кібервійна може включати різні форми саботажу і шпигунства з наміром нанесення шкоди нації або уряду. У наступній статті описується різниця між кіберзлочинністю і кібервійною:

http://www.pcworld.com/article/250308/when_is_a_cybercrime_an_act_of_cyberwar_.html

https://jnslp.com/?s=Cyberwar+Vs.+Cybercrime

"Introduction to Cybersecurity" – курс на платформі Codecademy. Курс знайомить з основними темами кібербезпеки, такими як криптографія, брандмауери та етичний хакінг, а також дає можливість попрактикуватися в реальних ситуаціях через інтерактивні вправи. Курс доступний для початківців і забезпечує цікавий досвід навчання.

https://www.codecademy.com/learn/introduction-to-cybersecurity

Наведені ресурси допоможуть краще зрозуміти ключові проблеми в банківській галузі, управлінні ризиками ланцюга поставок, відмінності між кіберзлочинністю та кібервійною, сформувати міцну базу знань з кібербезпеки.

ТЕМА 2. КУБ КІБЕРБЕЗПЕКИ

Фахівці з кібербезпеки – це експерти, які займаються захистом у кіберпросторі. Джон Мак-Камбер один з перших експертів з кібербезпеки, розробив широко використовувану конструкцію під назвою Куб Мак-Камбера або Куб кібербезпеки. Він використовується як інструмент для захисту мереж, доменів та Інтернету. Куб кібербезпеки чимось нагадує кубик Рубика.

Перший вимір Куба кібербезпеки визначає три принципи інформаційної безпеки. Фахівці з кібербезпеки називають ці три принципи (конфіденційність, цілісність, доступність) КЦД-тріадою (CIA Triad).

Другий вимір визначає три стани інформації або даних.

Третій вимір куба визначає необхідні дії для забезпечення захисту.

Ці виміри часто називають трьома категоріями гарантованої кібербезпеки.

У цій темі ми також розглянемо і модель кібербезпеки ISO – це міжнародної основи стандартизації та керування інформаційними системами.

2.1. ТРИ ВИМІРИ КУБА КІБЕРБЕЗПЕКИ

Перший вимір куба кібербезпеки визначає цілі захисту кіберпростору. Цілі, визначені в першому вимірі, є основоположними принципами. Цими трьома принципами є конфіденційність, цілісність і доступність. Ці принципи забезпечують орієнтир і дають змогу фахівцеві з кібербезпеки визначати пріоритети дій при захисті будь-якої мережевої системи (рис. 2.1).

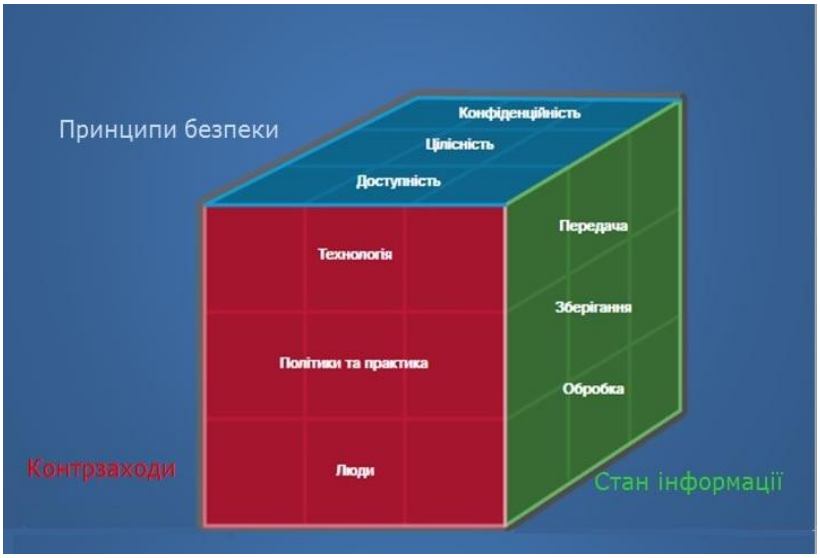


Рис. 2.1. Куб кібербезпеки[16]

[16] – https://aitac.jp/news/assets/f28bffb41aadab03f2c60e44cc9d070ab45954bc.pdf

Конфіденційність запобігає розкриттю інформації неавторизованим людям, ресурсам або процесам. Цілісність даних позначає їхню точність, узгодженість та достовірність. Нарешті, доступність гарантує, що інформація доступна авторизованим користувачам у разі потреби. Для означення цих трьох принципів використовують абревіатуру КЦД (англ. – CIA).

Другий вимір куба кібербезпеки зосереджений на проблемах захисту даних, які знаходяться у кіберпросторі в різних станах. Кіберпростір – це домен, що містить значну кількість критично важливих даних, тому експерти з кібербезпеки зосереджені на захисті даних. Дані мають три можливі стани:

- дані в передачі;
- дані в стані спокою або зберігання;
- дані в обробці.

Захист кіберпростору потребує, щоб фахівці в області кібербезпеки гарантували безпеку даних у всіх трьох станах.

Третій вимір куба кібербезпеки визначає навички і знання, які фахівець з кібербезпеки може використовувати для захисту у кіберпросторі. Фахівці з кібербезпеки повинні використовувати цілу низку наявних навичок і знань, коли захищають дані в кіберпросторі. Вони повинні це робити залишаючись при цьому на стороні закону.

Куб кібербезпеки визначає три типи навичок, які використовуються для забезпечення захисту.

Перша навичка включає в себе технології, пристрої та продукти для захисту інформаційних систем і запобігання діям кіберзлочинців. Фахівці з кібербезпеки повинні володіти спеціалізованими технологічними інструментами. Проте, Мак-Камбер нагадує їм, що для перемоги над кіберзлочинцями недостатньо самих лише технологічних засобів.

Друга навичка Професіонали з кібербезпеки також повинні вибудовувати потужний захист через налаштування політик, процедур та рекомендацій, які дають змогу користувачам кіберпростору залишатися у безпеці та дотримуватися принципів передової практики.

Третя навичка Нарешті, користувачі кіберпростору повинні прагнути більшої обізнаності щодо загроз у кіберпросторі та виробити культуру навчання та усвідомлення у сфері інформаційної безпеки.

2.2. ТРІАДА КЦД (конфіденційність, цілісність і доступність)

І. Конфіденційність запобігає розкриттю інформації неавторизованим особам, ресурсам або процесам. Синонімом конфіденційності є приватність. Організації обмежують доступ, щоб гарантувати, що тільки уповноважені оператори можуть використовувати дані або інші мережеві ресурси (рис.2.2).

Наприклад, програміст не повинен мати доступу до особистої інформації всіх співробітників.

Організації повинні навчати співробітників кращим методам захисту конфіденційної інформації, щоб захистити їх та себе від атак. Методи, які використовуються для забезпечення конфіденційності, включають шифрування даних, автентифікацію і контроль доступу.

Рис. 2.2. Конфіденційність[17]

Організації накопичують великий обсяг даних. Значна частина цих даних є відкритою і не потребує захисту, наприклад, імена співробітників та номери їх телефонів. Проте деякі дані потребують особливого захисту. Конфіденційна інформація – це дані, захищені від несанкціонованого доступу для гарантування безпеки окремій особі або організації.

Існує три типи конфіденційної інформації (рис. 2.3):

Рис. 2.3. Типи конфіденційної інформації

Персональна інформація – це особиста інформація, а саме дані, за допомогою яких можна визначити особистість людини.

[17] – https://aitac.jp/news/assets/f28bffb41aadab03f2c60e44cc9d070ab45954bc.pdf

- Ділова інформація – це інформація, яка у разі оприлюднення може створити проблеми для організації.
- Таємна інформація – це інформація, що належить державним органам, засекречена через високий рівень конфіденційності.

Контроль доступу визначає ряд схем захисту, які запобігають несанкціонованому доступу до комп'ютера, мережі, бази даних або інших ресурсів даних. Концепція ААО (англ. AAA) включає в себе три служби безпеки: автентифікація, авторизація та облік. Ці служби забезпечують основну структуру контролю доступу. Перше «А» в ААО (ААА) позначає автентифікацію.

Автентифікація перевіряє особу користувача для запобігання несанкціонованому доступу. Користувачі підтверджують свою особистість за ім'ям користувача або ідентифікатором.

Окрім того, користувачі повинні підтвердити свою особу за одним із способів (рис. 2.4):

- Надати інформацію яку вони знають (наприклад, пароль);
- Підтвердити наявність чогось (наприклад, токена або картки);
- Надати біометричну інформацію (наприклад, відбитки пальців).

Рис. 2.4. Автентифікація

Наприклад, для зняття готівки через банкомат, Вам потрібна ваша банківська картка та PIN-код. Це також є прикладом багатофакторної автентифікації. Для багатофакторної автентифікації потрібно декілька типів

автентифікації. Найбільш популярною формою автентифікації є використання паролів.

Авторизація, визначає через свою службу до яких ресурсів можуть отримати доступ користувачі, а також операції, які вони можуть виконувати (рис. 2.5). Деякі системи реалізують це за допомогою списку керування доступом або ACL (англ. Access Control List). ACL визначає, чи має користувач певні привілеї доступу після проходження автентифікації. Те, що ви можете увійти в корпоративну мережу, не означає, що у вас є дозвіл на використання високошвидкісного кольорового принтера. Авторизація також може контролювати, коли користувач має доступ до певного ресурсу. Наприклад, співробітники можуть мати доступ до бази даних продажів в робочий час, але система блокує їх у неробочий час.

Рис. 2.5. Авторизація

Облік, відстежує дії користувача, а саме, до яких даних вони зверталися, тривалість використання ресурсів та будь-які зроблені зміни. Наприклад, банк відстежує облікові записи кожного клієнта. Аудит цієї системи може виявити час і кількість всіх транзакцій, а також співробітника або системи, які виконували транзакції. Служби обліку кібербезпеки працюють так само. Система відстежує кожну транзакцію даних і надає результати аудиту. Для запровадження аудиту системи адміністратор може налаштувати політики комп'ютера.

Концепція AAO (AAA) (автентифікація, авторизація та облік) аналогічна використанню кредитної картки (рис. 2.6). Кредитна карта ідентифікує, хто може її використовувати, скільки може витратити цей користувач і веде облік товарів або послуг, які користувач придбав чи замовив.

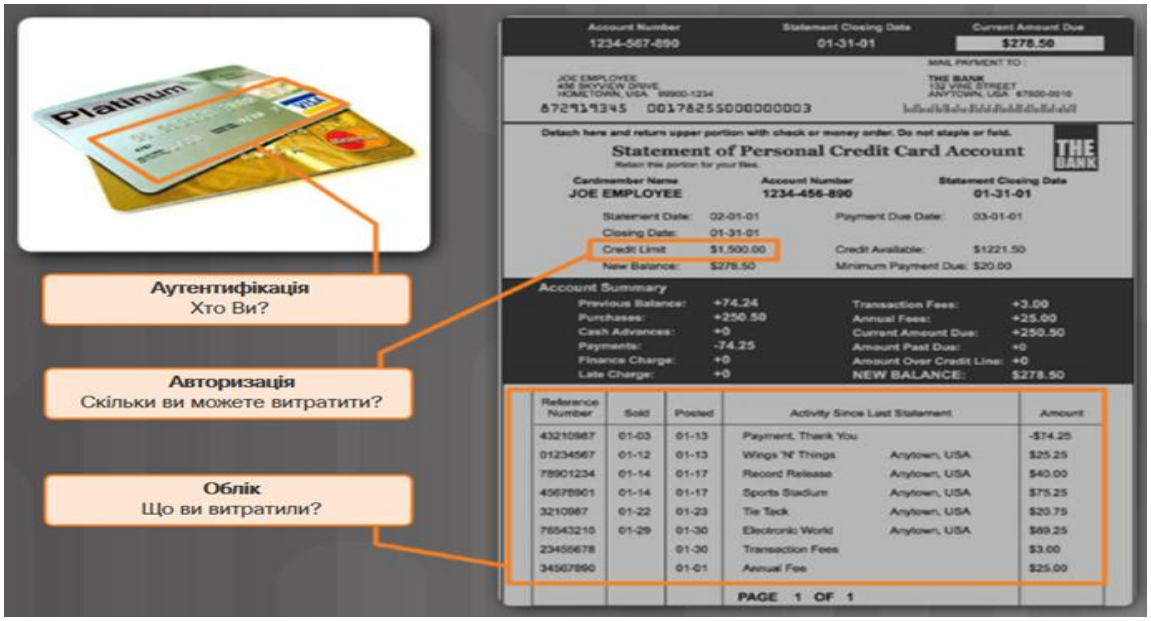


Рис. 2.6. Концепція ААО на прикладі кредитної картки[18]

У сфері кібербезпеки облік виконується у режимі реального часу й допомагає визначити, які ресурси використовуються найбільше, що дає змогу адміністратору вчасно виявляти потенційні загрози або аномальні дії в системі. Вебсайти, такі як Norse, показують атаки в режимі реального часу на основі даних, зібраних в рамках системи обліку або відстеження.

Конфіденційність і приватність здаються взаємозамінними, але з юридичної точки зору вони означають різні речі. Більшість приватних даних конфіденційні, але не всі конфіденційні дані є приватними. Доступ до конфіденційної інформації відбувається після підтвердження правильної авторизації. Фінансові установи, лікарні, медичні працівники, юридичні фірми та підприємства обробляють конфіденційну інформацію. Конфіденційна інформація має непублічний статус. Збереження конфіденційності – це скоріше етичний обов'язок.

Приватність пов'язана з правильним використанням даних. Коли організації збирають інформацію, надану клієнтами або співробітниками, вони повинні використовувати ці дані лише за прямим призначенням. Більшість організацій зажадають, щоб клієнт або співробітник підписали необхідний документ, надавши організації право використовувати дані.

Зростаюче число законів, що стосуються приватності, створює величезне навантаження для організацій, які збирають і аналізують дані. Політика – кращий спосіб для організації дотримуватися законів, що стосуються конфіденційності. Політики дають змогу організаціям застосовувати певні правила, процедури і процеси при зборі, зберіганні та спільному використанні даних.

[18] – https://encrypted-tbn1.gstatic.com/images?q=tbn:ANd9GcS01xA9L4NtCEwDjYA1DcnKjt__FU8j5OXON-cayGW3WEizc_PD

II. Цілісність – це точність, узгодженість і достовірність даних протягом всього життєвого циклу. Іншими словами цілісність – це якість. Дані піддаються деяким операціям, таким як збір, зберігання, вилучення, оновлення та передача. Дані повинні залишатися незмінними під час виконання всіх цих операцій неавторизованими суб'єктами.

Методи, які використовуються для забезпечення цілісності даних, включають хешування, перевірку достовірності даних, перевірку узгодженості даних і керування доступом. Хешування – це перетворення вхідного масиву даних довільної довжини у вихідний бітовий рядок фіксованої довжини (синоніми: хеш – функція, функція згортання, хеш-код, хеш-сума, дайджест повідомлення, хеш-таблиці). Системи цілісності даних можуть включати один або декілька методів, наведених вище.

Цілісність даних є фундаментальним компонентом інформаційної безпеки. Потреба в цілісності даних залежить від того, як організація використовує дані. Наприклад, Facebook не перевіряє дані, які користувач публікує в профілі. Банк або фінансова організація надають більшого значення цілісності даних, ніж Facebook. Транзакції і рахунки клієнтів повинні бути точними. В організації охорони здоров'я цілісність даних може бути питанням життя або смерті. Інформація в рецептах повинна бути точною.

Захист цілісності даних є постійною проблемою для більшості організацій. Втрата цілісності даних може призвести до того, що всі дані будуть недостовірними або непридатними для використання.

Перевірка цілісності – це спосіб вимірювання узгодженості набору даних (файлу, зображення або записів). Перевірка цілісності виконується за допомогою такого процесу як хеш-функції для миттєвого формування відбитка даних. Перевірка цілісності використовує цей відбиток аби переконатися, що дані залишилися незмінними.

Хешування – перетворення вхідного масиву даних довільної довжини у вихідний бітовий рядок фіксованої довжини. ***Синоніми***: хеш-функції, функція згортання, хеш-код, хеш-сума, хеш-функції, дайджест повідомлення, хеш-таблиці).

Контрольна сума є одним із прикладів хеш-функції. Контрольна сума підтверджує цілісність файлів або рядків символів до і після їх передачі з одного пристрою на інший через локальну мережу або Інтернет. Контрольна сума просто перетворює кожну частину інформації в значення і підсумовує їх. Щоб перевірити цілісність даних, система, яка отримала файл, повторює цей процес. Якщо дві суми рівні, дані дійсні. Якщо вони не рівні, десь в процесі передачі відбулася зміна.

На сьогодні день популярні такі хеш-функції, як MD5, SHA-1, SHA-256 і SHA-512. Ці хеш-функції використовують складні математичні алгоритми.

Значення хешу використовується для порівняння. Наприклад, після завантаження файлу користувач може перевірити його цілісність, порівнюючи хеш-значення джерела з тим, яке генерується будь-яким хеш-калькулятором.

Організації використовують контроль версій для запобігання випадковим змінам від авторизованих користувачів. Два користувачі не можуть оновити один і той самий об'єкт. Об'єктами можуть бути файли, записи бази даних або транзакції. Наприклад, у першого користувача, який відкрив документ, є дозвіл на зміну цього документа. У другого – є версія лише для читання.

Точні резервні копії допомагають зберегти цілісність даних, якщо дані пошкоджені. Організації необхідно перевірити результат резервного копіювання, щоб забезпечити цілісність резервного копіювання до втрати даних.

Авторизація визначає, хто має доступ до ресурсів організації, виходячи з необхідності. Наприклад, дозвіл на доступ до файлів і засоби контролю доступу користувачів гарантують, що тільки деякі користувачі можуть змінювати дані. Адміністратор може встановлювати дозволи для файлу тільки для читання. В результаті користувач, який одержує доступ до цього файлу, не може вносити жодних змін.

III. Доступність даних – це принцип, який використовується для опису необхідності постійно підтримувати доступність інформаційних систем і послуг. Кібератаки і збої системи можуть перешкоджати доступу до інформаційних систем і служб. Наприклад, перериванням доступності вебсайту шляхом виведення його з ладу можуть скористатися конкуренти. Ці атаки типу «відмова в обслуговуванні» (DoS) загрожують доступності системи і не дають змогу користувачам отримувати доступ до інформаційних систем і використовувати їх за необхідності.

Методи, які використовуються для забезпечення доступності, включають: системне резервування, резервне копіювання системи, підвищену відмовостійкість системи, технічне обслуговування обладнання, сучасні операційні системи та програмне забезпечення і плани із швидкого відновлення після непередбачених лих.

Люди використовують різні інформаційні системи в повсякденному житті. Комп'ютери та інформаційні системи контролюють зв'язок, транспорт і виробництво продукції. Постійна доступність інформаційних систем необхідна для сучасного життя. Термін «висока доступність» описує системи, призначені для запобігання простоям. Висока доступність забезпечує рівень продуктивності протягом більш тривалого, ніж зазвичай, періоду. Системи високої доступності найчастіше використовують три принципи проектування:

- усунути окремі точки відмови;
- виявити збої у міру їх виникнення;

- забезпечити надійний план швидкого відновлення роботи на випадок надзвичайної ситуації.

Мета полягає в тому, щоб продовжувати працювати в екстремальних умовах, наприклад під час атаки. Одна з найпопулярніших технологій високої доступності – п'ять дев'яток. Назва п'ять дев'яток пов'язана з доступністю ресурсу 99,999% часу. Це означає, що час простою становить менше 5,26 хвилин на рік.

Організації можуть забезпечити доступність, регулярно виконуючи дії:

- обслуговування обладнання;
- оновлення ОС та системи;
- резервне копіювання;
- планування дій на випадок стихійних лих;
- нові технологічні реалізації;
- моніторинг надзвичайної активності;
- перевірка доступності.

2.3. СТАНИ ДАНИХ. ПРОБЛЕМИ ЗАХИСТУ

Перший стан даних

Збережені дані належать до даних у стані спокою. Дані в стані спокою означають, що пристрій зберігання зберігає дані, коли жоден користувач або процес не використовує їх. Пристрій зберігання може бути локальним (на обчислювальному пристрої) або централізованим (в мережі). Існує багато опцій для зберігання даних.

Пряме сховище (direct-attached storage, DAS) – це сховище, що під'єднане до комп'ютера. Жорсткий диск або USB-накопичувач – приклад сховища з прямим підключенням. За замовчуванням системи не налаштовані для спільного використання сховища з прямим підключенням.

Резервний масив незалежних дисків (Redundant array of independent disks, RAID) використовує кілька жорстких дисків у масиві і являє собою об'єднання декількох дисків, які розглядаються операційною системою як один. RAID забезпечує підвищену продуктивність і відмовостійкість.

Мережевий пристрій зберігання даних (network attached storage, NAS) – це пристрій, підключений до мережі, який дає змогу авторизованим користувачами зберігати та отримувати дані з централізованого сховища. Пристрої NAS гнучкі і масштабовані, що дає змогу адміністраторам збільшувати ємність у разі необхідності.

Мережа зберігання даних (storage area network, SAN) – це мережева система зберігання, яка під'єднується до мережі за допомогою високошвидкісних інтерфейсів. Це дає змогу підвищити продуктивність і

забезпечує можливість підключення декількох серверів до централізованого дискового сховища.

Хмарне сховище (Cloud storage) – це вид віддаленого сховища, при якому використовується простір на накопичувачах в дата-центрі провайдера, доступ до даних може бути організований з будь-якого комп'ютера з доступом до мережі Інтернет. Google Drive, iCloud і Dropbox – все це приклади постачальників хмарних сховищ.

Збереження даних – це складне завдання для організацій. Для покращення зберігання даних організації можуть вдатися до автоматизації та виконувати централізоване резервне копіювання даних.

Сховище з прямим підключенням може бути одним з найскладніших типів зберігання даних з точки зору контролю та керування. Воно найбільш вразливе до шкідливих атак на локальний хост. Збережені дані можуть також містити дані резервного копіювання. Резервні копії можуть створюватися вручну або автоматично. Організації повинні обмежувати типи даних, що зберігаються в сховищі з прямим підключенням. Зокрема, на них не слід зберігати критично важливі дані.

Мережеві системи зберігання пропонують більш безпечний варіант. Такі мережеві системи зберігання даних як RAID, SAN і NAS забезпечують більшу продуктивність та надлишковість. Проте мережеві системи зберігання складніші для налаштування та керування. Також вони обробляють більші обсяги даних, що створює значний ризик для організації при виході пристрою з ладу. Особливу увагу при використанні мережевих систем зберігання даних слід приділяти налаштуванню, тестуванню і моніторингу системи.

Другий стан даних

Передача даних – це надсилання інформації з одного пристрою на інший. Існує багато способів передачі інформації між пристроями:

- Sneaker net – використовує знімні носії для фізичного переміщення даних з одного комп'ютера на інший;
- Дротові мережі – використовують кабелі для передачі даних;
- Бездротові мережі – використовують радіохвилі для передачі даних.

Організації ніколи не зможуть уникнути використання Sneaker net.

Дротові мережі включають в себе мідні та волоконно-оптичні кабелі. Дротові мережі можуть обслуговувати місцеву географічну зону (локальна мережа), або прокладатися на великі відстані (глобальні мережі).

Бездротові мережі замінюють дротові, стають швидшими і здатні забезпечити більшу пропускну здатність. Бездротові мережі збільшують кількість користувачів, які під'єднуються до них з мобільних пристроїв у невеликих офісах і корпоративних мережах. Бездротові мережі забезпечують

значну гнучкість у розгортанні, оскільки не потребують фізичних кабельних з'єднань, значно спрощують налаштування і модернізацію мереж (рис.2.7).

Рис. 2.7. Бездротові мережі[19]

У дротових і бездротових мережах використовуються пакети або блоки даних. Термін «пакет» означає одиницю даних, яка переміщується між джерелом і пунктом призначення в мережі. Стандартні протоколи, такі як протокол Інтернету (IP) і протокол передачі гіпертексту (HTTP), визначають структуру і формат пакетів даних. Ці стандарти мають відкриті вихідні коди і є загальнодоступними. Захист конфіденційності, цілісності та доступності переданих даних – один з найважливіших обов'язків фахівця в області кібербезпеки.

Захист переданих даних є однією з найскладніших задач фахівця з кібербезпеки. Зі зростання кількості мобільних і бездротових пристроїв фахівці в області кібербезпеки несуть відповідальність за щоденний захист даних, які перетинають їх мережу. Фахівець з кібербезпеки повинен вирішити кілька проблем захисту цих даних:

- Захист конфіденційності даних – кіберзлочинці можуть перехоплювати, зберігати і викрадати дані під час їх передачі між пристроями. Кіберпрофесіонали повинні вжити заходів для протидії цим процесам.
- Захист цілісності даних – кіберзлочинці можуть перехоплювати і змінювати дані в момент їх передачі. Для запобігання цим діям фахівці з кібербезпеки впроваджують системи підтримки цілісності даних, які перевіряють достовірність і автентичність переданих даних.
- Захист доступності даних – кіберзлочинці можуть використовувати шахрайські або неавторизовані пристрої для переривання доступ до даних. Простий мобільний пристрій може являти собою локальну точку бездротового доступу і вводити в оману звичайних користувачів. Кіберзлочинець може перехопити авторизоване підключення до захищеної служби або пристрою. Для протидії цим процесам фахівці з мережевої безпеки можуть впроваджувати системи взаємної автентифікації. Системи взаємної автентифікації потребують, щоб користувач авторизувався на сервері, а сервер у відповідь автентифікував користувача.

[19] – https://encrypted-tbn3.gstatic.com/images?q=tbn:ANd9GcT4tyQg7_7y4jvxPYRZUx3duidg2Sz-3Os3l2NdzdmAGqGf8Fpz

Третій стан даних

Дані в обробці. У цьому стані дані перебувають під час початкового введення, зміни, обчислення або виведення (рис.2.8).

Рис. 2.8. Дані в обробці[20]

Захист цілісності даних починається з початкового введення даних. Організації використовують кілька методів для збору даних, таких як ручне введення даних, форми сканування, завантаження файлів і зчитування даних з датчиків. Кожен з цих методів створює потенційну загрозу цілісності даних.

Прикладом пошкодження даних під час введення є помилки введення даних або відключені, несправні або непрацюючі системні датчики. До помилок введення належать також неправильне маркування і неправільні або неузгоджені формати даних.

Модифікація даних – це будь-яка зміна вихідних даних. Наприклад, коли користувач вручну змінює дані або програма обробляє та оновлює дані, або коли дані змінюються внаслідок відмови обладнання. Процеси, такі як кодування/декодування, компресія/декомпресія і шифрування/дешифрування, є прикладами модифікації даних Шкідливий код також призводить до пошкодження даних.

Пошкодження даних також відбувається під час процесу виведення даних. Вивід даних відповідає передачі даних на принтери, електронні дисплеї або безпосередньо на інші пристрої. Точність вихідних даних має вирішальне значення, оскільки вивід інформації впливає на прийняття рішень. Прикладами пошкодження вихідних даних можуть бути неправильне використання обмежувачів, невірні параметри з'єднання і невідповідно налаштовані принтери.

Захист даних від некоректних змін під час обробки може мати негативний вплив. Помилки програмного забезпечення є причиною багатьох невдач і катастроф. Наприклад, всього за два тижні до Різдва деякі зі сторонніх роздрібних продавців Amazon випадково виставили ціну в один цент на свої товари. Збій тривав одну годину. Помилка призвела до того, що тисячі покупців придбали за безцінь товари, а компанія втратила дохід. У 2016 році термостат Nest зазнав збій і залишив користувачів без тепла.

[20] – https://encrypted-tbn3.gstatic.com/images?q=tbn:ANd9GcRIQpbImKlJHWcYJSgfDRu7BKJUJSx1wiH3dJH_6oP5yh3aWPwS

Термостат Nest – це інтелектуальна технологія, що належить Google. Збій програмного забезпечення залишив користувачів, буквально, на холоді. Проблеми з оновленням програмного забезпечення призвели до розрядки акумуляторів пристрою, через що не було можливості контролювати температуру. В результаті клієнти не змогли обігріти свої будинки або отримати гарячу воду в один з найхолодніших вихідних в році.

Для захисту даних під час обробки потрібні ретельно спроектовані системи. Фахівці з кібербезпеки розробляють політики та процедури, які потребують тестування, обслуговування та оновлення систем, щоб вони працювали з найменшою кількістю помилок.

2.4. ЗАСОБИ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ

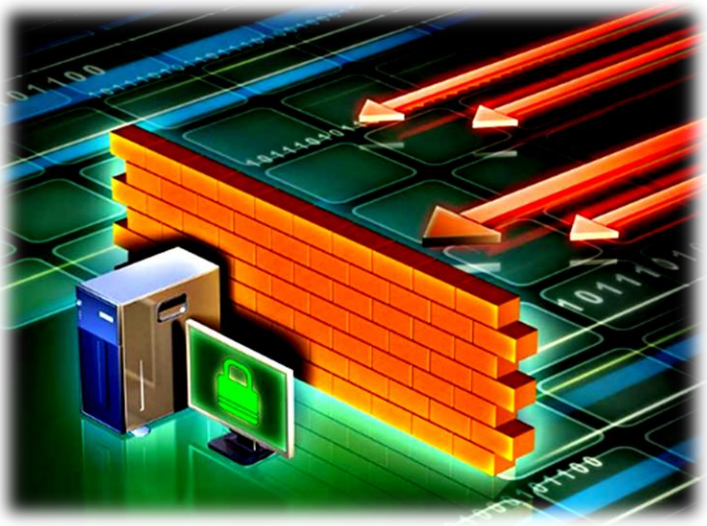


Рис. 2.9. Програмна протидія[21]

Розглянемо основні аспекти протидії кіберзлочинності: програмні, апаратні, мережеві та хмарні технології.

І. Програмні технології

Програмні засоби захисту – це програми і служби, які захищають операційні системи, бази даних та інші служби, що працюють на робочих станціях, портативних пристроях і серверах. Адміністратори встановлюють програмні запобіжні засоби на окремих хостах або серверах. Існує кілька програмних технологій, які використовуються для захисту даних організації (рис.2.9).

- Брандмауери керують віддаленим доступом до системи. Зазвичай брандмаурер входить до складу операційних систем, або користувач може придбати чи завантажити брандмауер від інших виробників.
- Сканери мережі та портів виявляють і контролюють відкриті порти на хості або сервері.
- Аналізатори протоколів або аналізатори сигнатур – це пристрої, які збирають і досліджують мережевий трафік. Вони виявляють проблеми з продуктивністю, неправильні конфігурації, додатки, що некоректно працюють, визначають шаблони типового та нормального трафіку і усувають (налагоджують) проблеми зі зв'язком.

[21] – https://encrypted-tbn1.gstatic.com/images?q=tbn:ANd9GcTMWFkDe6L2usHF14CTJLMq2x79fNQEkquCv5rgNU5PPQax_Fn4

- Сканери вразливостей – це комп'ютерні програми, призначені для оцінки слабких місць комп'ютерів або мереж.
- Системи виявлення вторгнень на базі хоста (IDS) перевіряють активність тільки на хост-системах. IDS генерує лог-файли (записи у системному журналі) та попереджувальні повідомлення при виявленні незвичної активності. Система, яка зберігає конфіденційні дані або надає критично важливі, може бути цільовою для використання системи виявлення вторгнень на базі хостів (IDS).

II. Апаратні технології

Існує кілька апаратних технологій, що використовуються для захисту даних організацій:

- Брандмауер (апаратний) блокує небажаний трафік на основі правил, які визначають вхідний і вихідний трафік, дозволений у мережі.
- Спеціалізовані системи виявлення вторгнень (IDS) виявляють ознаки атак або незвичного трафіку в мережі і надсилають сповіщення (рис. 2.10).

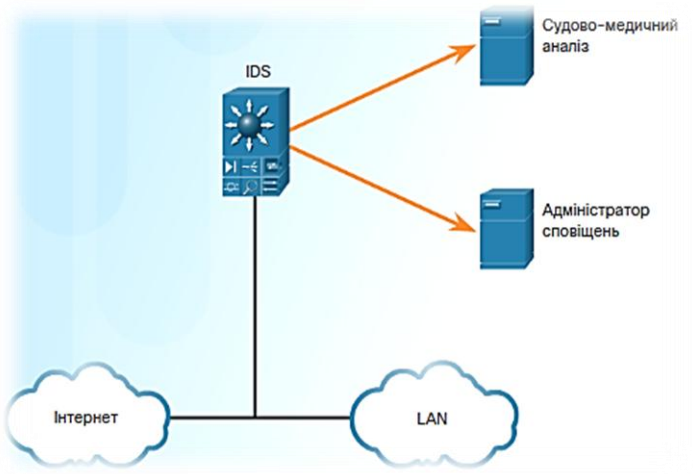


Рис. 2.10. Аналіз трафіку системою IDS

- Системи запобігання вторгненням (Intrusion Prevention Systems – IPS) виявляють ознаки атак або незвичного трафіку в мережі, генерують попередження і вживають коригувальних дій.
- Служби фільтрування контенту контролюють доступ і передачу небажаного або образливого вмісту.

III. Мережеві технології

Для захисту даних організації використовуються кілька мережевих технологій:

- Віртуальна приватна мережа (VPN) – це безпечна віртуальна мережа, що використовує загальнодоступну мережу (Інтернет). Безпека VPN полягає в шифруванні вмісту пакета між кінцевими точками.
- Контроль доступу до мережі (Network Access Control – NAC) – потребує набору перевірок, перш ніж дозволяти пристрою підключатися до мережі. Такі перевірки можуть стосуватися встановлення останньої версії антивірусного програмного забезпечення або оновлення операційної системи.
- Безпека бездротової точки доступу реалізується за допомогою автентифікації і шифрування.

IV. Хмарні технології

Хмарні технології, переносять технологічний компонент захисту від організації до провайдера хмарних обчислень. Існує три основні служби хмарних обчислень (рис.2.11):

Рис. 2.11. Хмарний захист[22]

- Програмне забезпечення як послуга (SaaS) дає змогу користувачам отримувати доступ до прикладного програмного забезпечення та баз даних. Хмарні провайдери управляють інфраструктурою. Користувачі зберігають дані на серверах хмарного провайдера.
- Інфраструктура як послуга (IaaS) забезпечує віртуальні обчислювальні ресурси через Інтернет. Провайдер надає у користування апаратне та програмне забезпечення, сервери і компоненти зберігання.
- Платформа як послуга (PaaS) забезпечує доступ до інструментів і служб розробки, які використовуються для створення застосунків.

Провайдери хмарних послуг розширили ці опції, включивши IT-службу (ITaaS), яка забезпечує IT-підтримку для моделей обслуговування IaaS, PaaS і SaaS. У моделі ITaaS організація укладає контракти з постачальником хмарних послуг для отримання необхідних послуг.

Постачальники хмарних послуг використовують віртуальні пристрої безпеки, які працюють у віртуальному середовищі з попередньо упакованою, спрощеною операційною системою, яка працює на віртуалізованому обладнанні.

Інвестування значних коштів у технології не спричинить належного ефекту, якщо люди в організації залишатимуться найслабшою ланкою в кібербезпеці. Програма інформування про безпеку надзвичайно важлива для організації. Співробітник може не навмисно вчиняти потенційно небезпечні дії, через те, що не знає як належить поводитись. Існує кілька способів реалізації офіційної навчальної програми:

- зробити тренінг з безпеки необхідним елементом для початку роботи у компанії;

враховувати обізнаність з питань безпеки при прийомі на роботу або при оцінці працездатності;

[22] – https://encrypted-tbn1.gstatic.com/images?q=tbn:ANd9GcTMWFkDe6L2usHF14CTJLMq2x79fNQEkquCv5rgNU5PPQax_Fn4

- проведення очних тренінгів;
- проводити онлайн-курси.

Таке навчання має проводитися на регулярних засадах, оскільки нові загрози з'являються постійно.

Члени організації повинні бути поінформовані про політику безпеки і мати необхідні знання, щоб зробити безпеку частиною їхньої повсякденної діяльності.

Активна програма інформування про безпеку залежить від:

- внутрішнього середовища організації;
- рівня загрози.

Створення культури обізнаності про кібербезпеку – це постійне зусилля, яке потребує ініціативи вищого керівництва і прихильності всіх користувачів і співробітників. Вплив культури кібербезпеки організації починається з розробки політики та процедур з боку керівництва. Наприклад, багато організацій мають дні обізнаності про кібербезпеку. Організації можуть також розміщувати банери і вивіски для підвищення загальної поінформованості про кібербезпеку. Створення семінарів орієнтованих на кібербезпеку допомагає підвищити рівень обізнаності.

Політика безпеки

Політика безпеки – це набір правил для компанії, який включають правила поведінки для користувачів і адміністраторів і визначають системні вимоги. Такі цілі, правила і вимоги в сукупності забезпечують безпеку мережі, даних і комп'ютерних систем всередині організації.

Комплексна політика безпеки виконує кілька завдань:

- Демонструє серйозне ставлення до безпеки.
- Встановлює правила поведінки.
- Забезпечує узгодженість в роботі системи, придбанні та використанні програмного і апаратного забезпечення, а також в його обслуговуванні.
- Визначає юридичні наслідки порушень.
- Надає співробітникам служби безпеки підтримку керівництва.

Політика безпеки інформує користувачів, персонал і керівників про вимоги організації до захисту технологічних і інформаційних активів. Політика безпеки також визначає механізми, необхідні для дотримання вимог безпеки.

Як показано на рисунку, політика безпеки зазвичай включає в себе:

- Політики ідентифікації і автентифікації – визначає уповноважених осіб, які можуть мати доступ до мережевих ресурсів і окреслює процедури перевірки.
- Політика паролів – забезпечує, щоб паролі відповідали мінімальним вимогам і регулярно змінювалися.
- Політика прийнятного використання – визначає мережеві ресурси використання яких, прийнятне для організації. Вона також може визначати наслідки порушень правил.

- Політика віддаленого доступу – визначає, як віддалені користувачі можуть отримати доступ до мережі і до чого саме надавати доступ.
- Політика мережевого обслуговування – визначає операційні системи мережевих пристроїв і процедури оновлення додатків для кінцевих користувачів.
- Політика обробки інцидентів – описує порядок дій у разі інцидентів пов'язаних з безпекою.

Одним з найбільш поширених компонентів політики безпеки є політика прийнятного використання (acceptable use policy – AUP). Цей компонент визначає, що користувачі можуть і не можуть робити з різними системними компонентами. Для уникнення непорозумінь, політика AUP повинна бути максимально докладною. Наприклад, AUP містить перелік конкретних вебсайтів, груп новин або програм з інтесивним трафіком, до яких користувачі не мають доступу з робочих комп'ютерів або через мережу компанії.

Стандарти

Стандарти допомагають IT-персоналу підтримувати узгодженість в роботі мережі. Стандартні документи визначають технології, які необхідні конкретним користувачам або програмам, а також програмні вимоги чи критерії, яких слід дотримуватися організації (рис.2.12). Це допомагає IT-фахівцям підвищити ефективність і спростити проектування, обслуговування та усунення неполадок.

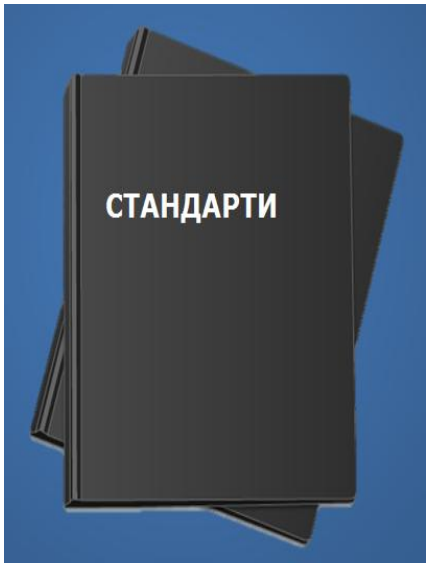


Рис. 2.12. Стандарти

Одним з найважливіших принципів безпеки є послідовність. З цієї причини організаціям необхідно встановлювати стандарти. Кожна організація розробляє стандарти для підтримки свого унікального операційного середовища. Наприклад, організація визначає політику паролів. Стандарт передбачає, що паролі повинні складатися мінімум з восьми букв у верхньому та нижньому регістрів, а також цифр і містити принаймні один спеціальний символ. Користувач повинен міняти пароль кожні 30 днів, а історія паролів з 12 попередніх паролів гарантує, що користувач створює унікальні паролі на один рік.

Методичні рекомендації

Методичні рекомендації – це список пропозицій про те, як робити речі більш ефективно і надійно. Вони схожі на стандарти, але більш гнучкі і зазвичай не є обов'язковими.

Ці рекомендації визначають, як розробляються стандарти і гарантують дотримання загальних політик безпеки.

Деякі з найбільш корисних рекомендацій складають кращі практики для роботи організації. Методичні рекомендації також доступні з наступних джерел:

- Національний інститут стандартів і технологій (NIST) Центр ресурсів комп'ютерної безпеки.
- Агентство національної безпеки (NSA).
- Загальні стандартні критерії.

Використовуючи приклад політики паролів, методичні рекомендації пропонують взяти фразу типу «I have a dream» і перетворити її на надійний пароль, Ihv@dr3@m. Користувач може створювати інші паролі з цієї фрази, змінюючи число, переміщаючи символ або змінюючи знак пунктуації.

Процедури

Документи процедури більш докладні і детальні, ніж стандарти і рекомендації. Документи процедури включають в себе деталі реалізації, які зазвичай містять покрокові інструкції.

Великі організації повинні використовувати процедурні документи для дотримання послідовності розгортання, необхідної політики для безпечного середовища.

2.5. СТРУКТУРА КЕРУВАННЯ ІТ БЕЗПЕКОЮ

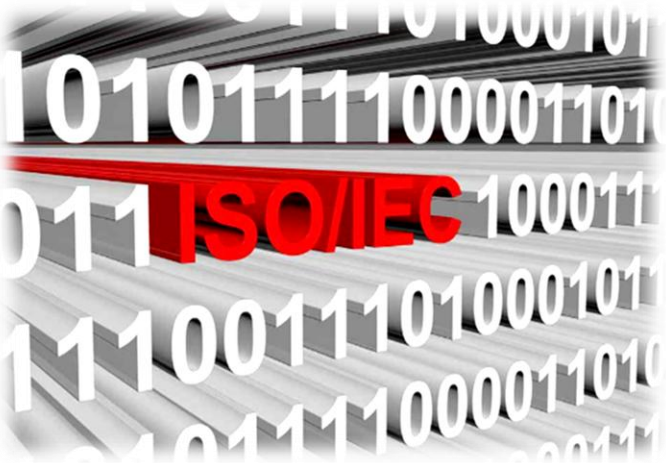


Рис. 2.13. ISO/IEC[23]

Фахівцям в області безпеки необхідно забезпечити захист інформації всередині організації. Це монументальне завдання і необґрунтовано очікувати, що одна людина має всі необхідні для цього знання. Міжнародна організація зі стандартизації (ISO) (рис.2.13) та Міжнародна електротехнічна комісія (IEC) розробила комплексну структуру для керування інформаційною безпекою. Модель кібербезпеки ISO/IEC має таке ж призначення для професіоналів в області кібербезпеки, що і мережева модель OSI для мережевих інженерів. Обидві моделі створюють основу для розуміння і виконання складних завдань, спрямованих на забезпечення безпеки. ISO/IEC 27000 – це стандарт інформаційної безпеки, овперше публікований в 2005 році, й з того часу регулярно переробляється та доповнюється.

[23] – https://encrypted-tbn3.gstatic.com/images?q=tbn:ANd9GcR_ecQXr5y1lM4SLSJE1tFceJXUUS1DchmAu8U1CH0oMELB4wpv

~~Незважаючи на те, що стандарти не є обов'язковими, більшість країн використовують їх як основу для забезпечення інформаційної безпеки~~

ISO/IEC 27000 – це стандарт інформаційної безпеки, опублікований в 2005 році, який регулярно переробляється та доповнюється. Незважаючи на те, що стандарти не є обов'язковими, більшість країн використовують їх як основу для забезпечення інформаційної безпеки.

Стандарти ISO 27000 описують впровадження комплексної системи керування інформаційною безпекою (ISMS). ISMS складається з усіх адміністративних, технічних і оперативних заходів контролю, що забезпечують безпеку інформації всередині організації. ISO 27000 охоплює практичні рекомендації в дванадцяти незалежних галузях. Ці дванадцять галузей забезпечують організаціям, на високому рівні, захист для широкого спектру інформації.

Структура моделі кібербезпеки ISO

Структура моделі кібербезпеки ISO відрізняється від моделі OSI тим, що вона використовує галузі, а не шари, для опису категорій безпеки (рис. 2.14). Причина цього в тому, що модель кібербезпеки ISO не є ієрархічною. Це однорангова модель, в якій кожна сфера має прямий зв'язок з іншою. Модель кібербезпеки ISO 27000 дуже схожа на модель OSI, тому для успішної побудови кар'єри фахівцеві з кібербезпеки дуже важливо розуміти обидві моделі.

Рис. 2.14. Структура моделі кібербезпеки ISO

Дванадцять галузей служать спільною основою для розробки стандартів безпеки і ефективних методів керування безпекою. Вони також допомагають полегшити взаємодію між організаціями.

Дванадцять галузей складаються з цілей контролю, визначених у частині стандарту ISO 27001. Цілі контролю визначають вимоги високого рівня для впровадження комплексного ISM (керування інформаційною безпекою). Керівництво організації використовує цілі контролю ISO 27001 для визначення і публікації політик безпеки організації. Цілі контролю забезпечують контрольний список для перевірок керування безпекою. Багато організацій мають пройти аудит ISMS, для отримання сертифіката відповідності стандарту ISO 27001.

Сертифікація та відповідність забезпечують довіру організацій, яким необхідно обмінюватися конфіденційними даними і операціями. Перевірки відповідності і безпеки підтверджують, що організації постійно вдосконалюють свою систему керування інформаційною безпекою.

Нижче наведено приклад завдання для контролю:

Контроль доступу до мереж з використанням відповідних механізмів автентифікації для користувачів і обладнання.

В ISO/IEC 27002 визначаються системи керування інформаційною безпекою. Елементи контролю більш деталізовані, ніж цілі. Цілі контролю повідомляють організації, що робити. Елементи контролю визначають, як досягти мети.

З метою контролю, для керування доступом до мереж з використанням відповідних механізмів автентифікації для користувачів і обладнання, можна надати таку вказівку:

Використовуйте надійні паролі. Сильний пароль містить не менше восьми символів, які є комбінацією літер, цифр і символів (@, #, $,% і т. д), якщо це дозволено. Паролі чутливі до регістру, тому сильний пароль містить літери як верхнього, так і нижнього регістрів.

Фахівці з кібербезпеки визнають таке:

- Елементи контролю не є обов’язковими, але вони широко прийняті і застосовуються.
- Елементи контролю повинні підтримувати нейтралітет по відношенню до постачальника, щоб уникнути схиляння до конкретного продукту або компанії.
- Елементи контролю подібні до рекомендацій. Це означає, що може бути більше одного способу досягнення мети.

2.6. ПРИНЦИПИ ПОБУДОВИ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

У сучасному світі, де інформація є одним із найцінніших ресурсів, система захисту інформації має критичне значення.

Система захисту інформації (СЗІ) — це сукупність організаційних, технічних, програмних та правових заходів, спрямованих на забезпечення конфіденційності, цілісності та доступності інформації, яка обробляється, зберігається чи передається в межах інформаційних систем (рис.2.15).

Рис. 2.15. Аспекти систем захисту[24]

Її значення полягає у забезпеченні надійного функціонування організацій, захисті конфіденційних даних та запобіганні ризикам, які можуть призвести до фінансових втрат, репутаційного збитку чи порушення законодавства.

СЗІ створюють під час організації або модернізації інформаційної інфраструктури підприємства чи установи. Це може відбуватись під час проєктування нових систем та їх блоків, під час переходу на більш сучасні платформи чи технології, у випадках розширення діяльності підприємства або його масштабуванні. Причиною створення системи можуть бути вимоги законодавства, й підприємство зобов'язане забезпечити захист інформації відповідно до стандартів (наприклад, ISO/IEC 27000) або регуляторних актів у певній галузі (фінанси, медицина, державне управління).

Основою для створення систем захисту інформації може бути будь-яке середовище, де здійснюється обробка, зберігання або передача даних. Це стосується підприємств (захист комерційної таємниці й фінансової інформації), державних установ (захист службової та державної таємниці), медичних закладів (захист персональних і медичних даних), освітніх і науково-дослідних установ (захист наукових розробок та інформації про студентів і викладачів), а також інтернет-сервісів та електронної комерції (захист персональних даних користувачів і платіжної інформації).

Головною метою створення системи захисту інформації є забезпечення відповідності діяльності організації вимогам національного та міжнародного законодавства у сфері інформаційної безпеки. Це включає захист персональної, комерційної та іншої інформації, що має юридично визначений статус, від несанкціонованого доступу, втрати, викрадення чи спотворення, тож із пріоритетним забезпеченням її конфіденційності, цілісності та доступності.

[24] - https://tl.kyiv.ua/wp-content/uploads/2019/05/informaczijni-tekhnologiyi.jpg

Конфіденційність передбачає захист даних, програмних, апаратних пристроїв та інфраструктури від доступу неавторизованих осіб під час накопичення, обробки, зберігання й передачі даних. Серед ключових методів забезпечення конфіденційності застосовують шифрування, парольний доступ, багатофакторну автентифікацію, обмеження доступу, методи захисту передачі даних через мережу, резервне копіювання, моніторинг та виявлення порушень.

Принцип цілісності гарантує, що дані залишаються незмінними та можуть бути перевірені на автентичність під час зберігання або передачі. Для цього використовуються хеш-функції, цифрові підписи та механізми перевірки автентичності. Цей принцип дає змогу виявляти несанкціоновані зміни та запобігати пошкодженню даних.

Доступність означає, що авторизовані користувачі мають можливість отримати доступ до інформації в потрібний час. Для реалізації цього принципу застосовуються системи резервного копіювання, розподілені обчислювальні ресурси та технології відновлення після збоїв.

При побудові системи інформаційної безпеки необхідно вирішувати низку завдань (рис.2.16) . Перш за все, важливо ідентифікувати потенційні загрози та оцінити рівень ризиків, які вони несуть. Це включає аналіз джерел загроз, таких як кібератаки, людські помилки чи технічні збої, а також визначення критичності даних і систем, що потребують захисту.

Наступним етапом є розробка політик і процедур, які регламентують правила доступу до інформації та її використання. Важливим є впровадження технологій захисту, таких як шифрування, автентифікація та системи виявлення вторгнень.

Рис.2.16. Принципи побудови КСЗІ

Особлива увага приділяється навчанню персоналу, оскільки саме людський фактор часто стає причиною успішних атак. Формування культури інформаційної безпеки є одним із ключових завдань для кожної організації.

Моніторинг і аудит систем захисту дають змогу підтримувати їхню ефективність на належному рівні. Регулярні перевірки допомагають вчасно виявляти вразливості та усувати їх. Крім того, важливо мати чітко розроблені плани реагування на інциденти, що забезпечують оперативне усунення наслідків атак і швидке відновлення роботи систем.

Таким чином, мета побудови систем захисту інформації досягається завдяки комплексному підходу, що поєднує технологічні, організаційні та людські фактори. Саме комплексна система захисту інформації (КСЗІ) створює надійний фундамент для безпечного функціонування інформаційних ресурсів.

Багаторівневий захист.

Описуючи ключові принципи побудови комплексної системи захисту інформації (КСЗІ), важливо зазначити принцип багаторівневого захисту (Defense in Depth). Цей підхід передбачає створення системи безпеки з декількома взаємопов'язаними рівнями, кожен з яких спрямований на захист певного аспекту інфраструктури, забезпечуючи її комплексну стійкість (рис.2.17).

Рис. 2.17. Багаторівневий захист

Перший рівень стосується даних. Захист даних зосереджується на інформації, яка зберігається у базах даних, хмарних сховищах чи додатках. Використовуються методи шифрування, контроль доступу та резервне копіювання.

Захист застосунків передбачає створення програмного забезпечення з урахуванням безпеки, виявлення вразливостей та зберігання конфіденційних даних у захищених сховищах.

Третій рівень – захист обчислювальних ресурсів, при якому забезпечується безпечний доступ до серверів, захист кінцевих точок та регулярне оновлення систем.

Мережевий захист – це четвертий рівень, на якому обмежується небажаний трафік, встановлюється захищений зв'язок із локальними мережами, мінімізується ризик несанкціонованого доступу з інтернету.

П’ятий рівень — периметр. Для захисту від зовнішніх атак Використовуються міжмережеві екрани, системи протидії DDoS-атакам для виявлення та блокування зовнішніх загроз.

Управління ідентифікацією та доступом: Контролюється доступ до інфраструктури через багатофакторну автентифікацію, одноразові паролі та аудит змін у системі.

Останній, сьомий рівень — це фізична безпека. Вона забезпечується завдяки охорони будівель, обмеження доступу до серверів та захисту обладнання в дата-центрах.

Багаторівнева система забезпечує стійкість до різних загроз, враховує фізичні та кіберризики, і навіть при компрометації одного рівня зберігає загальну ефективність захисту (рис.2.18).

Рис.2.18 Ідеї та приинципи КСЗІ[25]

Принцип мінімальних привілеїв

Користувачі та процеси отримують доступ лише до тієї інформації, яка необхідна для виконання їхніх завдань. Це зменшує ризик випадкового або зловмисного доступу до чутливих даних.

Принцип розділення обов’язків

Завдання розподіляються між різними користувачами або системами, щоб уникнути зловживань або помилок. Наприклад, одні працівники мають доступ до конфіденційних даних, а інші – до систем управління.

Принцип безперервного моніторингу

Постійний контроль за роботою системи захисту інформації дає змогу виявляти та реагувати на потенційні загрози. Для цього використовуються системи аналізу журналів подій, виявлення аномалій та оцінки вразливостей.

Принцип криптографічного захисту

Використання сучасних алгоритмів шифрування є ключовим елементом захисту інформації. Такі алгоритми, як AES, RSA, і протоколи, як-от SSL/TLS, забезпечують безпеку даних навіть у разі їх перехоплення.

Для впровадження ефективної системи захисту інформації необхідно інтегрувати зазначені принципи у всі етапи розробки, впровадження та експлуатації інформаційних систем.

Таким чином, система захисту інформації забезпечує конфіденційність, цілісність і доступність даних через багаторівневий підхід, мінімізацію ризиків, розподіл обов'язків, криптографію та безперервний моніторинг.

[25] - https://encrypted-tbn0.gstatic.com/images?q=tbn:ANd9GcQEP4kgC0DtUz6_HPsWBH_XcE2gpdnaphGB1A&s

2.7. РИЗИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Ризики інформаційної безпеки — це невід'ємний аспект управління сучасними організаціями, особливо в умовах цифровізації та широкого використання інформаційних технологій (рис.2.19). Ризик у цьому контексті визначається як поєднання ймовірності та наслідків несприятливих подій, що можуть вплинути на інформаційні активи. Його аналіз та оцінка є ключовими етапами управління інформаційною безпекою.

Рис.2.19. Аналіз ризиків[26]

Основними характеристиками ризику є невизначеність, можливість збитків, необхідність аналізу та практичне значення події. Ці характеристики потребують особливого підходу до оцінки, яка може бути кількісною чи якісною. Кількісний підхід включає оцінювання ймовірності загрози, рівня уразливості та можливого розміру збитків. Якісний підхід базується на шкалах типу «низький», «середній» або «високий», що дає змогу здійснювати оцінку навіть без точних числових даних.

Ризики інформаційної безпеки поділяються на кілька типів, зокрема операційні, стратегічні, репутаційні та інформаційні. Вони можуть бути результатом як внутрішніх, так і зовнішніх загроз. Важливим інструментом їх аналізу є таблиця ризиків (Таблиця 3), яка включає опис загрози, рівень ймовірності її реалізації, можливі збитки та інтегральний показник ризику. За результатами такого аналізу визначаються пріоритети для зниження ризиків.

Таблиця 3. Таблиця ризиків

Загроза	Збиток	Ймовірність атаки	Ризик = Збиток *Ймовірність
Спам (переповнення поштової скриньки)	1	4	4
Фішингова атака	2	7	14
Випадкове форматування жорсткого диска	3	1	3
…	…	…	
Результат :			21

[26] - https://www.h-x.technology/wp-content/uploads/2024/02/Risk-management-1024x585.jpg

На етапі аналізу таблиці ризиків задаються деяким максимально допустимим ризиком. Спочатку перевіряється кожен рядок таблиці на не перевищення ризику допустимого рівня. Якщо таке перевищення має місце, значить, даний рядок – це одна з першочергових цілей розробки політики безпеки.

Особливу увагу приділяють класифікації ризиків на допустимі, які можна залишити без додаткових заходів, і неприпустимі, що потребують негайного реагування. Залишкові ризики, які залишаються після реалізації заходів, також враховуються (рис.2.20).

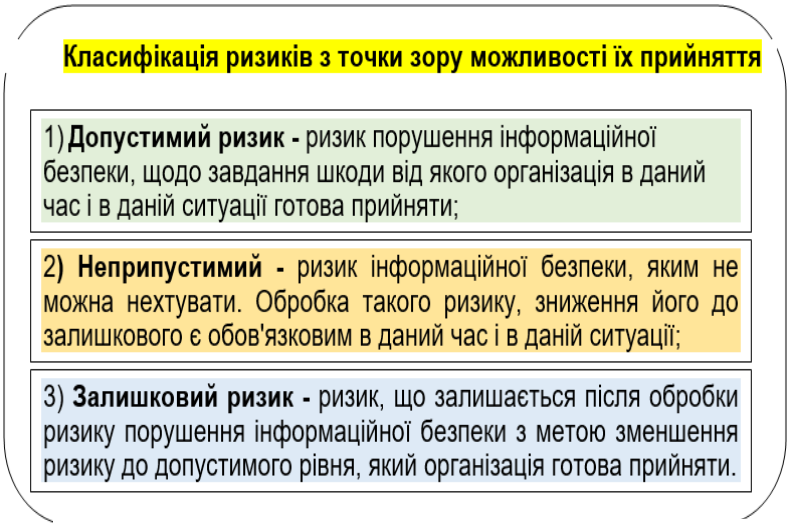


Рис.2.20. Класифікація ризиків

Ключовими міжнародними стандартами, які надають практичні рекомендації щодо управління ризиками є ISO 31000 та NIST SP 800-30. ISO 31000:2018 визначає принципи, основу та процеси для управління ризиками, акцентуючи увагу на інтеграції цього процесу в усі аспекти діяльності організації. Він надає узгоджений підхід до оцінки та мінімізації ризиків, що підходить для будь-якої сфери діяльності, зокрема інформаційної безпеки. У свою чергу, NIST (Національний інститут стандартів і технологій) пропонує специфічний підхід через NIST SP 800-30, який містить детальні інструкції з аналізу ризиків в інформаційних системах, фокусуючись на кіберзагрозах. Стандарт ISO/IEC 27005 надає рекомендації для менеджменту ризиками інформаційної безпеки організацій, особливо підтримує вимоги «Системи менеджменту інформаційної безпеки» (ISMS) згідно з ISO/IEC 27001.

Застосування цих стандартів дає змогу підвищити ефективність процесів управління ризиками, покращити захист і зміцнити довіру до організації.

Управління ризиками

Процес управління ризиками включає етапи ідентифікації, аналізу, оцінювання та обробки ризиків.

Управління ризиками інформаційної безпеки базується на системному підході, який включає не лише технічні, а й організаційні заходи. Це дає змогу забезпечити збереження конфіденційності, цілісності та доступності інформації, знижуючи при цьому можливі негативні наслідки для організації.

Сутність заходів з управління ризиками полягає в тому, щоб оцінити їх розмір, виробити ефективні і економічні заходи зниження ризиків, а потім переконатися, що ризики укладені в прийнятні рамки (і залишаються такими).

Управління ризиками включає в себе декілька видів діяльності, які чергуються циклічно. Основними з них є:

- **оцінка ризику (risk assessment)** – загальний процес ідентифікації ризику, аналізу ризику та оцінювання ризику;
- **обробка ризику (risk treatment)** – вибір економічно ефективних і заходів для нейтралізації ризиків.

Серед методів обробки виділяють зменшення ризику, ухилення від ризику, прийняття ризику або його передачу, наприклад, через страхування. Головна мета — знизити ризик до прийнятного рівня або усунути його.

Продемонструємо послідовність проведення основних процедур управління ризиками (рис. 2.21).

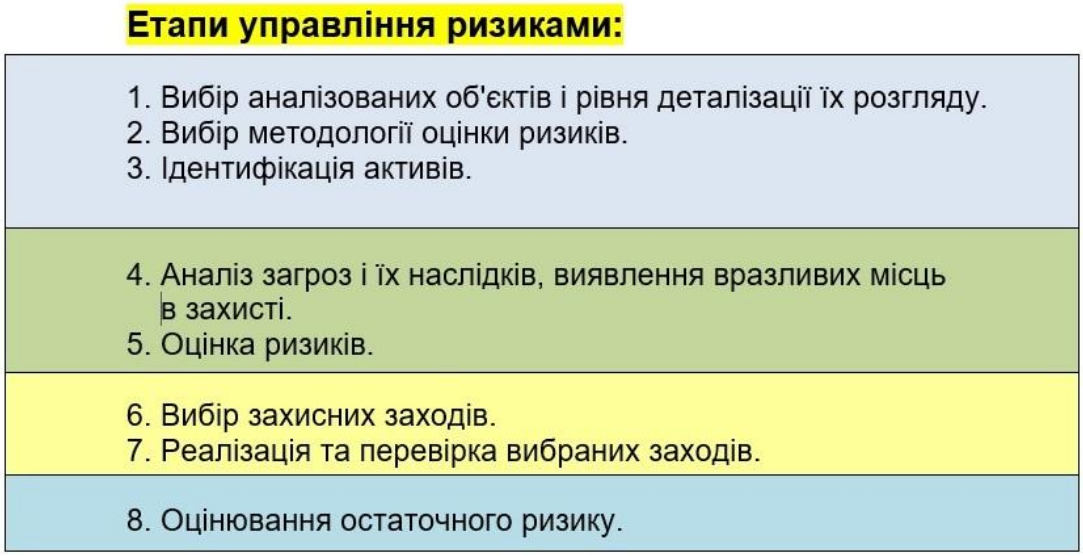


Рис. 2.21. Послідовність процедур в процесі управління ризиками

На підготовчому етапі визначають об’єкти аналізу й рівень деталізації. Для великих організацій аналіз зосереджується на критично важливих сервісах. Наступний крок — вибір методології оцінки ризиків. Ефективність заходів захисту порівнюється з прийнятними межами ризику та витратами на їх реалізацію. Для оцінки доцільно використовувати спрощені шкали, наприклад трибальні.

Третій етап – ідентифікація активів. Мається на увазі розробка карти інформаційної системи організації. Для ефективного управління ризиками така карта є важливою, оскільки вона дає чітке уявлення про сервіси, які були вибрані для аналізу, та про ті, якими довелося знехтувати. Якщо інформаційна система

змінюється, а карта постійно оновлюється, це дає змогу при перегляді ризиків одразу визначити, які сервіси потребують додаткового аналізу через значні зміни чи нововведення.

Важливо зазначити, що кожен елемент інформаційної системи може бути уразливим — від мережевого кабелю, який можуть пошкодити тварини, до баз даних, що можуть бути знищені через помилки адміністрування.

Зазвичай неможливо включити в аналіз всі деталі, тому вибирається певний рівень деталізації, залежно від потреб системи. Для нових систем бажано проводити більш детальний аналіз, а для старих, які зазнали незначних змін, можна обмежитись загальним оглядом.

При ідентифікації активів необхідно враховувати не лише компоненти інформаційної системи, але й інші ресурси, такі як інфраструктура, персонал та нематеріальні активи, наприклад, репутація організації. Ключовим є розуміння місії організації та основних напрямів діяльності, які потребують збереження за будь-яких обставин.

Одним з основних результатів процесу ідентифікації активів є створення детальної структури інформаційної інфраструктури організації та способів її використання. Мережа є основою для більшості організацій, тому до апаратних активів слід віднести комп'ютери (сервери, робочі станції, ПК), периферійні пристрої, інтерфейси, кабельну інфраструктуру та активне мережеве обладнання (мости, маршрутизатори та інші).

Програмні активи включають операційні системи (мережеві, серверні та клієнтські), прикладне програмне забезпечення, інструменти та засоби управління мережею і системами. Важливо вказати, де зберігається програмне забезпечення і як воно використовується в різних вузлах мережі.

До інформаційних активів відносяться також дані, що зберігаються, обробляються та передаються через мережу. Необхідно класифікувати дані за типами та рівнем конфіденційності, вказати місця їх зберігання і обробки, а також способи доступу до них. Це важливо для оцінки можливих наслідків порушень безпеки інформації.

Процес управління ризиками не є лінійним. Всі його етапи взаємопов'язані, і після завершення майже кожного етапу може виникнути потреба повернутись до попереднього. Наприклад, на етапі ідентифікації активів може бути виявлено, що межі аналізу слід розширити або підвищити рівень деталізації. Це особливо важливо на початкових етапах аналізу, коли повернення до початкових етапів є неминучим.

Аналіз загроз і їхніх наслідків, виявлення вразливих місць у захисті

Перший етап аналізу загроз полягає у їх виявленні. Важливо ретельно вибирати типи загроз, керуючись здоровим глуздом (наприклад, виключаючи

такі малоймовірні явища для нашого регіону, як цунамі, але включаючи можливість терористичних атак). Кожен вид загрози повинен бути максимально детально проаналізований.

Крім того, слід з'ясувати не тільки самі загрози, а й джерела їх виникнення, оскільки це дає змогу визначити додаткові заходи безпеки. Наприклад, несанкціонований доступ до системи може виникнути через неправомірне відтворення початкового діалогу, підбір пароля або підключення неавторизованого пристрою. Для кожного з цих способів слід застосовувати окремі засоби захисту, щоб уникнути загроз.

Після того, як загроза ідентифікована, потрібно оцінити ймовірність її здійснення. Одним з підходів є використання шкали ймовірності (низька, середня, висока), що дає змогу чітко визначити, наскільки ймовірне виникнення цієї загрози.

Окрім ймовірності, слід оцінити потенційний збиток від загрози. Наприклад, хоча пожежі трапляються рідко, їх наслідки можуть бути надзвичайно серйозними. Важливо також оцінювати збитки не лише з точки зору витрат на відновлення обладнання або інформації, але й з урахуванням довгострокових наслідків, таких як репутаційні втрати або втрата конкурентних позицій. Оцінка шкоди може включати потенційний вплив на бізнес-процеси та імідж компанії, а також втрати, що виникають від корупційних або шахрайських дій, як-от маніпулювання даними в бухгалтерії.

Вразливі місця в системах часто приваблюють не тільки зловмисників, а й співробітників, які можуть вдаватися до несанкціонованих дій з добрими намірами, але з певною мотивацією. Оцінка ймовірності загроз має враховувати не тільки статистичні дані, але й специфіку кожної конкретної організації. Це дає змогу більш точно визначити, де є найбільші ризики і де необхідно посилити захист.

Таким чином, для ефективного управління ризиками потрібно розглядати загрози в контексті конкретних умов організації, визначаючи їх потенційний вплив та ймовірність, а також виявляти вразливі місця, які можуть стати об'єктом як зовнішніх, так і внутрішніх загроз.

Оцінка ризиків

Після того, як зібрані вихідні дані та оцінено ступінь невизначеності, можна перейти до безпосередньої оцінки ризиків. Для цього можна застосувати простий підхід, наприклад, множення ймовірності на величину шкоди. Якщо для обох параметрів (ймовірності та збитку) використовувати трибальну шкалу, можливі значення оцінки будуть: 1, 2, 3, 4, 6 і 9. Таким чином, отримані результати можна класифікувати так: перші два значення вказують на низький рівень ризику, третє і четверте — на середній, а два останні — на високий рівень.

Згодом, можна привести ці результати до трьох рівнів оцінки ризиків. При оцінці прийнятності ризиків важливо ретельно розглядати випадки, коли отримане значення близьке до граничного. Це пов’язано з тим, що такі результати можуть бути наближеними, відповідно потребують додаткового аналізу для уникнення помилок при ухваленні рішень.

Якщо ризики виявляються неприпустимо високими, їх необхідно знижувати шляхом впровадження додаткових заходів захисту. Це може включати технічні, організаційні або фінансові заходи, які знижують ймовірність загрози або масштаби її наслідків у конкретних умовах організації.

Вибір захисних заходів

Зазвичай для усунення або зменшення вразливих місць в інформаційних системах, що роблять загрози реальними, існує декілька варіантів захисту, що відрізняються за ефективністю та вартістю. Наприклад, у разі високої ймовірності несанкціонованого доступу до системи можна ввести вимогу на складні паролі (не менше восьми символів), використовувати програму для генерації паролів або встановити інтегровану систему автентифікації, таку як система на основі смарт-карт. Якщо ймовірність умисного пошкодження серверів баз даних висока, можна встановити замки на двері серверної кімнати або навіть найняти охорону для кожного сервера.

Оцінюючи витрати на захисні заходи, важливо враховувати не лише вартість обладнання та програмного забезпечення, але й витрати на їх впровадження, зокрема навчання персоналу. Цю вартість також можна оцінити за три бальною шкалою і порівняти її з ризиком, що був обчислений раніше. Якщо заходи є економічно обґрунтованими, їх варто реалізувати, але навіть якщо витрати високі, не варто їх одразу відкидати — розрахунки можуть бути наближеними, і важливо враховувати специфіку ситуації.

Під час вибору механізмів захисту також варто врахувати можливість комбінування заходів для забезпечення захисту відразу кількох сервісів. Наприклад, у Массачусетському технологічному інституті захистили тисячі комп'ютерів через сервер автентифікації Kerberos, що дозволило знизити витрати і підвищити ефективність безпеки.

Не менш важливим аспектом є сумісність нових заходів з існуючою організаційною та технічною інфраструктурою. Заходи безпеки часто сприймаються як навантаження, і вони можуть викликати негативну реакцію серед співробітників. В таких випадках варто зберігати баланс між необхідністю забезпечення безпеки та підтриманням відкритості організаційної культури.

Існують ситуації, коли для нейтралізації ризику не існує ефективних або прийнятних за ціною заходів. Наприклад, компанії, що розташовані в сейсмічно активних зонах, можуть не мати змоги побудувати захищену будівлю. В такому

разі необхідно підвищити рівень прийнятного ризику і зосередити увагу на пом'якшенні наслідків. Наприклад, можна регулярно зберігати резервні копії даних у віддаленому місті та впроваджувати план відновлення після катастроф.

Контрзаходи — це спеціальні механізми чи дії, спрямовані на обмеження впливу потенційних загроз або вразливостей після початкової оцінки ризиків. Після застосування контрзаходів потрібно оцінити їх ефективність, щоб переконатися, що залишкові ризики стали прийнятними (Таблиця 4).

Таблиця 4. Ефективність контрзаходів

№	Ресурс	Первинний рівень ризику, %	Значення ризику після контрзаходів, %	Ефективність контрзаходів,%
1	Сервер головний	28.48	0.00	100.00
2	Сервер мультимедіа	24.40	5.51	77.43
3	Сервер БД	20.78	13.90	33.11
4	ПК каси	43.07	6.20	85.60
5	ПК відділу показів	25.45	9.86	61.25
6	Обладнання кінотеатру	53.51	7.27	86.42
7	ПК системного адміністратора	13.41	7.24	46.02
8	Управління кінопрокатом	92.68	40.83	55.94

У разі, якщо контрзаходи не забезпечують достатнього зниження ризику, слід здійснити коригування, застосовуючи додаткові заходи або інші альтернативні контрзаходи. Цей процес є циклічним і потребує постійного моніторингу для досягнення оптимального рівня захисту.

Реалізація та перевірка обраних заходів

Реалізація нових заходів захисту також потребує ретельного планування, включаючи фінансування, терміни навчання персоналу та, якщо йдеться про програмно-технічні механізми, розробку плану тестування (як автономного, так і комплексного). Це дозволить оцінити ефективність нових засобів до їх впровадження та забезпечити максимальну безпеку організації. Після прийняття заходів необхідно перевірити їх ефективність і впевнитися, що залишкові ризики відповідають допустимому рівню. Це можна зробития з застосуванням різних аналітичних методів, однак, достатньо застосовними є графічні способи аналізу ризиків (рис.2.22).

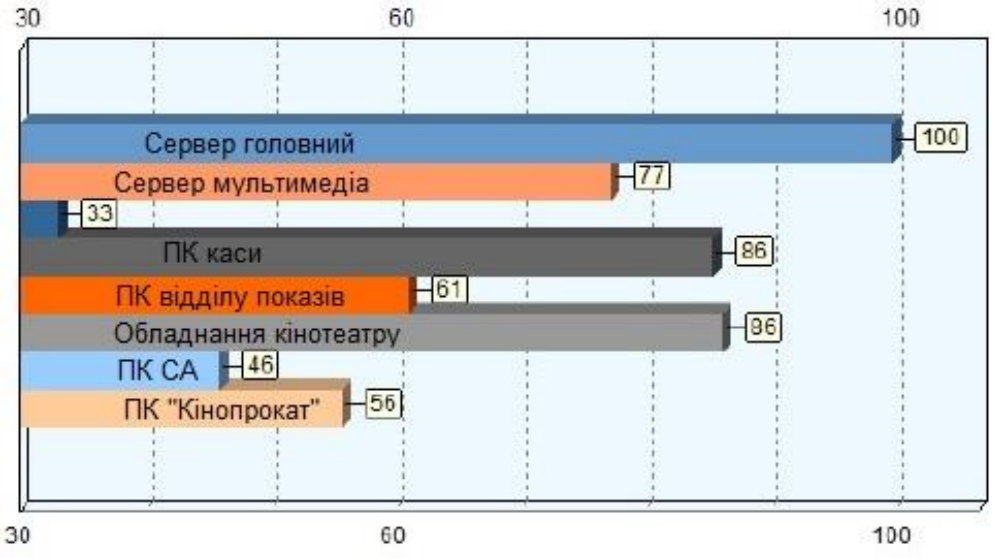


Рис.2.22. Графічний спосіб аналізу ризиків

Якщо це так, можна планувати наступну переоцінку, в іншому випадку слід виявити помилки та негайно провести повторний аналіз ризиків.

Оцінювання остаточного ризику

Оцінювання остаточного ризику є важливим етапом у процесі управління ризиками, що передбачає перевірку ефективності застосованих заходів захисту. Коли початково виявлені ризики виявляються надмірно високими, необхідно впровадити додаткові засоби для їх зниження, що може варіюватися за ефективністю та витратами. Після прийняття відповідних заходів слід оцінити залишкові ризики, щоб переконатися, що вони тепер перебувають на прийнятному рівні. Якщо ризики залишаються в межах норм, можна запланувати наступну переоцінку. Однак, якщо залишкові ризики все ще неприпустимі, потрібно провести повторний аналіз і коригування заходів захисту.

Цей процес включає постійну перевірку і корекцію стратегії управління ризиками, що гарантує постійну відповідність захисту реальним загрозам. Це дає змогу забезпечити високий рівень безпеки при врахуванні ресурсів організації, що витрачаються на захисні заходи, і мінливої обстановки, у якій вони застосовуються.

ВИСНОВКИ

Управління кібербезпекою охоплює кілька ключових аспектів, включаючи принципи захисту даних (конфіденційність, цілісність і доступність), політики й процедури забезпечення безпеки, а також важливість підвищення обізнаності користувачів.

Тріада КЦД забезпечує конфіденційність через методи шифрування і автентифікації, цілісність через хешування та перевірку достовірності, а доступність через резервування та відновлення.

Різні стани даних (зберігання, передача, обробка) потребують специфічних підходів до захисту, включаючи шифрування, автентифікацію, і виявлення помилок. Важливим етапом є оцінка ризиків, яка дає змогу визначити пріоритети для заходів захисту, зокрема через стандарти ISO 31000, NIST SP 800-30 та ISO/IEC 27005.

Ці стандарти допомагають підвищити ефективність управління ризиками, покращити захист інформаційних систем і зміцнити репутацію організацій. Крім того, системний підхід до управління ризиками дає змогу враховувати як технічні, так і організаційні заходи для підтримки високого рівня безпеки і адаптації до нових загроз.

ТЕРМІНИ І КОНЦЕПЦІЇ

Ця вправа призначена для того, щоб ви могли практикувати важливі терміни та концепції, викладені у цій темі.

1. ***ААО (AAA)***

– концепція контролю доступу, яка включає автентифікацію, авторизацію та облік користувачів.

2. ***Авторизація (Authorization)*** – визначення прав доступу користувачів до ресурсів і операцій, які вони можуть виконувати.

3. Автентифікація (Authentication)

– перевірка особи користувача за допомогою паролів, біометричних даних чи інших методів.

4. Багаторівневий захист (Defense in Depth)

– принцип створення кількох рівнів захисту для забезпечення стійкості інформаційної інфраструктури.

5. Багатофакторна автентифікація (Multifactor Authentication)

– перевірка особи за допомогою кількох методів, наприклад, пароля та відбитків пальців.

6. Брандмауер (Firewall)

– програмне чи апаратне забезпечення для контролю вхідного та вихідного трафіку в мережі.

7. Доступність (Availability)

– забезпечення постійного доступу до інформаційних систем і даних для авторизованих користувачів.

8. ISO/IEC 27001

– міжнародний стандарт для впровадження та керування системами інформаційної безпеки (ISMS).

9. Комплексна система інформаційної безпеки (КСІБ, Comprehensive Information Security System)

– багаторівнева система заходів, що забезпечує конфіденційність, цілісність і доступність інформації.

10. Конфіденційність (Confidentiality)

– запобігання несанкціонованому доступу до інформації, забезпечення приватності та захисту даних.

11. Контрзаходи (Countermeasures)

– технічні, організаційні або процедурні дії, спрямовані на зменшення ризиків або нейтралізацію загроз.

12. Куб кібербезпеки (Cybersecurity Cube)

– концепція, розроблена Джоном Мак-Камбером, що містить три виміри для забезпечення кібербезпеки: принципи інформаційної безпеки, стани даних і необхідні дії для захисту.

13. КЦД-тріада (CIA Triad)

– три основоположні принципи інформаційної безпеки: конфіденційність, цілісність і доступність.

14. Облік (Accounting)

– відстеження дій користувачів, зокрема доступу до ресурсів, змін даних і часу використання систем.

15. Політика безпеки (Security Policy)

– набір правил і процедур для забезпечення безпеки даних, систем і мереж організації.

16. Ризик (Risk)

– поєднання ймовірності та наслідків несприятливих подій, що можуть вплинути на інформаційні активи.

17. Система керування інформаційною безпекою (ISMS) – сукупність заходів і процесів для забезпечення захисту інформаційних активів організації.

18. Хешування (Hashing)

– процес перетворення даних у фіксовану довжину для забезпечення цілісності даних.

19. Хмарне сховище (Cloud Storage)

– віддалене зберігання даних у дата-центрах провайдерів із доступом через Інтернет.

20. Цілісність (Integrity)

– збереження точності, узгодженості та достовірності даних протягом усього життєвого циклу.

ПРАКТИЧНЕ ЗАВДАННЯ 2.1. ЩО БУЛО ЗРОБЛЕНО?

Цілі завдання

Знайти інформацію та прочитати про деякі нещодавні порушення безпеки.

Довідкова інформація / Сценарій

Порушення безпеки виникають, коли користувачі або програми-застосунки (applications) намагаються отримати несанкціонований доступ до даних, програм, служб або пристроїв. Під час цих порушень нападники, не залежно від того, чи є вони інсайдерами (людьми, які за службовим становищем мають доступ до конфіденційної інформації) чи ні, намагаються отримати інформацію, яку вони можуть використати для отримання фінансової вигоди або інших переваг. У цій роботі ви ознайомитесь з декількома інцидентами порушення безпеки, щоб визначити, що було зроблено, які експлойти було використано, і що ви можете зробити, щоб захистити себе.

Необхідні ресурси

ПК або мобільний пристрій з доступом до Інтернету

ХІД ВИКОНАННЯ

a) Використайте два надані посилання, в яких описано порушення безпеки у різних секторах, щоб заповнити таблицю нижче.

b) Знайдіть декілька (два) додаткових цікавих випадків порушень кібербезпеки та зазначте висновки у таблиці нижче.

Дослідження порушення безпеки

Дата інциденту	Постраждала організація	Кількість постраждалих/ Що було зроблено?	Які експлойти використовувалися? Яким чином налагоджено захист у вас?	Посилання на джерело
				Securityweek
				BBC

Дайте відповідь на запитання

Прочитавши про порушення безпеки, що ви можете зробити для запобігання подібним порушенням?

ПРАКТИЧНЕ ЗАВДАННЯ 2.2. ДВОФАКТОРНА АВТЕНТИФІКАЦІЯ

Цілі завдання

Ознайомитися з роботою двохфакторної авторизації.

Довідкова інформація/Сценарій

Двофакторна авторизація – це спосіб входу до акаунту, за якого потрібно **крім введення логіна та пароля** виконати певну додаткову дію, наприклад **ввести код**, отриманий:

- в СМС;
- на електронну пошту;
- в голосовому повідомлення.

Також, для дуже важливих акаунтів використовуються:

- унікальні зовнішні накопичувачі;
- зчитувачі біометричних даних.

Окремо варто виділити мобільні додатки, які використовуються сервісами для здійснення логування.

Необхідні ресурси

ПК з доступом до Інтернету.

ХІД ВИКОНАННЯ

Для переходу до налаштувань двофакторної авторизації просто клікніть по потрібному сервісу (звісно ж Ви маєте вже бути в ньому зареєстровані):

Мета-акаунти: Google, Apple, Microsoft

Соціальні мережі: Facebook, Twitter, LinkedIn, Instagram

Хмарні сховища: Dropbox

Задача 1

1. Налаштуйте двофаторну автентифікацію щонайменше для двох довільних сервісів. Усі кроки налаштування опишіть та відобразіть у звіті виконаня.

Задача 2.

2. Коротко опишіть принцип дії і мету роботи сторонніх додатків для двофакторної автентифікації (Authy, SAASPASS, Генератор кодів GOOGLE, Authenticator).

У висновку підсумуйте виконану роботу та важливість двохфакторної автентифікації

ТЕМА 3. АТАКИ, ПОНЯТТЯ ТА МЕТОДИ

Описано методи, які використовують експерти з кібербезпеки для аналізу наслідків кібератак. Розглянуто проблеми вразливості апаратного та програмного забезпечення, а також різні категорії вразливостей системи безпеки.

Обговорення різних типів зловмисного програмного забезпечення (malware – шкідливе ПЗ) та симптоми його присутності. Розглянуто різні способи, які використовуються хакерами для проникнення у систему, а також описано атаки відмови в обслуговуванні.

Більшість сучасних кібератак вважаються змішаними атаками. Змішані атаки використовують одразу кілька методів, щоб проникнути до системи і здійснити атаку. Коли атаці неможливо запобігти, завдання експерта з кібербезпеки полягає у зменшенні наслідків нападу.

3.1. ПОШУК ВРАЗЛИВОСТЕЙ В СИСТЕМІ БЕЗПЕКИ

Вразливості системи безпеки – це будь-які дефекти програмного або апаратного забезпечення. Після отримання інформації про вразливість, зловмисники намагаються її використати (рис.3.1). *Експлойт* – це термін, який вживають для опису програми, що написана для використання відомої вразливості. Використання експлойта для вразливості називається атакою. Мета атаки – отримати доступ до системи та розміщених на ній даних або до певного ресурсу.

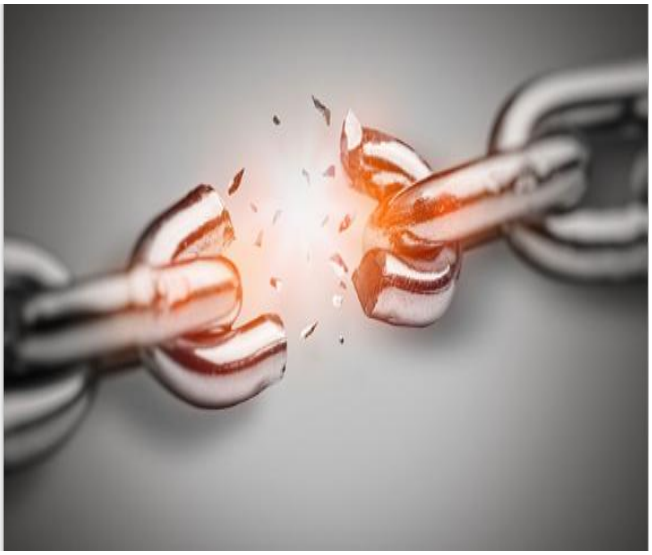


Рис. 3.1. Вразливість[27]

Вразливості програмного забезпечення

Вразливості програмного забезпечення зазвичай є наслідками помилок в коді операційної системи або коді застосунку. Незважаючи на всі зусилля компаній з пошуку та виправлення вразливих місць ПЗ, регулярно виявляються нові вразливості. Microsoft, Apple та інші виробники операційних систем випускають виправлення та оновлення майже щодня.

[27] – https://as1.ftcdn.net/v2/jpg/00/91/95/56/1000_F_91955660_zzg7dt615mnjHDdm1GdVwAzg97uUmX0c.jpg

Оновлення прикладних програм також є загальноприйнятою практикою.

Такі програми, як веббраузери, мобільні застосунки та вебсервери часто оновлюються компаніями та організаціями, які за них відповідають. Наприклад, Microsoft регулярно випускає оновлення для своїх операційних систем та програмного забезпечення, таких як Windows, що включають виправлення вразливостей, підтримку нових функцій та покращення безпеки.

У 2015 році в ОС Cisco IOS була виявлена суттєва вразливість під назвою SYNful Knock. Ця вразливість дозволяла хакерам отримати контроль над маршрутизаторами корпоративного класу, такими як застарілі моделі Cisco 1841, 2811 та 3825. Після чого зловмисники могли відстежувати всі сеанси передачі даних у мережі та заражати інші мережеві пристрої. Ця вразливість з'являлась у системі, після встановлення на маршрутизаторах модифікованої версії IOS. Щоб уникнути такої ситуації, завжди перевіряйте цілісність завантаженого образу IOS та надавайте фізичний доступ до обладнання тільки авторизованому персоналу.

Програмне забезпечення оновлюється з метою підтримки його актуального стану та запобігання використанню вразливостей. В деяких компаніях наявні групи для тестування проникнення, які спеціалізуються на пошуку та виправленні вразливостей ПЗ до того, як вони будуть використані зловмисниками. Сторонні дослідники у галузі безпеки також спеціалізуються на виявленні вразливостей ПЗ.

Проект Project Zero від Google є чудовим прикладом такої практики. Після виявлення кількох вразливостей у різному ПЗ, що використовується кінцевими користувачами, Google створив постійну команду для пошуку вразливостей програмного забезпечення.

Вразливості апаратного забезпечення

Вразливості апаратного забезпечення часто обумовлені недоліками його проектування. Наприклад оперативна пам'ять (RAM), за своєю суттю, є набором дуже близько розташованих один до одного конденсаторів. Було виявлено, що через конструктивні особливості постійні зміни в одному з цих конденсаторів можуть впливати на сусідні. На основі цього конструктивного недоліку було створено експлойт Rowhammer. Постійно перезаписуючи пам'ять за тими самими адресами, експлойт Rowhammer дає змогу змінювати значення даних у сусідніх комірках адресної пам'яті, навіть якщо вони захищені.

Вразливості апаратного забезпечення характерні для конкретних моделей пристроїв і зазвичай не використовуються під час випадкових спроб компрометації. Оскільки експлойти апаратного забезпечення характерні для цілеспрямованих атак, традиційні засоби захисту від зловмисного ПЗ та фізична безпека є достатніми для безпеки пересічного користувача.

3.2. КЛАСИФІКАЦІЯ ВРАЗЛИВОСТЕЙ СИСТЕМИ БЕЗПЕКИ

Більшість вразливостей програмного забезпечення належать до однієї з нижченаведених категорій (рис.3.2).

Переповнення буфера (Buffer overflow) – ця вразливість виникає, коли дані записуються за межами буфера. Буфери – це області пам'яті, виділені застосунку. Змінюючи дані за межами буфера, застосунок отримує доступ до пам'яті, яка була виділена для інших процесів, що може спричинити крах системи, компрометацію даних або отримання повноважень більш високого рівня.

Рис. 3.2. Зловмисний пошук[28]

Неперевірені вхідні дані (Non-validated input) – програми часто працюють з вхідними даними. Ці дані, що надходять до програми, можуть мати зловмисний вміст, який здатен спричинити непередбачену поведінку програми. Розглянемо програму, яка отримує зображення для обробки. Зловмисник може створити файл зображення із некоректними розмірами. Некоректні розміри можуть примусити програму виділити буфери неправильних розмірів.

Стан гонитви (Race conditions) – ця вразливість полягає в тому, що результат події залежить від того, в якій послідовності, або ж з якою тривалістю виконуються деякі окремі події. Стан гонитви стає джерелом вразливості, коли події, які потребують впорядкування або часової синхронізації, не відбуваються у правильному порядку або не вкладаються у належні часові межі.

Недоліки реалізації системи безпеки (Weaknesses in security practices) – системи та конфіденційні дані можуть бути захищені за допомогою таких методів, як автентифікація, авторизація та шифрування. Розробники не повинні намагатися створювати власні алгоритми безпеки, оскільки це, найпевніше, додасть вразливостей. Настійно рекомендується використовувати готові бібліотеки безпеки, які вже протестовані та перевірені.

Проблеми контролю доступу (Access-control problems) – контроль доступу – це процес, який визначає дозволи на певні дії. Він охоплює питання від управління фізичним доступом до обладнання, до визначення, хто має доступ до ресурсу, наприклад, файлу, і що він з ним може робити: читати чи змінювати. Багато вразливостей безпеки з'являється через неправильне використання засобів контролю доступу (рис. 3.3).

[28] – https://encrypted-tbn1.gstatic.com/images?q=tbn:ANd9GcT9_syhnjAzTkMmE5TG6IhjOEOdW-yKPFgfwsN0nrvrC2GAKLWq

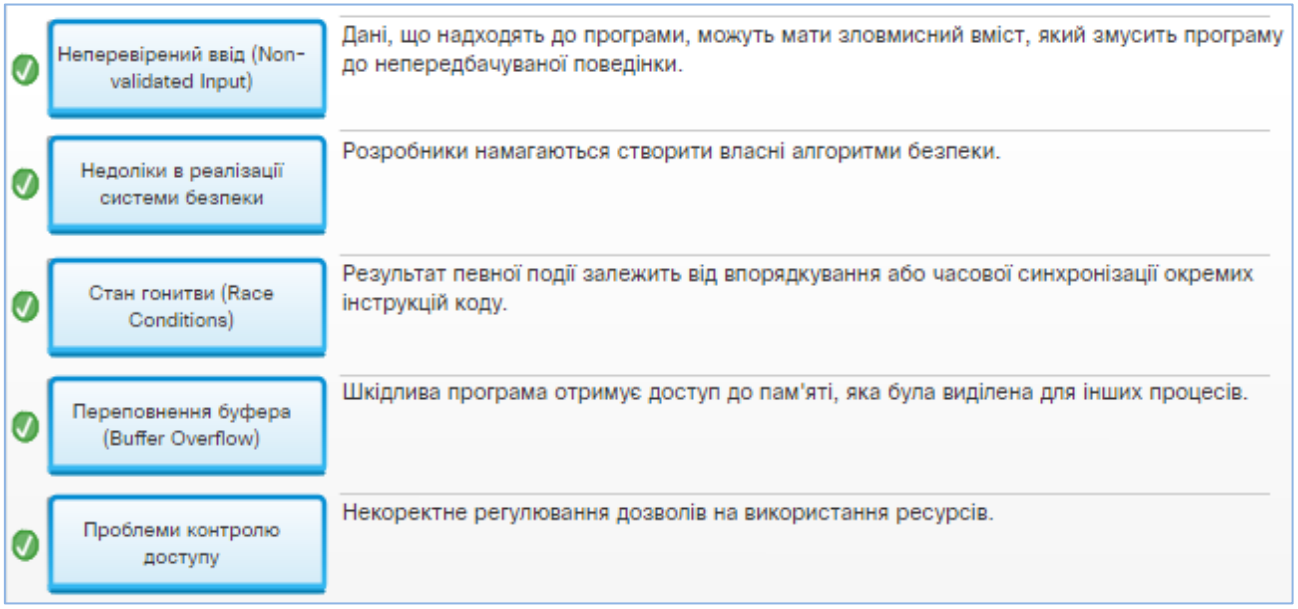


Рис. 3.3. Ідентифікація категорій вразливостей

Майже всі засоби контролю доступу та заходи безпеки можна обійти, якщо зловмисник має фізичний доступ до цільового обладнання. Наприклад, немає значення які дозволи ви встановили для файлу, ОС не може заборонити зловмиснику зчитати дані безпосередньо з диска в обхід операційної системи. Для захисту пристроїв та розміщених на них даних потрібно застосовувати обмеження фізичного доступу. Для захисту даних від крадіжки або пошкодження слід використовувати методи шифрування.

3.3. ТИПИ ЗЛОВМИСНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Зловмисне програмне забезпечення (Malicious Software) – це будь-який код, який може використовуватися для викрадання даних, обходу системи керування доступом, пошкодження або компрометації системи (рис.3.4). Нижче наведено кілька загальних типів зловмисного ПЗ.

Рис. 3.4. Атаки на системи[29]

Шпигунські програми (Spyware) – це зловмисне програмне забезпечення, призначене для стеження та шпигування за користувачем.

[29] - https://i.makeagif.com/media/7-05-2016/fPinQY.mp4

Намагаючись подолати заходи безпеки шпигунські програми часто змінюють налаштування безпеки. Шпигунські програми часто прив'язуються до легального програмного забезпечення або до троянських коней.

Рекламне ПЗ (Adware) – призначене для автоматичного поширення реклами. Рекламне ПЗ часто встановлюється разом з деякими версіями програмного забезпечення. Іноді рекламне ПЗ призначене лише для поширення реклами, але досить часто з ним поширюється шпигунське ПЗ.

Бот (Bot) – походить від слова robot, бот – це шкідлива програма, призначена для автоматичного виконання дій, зазвичай в Інтернеті. Хоча більшість ботів безпечні, зростання кількості зловмисних ботів призводить до створення бот-мереж (botnet). Певна кількість комп'ютерів інфікується ботами, які запрограмовані спокійно очікувати команди від зловмисника.

Програми-вимагачі (Ransomware) – це шкідливе ПЗ призначене для блокування комп'ютерної системи або розміщених на ній даних до моменту здійснення викупу. Такі програми зазвичай шифрують дані на комп'ютері за допомогою невідомого користувачу ключа. Деякі інші версії програм-вимагачів можуть для блокування системи використати її певні вразливості. Ransomware розповсюджується через завантажений файл або певну вразливість програмного забезпечення.

Псевдоантивірус (Scareware) – це тип шкідливого ПЗ, що переконує користувача виконати конкретну дію, використовуючи його страх. Scareware створює спливаючі вікна, схожі на діалогові вікна операційної системи. Ці вікна відображають підроблені повідомлення про те, що система перебуває під загрозою або необхідне виконання відповідної програми для повернення до нормальної роботи. Насправді жодних проблем на комп'ютері немає, і якщо користувач погоджується та дає змогу запустити зазначену програму, його система буде заражена шкідливим ПЗ.

Руткіт (Rootkit) – це зловмисне програмне забезпечення, призначене для змін в операційній системі з метою створення чорного ходу (backdoor). Після чого нападники використовують цей чорний хід для віддаленого доступу до комп'ютера. Більшість руткітів використовують вразливості ПЗ для підвищення привілеїв та модифікації системних файлів. Руткітам також притаманні зміни в системних інструментах експертизи та моніторингу, що дуже ускладнює виявлення цього зловмисного ПЗ. Часто для знищення руткіту необхідно повністю очистити ПК та перевстановити операційну систему.

Вірус (Virus) – це шкідливий виконуваний код, який прикріплюється до інших виконуваних файлів, часто легітимних програм. Більшість вірусів потребує активації з боку кінцевих користувачів і може справцьовувати у певний день або час. Віруси можуть бути нешкідливими і просто відображати рисунок або можуть мати руйнівні наслідки, такі, як зміна або видалення даних. Віруси

також можуть бути запрограмовані на мутацію для запобігання виявленню. На сьогодні більшість вірусів поширюється через USB-накопичувачі, оптичні диски, мережеві ресурси або електронною поштою.

Троянський кінь (Trojan horse) – це зловмисне ПЗ, яке здійснює шкідливі дії під виглядом бажаної операції. Цей шкідливий код використовує привілеї користувача, який його запускає. Часто трояни містяться в файлах зображень, аудіофайлах або іграх. Троянський кінь відрізняється від вірусу тим, що він приєднується до невиконуваних файлів.

Черв'яки або хробаки (Worms) – це шкідливий код, який клонує себе, самостійно використовуючи вразливості в мережах. Хробаки зазвичай уповільнюють роботу мереж. Якщо для активації вірусу необхідно запустити на виконання програму-носій, то хробаки можуть працювати самостійно. Участь користувача потрібна тільки під час первинного зараження. Після того, як хост заражений, хробак може швидко поширюватися мережею. Хробаки мають схожі шаблони поведінки. А саме, використовують вразливість системи, мають здатність до самостійного розповсюдження і виконання дій на користь зловмисника.

Хробаки є причиною деяких найбільш руйнівних атак в Інтернеті. Так, у 2001 році хробак Code Red інфікував 658 серверів й за 19 годин він інфікував понад 300 000 серверів.

Людина посередині (Man-In-The-Middle або MitM) – дає змогу зловмиснику контролювати потік даних між користувачами без їх відома. За допомогою такого рівня доступу зловмисник може перехоплювати, збирати та підмінювати інформацію користувача перш ніж предати її одержувачу. Атаки MitM широко використовуються для викрадення фінансової інформації. Існує безліч зловмисних програм та методик, які наділяють атакуючих можливостями MitM.

Посередник в мобільному телефоні (Man-In-The-Mobile або MitMo) – варіант атаки "Людина посередині", який використовується для отримання контролю над мобільним пристроєм. Заражений мобільний пристрій може отримати наказ зібрати конфіденційну інформацію користувача і відправити її нападникам. ZeuS, як приклад експлойта з можливостями MitMo, дає змогу атакуючим непомітно перехоплювати SMS-повідомлення, які надсилаються користувачам під час проведення 2-етапної перевірки.

3.4. СИМПТОМИ ЗАРАЖЕННЯ ШКІДЛИВИМ ПЗ

Незалежно від того, яким типом зловмисного ПЗ інфікована система, можна виділити найпоширеніші симптоми того, що пристрій заражено (рис.3.5):

– збільшується навантаження на центральний процесор;

– знижується швидкодія комп'ютера;

– комп'ютер часто зависає або дає збої;

– знижується швидкість перегляду вебсторінок;

– з'являються незрозумілі проблеми з мережевими з'єднаннями;

– файли модифікуються;

– файли видаляються;

– з'являються невідомі файли, програми або значки на робочому столі;

Рис. 3.5. Вірусний ефект[30]

– запускаються невідомі процеси;

– програми самостійно припиняють виконання або змінюють свої налаштування;

– електронна пошта надсилається без відома та згоди користувача.

Соціальна інженерія

Соціальна інженерія – це психологічна атака доступу, яка намагається маніпулювати особами з метою спонукання їх до виконання певних дій або розголошення конфіденційної інформації (рис.3.6). Соціальні інженери часто використовують бажання людей допомогти іншим, а також їхні слабкості. Наприклад, зловмисник може подзвонити уповноваженому працівнику з приводу нагальної проблеми, вирішення якої потребує негайного доступу до мережі. Зловмисник може розраховувати на марнославство співробітника, посилатися на авторитет або скористатися жадібністю працівника.

Рис. 3.6. Психологічна атака[31]

Розглянемо три основні види атак соціальної інженерії: ***Претекстінг, Тейлгейтінг, Послуга за послугу***

[30] – https://www.shutterstock.com/ru/image-illustration/mouth-germs-contagious-disease-transmitting-virus-314937239

[31] – https://www.shutterstock.com/ru/image-illustration/illustration-person-controlling-two-puppets-262913144

- ***Претекстінг (Pretexting)*** – атакуючий дзвонить особі і обманом намагається отримати доступ до привілейованих даних. Наприклад, зловмисник вимагає надати особисті або фінансові дані для підтвердження особи одержувача.
- ***Тейлгейтінг (Tailgating)*** – несанкціонований прохід за однією перепусткою. Це ситуація, коли зловмисник швидко прослизає через пункт контролю слідом за легальним працівником до зони, яка охороняється.
- ***Послуга за послугу (Quid pro quo)*** – це коли злочинець запитує особисту інформацію від учасника в обмін на щось, наприклад, безкоштовний подарунок.

Злам пароля від Wi-Fi

Злам пароля Wi-Fi – це процес пошуку пароля, який використовується для захисту бездротової мережі. Ось деякі методи, які використовуються, щоб зламати пароль.

Соціальна інженерія (Social engineering) – зловмисник маніпулює людиною, яка знає пароль, змушуючи розкрити його.

Атаки грубої сили (Brute-force attacks) – нападник перебирає велику кількість можливих комбінацій у спробі вгадати пароль. Наприклад, якщо пароль – це 4-значне число, зловмиснику доведеться перевірити кожну з 10 000 комбінацій. Атаки грубої сили зазвичай залучають файл зі списком слів. Цей текстовий файл містить список слів, узятих зі словника. Далі програма підставляє кожне слово та поширені комбінації. Атаки грубої сили потребують часу, тож процес вгадування складних паролів буде значно тривалішим (рис.3.7). До інструментів для зламу паролів через атаку грубої сили належать Ophcrack, L0phtCrack, THC Hydra, RainbowCrack і Medusa.

Рис. 3.7. Вплив атак[32]

Прослуховування мережі (Network sniffing) – під час прослуховування та захоплення пакетів зловмисник може виявити пароль, якщо він пересилається у незашифрованому (відкритому) вигляді. Якщо пароль зашифрований, зловмисник, як і раніше, може розкрити його, використовуючи інструмент для зламу паролів.

[32] - https://www.researchgate.net/profile/Md-Miah-107/publication/356918824/figure/fig6/AS:1099479348453379@1639147712554/Figure-Wi-Fi-password-cracking_W640.jpg

Фішинг

Фішинг, це коли зловмисник надсилає шахрайського електронного листа, який виглядає як повідомлення від легального надійного джерела. Мета цього повідомлення – змусити одержувача встановити зловмисне ПЗ на своєму пристрої або розкрити особисту чи фінансову інформацію (рис.3.8). Прикладом фішингу є підробка листів електронної пошти, які виглядають як повідомлення, надіслані роздрібним магазином з проханням до користувача натиснути на посиланні для участі у розігруванні призів. Посилання може переадресовувати на підроблений сайт, який запитує особисту інформацію, або може встановити вірус.

Рис. 3.8. Фішинг[33]

Спрямований фішинг – це цілеспрямована фішингова атака. Щоб дістатися жертв фішинг і спрямований фішинг використовують електронні листи, але спрямований фішинг націлений на конкретну особу. Переш ніж надіслати електронне повідомлення нападник вивчає інтереси жертви. Наприклад, зловмисник дізнався, що жертва цікавиться автомобілями і хоче купити конкретну модель. Зловмисник приєднується до того ж дискусійного автомобільного форуму, що і жертва, готує пропозицію продажу автомобіля і надсилає її жертві електронною поштою. Електронний лист містить посилання на фотографію автомобіля. Коли жертва натискає на посилання, шкідливе ПЗ встановлюється на її комп'ютер.

3.5. НЕСАНКЦІОНОВАНІ ПРОНИКНЕННЯ ТА АТАКИ

Використання вразливостей

Використання вразливостей – це ще один розповсюджений метод проникнення. Нападники сканують комп'ютери, щоб отримати інформацію про них. Нижче наведено загальний метод використання вразливостей:

Крок 1. Збір інформації про систему жертви. Це можна зробити багатьма різними способами, такими як сканування портів або застосування методів соціальної інженерії. Мета полягає в тому, щоб дізнатись якомога більше про комп'ютер жертви.

[33] - https://finclub.net/media/k2/items/cache/5b2fb447d366d17598f0ac6d22b4f284_XL.jpg

Крок 2. На кроці 2 зловмисник може дізнатися інформацію, як встановлена операційна система, її версія та перелік сервісів, які працюють на ній.

Крок 3. Коли операційна система та її версія відомі, атакуючий шукає будь-які специфічні вразливості, виявлені для цієї версії ОС або інших сервісів.

Крок 4. Коли виявлена вразливість, атакуючий шукає раніше написаний для неї експлойт. Якщо таких експлойтів не було створено, зловмисник може розглянути можливість його написання.

На рисунку 3.9 зображений зловмисник, який використовує загальнодоступну Інтернет-базу даних **Whois**, яка містить інформацію про доменні імена та їх реєстраторів.

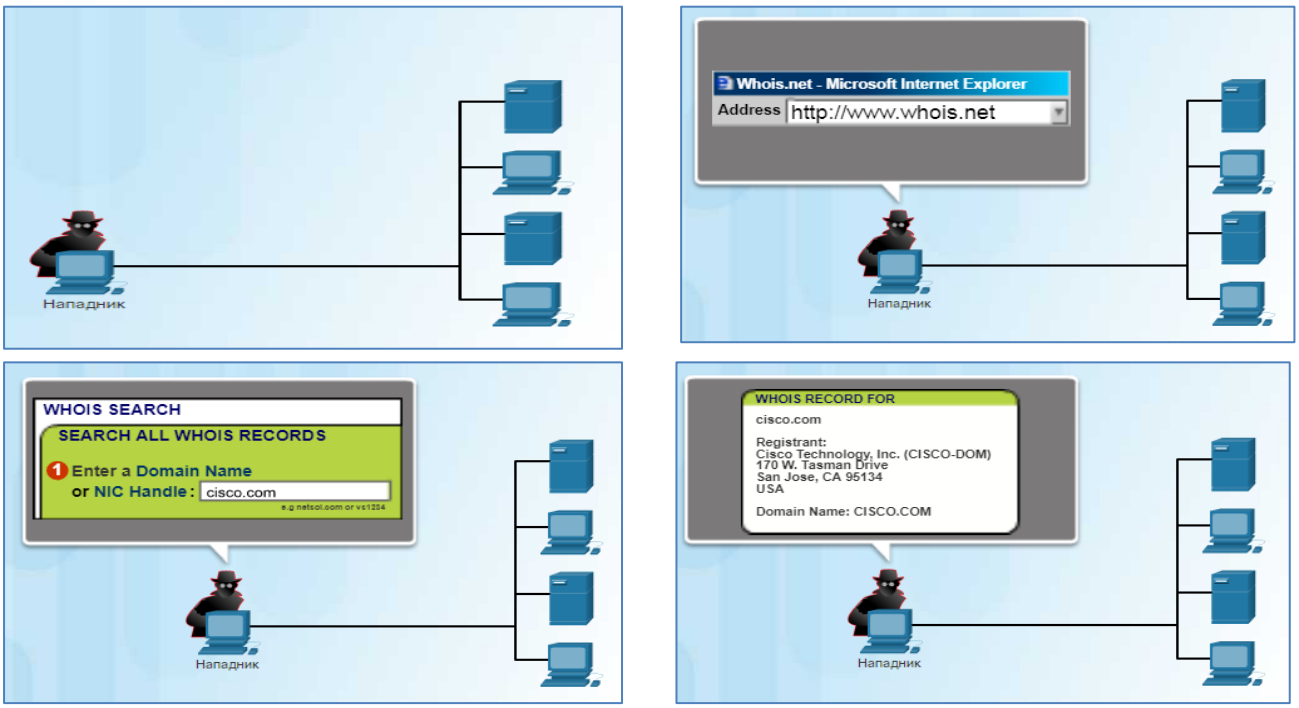


Рис. 3.9. Застосування зловмисником інструменту WHOIS[34]

На рисунку 3.10 зображений зловмисник, який застосовує інструмент **Nmap**, що є популярним сканером портів. За допомогою Nmap зловмисник може сканувати порти комп'ютера жертви, щоб дізнатись, які служби на ньому працюють. Інструмент Nmap є лише одним із багатьох доступних засобів для пошуку вразливостей у системах. Крім нього, зловмисники часто використовують спеціалізовані фреймворки, такі як Metasploit, які дають змогу автоматизувати процес виявлення та експлуатації вразливостей. Ці інструменти дають змогу не лише ідентифікувати відкриті порти чи працюючі служби, але й перевіряти їх на наявність відомих вразливостей, надаючи можливість швидко застосовувати відповідні експлойти.

[34] – This figure was uploaded by MD FOYSAL MIAH, https://www.researchgate.net/profile/Md-Miah-107

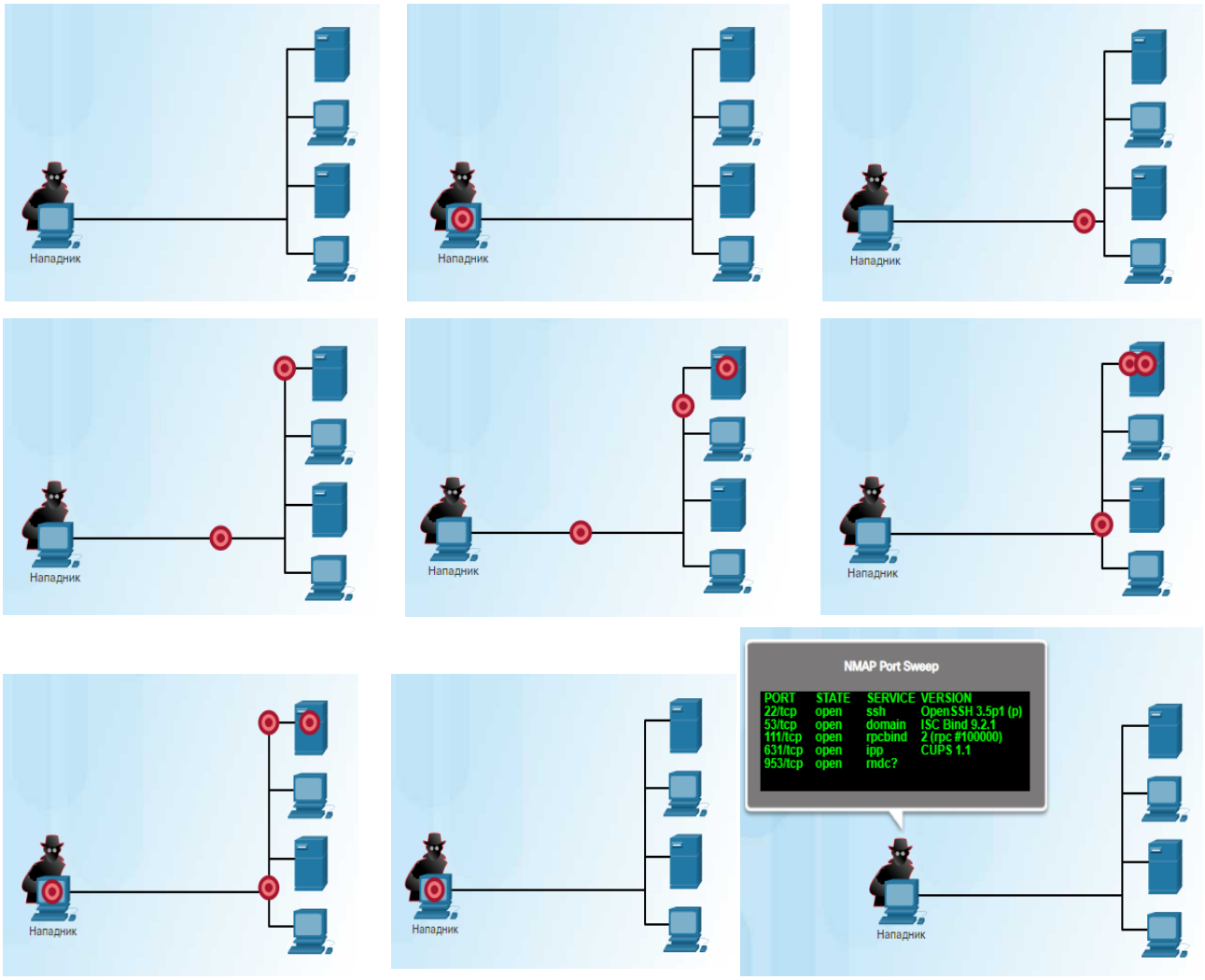


Рис. 3.10. Застосування зловмисником сканера портів NMAP[35]

Вдосконалені постійні загрози

Ще один зі способів проникнення – це вдосконалені постійні загрози (advanced persistent threats – APTs). Вони складаються з багатофазних, довготривалих, непомітних та складних дій, спрямованих на конкретну жертву. APT-атаки є складними і для їх виконання необхідні досвід та високий рівень кваліфікації нападника, тому вони зазвичай добре фінансуються. APT спрямовані на організації або країни з комерційних або політичних причин.

Метою APT є розгортання спеціального шкідливого програмного забезпечення на одній або кількох системах жертви. Зазвичай атаки пов’язані зі шпигунством в мережах та залишаються невиявленими. Через багатоетапне виконання та використання декількох типів налаштовуваних шкідливих програм, які впливають на різні пристрої та виконують визначені функції, окремий нападник часто не має навичок, ресурсів або наполегливості для виконання APT.

35 - This figure was uploaded by researchgate, https://www.researchgate.net/profile/Md-Miah-107

DoS атаки

Атака "Відмова в обслуговуванні" (DoS) – це тип мережевої атаки. Результатом DoS-атаки є переривання роботи мережевих сервісів для користувачів, пристроїв або застосунків. На рисунку 3.11 зображений процес перебігу DoS-атаки.

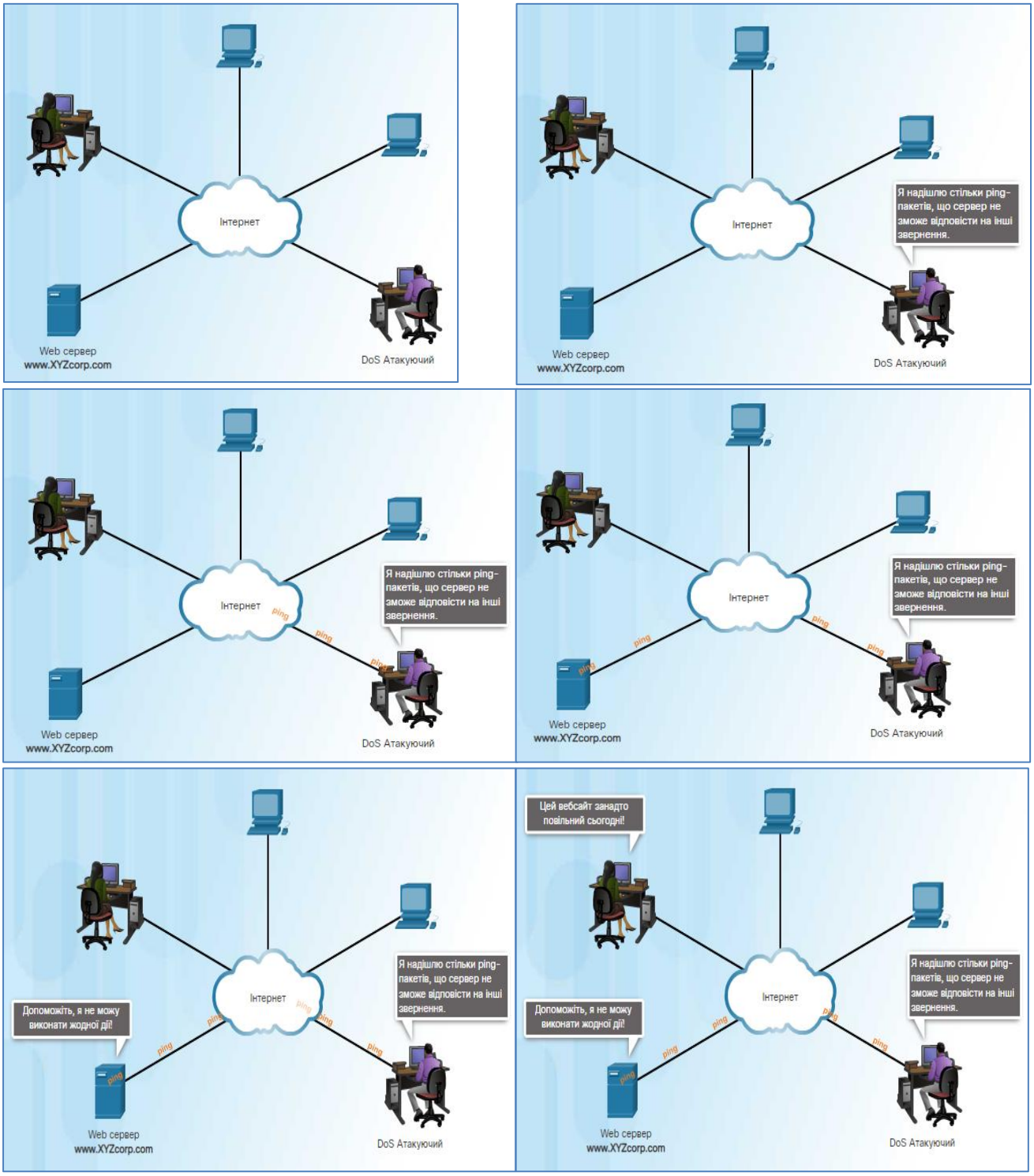


Рис. 3.11. DoS-атака на Web сервер[36]

[36] – This figure was uploaded by slideshare.net, https://www.slideshare.net/mohamedloey/computer-security-ccna-security-lecture-1

Розрізняють два основні типи DoS-атак:

Надмірна кількість даних (Overwhelming Quantity of Traffic) – це коли до мережі, хоста або програми надсилається величезна кількість даних з такою швидкістю, що вони не спроможні їх обробити. Це спричиняє затримку передачі чи відгуку, або відмову пристрою, аварійне завершення роботи сервісу.

Пакети зловмисного формату (Maliciously Formatted Packets) – це коли пакет зловмисного формату надсилається до хоста або програми і одержувач не здатен його обробити. Наприклад, зловмисник пересилає пакети, що містять помилки, які не можуть бути ідентифіковані програмою, або передає неправильно відформатовані пакети. Це може викликати сповільнення роботи або відмову пристрою-отримувача.

DoS атаки вважаються серйозною загрозою, оскільки вони можуть легко переривати зв’язок та викликати значну втрату часу та грошей. Ці атаки відносно прості для виконання навіть некваліфікованим нападником.

DDoS

Розподілена DDoS атака (Distributed DoS Attack, DDoS) подібна до атаки DoS, але вона походить від декількох скоординованих джерел (рис. 3.12).

Розподілена атака типу DDoS (Distributed Denial of Service) є масштабним і складним методом кібератак, при якому зловмисники використовують численні комп'ютери або інші пристрої для перевантаження серверів, мережевих ресурсів чи вебсайтів, щоб зробити їх недоступними для користувачів. Вона відрізняється від традиційної DoS-атаки тим, що атакуючі не використовують один комп'ютер для здійснення атаки, а замість цього задіюють мережу з численних заражених пристроїв, що часто називаються ботами. Ці пристрої можуть включати комп'ютери, маршрутизатори, мобільні пристрої, які заражені шкідливим програмним забезпеченням, наприклад, троянами.

Типова атака DDoS може включати кілька підвидів: атаки на рівні протоколів, атаки на рівні мережі, атаки на рівні додатків.

Один із відомих прикладів розподілених DDoS-атак — це **Mirai Botnet**, яка атакувала великі онлайн-платформи, використовуючи мільйони заражених пристроїв, таких як камери спостереження та маршрутизатори. Це було однією з найбільших розподілених атак за всю історію Інтернету.

Наприклад, атака DDoS може відбуватися таким чином:

1. Нападник створює мережу заражених хостів, яка називається ботнетом. Заражені хости називаються "зомбі". Їх контролюють системи керування.

2. Зомбі-комп’ютери постійно сканують і заражають нові хости, збільшуючи кількість "зомбі".

3. У призначений час, хакер наказує центрам керування розпочати DDoS-атаку за участі зомбі-ботнету.

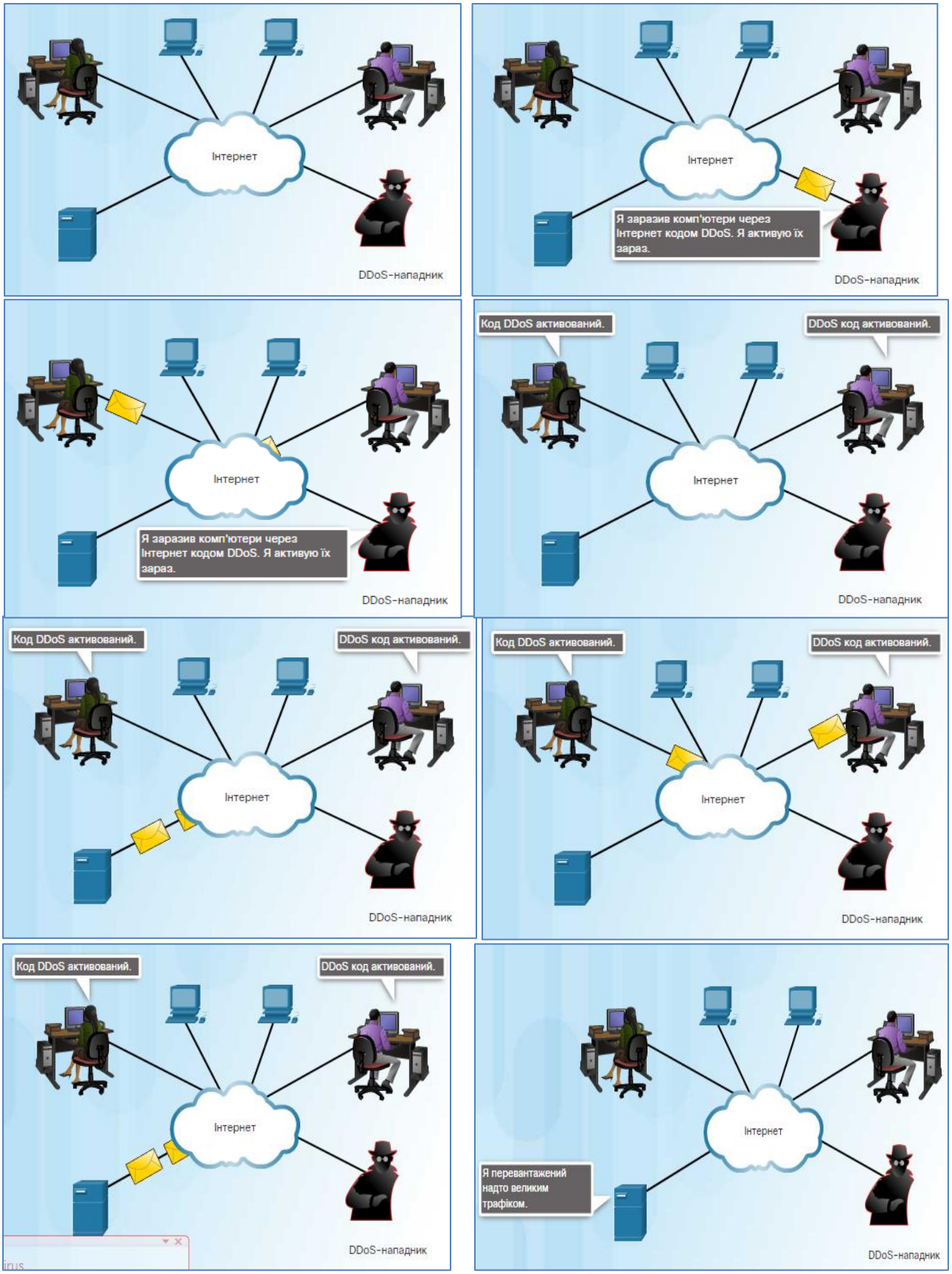


Рис. 3.12. Розподілена атака відмови в обслуговуванні DDoS-атака[37]

[37] – This figure was uploaded by slideshare.net, https://image.slidesharecdn.com/computersecurity-ccna-lecture1-180221222231/85/Computer-Security-CCNA-Security-Lecture-1-25-638.jpg

Отруєння SEO

Пошукові системи, такі як Google, працюють шляхом ранжування сторінок та надання релевантних результатів на основі пошукових запитів користувачів. Залежно від значимості вмісту вебсайту, він може відображатися вище або нижче в переліку результатів пошуку. Пошукова оптимізація (Search Engine Optimization, SEO) – це набір методів, що використовуються для покращення рейтингу вебсайту в пошуковій системі (рис.3.13). В той час як багато легальних компаній спеціалізуються на оптимізації вебсайтів з метою їх кращого позиціонування, зловмисник може використовувати SEO для того, щоб його шкідливий вебсайт відображався вище у результатах пошуку. Ця техніка називається "отруєння SEO".

Рис. 3.13. Отруєння SEO[38]

Характерні ознаки атак різного типу наведені в таблиці 5.Таблиця містить опис типів атак, таких як DoS (Denial of Service), DDoS (Distributed Denial of Service) та атаки, пов’язані з отруєнням SEO (Search Engine Optimization) й систематизує характеристики атак для їх розуміння та ідентифікації.

Таблиця 5. Ознаки атак[39]

Опис	DoS	DDoS	Отруєння SEO
Порівняно просто реалізувати, навіть для некваліфікованого нападника.	✓		
Походить від декількох скоординованих джерел.		✓	
"Зомбі" контролюються системами керування.		✓	
Зловмисно сформований пакет надсилається комп'ютеру або застосунку й одержувач не може його обробити.	✓		
Зловмисний веб-сайт піднімається в результатах пошуку.			✓
Збільшує трафік на зловмисні сайти, які можуть роздавати шкідливе ПЗ або здійснювати атаки соціальної інженерії.			✓
Нападник створює мережу заражених хостів, так звану ботнет.		✓	
Мережа, комп'ютер або програма надсилає величезну кількість даних зі швидкістю, з якою неможливо їх обробити.	✓		

[38] - https://psycab.com.ua/wp-content/uploads/2017/09/toksichny-e-lyudi.jpg

[39] – https://contenthub.netacad.com/legacy/I2CS/2.1/uk/index.html#2.1.5.4

Що таке змішані атаки?

Змішані атаки (Blended attacks) – це атаки, які використовують кілька методів для компрометації жертви. Використовуючи одразу декілька різних методів атаки (рис.3.15), зловмисники застосовують шкідливі програми, які є гібридом хробаків, троянських коней, шпигунських програм, клавіатурних шпигунів, спаму та фішингових схем. Тенденція змішаних атак схильна до використання більш складного зловмисного програмного забезпечення та створює великі ризики для користувачів.

Рис. 3.14. Змішані атаки[40]

Найпоширеніший тип змішаної атаки використовує спам-листи, миттєві повідомлення або легальні вебсайти для поширення посилань через які шкідливе або шпигунське програмне забезпечення непомітно завантажується на комп’ютер. Ще однією поширеною змішаною атакою є використання DDoS у поєднанні з фішинговими електронними листами. Спочатку DDoS-атака використовується для блокування вебсайту популярного банку та надсилання його клієнтам електронних листів з вибаченнями за незручності. Ці електронні листи також скеровують користувачів до підробленого "аварійного сайту", де їх інформація авторизації може бути викрадена.

Більшість з найнебезпечніших комп’ютерних черв’яків, таких як Nimbda, CodeRed, BugBear, Klez і Slammer, краще класифікувати як змішані атаки:

- Деякі різновиди Nimbda розповсюджувалися через вкладення в електронні листи; завантаження файлів зі скомпрометованого вебсервера та обмін файлами Microsoft (наприклад, через анонимні ресурси).
- Інші різновиди Nimbda змінювати привілеї гостьових облікових записів системи, надавали зловмиснику або шкідливому коду адміністративні права.

До змішаних атак також належать нещодавно створені черв’яки Conficker і ZeuS/LICAT. Conficker використовував всі традиційні методи розповсюдження.

Змішані атаки відрізняються високим рівнем складності через багатоступеневий підхід до ураження систем. Наприклад, черв'як Conficker не лише поширювався традиційними методами, такими як використання вразливостей у протоколах Windows або підключення до незахищених USB-накопичувачів, але й створював ботнети для здійснення подальших атак, зокрема DDoS чи крадіжки даних.

[40] - https://www.shutterstock.com/ru/image-illustration/security-concept-lock-on-digital-screen-315218069

Що таке зменшення наслідків?

Рис. 3.15. Наслідки[41]

Хоча більшість успішних компані сьогодні знають про спільні проблеми безпеки і докладають значних зусиль для їх запобігання, жоден комплекс заходів захисту не є на 100% ефективним. Якщо у зловмисників є можливість отримати значну вигоду, то злам, скоріш за все відбудеться, тож компанії та організації мають бути готові мінімізувати можливі збитки.

Важливо розуміти, що наслідки порушення безпеки стосуються не лише технічного аспекту, крадіжки даних, пошкоджених баз даних або порушення прав інтелектуальної власності, а також впливають на репутацію компанії. Реагувати на злам потрібно дуже динамічно.

Нижче наведені деякі важливі заходи, яких, на думку багатьох експертів з питань безпеки, компанія повинна вжити при виявленні зламу.

- Повідомте про проблему. Співробітники компанії мають бути поінформовані про проблему і закликані до дій. З зовнішніми клієнтами необхідно зв'язатися безпосередньо, а також потрібно зробити офіційне повідомлення. Це забезпечує прозорість, що має вирішальне значення в таких ситуаціях.
- Будьте щирими та визнайте свою відповідальність, якщо злам відбувся з вини компанії.
- Надайте детальну інформацію. Поясніть, чому ситуація відбулася і що конкретно було скомпрометовано. Очікується також, що компанія оплачує сервіси захисту від викрадання ідентифікаційних даних клієнтів.
- Зрозумійте, що стало причиною та сприяло зламу. Якщо необхідно, для дослідження та вивчення деталей найміть експертів-криміналістів.
- Застосуйте результати експертизи, щоб уникнути подібних порушень у майбутньому.
- Переконайтеся, що не було скомпрометовано щось інше, всі системи є вичищені і не було встановлено backdoors-закладок. Зловмисники часто намагаються залишити чорні ходи для полегшення майбутніх втручань. Переконайтеся, що цього не відбулось.

Навчіть співробітників, партнерів та клієнтів, як запобігти зламам у майбутньому.

[41]– https://stock.adobe.com/kz/search?k=broken%20wire%20fence

ВИСНОВКИ

Вразливості системи безпеки є однією з основних загроз для інформаційних технологій, оскільки дають змогу зловмисникам отримувати несанкціонований доступ до даних та ресурсів. Зрозуміння природи цих вразливостей, а також методів їх виявлення і виправлення, є критично важливим для забезпечення належного рівня захисту в сучасному цифровому середовищі.

У цій темі розглянуто способи, за допомогою яких фахівці з кібербезпеки аналізують наслідки кібератаки. Пояснено різні категорії вразливостей програмного та апаратного забезпечення та систем безпеки.

Обговорено різні типи зловмисного програмного забезпечення (відомого як malware) та їх симптоми. Розглянуто деякі типи шкідливих програм: вірус, хробак, троянський кінь, шпигунські програми, рекламне ПЗ та інші.

Наведено способи проникнення зловмисників до системи: соціальна інженерія, злам пароля Wi-Fi, фішинг та використання вразливостей. Також було пояснено різні типи атак відмови в обслуговуванні.

Змішані атаки використовують кілька методів для втручання та нападу на систему. Більшість з найнебезпечніших комп'ютерних черв'яків, таких як Nimbda, CodeRed, BugBear, Klez і Slammer класифікують як змішані атаки. Коли атаці неможливо запобігти, задача експерта з кібербезпеки полягає у зменшенні наслідків цього нападу.

ТЕРМІНИ І КОНЦЕПЦІЇ

Вправа призначена для того, щоб ви могли практикувати важливі терміни та концепції, які були викладені у темі.

1. Аналіз трафіку

- використання програмного забезпечення для захоплення пакетів у бездротовій мережі. Незашифровані паролі можуть бути захоплені і використані для атаки, а зашифровані паролі можуть бути зламані програмним інструментом.

2. Апаратні вразливості

- недоліки безпеки, викликані недоліками архітектури комп'ютерних пристроїв і компонентів. Зазвичай вони обмежені конкретними моделями пристроїв і часто використовуються для цілеспрямованих атак.

3. Атаки грубої сили (brute-force)

- використання програми для підбору пароля методом перебору усіх можливих комбінацій символів, що можуть бути використані для пароля, або списку слів, які часто використовуються у якості паролів. Складні паролі підібрати набагато важче.

4. Бот

- програмне забезпечення, яке виконує автоматизовані завдання через Інтернет. Можуть бути як корисними, так і шкідливими. Корисні боти використовуються для пошукових систем, наприклад. Шкідливі служать основою DDoS-атак.

5. Ботнет

- мережа розподілених заражених хостів, яка використовується для запуску DDoS-атаки.

6. Відмова в обслуговуванні (DoS)

- атака, яка перериває роботу мережевих служб для користувачів, пристроїв або додатків.

7. Використання вразливостей

- використання різних методів, включаючи програмні засоби або соціальну інженерію, для отримання інформації про систему. Зловмисник використовує цю інформацію для пошуку недоліків, що існують в цій конкретній системі.

8 Виправлення і оновлення системи безпеки

- випускаються виробниками операційних систем і додатків, щоб уникнути використання вразливостей.

9. Вірус

- злочинний виконуваний код, який може бути прикріплений до легальних програм. Віруси зазвичай потребують активації кінцевим користувачем і можуть бути відносно нешкідливими або дуже руйнівними. Вони часто поширюються за допомогою USB-накопичувачів, оптичних носіїв, мережевих ресурсів або електронної пошти.

10. Вразливість системи безпеки

- будь-який тип апаратного або програмного дефекту, який зловмисники намагаються використати.

11. ***DoS-атака (Denial of Service Attack)***

– кібератака, що перешкоджає доступу до інформаційних систем шляхом перевантаження сервера.

12. Експлойт

- програма, написана для використання відомої вразливості системи безпеки.

13. Зараження Системи Пошукової Оптимізації (SEO)

- маніпулювання ранжуванням зловмисного вебсайту з метою залучення користувачів на сайт, який поширює зловмисний код або використовує соціальну інженерію для збору конфіденційної інформації.

14. Злам пароля Wi-Fi

- виявлення пароля, який використовується для захисту бездротової мережі.

15. Зловмисні програми

- будь-який комп'ютерний код, який може використовуватися для крадіжки даних, обходу контролю доступу, шкоди або компрометації системи.

16. Зменшення впливу

- використання методів обмеження шкоди, викликаної успішною атакою. Ці методи включають способи передачі інформації про атаку співробітникам і клієнтам, розслідування атак і заходи для запобігання майбутнім атакам.

17. Змішана атака

- використання декількох методів для компрометації цілі.

18. Кібератака

- використання експлойта проти вразливості з метою зламу цільової системи.

19. Людина посередині (MitM)

- метод, в якому зловмисник може управляти пристроєм без відома власника. Зловмисник може перехоплювати і зберігати інформацію, яка проходить через його пристрій на шляху до іншого пункту призначення.

20. Man-in-the-mobile (MitMO)

- атака, яка є варіацією атаки Людина посередині. Мобільний пристрій заражається зловмисними програмами, які керують ним і змушують його пересилати конфіденційну інформацію зловмисникам.

21. Nmap

- популярний інструмент сканування портів, який можна використовувати для виявлення вразливостей в мережевих системах.

22. Неперевірене введення

- вразливість, при якій дані, надані програмі користувачем або експлойтом, змушують додаток поводитися не так, як очікувано.

23. Нездолання кількість даних

- атака DoS, в якій величезна кількість пакетів відправляється в мережу зі швидкістю, яку мережеві системи не можуть витримати. Це призводить до уповільнення мережевої передачі або відповіді, або збою пристрою або служби.

24. Пакети зловмисного формату

- використання пакетів даних, які були створені для порушення роботи мережевих пристроїв.

25. Переповнення буфера

- вразливість програмного забезпечення, яка виникає, коли дані записуються за межі областей пам’яті, виділених для програми. Ця вразливість може призвести до того, що додаток отримає доступ до пам’яті, яка виділена для інших процесів.

26. Проблеми з контролем доступу

- неналежне використання методів управління фізичним контролем обладнання, даних або додатків.

27. Претекстинг

- тип атаки соціальної інженерії, в якій людина обманює, щоб отримати доступ до привілейованої інформації.

28. Програми вимагачі

- тип зловмисного ПЗ, яке блокує комп’ютерну систему, часто, зашифровуючи основні дані, до тих пір, поки зловмисник не отримає викуп.

29. Програмні вразливості

- зазвичай викликані помилками в операційній системі або коді програми.

30. Project Zero

- створений Google приклад сторонньої постійної групи дослідників, яка займається пошуком програмних вразливостей.

31. Рекламні програми

- програмне забезпечення, яке автоматично показує рекламу. Деякі типи містять шпигунські програми.

32. Розвинута стійка загроза (APT)

- багатофазний, довгостроковий, прихований і просунутий напад на конкретну ціль. APT зазвичай націлені на організації або держави з метою отримання бізнесової чи політичної вигоди.

33. Розподілена відмова в обслуговуванні (DDoS)

- використання декількох розподілених систем для передачі даних, які порушують роботу служб, що надаються мережами і мережевими пристроями.

34. Руткіт

- зловмисне ПЗ, призначене для модифікації операційних систем, щоб дозволити несанкціонований віддалений доступ через чорний хід. Руткіти можуть змінювати призначені для користувача привілеї, системні файли і засоби моніторингу, що робить їх надзвичайно важкими для виявлення і видалення.

35. Соціальна інженерія

- спосіб отримати доступ до ресурсів, який маніпулює окремими особами для виконання дій або розголошення конфіденційної інформації. Атакуючі намагаються використовувати нашу готовність допомогти або наші слабкості.

36. Спрямований фішинг (spear phishing)

- націлена атака, в якій електронні листи, що виглядають як відправлені з легітимного джерела, налаштовуються спеціально для конкретних осіб. Зловмисник досліджує інтереси жертви, щоб створити електронний лист, який придатний для обману конкретної людини.

37. Стан гонитви

- вразливість, яка виникає, коли впорядкований за часом або встановлений порядок процесів порушений або змінений експлойтом.

38. Троян

- зловмисна програма, яка займається шкідливою діяльністю, імітуючи виконання бажаної користувачем функції. Вони включені в невиконувані файли, на відміну від вірусів, які виконуються.

39. Tailgating

- тип атаки соціальної інженерії, в якій зловмисник проникає за легальною особою через пропускний пункт.

40. Whois

- загальнодоступна база даних Інтернету, з інформацією про імена доменів в Інтернеті, людей або організації, які зареєстрували ці домени. Це джерело інформації можна використовувати для експлуатації вразливостей системи.

41. Фішинг

- використання шахрайського електронного листа, який виглядає, як відправлений надійним джерелом. Електронний лист обманом змушує людей встановлювати зловмисне ПЗ або поширювати конфіденційну інформацію.

42. Хробаки

- зловмисне ПЗ у вигляді шкідливого коду, який самостійно реплікується, використовуючи вразливості в мережах. Швидко поширюються мережею.

43. Шпигунське програмне забезпечення

- зловмисне ПЗ, призначене для відстеження дій користувачів і збору даних.

44. Щось за щось

- тип атаки соціальної інженерії, в якій зловмисник запитує особисту інформацію в обмін на щось, наприклад, безкоштовний подарунок.

ПРАКТИЧНЕ ЗАВДАННЯ 3.1. ПЕРЕХОПЛЕННЯ МЕРЕЖЕВИХ ПАКЕТІВ

Ціль завдання: перехоплення мережевих пакетів і їх розшифрування за допомогою програмного забезпечення wireshark та intercepter

Частина 1. Завантажте із сайту https://www.wireshark.org/ і встановіть програмне забезпечення Wireshark на комп'ютер або віртуальну машину.

Зверніть увагу, що після запуску програми Wireshark слід обрати активний інтерфейс для захоплення даних. В активному інтерфейсі будуть відображатися відомості про трафік (рис.3.16).

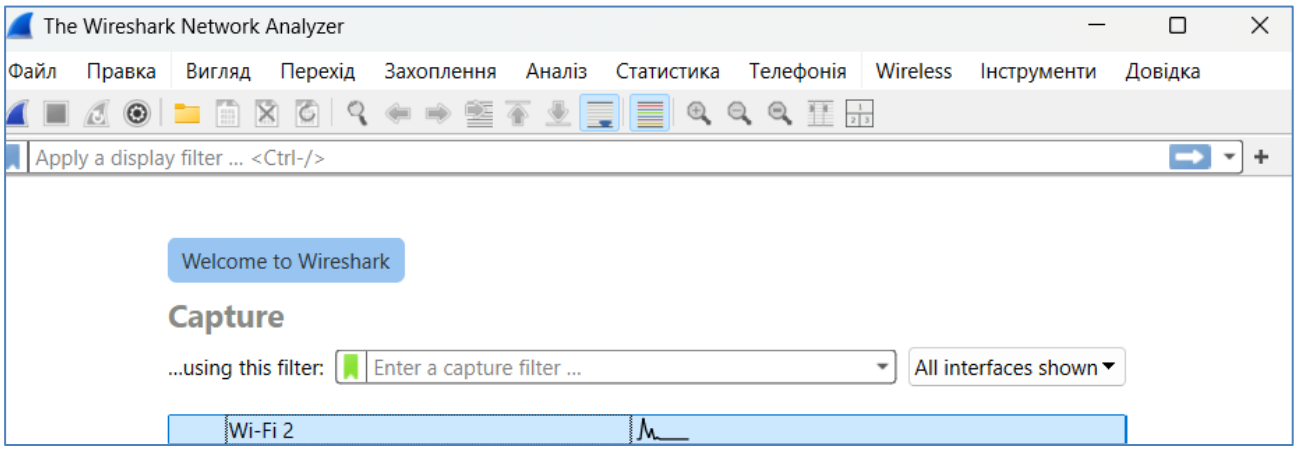


Рис.3.16. Перший екран Wireshark

Необхідним інструментом в подальшій роботі з пакетом є кнопки Start (Почати) та STOP, розміщені зліва у рядку піктографічного меню.

Натискання кнопки START сприяє початку захоплення пакетів. Після відкриття сторінки натискають STOP.

Ознайомтесь з інструкцією з роботи програми. Налаштуйте її для застосування на вашому ПК. Знайдіть незахищені сайти й отримайте логін і пароль від нах.

Частина 2. Завантажте, розархівуйте та встановіть програму Intercepter за посиланням https://github.com/intercepter-ng/mirror

Дослідіть усі доступні можливості програми та продемонструйте отримання логіна і пароля від незахищених сайтів (3-4 сайти).

У висновку до роботи опишіть можливості цих програм і проблеми захисту даних, які при цьому виникають, та дайте відповіді на питання:

1. Як уникнути перехоплення особистих даних?
2. Що означає захищений сайт?
3. Чим відрізняється протокол HTTP від HTTPS?
4. Що таке SSL і чим він відрізняється від TLS? Як він пов'язаний із HTT?

КОНТРОЛЬНА РОБОТА ДО ТЕМИ 3

Ця контрольна робота охоплює матеріал теми. Вона призначена для надання додаткових можливостей по практикувати навички та знання, подані у темі і підготовки до Іспиту.

1. Яке призначення руткітів?

– маскування під легальну програму

– отримання привілейованого доступу до пристрою, приховуючи власну присутність

– відтворення себе незалежно від будь-яких інших програм

– постачання реклами без згоди користувача

Пояснення

Шкідливе програмне забезпечення можна класифікувати таким чином:

– Вірус (самостійно розмножується шляхом приєднання до іншої програми або файлу);

– Хробак (Worm) (відтворюється незалежно від інших програм);

– Троянський кінь (маскується під легальний файл або програму);

– Руткіт (отримує привілейований доступ до пристрою, приховує себе);

– Шпигунське ПЗ (Spyware)(збирає інформацію з системи-жертви);

– Рекламна програма (Adware) (демонструє рекламу з дозволу чи без нього);

– Бот (чекає команд від хакера);

– Вимагач (Ransomware) (зупиняє комп'ютерну систему або дані, утримуючи їх у заручниках до отримання платежу).

отримання привілейованого доступу до пристрою, приховуючи власну присутність

2. Який інструмент використовується для надання списку відкритих портів на мережевих пристроях?

– Whois

– Ping

– Tracert

– Nmap

Пояснення

Інструмент Nmap – сканер портів, який використовується для визначення відкритих портів на певному мережевому пристрої. Сканер портів використовується перед початком атаки.

Nmap

3. Яка найпоширеніша мета інфікування пошукової оптимізації (search engine optimization (SEO)?

– переповнити мережевий пристрій шкідливо сформованими пакетами

– збільшити вебтрафік на шкідливі сайти

– побудувати ботнет зомбі

– Змусити когось інсталювати шкідливе програмне забезпечення або розкрити особисту інформацію

Пояснення

Користувач-зловмисник може створити SEO таким чином, щоб шкідливий вебсайт відображався вище в результатах пошуку. Шкідливий вебсайт зазвичай містить шкідливе програмне забезпечення або використовується для отримання інформації за допомогою методів соціальної інженерії.

збільшити вебтрафік на шкідливі сайти

4. Який з прикладів ілюструє спосіб приховання шкідливого програмного забезпечення?

– Електронний лист надсилається працівникам організації із вкладенням (attachment), яке виглядає як антивірусне оновлення, але фактично містить шпигунську програму.

– Ботнет зомбі передає хакеру особисту інформацію.

– Хакер використовує методики підвищення рейтингу вебсайту для перенаправлення користувачів на шкідливий сайт.

– Започатковано атаку проти публічного вебсайту інтернет-магазину з метою блокування відгуків на запити відвідувачів.

Пояснення

Вкладення електронної пошти, яке виглядає як легальне програмне забезпечення, але насправді містить шпигунську програму, демонструє спосіб приховання шкідливого програмного забезпечення. Напад з метою блокування доступу до вебсайту – це атака DoS. Хакер використовує отруєння пошукової оптимізації (search engine optimization (SEO)) для покращення рейтингу вебсайту, щоб користувачі спрямовувались до зловмисного сайту, на якому розміщено шкідливе програмне забезпечення або використовуються методи соціальної інженерії для отримання інформації. Ботнет зомбі-комп'ютерів використовується для запуску атаки DDoS.

Електронний лист надсилається працівникам організації із вкладенням (attachment), яке виглядає як антивірусне оновлення, але фактично містить шпигунську програму.

5. Яким чином в атаках використовуються зомбі?

– Це заражені машини, які проводять атаку DDoS.

– Вони досліджують групу машин з метою виявлення відкритих портів, щоб дізнатись, які служби працюють.

– Вони спрямовуються на конкретних людей задля отримання корпоративної або особистої інформації.

– Вони є зловмисно сформованими сегментами коду, які використовуються для заміни легітимних програм.

Пояснення

Зомбі – це заражені комп'ютери, які складають ботнет. Вони використовуються для розгортання розподіленої атаки відмови в обслуговуванні (DDoS).

Це заражені машини, які проводять атаку DDoS.

6. Який тип атаки дає змогу зловмиснику використовувати підхід грубої сили?

– відмова в обслуговуванні (denial of service)

– злам пароля (password cracking)

– прослуховування пакетів (packet sniffing)

– соціальна інженерія

Пояснення

Загальні способи, які використовуються для зламу паролів Wi-Fi, включають в себе соціальну інженерію, атаки грубої сили та прослуховування мережі.

злам пароля (password cracking)

ДОДАТКОВІ РЕСУРСИ ТА ЗАВДАННЯ

Піонер Google Hacking

Джонні Лонг вперше розробив концепцію Google Hacking. Відомий експерт з інформаційної безпеки, автор та співавтор багатьох книг з комп'ютерної безпеки. Його книгу *Google Hacking for Penetration Testers* (Злам за допомогою Google для білих хакерів) має прочитати кожен, хто зацікавлений сферою Google Hacking. Він також підтримує вебсайт, де надається підтримка некомерційним організаціям та проводиться навчання для найбідніших громадян світу.

http://www.hackersforcharity.org

Центр захисту Microsoft від зловмисних програм

Центр захисту Microsoft від зловмисних програм (Microsoft Malware Protection Center, MMPC) — це підрозділ компанії Microsoft, який спеціалізується на виявленні, аналізі, запобіганні та нейтралізації шкідливого програмного забезпечення. Центр забезпечує підтримку антивірусних і антималварних рішень Microsoft, таких як Microsoft Defender, а також займається розробкою нових методів захисту від сучасних кіберзагроз. Цей сайт Microsoft надає інструмент для пошуку інформації про конкретний тип зловмисних програм.

http://www.microsoft.com/security/portal/threat/threats.aspx

Зловмисне ПЗ

Статті, які детально висвітлюють історію та вплив зловмисного ПЗ Stuxnet. Britannica пропонує огляд його технічних характеристик, зокрема цілеспрямовану атаку на промислові системи Siemens SCADA, що контролювали іранські ядерні центрифуги, підкреслюючи значущість Stuxnet як першої кіберзброї у світі. IEEE Spectrum додає глибокий аналіз складності коду Stuxnet, відзначаючи використання чотирьох zero-day вразливостей і підтверджуючи, що його розробка, ймовірно, фінансувалася державами. Обидві статті висвітлюють політичний контекст створення Stuxnet і його революційний вплив на кібербезпеку:

https://www.britannica.com/technology/Stuxnet

https://spectrum.ieee.org/the-real-story-of-stuxnet

Зловмисна програма Flame

Stuxnet є однією з найбільш відомих зловмисних програм, розроблених для кібервійни. Однак існує багато інших, менш відомих загроз. У цій статті розглядається зловмисне ПЗ Flame, яке було розроблено як інструмент шпигунства за машинами, розташованими в основному в Ірані та інших країнах Близького Сходу. Щоб дізнатися більше про цю зловмисну програму, перейдіть за цим посиланням:

https://www.wired.com/2012/05/flame/

Каталог експлойтів NSA

Агентство національної безпеки США (National Security Agency, NSA) розробило і підтримує каталог експлойтів практично для всіх основних програмних, апаратних засобів і прошивок. Використовуючи ці інструменти та інші експлойти, NSA може відстежувати практично кожен рівень нашого цифрового життя. Щоб дізнатися більше про каталог експлойтів NSA, перейдіть за цим посиланням:

http://leaksource.wordpress.com/2013/12/30/nsas-ant-division-catalog-of-exploits-for-nearly-every-major-software-hardware-firmware/

Група швидкого реагування на комп'ютерні інциденти в США (US-CERT)

В рамках Департаменту національної безпеки США Група швидкого реагування на комп'ютерні інциденти (United States Computer Emergency Readiness Team, US-CERT) вирішує задачі визначення національної концепції кібербезпеки, обміну інформацією та керування ризиками кібербезпеки, захищаючи права американців. Щоб дізнатися більше про US-CERT, перейдіть за цим посиланням:

https://www.us-cert.gov/

Якщо ви хочете отримати подібну інформацію для конкретної країни, перейдіть за цим посиланням і знайдіть потрібну.

http://www.cert.org/incident-management/national-csirts/national-csirts.cfm

ТЕМА 4. ЗАХИСТ ДАНИХ І КОНФІДЕНЦІЙНІСТЬ

Тема присвячена персональним пристроям та особистим даним. Вона містить поради щодо захисту пристроїв, створення надійних паролів і безпечного використання бездротових мереж. Також розглядається питання безпечного збереження ваших даних.

Ваші дані в Інтернеті завжди мають певну цінність для кіберзлочинців. У цій темі коротко розглядаються методи автентифікації, які допоможуть безпечно зберігати ваші дані. Також описані способи посилення безпеки ваших онлайн-даних та правила поведінки в мережі Інтернет.

4.1. ЗАХИСТ ЦИФРОВИХ ПРИСТРОЇВ

Цифрові пристрої (рис.4.1) зберігають ваші дані та є порталом до вашого онлайн-життя. Нижче наведено короткий перелік кроків, які ви маєте зробити для захисту своїх комп'ютерних пристроїв від вторгнення

Рис.4.1. Цифрові пристрої[42]

Крок 1. Тримайте міжмережевий екран увімкненим – незалежно від того, чи це програмний брандмаурер, чи апаратний фаєрвол на маршрутизаторі, він має бути завжди увімкнений та періодично оновлюватися, щоб запобігти доступу хакерів до ваших особистих даних чи даних компанії. **Брандмауер** (Firewall) — це інструмент, що захищає ваш комп'ютер від небажаних або шкідливих мережевих з'єднань. Він контролює, які програми або пристрої можуть отримувати доступ до вашого комп'ютера через інтернет або локальну мережу. Наприклад, він може блокувати підозрілі програми, що намагаються передати дані без вашого дозволу.

Міжмережевий екран — це частина функціональності брандмауера, яка стежить за вхідними і вихідними з'єднаннями, аналізуючи мережеві пакети. Його основне завдання — фільтрувати трафік, дозволяючи лише безпечні підключення, щоб захистити пристрій від хакерських атак чи вірусів.

Разом вони забезпечують перший рівень безпеки в інтернеті, роблячи ваш пристрій менш вразливим до зовнішніх загроз.

[42] - https://www.istockphoto.com/ru/фото/гаджеты-включая-смартфон-smartwatch-цифровой-планшет-и-ноутбук-3d-рендеринг-gm480730837-37254408

Як увімкнути міжмережевий екран для Windows 10/11?

Відкрийте меню Пуск і перейдіть до Налаштування (Settings). Виберіть Безпека у Windows - перейдіть до розділу Мережа та Інтернет (Firewall & Network Protection). На цій сторінці відкрийте розділ БрандмауерWindows і переконайтеся, що міжмережевий екран увімкнений для всіх мережевих профілів: Мережі домену, Приватної мережі та Загальнодоступної мережі.

Для перевірки міжмережевого екрану у системі Windows перейдіть до **"Мережа та Інтернет" > Міжмережевий екран**, щоб перевірити статус.

Брандмауер Windows є базовим засобом захисту, що підходить для звичайних користувачів. Однак для розширеного захисту у складних мережах або проти просунутих загроз доцільно використовувати сторонні рішення або апаратні міжмережеві екрани.

Брандмауер в macOS Sonoma

Сучасними версіями macOS, які підтримуються Apple є **macOS Sonoma** (вийшла у 2023 році), **macOS Ventura** (випущена у 2022 році) та **macOS Monterey** (випущена у 2021 році). Apple більше не підтримує попередні версії, зокрема, macOS 10.5.1, тому вона вразлива до сучасних загроз безпеки.

У macOS Sonoma доступний **брандмауер додатків**, який дає змогу керувати мережевими підключеннями до вашого комп’ютера від інших пристроїв у мережі.

Цей брандмауер працює на рівні додатків, а не портів, що значно спрощує його налаштування. Він дає змогу блокувати небажані програми, запобігаючи їхньому доступу до відкритих портів, які використовуються для роботи авторизованих програм. Це забезпечує більш гнучкий і зручний контроль над мережевою безпекою вашого Mac, відповідаючи сучасним вимогам захисту.

Як увімкнути брандмауер в macOS Sonoma

1. **Відкрийте "Системні налаштування":**
   - Клацніть на значок **Apple** у верхньому лівому куті панелі меню.
   - Виберіть **"Системні налаштування" (System Settings)**.
2. **Перейдіть до розділу Безпека та конфіденційність:**
   - У списку знайдіть і виберіть **"Безпека та конфіденційність" (Security & Privacy)**.
3. **Перейдіть до вкладки Брандмауер:**
   - У вікні **"Безпека та конфіденційність"** натисніть на вкладку **"Брандмауер" (Firewall)**.
4. **Розблокуйте налаштування:**
   - Натисніть на значок **замка** у нижньому лівому куті.

- Введіть ім'я користувача та пароль адміністратора, щоб дозволити зміни.

5. **Увімкніть брандмауер:**
   - Натисніть кнопку **"Увімкнути брандмауер" (Turn On Firewall)**.
6. **Налаштуйте додаткові параметри (за необхідністю):**
   - Натисніть кнопку **"Параметри брандмауера" (Firewall Options)**, щоб налаштувати дозволи для конкретних додатків або активувати функцію **"Блокування всіх вхідних з'єднань" (Block all incoming connections)**.

Налаштування додаткових опцій:

1. **Дозвіл окремим додаткам:**
   - У вікні **"Параметри брандмауера",** натисніть "+", щоб додати потрібний додаток для дозволу мережевого доступу.
2. **Блокування всіх вхідних підключень:**
   - Активуйте опцію **"Блокувати всі вхідні з'єднання",** щоб заборонити будь-який доступ до комп'ютера ззовні.
3. **Дозвіл лише підписаним додаткам:**
   - Переконайтеся, що функція **"Дозволяти підписані програми"** увімкнена. Це дозволить лише надійним додаткам отримувати доступ до мережі.

Перевірка роботи брандмауера:

Після увімкнення можна перевірити, чи все працює, в розділі **"Системні налаштування" > "Безпека та конфіденційність" > "Брандмауер".**

Обмеження брандмауера

Брандмауер у macOS Sonoma підтримує сучасні функції керування з'єднаннями, включаючи протоколи TCP і UDP та режим Stealth для приховування пристрою. Старі протоколи, такі як AppleTalk, і технологія **ipfw** більше не є актуальними і були замінені новими підходами, такими як **pf**.

Крок 2. Використовуйте антивірусні та антишпигунські програми – зловмисне програмне забезпечення, таке як віруси, троянські коні, хробаки, програми-здирники та шпигунські програми, встановлюються на ваших комп'ютерних пристроях без вашого дозволу, щоб отримати доступ до вашого комп'ютера та даних. Віруси можуть знищити ваші дані, уповільнити роботу комп'ютера або взяти його під контроль. Яким чином віруси можуть використовувати ваш комп'ютер? Наприклад, можуть дозволити спамерам розсилати електронні листи через ваш обліковий запис. Шпигунське програмне забезпечення може контролювати ваші дії в Інтернеті, збирати вашу особисту інформацію або відкривати небажані спливаючі вікна з рекламою у вашому

веббраузері під час роботи в Інтернеті. Візьміть за правило завантажувати програмне забезпечення лише з надійних вебсайтів, щоб уникнути встановлення шпигунських програм. Антивірусне програмне забезпечення призначене для сканування комп'ютера та вхідної електронної пошти на наявність вірусів та їх видалення. Іноді антивірусне програмне забезпечення також містить антишпигунське ПЗ. Для захисту комп'ютера від найновіших шкідливих програм регулярно оновлюйте своє програмне забезпечення.

Крок 3. Керуйте операційною системою та веббраузером – хакери завжди намагаються скористатися вразливостями операційних систем та веббраузерів. Щоб убезпечити свій комп'ютер і дані, встановіть середній або високий рівень захисту на вашому комп'ютері та у веббраузері. Оновлюйте операційну систему, веббраузери, регулярно завантажуйте та встановлюйте останні виправлення програмного забезпеченн та оновлення системи безпеки від постачальників ПЗ.

Крок 4. Захищайте всі свої пристрої – ваші комп'ютерні пристрої, зокрема ПК, ноутбуки, планшети або смартфони, повинні бути захищені паролем для запобігання несанкціонованому доступу. Збережена на них інформація, а особливо важливі або конфіденційні дані, мають бути зашифровані. На мобільних пристроях зберігайте лише необхідну інформацію, з урахуванням того, що ці пристрої можуть бути вкрадені або втрачені, коли ви перебуваєте далеко від дому. Якщо будь-який з ваших пристроїв скомпрометовано, злочинці можуть отримати доступ до всіх ваших даних через постачальника послуг хмарного сховища, наприклад iCloud або Google Drive.

IoT-пристрої створюють ще більші ризики, ніж інші комп'ютерні пристрої. Якщо для настільних ПК, ноутбуків та мобільних платформ часто виходять і розсилаються оновлення програмного забезпечення, то більшість IoT-пристроїв мають тільки оригінальну прошивку (firmware). Якщо в прошивці будуть виявлені деякі недоліки, IoT-пристрій, ймовірно, залишатиметься вразливим. Проблему ускладнює і те, що IoT-пристрої часто передбачають зв'язок користувача з домом та потребують доступу до Інтернету. Щодо виходу в Інтернет, більшість виробників IoT-пристроїв покладаються на локальну мережу клієнта. В результаті IoT-пристрої можуть бути скомпрометовані з високим рівнем ймовірності і після цього дають змогу зловмисникам отримати доступ до локальної мережі та даних клієнта. Найкращий спосіб захиститися від такого сценарію – це використовувати для IoT-пристроїв ізольовану мережу, яку вони поділяють лише з іншими IoT-пристроями.

Існують спеціалізовані вебсканер для пошуку IoT-пристроїв та інших систем, підключених до Інтернету (рис.4.2). Наприклад, вебсканер **Shodan**

(https://www.shodan.io). Він сканує відкриті IP-адреси, порти й аналізує відповіді пристроїв, виявляючи такі об'єкти, як вебкамери, роутери, сервери, смарт-пристрої та промислові системи. Shodan використовується фахівцями з кібербезпеки для виявлення вразливостей, аналізу інфраструктури та перевірки рівня захисту, хоча він також може становити ризик, якщо потрапить до рук зловмисників. Цей інструмент допомагає оцінювати ризики в мережах і підвищувати безпеку IoT-систем.

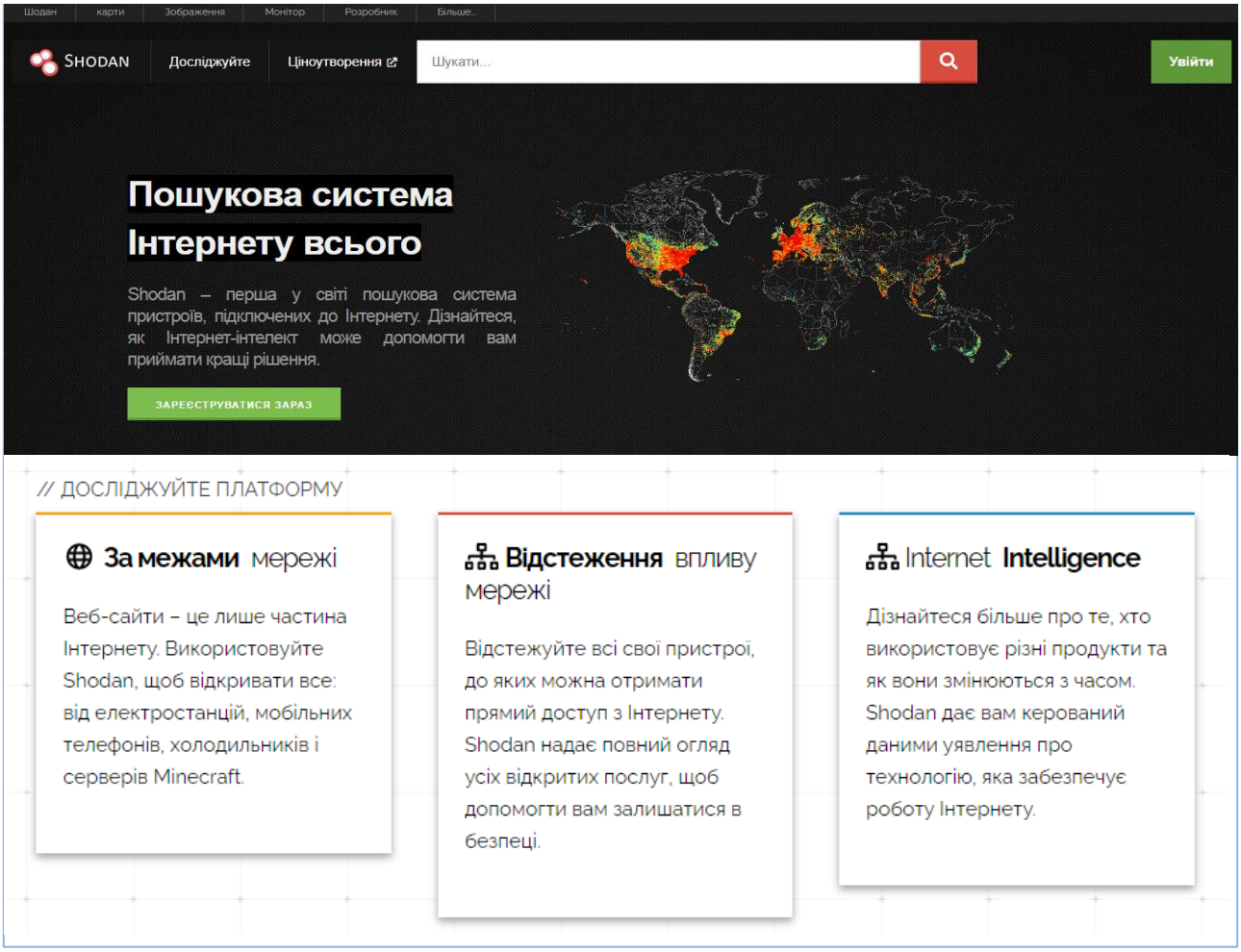


Рис.4.2. Вебсканер IoT-пристроїв Shodan

Крок 5. Використовуйте бездротові мережі безпечно

Бездротові мережі (рис.4.3) дають можливість пристроям з Wi-Fi-доступом, таким як ноутбуки і планшети, підключитися до мережі, використовуючи ідентифікатор мережі, відомий як Service Set Identifier (SSID). Щоб запобігти вторгненню до вашої домашньої бездротової мережі, потрібно змінити попередньо заданий SSID та пароль за замовчуванням для доступу до адміністративного вебінтерфейсу. Хакери в змозі знайти інформацію для доступу, задану за замовчуванням. Як варіант, можна вимкнути на бездротовому маршрутизаторі функцію широкомовного поширення SSID, що створить

Рис.4.3. Бездротове з’єднання[43]

додатковий бар’єр для виявлення мережі. Проте, цей підхід не вважається адекватним захистом бездротової мережі. Крім того, слід шифрувати бездротове з’єднання, активувавши бездротову безпеку та функцію шифрування WPA2 на бездротовому маршрутизаторі. Хоча при використанні шифрування WPA2, бездротова мережа може все ще залишатися вразливою.В жовтні 2017 у протоколі WPA2 було виявлено слабке місце у захисті. Цей недолік дає можливість нападникові зламувати шифрування між бездротовим маршрутизатором і клієнтом, втручатися у з’єднання і маніпулювати мережевим трафіком. Ця вразливість може використовуватися через атаку перевстановлення ключів (Key Reinstallation Attacks – KRACK). Це вплинуло на всі сучасні, захищені Wi-Fi мережі. Для зменшення впливу від атаки користувачу слід оновлювати усі продукти, що зазнали впливу: бездротові маршрутизатори і будь-які бездротові пристрої, такі як ноутбуки та мобільні пристрої, щойно з’явиться оновлення. Для ноутбуків та інших пристроїв з дротовою мережевою карткою, цю вразливість можна виправити завдяки кабельному з’єднанню. Крім того, можна також скористатися довіреною послугою VPN для запобігання неавторизованому доступу до даних при використанні бездротової мережі.

Перебуваючи за межами вашої домашньої мережі, публічні Wi-Fi точки доступу (hot spot) дають змогу отримувати доступ до вашої онлайн-інформації та мандрувати Інтернетом. Тим не менш, краще не підключитися і не надсилати будь-яку важливу особисту інформацію через загальнодоступну бездротову мережу. Перевірте, чи налаштований ваш комп’ютер на спільне використання файлів, і чи потрібна для цього автентифікація користувача та шифрування. Щоб запобігти перехопленню вашої інформації (так званого "прослуховування") під час використання публічної бездротової мережі, використовуйте VPN-тунелі та сервіси з послугою шифрування.

[43] - з сайтів https://www.bigstockphoto.com/ru/image-145500347/stock-photo-e-business-e-commerce-global-business-concept/ та https://depositphotos.com/ru/photos/bluetooth-speaker.html

VPN-сервіс надає безпечний доступ до Інтернету, використовуючи зашифрований зв’язок між вашим комп’ютером та VPN-сервісом на VPN-сервері провайдера.

При використанні зашифрованого VPN-тунелю, навіть в разі перехоплення, передані дані не піддлягають дешифруванню.

Поради щодо безпеки бездротових з’єднань і Bluetooth

Мережі Wi-Fi та Bluetooth-з’єднання можуть стати вразливими для крадіжки даних або несанкціонованого доступу. Проте дотримання простих рекомендацій допоможе зменшити ризики.

Перше. Шифрування – найефективніший спосіб захистити особисті дані. Воно працює шляхом перетворення інформації у формат, доступний лише для авторизованих одержувачів. Якщо адреса вебсайту, який ви відвідуєте, починається з **"https"** – це свідчить про зашифроване з’єднання між вашим браузером і сайтом. Й це надає вам гарантії безпеки.

Другою рекомендацією є використання сучасних протоколів безпеки, таких як **WPA3** або, як мінімум, **WPA2** для домашніх Wi-Fi мереж. Застарілі стандарти, такі як WEP, не забезпечують належного рівня захисту.

Bluetooth-з’єднання також може бути використане хакерами для перехоплення даних, встановлення шкідливого ПЗ або отримання віддаленого доступу. Щоб мінімізувати ці ризики, слід вимикати Bluetooth, якщо ви ним не користуєтеся, встановити режим "Невидимий" (Invisible), щоб запобігти несанкціонованим спробам підключення й, безумовно, регулярно оновлювати прошивку пристроїв для усунення відомих вразливостей.

Дотримання цих простих правил забезпечить захист вашої інформації під час використання бездротових технологій.

Громадський доступ до Wi-Fi

Багато користувачів Wi-Fi вирішують використовувати загальнодоступні мережі замість тарифних планів даних своїх пристроїв для віддаленого доступу до Інтернету. Але зручність загальнодоступного Wi-Fi може бути ризикованою. Якщо ви не будете обережні, хакери можуть швидко отримати доступ до вашого з’єднання та зламати конфіденційну інформацію, що зберігається на вашому пристрої та в онлайн-облікових записах. Наведемо кілька кроків, які можна зробити, щоб мінімізувати ризик.

- Перевірте дійсність доступних точок доступу Wi-Fi. Якщо з’являється кілька точок доступу, які стверджують, що належать до закладу, у якому ви перебуваєте, зверніться до персоналу, щоб уникнути підключення до шахрайської точки доступу.

- Переконайтеся, що всі вебсайти, з якими ви обмінюєтеся інформацією, мають "https" на початку вебадреси. Якщо так, ваші передані дані будуть зашифровані.
- Встановіть додаток додатка, який змушує ваші вебпереглядачі використовувати шифрування під час підключення до вебсайтів – навіть відомих сайтів, які зазвичай не шифрують свої повідомлення.
- Відрегулюйте налаштування свого смартфона, щоб він не підключався автоматично до найближчих мереж Wi-Fi. Це дає вам більше контролю над тим, де і коли ви підключаєтеся.
- Якщо ви регулярно використовуєте загальнодоступні точки доступу Wi-Fi, подумайте про використання віртуальної приватної мережі, яка шифруватиме всі передачі між вашим пристроєм та Інтернетом. Багато компаній пропонують своїм співробітникам VPN для робочих цілей, а окремі особи можуть підписатися на VPN самостійно.
- Під час передачі конфіденційної інформації використання тарифного плану мобільного телефона замість Wi-Fi може бути більш безпечним.

Багато мобільних пристроїв, наприклад смартфони та планшети, підтримують бездротовий протокол Bluetooth. Ця можливість дає змогу пристроям з підтримкою Bluetooth підключитися один до одного для обміну інформацією. На жаль, Bluetooth можуть використовувати хакери з метою прослуховування пристроїв, встановлення віддаленого контролю доступу, поширення шкідливого ПЗ та виснаження акумуляторів. Щоб уникнути цих проблем, вимикайте Bluetooth, коли ви ним не користуєтесь.

Використовуйте унікальні паролі для кожного облікового запису в мережі

Ви, напевно, маєте більше ніж один обліковий запис в Інтернеті, і для кожного з них слід використовувати унікальний пароль. Отож, доводиться пам’ятати багато паролів. Проте, нехтування правилом використання сильних та унікальних паролів залишає вас і ваші дані вразливими для кіберзлочинців (рис. 4.4). Використання однакового пароля для усіх облікових записів в Інтернеті – це те саме, що й використання одного ключа для замикання усіх дверей. Якщо зловмиснику вдасться отримати ваш ключ, він зможе дістатися до всього,

Нормальний	Хороший	Ефективний
allwhitecat	a11whitecat	A11whi7ec@t
Fblogin	1FBLogin	1.FB.L0gin$
amazonpass	AmazonPa55	Am@z0nPa55
ilikemyschool	ILikeMySchool	!Lik3MySch00l
Hightidenow	HighTideNow	H1gh7id3Now

Рис.4.4. Приклади паролів

чим ви володієте. Наприклад, якщо злочинці отримають ваш пароль через фішингову атаку, вони намагатимуться потрапити до інших ваших облікових записів в Інтернеті. Якщо ви використовуєте один пароль для всіх облікових записів, вони можуть отримати доступ до них усіх, поцупити або видалити всі ваші дані, або видавати себе за вас.

Ми використовуємо велику кількість облікових записів, для яких потрібен пароль, тож цю інформацію важко запам'ятати. Одним із способів уникнення повторного використання паролів або вибору слабких паролів є встановлення менеджера паролів. Менеджер паролів зберігає та шифрує всі ваші різні та складні паролі. Він може допомогти вам автоматично входити до облікових записів в Інтернеті. Вам потрібно лише пам'ятати ваш майстер-пароль, щоб отримати доступ до менеджера паролів і керувати всіма вашими обліковими записами та паролями.

Поради щодо правильного вибору пароля

1) Не використовуйте слова зі словника або імена будь-якою мовою.
2) Не використовуйте слова з орфографічними помилками.
3) Не використовуйте імена комп'ютерів або імена облікових записів.
4) Якщо це можливо, використовуйте спеціальні символи, такі як ! @ # $ % ^ & * ( )
5) Використовуйте пароль з десяти або більше символів.

Віддавайте перевагу парольній фразі, а не звичайному пароля

Щоб запобігти несанкціонованому фізичному доступу до ваших комп'ютерних пристроїв, надавайте перевагу парольним фразам над простими паролями. Створити довгу парольну фразу, простіше ніж пароль, оскільки вона зазвичай має форму речення, а не окремого слова. Більша довжина робить парольні фрази менш вразливими до атак перебору за словником, або атак грубої сили. Крім того, парольну фразу легше запам'ятати, особливо коли потрібно часто змінювати пароль. Надамо кілька порад для вибору надійних паролів або парольних фраз (рис. 4.5).

Поради для вибору надійної парольної фрази:

- вибирайте значуще для вас речення.
- додайте спеціальні символи, такі як ! @ # $ % ^ & * ( )
- чим фраза довша, тим краще.
- уникайте загальновідомих або популярних висловлювань, наприклад, текстів із відомої пісні.

У Додатку 2 ви знайдете детальні поради щодо захисту паролів, які є одним із ключових засобів доступу до ваших даних.

Нещодавно, Національний інститут стандартів і технологій (National Institute for Standards and Technology, NIST) Сполучених Штатів опублікував удосконалені вимоги до паролів.

Нормальна	Thisismypassphrase.
Хороша	Acatthatlovesdogs.
Ефективна	Acat th@tlov3sd0gs.

Рис. 4.5. Створення надійної парольної фрази

Стандарти NIST призначені для державного застосування, проте можуть також слугувати стандартом для інших. Нові рекомендації мають на меті покращення взаємодії користувачів і покладання відповідальності за перевірку користувачів на провайдерів.

Короткий огляд рекомендацій (рис. 4.6):

- Довжина не менше 8 і не більше 64 символів.
- Не використовувати поширені паролі, які легко вгадати, такі як password, abc123.
- Немає вимог щодо складу, зокрема, необхідності використання великих чи малих літер або цифр.
- Покращити правильність введення, дозволивши користувачу бачити пароль під час набору.
- Дає змогуться використовувати усі друковані символи та пробіли.
- Жодних підказок щодо пароля.
- Відсутність періодичного або випадкового терміну дії пароля.
- Відсутність автентифікації на основі знань, таких як секретне запитання, маркетингові дані, історія транзакцій.

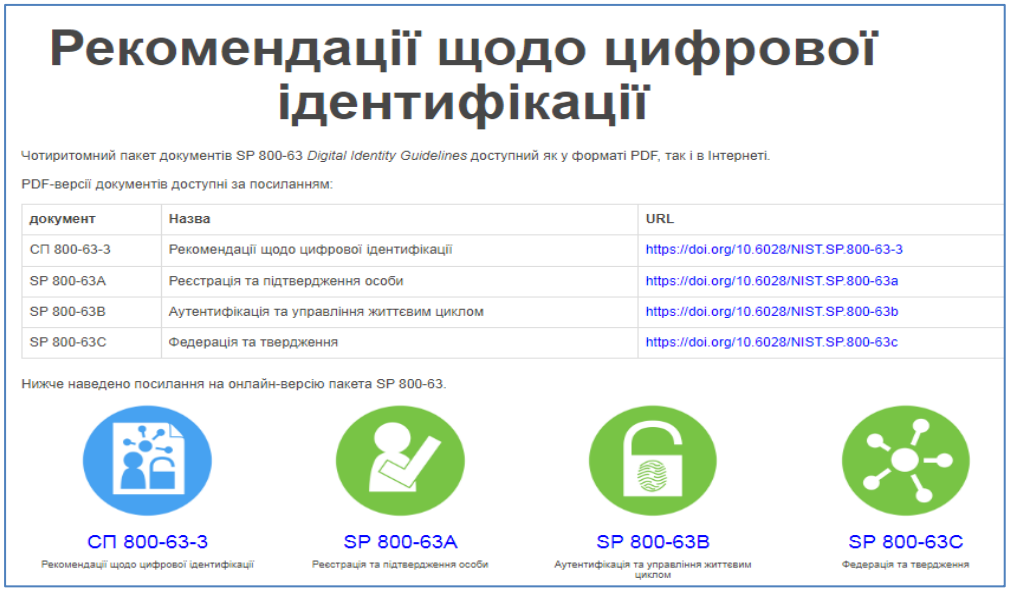


Рис. 4.6. Вдосконалені вимоги до паролів, запропоновані NIST

Навіть якщо доступ до ваших комп’ютерів та мережевих пристроїв захищений, важливо також захистити та зберегти ваші дані.

Шифрування ваших даних

Ваші дані завжди мають бути зашифровані (рис.4.7) . Ви можете подумати, що у вас немає секретів, і вам немає чого приховувати, тому навіщо використовувати шифрування? Можливо, ви думаєте, що ваші дані нікого не цікавлять? Однак, швидше за все, це не так.

Чи готові ви показати всі свої фотографії та документи незнайомцям? Чи готові ви поділитися з друзями фінансовою інформацією, яка зберігається на вашому комп'ютері? Чи хочете оприлюднити для широкого загалу свої електронні листи та паролі до облікових записів?

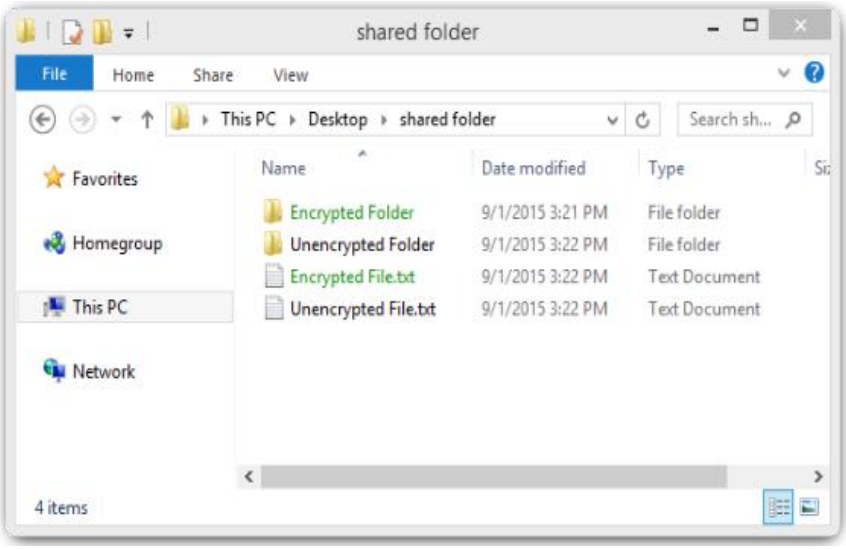


Рис.4.7. Шифровані файли

Ще більш критичною може бути ситуація, коли зловмисна програма заражає ваш комп'ютер або мобільний пристрій і викрадає потенційно важливу інформацію, таку як номери рахунків, паролі та іншу конфіденційну інформацію. Це може призвести до крадіжки особистих даних, шахрайства чи шантажу. Злочинці можуть просто зашифрувати ваші дані, унеможлививши їх використання до сплати вами викупу.

Що таке шифрування? Шифрування – це процес перетворення інформації у форму, в якій неавторизована сторона не зможе її прочитати. Лише довірена, уповноважена особа, яка має секретний ключ або пароль, може розшифрувати дані та отримати їх в оригінальній формі. Саме лише шифрування не може завадити зловмиснику перехопити дані. Шифрування може тільки завадити неавторизованій особі переглядати або отримувати доступ до вмісту даних.

Існують програми, які використовуються для шифрування файлів, папок і навіть цілих дисків.

Шифрована файлова система (Encrypting File System – EFS) – це функція Windows, яка може шифрувати дані. EFS безпосередньо пов'язана з певним обліковим записом користувача. Лише користувач, який зашифрував дані, матиме доступ до них після того, як вони будуть зашифровані EFS. Щоб зашифрувати дані за допомогою EFS для всіх версій Windows, виконайте наступні кроки:

Крок 1. Виберіть один або декілька файлів або папок.

Крок 2. Натисніть праву кнопку миші на вибраних даних і перейдіть до пункту> Властивості (Properties).

Крок 3. Натисніть Додаткові (Advanced)…

Крок 4. Встановіть прапорець Шифрувати вміст для захисту даних (Encrypt contents to secure data).

Крок 5. Файли та папки, зашифровані EFS, відображаються зеленим кольором, як показано на рисунку.

Зауважимо, що перед використанням EFS або будь-якої іншої технології шифрування, рекомендується створити резервну копію даних, оскільки втрата ключів шифрування зробить файли недоступними.

Робіть резервні копії ваших даних

Ваш жорсткий диск може вийти з ладу. Ваш ноутбук може бути втрачений. Ваш смартфон можуть викрасти. Ви можете видалили оригінальну версію важливого документа. Наявність резервних копій зможе запобігти втраті унікальних даних, наприклад, сімейних фотографій (рис.4.8). Для належного виконання резервного копіювання даних, вам знадобиться додаткове сховище даних, до якого потрібно копіювати дані регулярно й автоматично.

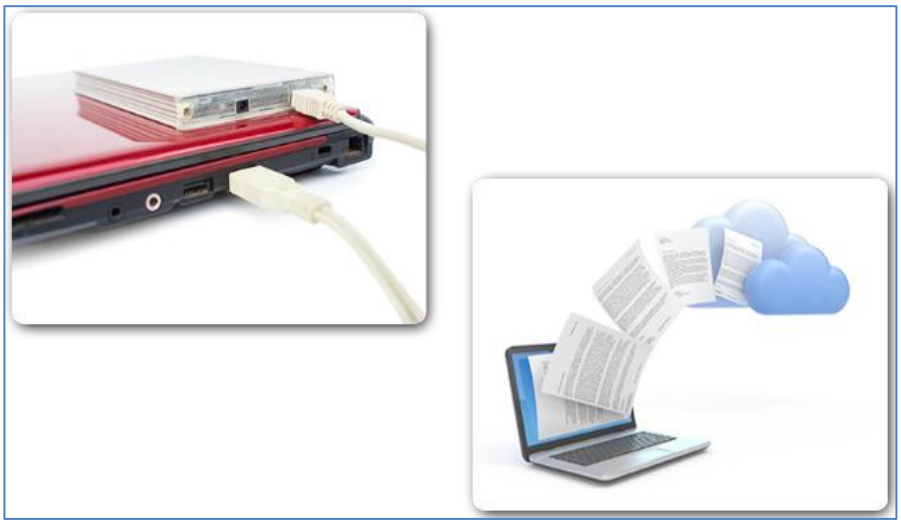


Рис.4.8. Резервне копіювання[44]

Додаткове місце для розміщення резервних файлів можна знайти у вашій домашній мережі, іншому місці або у хмарі. Зберігаючи резервну копію даних локально, ви повністю їх контролюєте. Ви можете вирішити скопіювати всі свої дані до мережевого сховища (Network Attached Storage, NAS), на звичайний зовнішній жорсткий диск або, можливо, вибрати лише кілька важливих папок для резервного копіювання на флеш-накопичувачі, CD/ DVD-диски або навіть стрічки.

За таким сценарієм ви як власник несете повну відповідальність за витрати на придбання та технічне обслуговування пристрою зберігання. Якщо передплатити послугу хмарного зберігання, її вартість залежатиме від необхідного обсягу пам’яті для зберігання.

[44] - https://foni.papik.pro/uploads/posts/2024-09/foni-papik-pro-xlba-p-kartinki-informatsiya-na-prozrachnom-fone-6.png.

Скориставшись сервісом хмарного сховища, наприклад Amazon Web Services (AWS), ви маєте доступ до резервних копій даних допоки у вас є доступ до власного облікового запису. Використовуючи онлайн-сервіси для зберігання даних, ви маєте ретельніше обирати дані, для яких важливо робити резервні копії, через високу вартість зберігання та постійний процес передачі даних в Інтернет. Однією з переваг зберігання резервної копії в альтернативному місці є безпека на випадок пожежі, крадіжки або інших катастроф, окрім несправностей пристрою зберігання.

Видаляйте свої дані остаточно

При переміщенні файлу до кошика для сміття та його остаточному видаленні, файл стає недоступним тільки для операційної системи (рис.4.9). Кожен, хто скористається правильним експертно-криміналістичним інструментарієм, все ще може відновити файл, використовуючи магнітний слід, залишений на жорсткому диску.

Рис. 4.9. Видалення даних[45]

Щоб видалити дані остаточно, без можливості відновлення, потрібно кілька разів перезаписати поверх них одиниці та нулі.

Для запобігання відновленню видалених файлів, вам можуть знадобитися інструменти, спеціально розроблені для виконання вищезазначених операцій. Програма SDelete від Microsoft (для Vista і більш нових версій ОС), за ствердженням виробника, дає можливість видаляти конфіденційні файли остаточно. Shred для Linux та Secure Empty Trash для Mac OSX – це утиліти, які можуть надати аналогічний сервіс.

Єдиний спосіб переконатися, що дані або файли не підлягають відновленню, – це фізичне знищення жорсткого диска або іншого пристрою зберігання. Помилка багатьох злочинців полягала в тому, що вони думали, ніби їх файли неможливо прочитати або відновити.

[45] - https://www.shutterstock.com/ru/image-illustration/3d-laptop-data-transfer-deleting-recycle-79677193, https://www.shutterstock.com/ru/image-photo/paper-pulp-symbolic-photo-data-destruction-265958618

Ваші дані можуть зберігатися не тільки на локальних жорстких дисках, але й в Інтернеті у хмарі. Ці копії також необхідно видалити. Знайдіть час, щоб запитати себе, "Де я зберігаю свої дані? Чи десь зберігаються резервні копії? Вони зашифровані?" Коли вам потрібно видалити свої дані або позбутися жорсткого диска чи комп'ютера, запитайте себе: "Чи захистив я дані так, щоб вони не потрапили до зловмисників?"

4.2. ДВОФАКТОРНА АВТЕНТИФІКАЦІЯ

Популярні онлайн-сервіси, такі як Google, Facebook, Twitter, LinkedIn, Apple та Microsoft, використовують двофакторну автентифікацію для забезпечення додаткового рівня захисту при вході до облікових записів. Крім імені користувача та пароля, або особистого ідентифікаційного номера (PIN) чи шаблону, для двофакторної автентифікації потрібен додатковий токен безпекиє

Токен безпеки – це додатковий елемент автентифікації, який використовується для підтвердження особи користувача при доступі до системи або облікового запису. Він додає другий рівень захисту й ускладнює зловмисникам доступ до ваших даних.

Токеном може бути (Рис.4.10):

- **фізичний об'єкт** – кредитна картка, телефон або ключ-брелок;
- **програмний токен** - одноразовий код, який генерується у мобільному додатку чи надсилається електронною поштою;
- **Біометричний токен** – відбиток пальця, відбиток долоні, розпізнавання обличчя або голосу.

Рис.4.10. Двофакторна аутентфікація[46]

Двофакторна автентифікація значно підвищує рівень безпеки, оскільки навіть якщо зловмисник здобуде пароль користувача, він все одно не зможе отримати доступ без додаткового токена безпеки. Але навіть при застосуванні двофакторної автентифікації хакери можуть отримати доступ до ваших облікових записів в Інтернеті через такі атаки, як фішинг, зловмисне програмне забезпечення та соціальна інженерія. Для зменшення ризиків рекомендується завжди використовувати офіційні програми-автентифікатори та уважно перевіряти джерела будь-яких запитів на введення одноразового коду.

[46] - https://encrypted-tbn0.gstatic.com/images?q=tbn:ANd9GcSkvFOF7yghQZ3bttBL7n58a0Svty6lXTjwmw&s

Огляд

Після багатьох резонансних і поширених серйозних зломів даних, які поставили під загрозу мільйони людей, багато людей стали більше розуміти про безпеку паролів і той факт, що простий пароль не може захистити профілі в Інтернеті. Це призвело до зростання популярності двофакторної автентифікації, додаткового рівня безпеки, який може захистити облікові записи (рис.4.11).

Фактори автентифікації

Фактор автентифікації – це категорія облікових даних безпеки, яка використовується для перевірки ідентичності та авторизації користувача, перш ніж дозволити цьому користувачеві отримати доступ до свого облікового запису, надсилати повідомлення або запитувати дані із захищеної мережі, системи чи програми.

Є три загальні фактори автентифікації: те, що ви є, те, що ви знаєте, і те, що ви маєте. Розберемо їх далі:

- **те, що ви є**. Цей тип 2FA включає біометричні методи, такі як відбитки пальців, сканування сітківки або обличчя, аналіз почерку або розпізнавання голосу. Більшість сучасних смартфонів використовують розпізнавання обличчя, ноутбуки часто використовують зчитувачі відбитків пальців, і вас можуть навіть попросити ввести відбиток руки, якщо ви купуєте абонемент у парк розваг. Хоча цей тип 2FA забезпечує найнадійнішу автентифікацію серед будь-якого методу двофакторної автентифікації, він не є ідеальним.

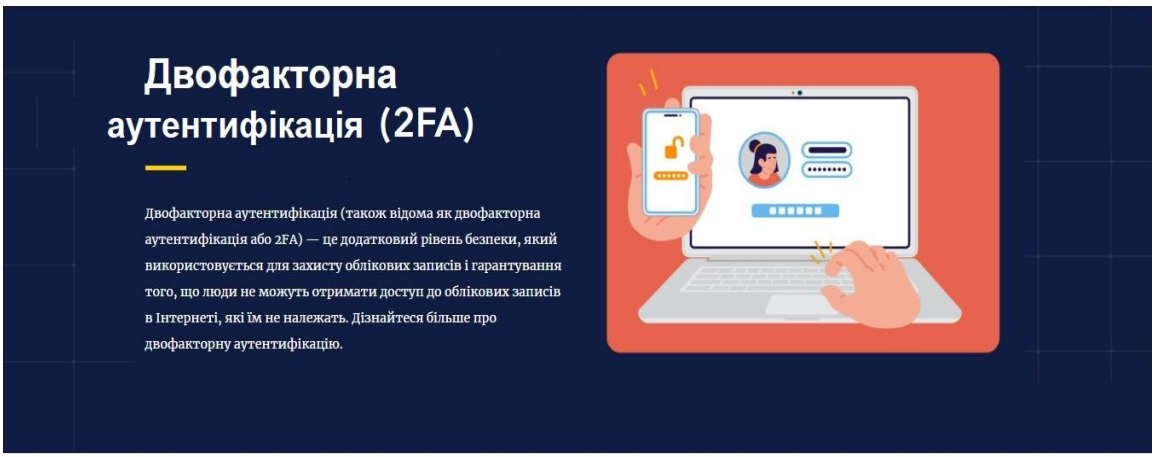


Рис. 4.11. Сутність 2FA

Кожен, хто коли-небудь мав пристрій зі здатністю сканувати обличчя або відбитки пальців, відчував розчарування, намагаючись змусити свій iPhone прийняти їх обличчя або відбитки пальців, знає це.

- **те, що ви знаєте**. Це може бути найпоширенішим фактором, який використовується при двофакторній автентифікації. Як правило, це буде пароль

або персональний ідентифікаційний номер (PIN-код). На жаль, ці фактори автентифікації також є найбільш вразливими до атак безпеки. Багато людей використовують одні й ті ж паролі для облікового запису за обліковим записом, і якщо є порушення навіть в одному обліковому записі, це означає, що кожен обліковий запис скомпрометований.

- **те, що ви маєте**. Цей тип фактора зазвичай контролюється за допомогою пристрою, який, як відомо, є у законного користувача (зазвичай смартфон). Спочатку користувач реєструється для облікового запису з адресою електронної пошти та паролем, а потім записує свій номер телефону. Потім користувач входить у свій обліковий запис з цією адресою електронної пошти та паролем, після чого одноразовий пароль надсилається на номер мобільного телефону користувача. Щойно користувач вводить це на свій пристрій, він отримує доступ до свого облікового запису та системи.

Що таке двофакторна автентифікація?

Двофакторна автентифікація (2FA) – це процес безпеки, за якого користувачі повинні надати два різних фактори автентифікації, щоб підтвердити свою особу та отримати доступ до свого облікового запису. Цей процес забезпечує кращий захист особистої інформації, облікових даних та інших активів користувача, а також покращує безпеку ресурсів, до яких користувач може отримати доступ.

Звичайно, двофакторна автентифікація забезпечує вищий рівень безпеки, ніж методи автентифікації, які покладаються лише на один фактор автентифікації (однофакторна автентифікація), де користувач надає лише один фактор (зазвичай пароль або PIN-код). Метод 2FA вимагатиме від користувача не просто пароля чи PIN-коду, а й другого фактора, починаючи від біометричного фактора (сканування обличчя, сітківки або відбитків пальців) до фактора володіння (одноразового коду, надісланого на смартфон, який, як відомо, є у користувача).

Цей додатковий рівень безпеки означає, що навіть якщо зловмисник знає пароль користувача, йому не буде дозволено отримати доступ до свого облікового запису в Інтернеті чи мобільного пристрою. Насправді, двофакторна автентифікація вже давно використовується для контролю того, хто може отримати доступ до конфіденційних даних і систем, і фахівці з безпеки закликають увімкнути двофакторну автентифікацію на всіх ваших онлайн-облікових записах, комп’ютерах і мобільних пристроях.

Двофакторна автентифікація є ключовим компонентом кібербезпеки та роботи, яку виконують аналітики кібербезпеки. Вона дає змогу забезпечити додатковий рівень захисту, оскільки навіть якщо зловмисник отримує доступ до

пароля, він не зможе увійти без фізичного доступу до пристрою чи іншого фактора автентифікації.

Що означає 2FA?

Двофакторна автентифікація (2FA) відноситься до методу безпеки, який використовується для захисту облікових записів і систем від несанкціонованого доступу, вимагаючи від потенційних користувачів надати якусь додаткову перевірку своєї особистості.

Двофакторну автентифікацію можна використовувати для посилення безпеки телефона, облікового запису в Інтернеті або навіть дверей. Вона працює, вимагаючи від користувача двох типів інформації: першим фактором зазвичай є пароль або персональний ідентифікаційний номер (PIN), а другий фактор може бути відбитком пальця або одноразовим кодом, надісланим на ваш телефон.

Хоча двофакторна автентифікація покращує безпеку, вона не є повністю надійною. Зловмисники можуть використовувати фішингові атаки або інші методи, щоб отримати доступ до одного з факторів автентифікації, що може призвести до компрометації облікового запису.

Двоетапна перевірка проти двофакторної автентифікації

Хоча ми часто використовуємо двофакторну автентифікацію і двоетапну перевірку як взаємозамінні і, здається, значно перетинаються, вони не зовсім однакові.

Apple розрізняє двоетапну перевірку та 2FA, вказуючи на двоетапну перевірку як на старіший і нижчий метод безпеки, коли користувач повинен ввести як пароль, так і одноразовий код, який було надіслано на його iPhone або інший надійний пристрій.

Хоча це одна з форм, двофакторна автентифікація також включає методи автентифікації, які використовуються на сучасному iPhone, оснащеному технологією сканування обличчя, і Macbook, доступ до яких можна отримати після сканування відбитків пальців.

Що таке двофакторний код автентифікації?

Двофакторний код автентифікації – це одноразовий код, який створюється для підтвердження особи користувача, коли він намагається отримати доступ до облікового запису або системи в Інтернеті. Код буде надіслано за допомогою текстового повідомлення або автоматичного телефонного дзвінка на номер телефону, пов’язаний з користувачем. Після введення двофакторного коду автентифікації користувач отримує доступ до свого облікового запису в Інтернеті.

Ці коди часто закінчуються через короткий проміжок часу, якщо не використовуються. Код забезпечує додатковий рівень безпеки, оскільки його не

можна використовувати повторно, і він є доступним лише на пристрої, який зареєстрований за користувачем.

Переваги двофакторної автентифікації

Переваги двофакторної автентифікації полягають у тому, що вона додає вкрай необхідний додатковий рівень захисту від атак і може підвищити безпеку систем, компаній і звичайних людей.

2FA забезпечує додатковий рівень захисту для користувачів, оскільки імені користувача та пароля більше не достатньо. По-перше, кількість крадіжок особистих даних зростає зі зловісними темпами. У 2018 році дослідження Javelin Strategy & Research показало, що шахрайство з ідентифікацією зросло на вісім відсотків лише в 2017 році, до 16,7 мільйонів споживачів у США. Загальна вартість шахрайства досягла 16,8 мільйона доларів. Запровадження двофакторної автентифікації, що не залежить від пароля, значно підвищує безпеку та знижує ризик крадіжки особистих даних.

Крім того, численні порушення даних, які ми спостерігали протягом останніх кількох років, створили ситуацію, коли мільйони людей мимоволі виявили свою особисту інформацію (включаючи своє ім'я користувача та пароль) доступною для перегляду будь-кому. Крім того, багато людей використовують один і той самий пароль на кількох сайтах, тому хакер може спробувати використати ту саму інформацію для входу на різних сайтах, поки не знайде той, який працює. У звіті Verizon 2017 року щодо розслідувань злому даних було виявлено, що 81 відсоток порушень облікових записів можна пояснити паролями, які були або розголошені таким чином, або паролями, які були занадто слабкими і їх можна було вгадати.

Проте недостатньо людей прийняли 2FA. Google, наприклад, нещодавно показав, що менше 10 відсотків користувачів Gmail використовують доступні заходи безпеки 2FA для захисту своїх облікових записів.

Для компаній переваги впровадження 2FA очевидні – сьогодні ніхто не може дозволити собі нехтувати кібербезпекою. Двофакторна автентифікація також може допомогти зменшити витрати на IT. Скидання пароля є однією з найпоширеніших причин, чому люди звертаються до служби підтримки – дослідження, проведене галузевою асоціацією HDI, показало, що більше третини заявок до служби підтримки пов'язані зі скиданням пароля.

Чи можна зламати двофакторну автентифікацію?

Хоча двофакторну автентифікацію можна зламати, шанси дуже низькі, і 2FA, безумовно, є найкращою практикою, коли йдеться про захист облікових записів і систем. Двофакторну автентифікацію можна зламати одним із способів

– за допомогою методу SMS або, іншими словами, методу, за допомогою якого одноразовий код надсилається на номер телефону користувача за допомогою SMS або автоматичного телефонного дзвінка.

Були історії про хакерів, які обманювали операторів мобільного зв'язку, щоб вони передали чужий номер телефону на свій власний телефон. Хакери зв'язуються з операторами, прикидаючись їхніми жертвами, запитуючи нову SIM-карту з номером жертви. Потім вони мають доступ до будь-якого коду автентифікації, надісланого на цей номер телефону. Це, мабуть, найпоширеніший спосіб обійти 2FA.

Але власні процеси безпеки операторів удосконалюються, і навіть попри ці ризики, 2FA залишається сильним і важливим інструментом у боротьбі з кібератаками та шахрайством особистих даних.

Типи 2FA

Існує кілька основних типів 2FA, які широко використовуються, і варто знати відмінності, та відповідні переваги та недоліки різних методів.

Як працює 2FA?

Двофакторна автентифікація працює, додаючи ще один рівень безпеки до онлайн-облікових записів і систем. 2FA працює, вимагаючи, щоб будь-який користувач, який намагається ввійти, поєднував свій перший фактор автентифікації – пароль або особистий ідентифікаційний номер – з другим фактором, який зазвичай є тим, що ви знаєте, чимось, що у вас є або тим, чим ви є. З 2FA користувачам потрібно буде надати обидва ці фактори, щоб отримати доступ до своїх облікових записів або системи.

При правильному застосуванні 2FA має унеможливлювати доступ хакерів до вашого облікового запису, використовуючи лише вкрадені паролі та дані для входу. Хоча це не є абсолютно непроникним, оскільки хакери розробили деякі обхідні шляхи, 2FA, безумовно, пропонує значно більше безпеки, ніж просто вимога імені користувача або адреси електронної пошти та пароля.

Приклади двофакторної автентифікації

Якщо бентежить визначення факторів у 2FA як те, що у вас є, що ви є, або щось, що ви знаєте, може допомогти розглянути деякі реальні приклади двофакторної автентифікації.

«Те, що ви є» зазвичай переносить нас у сферу біометричних даних, де комп'ютери використовують елемент вашої фізичної особи (наприклад, ваш відбиток пальця, обличчя, голос чи сітківку), щоб підтвердити вашу особу. Якщо ви купили телефон протягом останніх кількох років, швидше за все, ви зможете швидко отримати до нього доступ після того, як він відсканує ваше обличчя або

відбиток пальця – щось, що здавалося б науковою фантастикою кілька десятиліть тому. Існують обґрунтовані сумніви щодо біометричних даних – бази даних фізичних даних можна зламати, як і будь-який інший список паролів, – але зручна природа біометричної 2FA означає, що вона залишиться тут.

Далі ми можемо подивитися на «щось, що у вас є». Одним із ініціаторів цього типу фактора безпеки був RSA SecurID, невеликий пристрій з невеликим екраном, який відображав випадкові числа, які періодично змінювалися. Випущений у 1993 році, пристрій вимагає від користувача в будь-який момент мати пароль і номер із токена SecurID для входу в систему. Існують інші гаджети, які виконують цей тип 2FA, включаючи смарт-картки або фізичний ключ безпеки для підключення. на комп'ютери через USB або Bluetooth. Google використовує їх внутрішньо.

Але більшість людей не мають такого спеціалізованого гаджета, тому є ще один приклад «щось, що у вас є», коли справа доходить до 2FA: ваш телефон. Щоразу, коли ви намагаєтеся увійти на свій вебсайт і на ваш телефон надсилається спеціальний код - це 2FA в дії. Є також програми, які сканують QR-коди, щоб підтвердити вашу особу.

Нарешті, «щось, що ви знаєте» може означати вторинний пароль або таємне запитання на основі знань, наприклад, запитати дівоче прізвище вашої матері або ім'я вашого вихованця з дитинства. Деякі стверджують, що це не відповідає дійсності 2FA, оскільки будь-який хакер, який володіє інформацією для входу, може так само легко отримати відповіді на типові питання безпеки.

Поширені типи 2FA

Оскільки двофакторна автентифікація набуває все більшого визнання як абсолютна безпека, необхідна як для окремих осіб, так і для компаній, варто розглянути найпоширеніші типи 2FA:

SMS-повідомлення та голосова 2FA

Завдяки текстовому SMS-повідомленню та голосовій двофакторній автентифікації користувачі вказують номери телефонів під час реєстрації, і щоразу, коли їм потрібно ввійти до свого облікового запису, генерується одноразовий код, який надсилається на номер телефону, на який вони зареєструвалися (за допомогою текстового повідомлення або автоматичного телефонного дзвінка).

Кожен, хто проводив будь-який час в Інтернеті, знає, що це дуже популярний варіант, оскільки він зручний і не потребує спеціального обладнання. Хоча будь-яка форма 2FA краща, ніж нічого, експерти з безпеки все частіше застерігають від цієї форми 2FA. Рівень безпеки просто не такий високий, як у інших форм 2FA, тому що є різноманітні обхідні шляхи, які хакери

можуть використовувати, щоб поставити під загрозу безпеку вашого облікового запису.

Наприклад, зловмисники можуть змусити користувачів встановити шкідливий додаток на свій телефон, який потім зможе читати та пересилати SMS-повідомлення. Інший експлойт включає злом стільникового сервісу для перенаправлення SMS-повідомлень за допомогою різноманітних технічних методів або за допомогою соціальної інженерії.

Інші мінуси? Деяким людям непросто надавати свій номер телефону вебсайту, програмі чи платформі. І легко зрозуміти їх побоювання, оскільки багато компаній неправильно використовували цю інформацію з такими речами, як цільова реклама та відстеження конверсій. Дозвіл скидання пароля на основі номера телефону, наданого для 2FA, може бути серйозною проблемою безпеки пароля, оскільки зловмисники, які використовують захоплення телефонних номерів, можуть отримати доступ до вашого облікового запису, навіть якщо вони не мають вашого пароля.

SMS 2FA також не працюватиме, якщо ваш телефон не працює або не може підключитися до мобільної мережі. Це може бути великою проблемою для людей, які подорожують за кордон.

Push-повідомлення для 2FA

Кожен, хто глибоко заглибився в екосистему Apple, був би знайомий з цим типом двофакторної автентифікації завдяки методу Apple Trusted Devices. Цей метод надсилає запит на різні пристрої користувача щоразу, коли робиться спроба входу від імені цього користувача. Підказка містить приблизне розташування для входу на основі IP-адреси. У таких системах, як цей метод Trusted Devices, користувач вирішує, схвалити чи відхилити спробу входу.

Але для роботи надійних пристроїв та інших систем push-повідомлень (ще одним прикладом є Duo Push), вашому пристрою потрібне підключення до Інтернету або даних.

Цей спосіб трохи зручніший, ніж мати справу з QR-кодами. Крім того, оскільки ці сповіщення зазвичай показують приблизне місце спроби входу – і оскільки дуже мало фішингових атак відбувається з тієї ж IP-адреси, що й жертва, цей метод може допомогти вам помітити фішингову атаку.

Програмні токени для 2FA / Authenticator App / TOTP 2FA

Форма 2FA вимагає, щоб користувач спершу завантажив та встановив програму двофакторної автентифікації на своєму телефоні або робочому столі. На будь-якому сайті, сумісному з програмою автентифікації, користувачі можуть спочатку ввести ім’я користувача та пароль, перш ніж перейти до програми автентифікації, щоб знайти згенерований програмним забезпеченням одноразовий пароль (також званий TOTP або програмний маркер), який їм

потрібен. щоб завершити спробу входу.

Google Authenticator, Microsoft Authenticator, Duo Mobile від Duo Security і FreeOTP – кілька популярних програм для цього. Основна технологія цього стилю 2FA називається одноразовим паролем на основі часу (TOTP).

Якщо сайт пропонує цей стиль 2FA, він покаже QR-код, що містить секретний ключ. Ви можете відсканувати цей QR-код у своїй програмі. Код можна сканувати кілька разів, і ви можете зберегти його в безпечному місці або роздрукувати. Після сканування QR-коду ваша програма вироблятиме новий шестизначний код кожні 30 секунд, і вам знадобиться один із цих кодів разом із вашим ім'ям користувача та паролем для входу.

Перевага цього стилю двофакторної автентифікації полягає в тому, що вам не потрібно підключатися до мобільної мережі. Якщо хакер переспрямує ваш номер телефону на свій телефон, він все одно не отримає ваших QR-кодів. Але недоліком є те, що якщо ви часто входите в систему на різних пристроях, може бути незручно розблокувати телефон, відкривати програму та щоразу вводити код.

Апаратні токени для 2FA

Мабуть, найстаріша форма 2FA, апаратні токени виробляють новий числовий код через регулярні проміжки часу. Коли користувач хоче отримати доступ до облікового запису, йому просто потрібно перевірити пристрій – він, як правило, маленький, як брелок – і ввести код 2FA, який відображається на сайті або в додатку. Інші версії цієї технології 2FA можуть автоматично передавати двофакторний код автентифікації, коли ви підключаєте ключ безпеки до порту USB.

Як правило, апаратна двофакторна автентифікація частіше використовується підприємствами, але її можна реалізувати і на персональних комп'ютерах. Великі технологічні та фінансові компанії створюють стандарт, відомий як U2F, і тепер можна використовувати фізичний апаратний токен U2F для захисту ваших облікових записів Dropbox, Google і GitHub. Це лише маленький USB-ключ, який ви надягаєте на брелок. Коли ви хочете увійти в обліковий запис з нового комп'ютера, ви вставляєте USB-ключ і натискаєте на ньому кнопку. Це так просто – коди не потрібні. Колись ці пристрої повинні працювати з NFC і Bluetooth для зв'язку з мобільними пристроями без USB-портів.

Переваги цього методу в тому, що він безпечний і не потребує підключення до Інтернету. Мінус? Вартість налаштування й обслуговування, а пристрої можуть бути викрадені або пошкоджені.. Але в цілому метод забезпечує високий рівень безпеки, оскільки зловмисники не можуть отримати доступ до токена без фізичного пристрою.

Біометричний 2FA

За останні два десятиліття біометрична двофакторна автентифікація (2FA) еволюціонувала від футуристичної ідеї до повсюдного явища. Сьогодні багато користувачів навіть не помічають, як часто вони отримують доступ до своїх пристроїв, просто "будучи собою".

При біометричній перевірці користувач сам стає маркером. Його обличчя, відбиток пальця, сітківка ока або голос використовуються як фактор автентифікації для підтвердження особи та доступу до облікових записів.

Сучасні технології роблять цей метод звичним у повсякденному житті. Найновіші моделі, як-от iPhone, оснащені сканерами обличчя, а більшість інших смартфонів використовують сканування відбитків пальців, щоб забезпечити користувачам зручний і швидкий доступ. Багато сучасних моделей можуть розблокуватися за відбитком пальця, і є багато інших пристроїв, які можуть підтвердити вашу особу, скануючи ваші фізичні характеристики або голос.

Біометричний 2FA вважається одним із найбезпечніших методів, адже зламати унікальні фізичні маркери складніше, ніж, наприклад, пароль. До того ж, цей спосіб зручний для користувача, адже не потребує запам’ятовування додаткових даних – достатньо лише бути собою.

Попри переваги, біометричні технології ще вдосконалюються й іноді можуть помилятися у підтвердженні особи. Також є певне занепокоєння, пов’язане зі складнощами забезпечення надійного захисту біометричних даних, їх конфіденційності та захисту від несанкціонованого доступу. Збереження інформації про фізичні характеристики людини (наприклад, відбитки пальців, скан обличчя, голосові зразки) у цифровій формі може становити ризик. Ці дані є унікальними для кожної людини, тому, якщо вони потраплять до хакерів або будуть неправильно використані, особа може зіткнутися зі значними загрозами.

Крім того, для проведення біоідентифікації потрібні спеціальні пристрої, як-от сканери та камери. Тож біометрична автентифікація – це зручний і перспективний напрямок, але її ефективність і безпека залежать від подальшого розвитку технологій та врахування ризиків конфіденційності.

Інші форми 2FA

Іншим поширеним методом є 2FA через електронну пошту. Принцип роботи полягає в тому, що автоматичне повідомлення надсилається на зареєстровану адресу електронної пошти користувача, коли відбувається спроба входу. Подібно до SMS або телефонного дзвінка, цей електронний лист буде містити код або просто посилання, натискання якого підтвердить, що це законна спроба входу.

Як і 2FA через телефон або SMS, це легко реалізувати та інтуїтивно зрозуміло для користувачів і працює як на комп’ютерах, так і на телефонах. Але

на відміну від опцій SMS і телефону 2FA, користувачу потрібно буде підключитися до Інтернету, щоб отримати свій код або активувати своє унікальне посилання.

На жаль, це найменш безпечна форма 2FA і в результаті втрачає свою популярність. Захист паролів є занадто поширеною проблемою, щоб це було ефективним. Незважаючи на багаторічні попередження, багато людей використовують ідентичні паролі для багатьох облікових записів і пристроїв, і, можливо, або навіть ймовірно, що їхня реєстраційна інформація для облікового запису, до якого вони намагаються отримати доступ, і їхня адреса електронної пошти ідентичні.

Є й інші проблеми. Є велика ймовірність, що електронна пошта може опинитися в папці зі спамом, і якщо хакери мають правильний пароль для чиїхось онлайн-аккаунтів, є велика ймовірність, що вони також можуть мати свій пароль електронної пошти.

Як отримати 2FA

Безпека вашого облікового запису є життєво важливою, тому більшість сайтів, програм і пристроїв тепер пропонують деяку форму двофакторної автентифікації, хоча спосіб отримання 2FA залежить від платформи, пристрою чи вебсайту, про які йдеться.

Apple може провести вас через процес увімкнення двофакторної автентифікації для всіх своїх пристроїв, хоча цю функцію можна знайти в розділі «Пароль і безпека» в налаштуваннях iPhone або «Системні налаштування» на Mac. Google, Facebook, Amazon, Twitter, Reddit та багато інших популярних сайтів пропонують посібники про те, як налаштувати двофакторну автентифікацію у вашому обліковому записі.

Як увімкнути 2FA

Щоб увімкнути 2FA, ви можете або перейти до системних налаштувань або до налаштувань усіх ваших пристроїв та онлайн-облікових записів і ввімкнути двофакторну автентифікацію, де це можливо, або ви можете завантажити та встановити програму автентифікації.

Отримання програми автентифікації (також відомої як програма автентифікації) – це один із способів активного впливу на свою безпеку в Інтернеті. Після зв’язування з вашими обліковими записами програма автентифікатора відображає постійно змінюваний набір кодів, які можна використовувати, коли це необхідно, навіть без підключення до Інтернету. Лідером у сфері додатків для автентифікації є Google Authenticator, а інші варіанти включають Twilio Authy, Duo Mobile від Duo Security і LastPass Authenticator. Більшість менеджерів паролів також пропонують двофакторну

автентифікацію за замовчуванням.

Ви повинні знати, що налаштування 2FA іноді може порушити доступ до деяких старих служб, що змушує вас покладатися на паролі додатків. Використовуються такими компаніями, як Facebook, Microsoft і Yahoo, паролі додатків генеруються на головному сайті для використання з певною програмою.

Пам'ятайте про це, коли ви панікуєте через те, як важко все це звучить: бути в безпеці нелегко. Погані хлопці розраховують на те, що ви не захищаєте себе. Запровадження двофакторної автентифікації означатиме, що кожен раз вхід на новому пристрої займає трохи більше часу, але це того варте, щоб уникнути серйозної крадіжки, будь то вашої особи, даних чи грошей.

Майбутнє двофакторної автентифікації

Хоча 2FA повністю підвищує безпеку загалом, майбутнє двофакторної автентифікації має базуватися на створенні ще більш безпечних систем, які позбавлені слабких місць, які все ще існують.

Коли 2FA зазнала невдачі

Нам не доведеться далеко шукати приклади компрометації 2FA. У серпні 2019 року порушники зламали обліковий запис генерального директора Twitter Джека Дорсі, і грубі повідомлення, опубліковані в його акаунті, не були гарною рекламою системи безпеки 2FA. Через місяць з'явилися повідомлення про те, що 23 мільйони користувачів YouTube були зламані, незважаючи на використання 2FA, оскільки хакери використовували інструменти зворотного проксі для перехоплення кодів двофакторної автентифікації, надісланих за допомогою SMS. Криптовалютна біржа Binance скомпрометувала свою систему 2FA і втратила десятки мільйонів.

Одним з найпростіших і найпоширеніших методів злому системи 2FA є заміна симулятора. У цьому сценарії хакер може використовувати будь-яку кількість методів, щоб змінити номери телефону жертв, щоб будь-які наступні повідомлення або телефонні дзвінки, наприклад, з кодом 2FA, перенаправлялися на новий телефон. Це одна з причин, чому експерти все частіше закликають відмовитися від систем 2FA на основі SMS і телефонних дзвінків.

Також відомо, що деякі системи двофакторної автентифікації скомпрометовані шкідливим програмним забезпеченням. Навіть, наприклад, програма автентифікації Google Authenticator, що широко використовується, не є ідеальною – у лютому 2020 року було виявлено, що зловмисне програмне забезпечення на базі Android вкрало коди 2FA.

Зловмисне програмне забезпечення TrickBot – це ще один інструмент обходу двофакторної автентифікації й перехоплення одноразових кодів, які надсилаються банківськими додатками з застосуванням SMS і push-повідомлень.

Тож двофакторна ідентифікація зараз вразлива? У сценаріях соціальної інженерії хакер може зв'язатися з клієнтом й представитись, наприклад, їхнім банком, попросити підтвердити особу, продиктувати код підтвердження, який щойно ніби то надіслав жертві. З цих та інших причин багато експертів з безпеки вважають, що майбутнє 2FA полягає в розширенні біометричної безпеки.

Біометричні методи тільки покращаться

За короткий час біометрична автентифікація пройшла шлях від футуристичної ідеї до повсякденної реальності. Приклади біометричної 2FA оточують нас: ви використовуєте її, коли банк підтверджує вашу особу за допомогою голосу, коли смартфон розпізнає вас за обличчям або коли ви входите в систему одним дотиком пальця.

Однак варто визнати, що в наш час біометричні системи поки не є абсолютно надійними. Наприклад, відомі випадки, коли системи розпізнавання обличчя обдурювали 3D-рендерами фотографій із соціальних мереж.

Крім того, користувачі іноді стикаються з помилковими спрацьовуваннями. Помилкові позитиви виникають, коли система помилково ідентифікує людину як правильного користувача, що особливо актуально для технології розпізнавання обличчя. Помилкові негативи трапляються, коли справжній користувач не проходить перевірку — це часто стається при використанні сканерів відбитків пальців, де навіть незначна вологість або пошкодження шкіри можуть спричинити відмову доступу. До того ж, деякі люди мають відбитки, які складно зчитати.

У перспективі розумні пристрої стануть ще потужнішими, а біометрична автентифікація — ще швидшою й зручнішою. Камери підвищуватимуть роздільну здатність, з'являтимуться інфрачервоні сенсори, а також зростатиме увага до сканування райдужної оболонки ока — одного з методів автентифікації, котрий вважається одним з найбільш перспекивних для застосування.

У майбутньому біометрична 2FA стане ще точнішою, чутливішою та безперебійною: алгоритми зможуть краще відрізняти справжніх користувачів від зловмисників, зменшиться кількість хибних спрацьовувань, а процес автентифікації відбуватиметься практично миттєво та без необхідності активної участі користувача. Системи зможуть краще адаптуватися до змін зовнішності, чи умов освітлення, що зробить автентифікацію надійною навіть у складних обставинах

Багатофакторна автентифікація та бази даних

Якщо двофакторна автентифікація здається вам незручністю, це може бути не бажаною новиною тому що майбутнє, ймовірно, включатиме все більшу увагу до багатофакторної автентифікації. Поєднання трьох (або більше) рівнів

автентифікації з певною формою біометричних даних забезпечить надійний рівень безпеки, якого не змогла б проста 2FA. Організації, де системи містять конфіденційну інформацію, швидше за все, вже використовують багатофакторну автентифікацію, і незабаром її впровадять інші. Методи збереження конфіденційної інформації – ще одна сфера, яка з часом буде розвиватися. Багато експертів з безпеки вважають, що будь-який метод автентифікації на основі пристрою врешті-решт недостатній. Натомість вони рекомендують організаціям розглянути можливість безпечного зберігання ідентифікаційних даних у централізованій базі даних. Це може бути поки складним для деяких компаній, але поширення біометричної автентифікації показало, як швидко ці технології можуть розвиватися і стати значною частиною нашого повсякденного життя.

OAuth 2.0

Відкрита авторизація (Open Authorization, OAuth) – це протокол відкритого стандарту, який дає змогу використовувати облікові дані кінцевого користувача для отримання доступу до сторонніх програм, не розкриваючи пароль користувача (рис. 4.12). OAuth діє як посередник при вирішенні питання, чи надавати кінцевим користувачам доступ до сторонніх програм. Наприклад, ви бажаєте отримати доступ до вебзастосунку XYZ, але не маєте облікового запису користувача для доступу до нього. Однак, XYZ має варіант входу, при якому використовуються облікові дані з вебсайту соціальної мережі ABC. Таким чином, ви отримуєте доступ до вебсайту, використовуючи дані для входу до соціальної мережі.

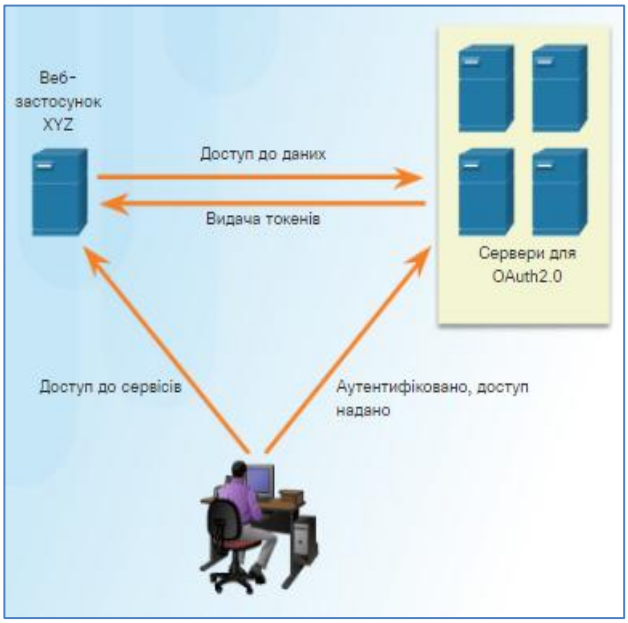


Рис.4.12. Робота за протоколом OAuth[47]

Для того, щоб це працювало, застосунок XYZ повинен бути зареєстрованим та схваленим застосунком в ABC. Для доступу до застосунку XYZ, ви використовуєте ваші облікові дані в мережі ABC.

Далі XYZ запитує від вашого імені токен доступу у ABC. Після чого ви маєте доступ до XYZ. XYZ не знає нічого про вас і ваші облікові дані, а ця взаємодія відбувається абсолютно непомітно для користувача. Використання токенів безпеки не дає можливості шкідливому застосунку отримати інформацію про вас і ваші дані.

[47] - This figure was uploaded by slideshare.net

Протокол OAuth 2.0 це один із найпопулярніших стандартів для авторизації, що використовується багатьма сервісами та платформами, включаючи Google, Facebook, Microsoft, GitHub тощо. OAuth 2.0 забезпечує безпечний спосіб надання доступу до ресурсів стороннім додаткам без передачі облікових даних користувача.

Навіть попри те, що з'являються нові стандарти, наприклад, OAuth 2.1 (який уточнює й спрощує деякі аспекти OAuth 2.0), версія 2.0 залишається значно поширеною і підтримуваною.

Не поширюйте занадто багато інформації в соціальних мережах

Якщо ви хочете зберегти вашу конфіденційність у соціальних мережах, поширюйте якомога менше інформації (рис.4.13). Вам не варто ділитися у профілі такою інформацією, як дата вашого народження, електронна адреса або номер телефону. Люди, яким потрібно знати вашу особисту інформацію, напевно вже мають її. Не заповнюйте свої профілі в соціальних мережах повністю, надайте лише мінімально необхідну інформацію. Окрім того, перевірте свої налаштування в соціальних мережах, дозволяйте лише знайомим людям переглядати інформацію про вашу активність і писати вам.

Рис. 4.13. Інформація в INET[48]

Чим більше особистої інформації ви поширюєте в Інтернеті, тим легше зловмисникам зібрати досьє на вас і використати його проти вас у реальному житті.

Чи коли-небудь ви забували ім’я користувача та пароль від облікового запису в Інтернеті? Секретні питання, такі як "Дівоче прізвище вашої матері?" або "В якому місті ви народилися?" допоможуть додатково захистити ваш обліковий запис від зламу. Однак, той хто хоче отримати доступ до ваших облікових записів, може знайти відповіді на ці запитання в Інтернеті. Ви можете встановити у якості відповіді на ці запитання неправдиву інформацію, якщо самі здатні запам’ятати ці фальшиві відповіді. Якщо у вас виникають проблеми із запам’ятовуванням цієї інформації, варто використовувати менеджер паролів.

[48] - https://www.shutterstock.com/ru/image-illustration/social-media-concept-present-by-hand-111037400

Конфіденційність електронної пошти та веббраузера

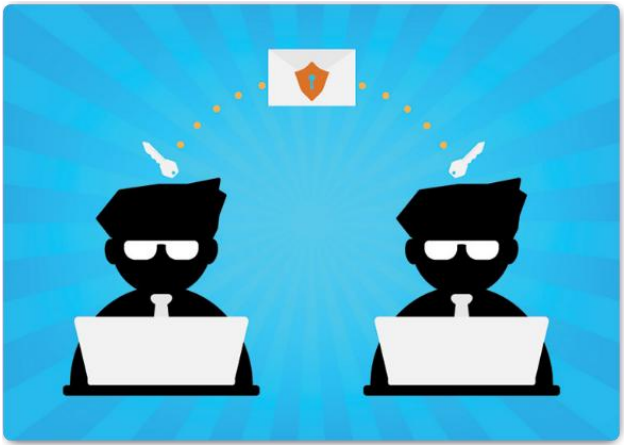


Рис. 4.14. Конфіденційність[49]

Щодня мільйони повідомлень електронної пошти використовуються для спілкування з друзями та ведення бізнесу (рис.4.14). Електронна пошта – це зручний спосіб швидкого спілкування. Коли ви надсилаєте електронного листа, це схоже на відправлення поштової листівки. Повідомлення на листівці під час траспортування потрапляє у поле зору кожного, хто має доступ до неї. Повідомлення електронної пошти також передається у незашифрованому вигляді і може бути прочитане усіма, хто має до нього доступ. Також ці повідомлення передаються між різними серверами поки досягнуть пункту призначення. Навіть коли ви видаляєте свої повідомлення електронної пошти, деякий час вони можуть зберігатися на поштових серверах.

Кожен, хто має фізичний доступ до вашого комп'ютера або маршрутизатора, може бачити, які вебсайти ви відвідали, використовуючи історію веббраузера, кеш-пам'ять та, можливо, файли журналів. Цю проблему можна звести до мінімуму, увімкнувши у веббраузері режим приватного (анонімного) перегляду. Більшість популярних веббраузерів мають свою назву для режиму приватного перегляду:

- **Microsoft Internet Explorer**: InPrivate
- **Google Chrome**: Incognito
- **Mozilla Firefox**: Private tab / private window
- **Safari**: Private: Private browsing

Коли приватний режим увімкнено, файли cookie не зберігаються, тимчасові файли Інтернету та історія веббраузера видаляються після закриття вікна або програми.

Захист вашої історії перегляду вебсторінок може завадити збирати інформацію про ваші дії в Інтернеті. Це дає змогу уникнути цілеспрямованої реклами для заохочення вас до покупок. Навіть в режимі приватного перегляду із забороною використання файлів cookie, компанії розробляють різні способи спостереження за активністю користувачів з метою збору інформації та відстеження їх поведінки.

[49] - https://www.shutterstock.com/ru/image-vector/two-businessman-computer-laptop-send-email-355094873

Наприклад, проміжні пристрої, такі як маршрутизатори, можуть мати інформацію про історію вебсерфінгу користувача.

Зрештою ви відповідаєте за захист ваших даних, комп'ютерних пристроїв і за те, щоб ніхто не видавав себе за вас. Коли ви надсилаєте електронного листа, чи варто вносити до нього записи зі своєї медичної картки? Наступного разу, коли ви мадруватимете Інтернетом, чи безпечно будуть передаватися ваші дані? Кілька простих заходів безпеки можуть позбавити вас від проблем у майбутньому.

ВИСНОВКИ

В темі розглянуто актуальні аспекти інформаційної безпеки та методів захисту персональних пристроїв та особистих даних. Визначено основні фактори, які впливають на безпеку, а також обговорено ефективні способи мінімізації ризиків несанкціонованого доступу або їх втрати.

Ви отримали поради щодо захисту персональних пристроїв, зокрема методи створення надійних паролів, що унеможливлюють несанкціонований доступ до облікових записів. Акцент було зроблено на безпечному використанні бездротових мереж, оскільки вони можуть стати вразливими точками для зловмисників, що намагаються отримати доступ до конфіденційних даних.

Автентифікація також була ключовим моментом аналізу. Розглянуто різні методи автентифікації, такі як двофакторна автентифікація (2FA) та біометричні методи, які значно підвищують рівень безпеки особистих даних. Застосування біометричних методів, таких як сканування обличчя, відбитків пальців або голосу, було відзначено як зручний і надійний спосіб захисту доступу до даних, проте було також відзначено виклики, зокрема питання конфіденційності та необхідність спеціальних технічних засобів.

Отже, підтримка захисту персональних даних потребує поєднання технічних методів, таких як паролі, автентифікація та шифрування, і усвідомленого підходу до власної поведінки в Інтернеті. Завдяки цим заходам можна мінімізувати ризики та захистити свої особисті дані від різних загроз

ТЕРМІНИ І КОНЦЕПЦІЇ

Ця вправа призначена для того, щоб ви могли практикувати важливі терміни та концепції, викладені в темі.

1. Антивірус

- програма, яка сканує комп'ютер на наявність зловмисного програмного забезпечення і видаляє його.

2. Вірус

- знищує дані і може уповільнити роботу комп'ютера.

3. Захист браузера і операційної системи

- використовувати останні оновлення програмного забезпечення та виправлення безпеки.

4. Відключення трансляції SSID

- додатковий бар'єр для виявлення бездротової мережі, що забезпечує мінімальну безпеку.

5. Відкрита авторизація (OAuth)

- відкритий стандартний протокол, який дає змогу кінцевому користувачу отримувати доступ до сторонніх додатків без розкриття його пароля.

6. Двофакторна автентифікація

- на додаток до імені користувача та пароля, вимога другого токена, такого як кредитна карта або номер телефону, для перевірки облікових даних користувача, метод захисту облікових записів, що використовує два рівні перевірки особи для підтвердження доступу.

7. Менеджер паролів

- програмне забезпечення або служба, яка зберігає та шифрує різні та складні паролі для використання онлайновими обліковими записами.

8. Публічна точка доступу Wi-Fi

- публічне місце для доступу в Інтернет, але через неї краще не отримувати доступ до будь-якої конфіденційної приватної інформації та не надсилати її.

9. Резервне копіювання даних

- запобігає втраті цінних даних, використовуючи локальне або хмарне сховище.

10. Shodan

- сканер вебпристроїв.

11. Service Set Identifier (SSID)

- підключення до певної бездротової мережі за допомогою її мережевого ідентифікатора.

12. Способи збереження конфіденційності історії інтернет-перегляду, за допомогою автоматичного відключення файлів cookie, видалення тимчасових інтернет-файлів і видалення історії переглядів після закриття вікна або програми

- Microsoft Internet Explorer: Приватний перегляд, Google Chrome: Інкогніто, Mozilla Firefox: Приватна вкладка / приватне вікно, Safari: Приватний перегляд.

13. Точка доступу

— пристрій або програмне забезпечення, яке дає змогу користувачам підключатися до мережі, зазвичай бездротової. У контексті Wi-Fi, точка доступу (Wi-Fi Access Point) забезпечує зв'язок між пристроями користувачів та основною мережею, підключаючи їх до інтернету або локальної мережі

14. Фаєрвол (брандмауер)

- обладнання або програмне забезпечення, яке не дає змогу хакерам отримувати доступ до ваших особистих даних або даних підприємства.

15. TrickBot — модульне шкідливе програмне забезпечення (троян), яке використовується для крадіжки даних, поширення інших вірусів та здійснення кіберзлочинів.

16. Шифрування (encryption)

- процес перетворення інформації у таку форму, що неавторизована сторона не зможе її прочитати.

17. Шифрування бездротового зв'язку

- включіть безпеку бездротовоїї мережі і використовуйте функцію шифрування WPA2.

18. Шифрована VPN

- зашифроване з'єднання між комп'ютером і VPN-сервером для запобігання перехопленню даних.

19. Шпигунське програмне забезпечення

- стежить за діями користувача в Інтернеті і збирає особисту інформацію без дозволу.

20. Як ви можете зробити файл невідновлюваним?

- Фізично знищити жорсткий диск або пристрій зберігання.

21. Як ви можете створити безпечний пароль?

- Не використовуйте слова й терміни зі словників, або імена будь-якою мовою. Не допускайте поширені орфографічні помилки в словах-паролях. Не використовуйте імена комп'ютерів або коди облікових записів. Якщо це можливо, використовуйте спеціальні символи, такі як ! @ # $ % ^ & * ( ). Використовуйте паролі довжиною не менше десяти символів.

ПРАКТИЧНЕ ЗАВДАННЯ 4.1. СТВОРЕННЯ, ЗБЕРЕЖЕННЯ НАДІЙНИХ ПАРОЛІВ

Цілі завдання

Зрозуміти концепцію надійного пароля.

Частина 1: Дослідження концепцій створення надійного пароля.

Частина 2: Дослідження концепцій безпечного збереження паролів.

Довідкова інформація / Сценарій

Паролі широко використовуються для захисту доступу до ресурсів. Зловмисники можуть використовувати багато методів для вивчення паролів користувачів та отримання несанкціонованого доступу до ресурсів або даних.

Щоб краще захистити себе, важливо розуміти, що робить пароль надійним і як його безпечно зберігати.

Необхідні ресурси

ПК або мобільний пристрій з доступом до Інтернету

ХІД ВИКОНАННЯ

Частина 1: Створення надійного пароля

Надійні паролі мають відповідати вимогам, які перераховані в порядку важливості:

1) Користувач може легко запам’ятати пароль.

2) Для будь-якої іншої людини вгадати цей пароль не є тривіальною задачею.

3) Вгадати або визначити цей пароль не є тривіальною задачею для програми.

4) Пароль має бути складним, містити цифри, символи та суміш літер у верхньому та нижньому регістрах.

Виходячи з зазначеного вище списку, перша вимога, мабуть, є найважливішою, оскільки Вам потрібно Ваш пароль пам’ятати. Наприклад, пароль **#4ssFrX^-aartPOknx25_70!xAdk<d!** вважається надійним, оскільки він задовольняє останнім трьом вимогам, але його дуже важко запам’ятати.

Багато організацій вимагають, щоб паролі містили комбінацію цифр, символів та літер у нижньому та верхньому регістрах. Паролі, які відповідають цій політиці, вважаються придатними для використання, якщо вони легко запам’ятовуються.

Нижче наведено приклад політики створення надійного пароля для типової організації.

Політика:

1) Довжина пароля має бути мінімум 8 символів.
2) Пароль повинен містити символи у верхньому і нижньому регістрах.
3) Пароль має містити число.
4) Пароль має містити неалфавітний символ.

Надайте відповідь на питання: Чи враховуються в політиці перші два пункти вимог створення надійного пароля? Поясніть.

_____

Застосовною практикою створення надійних паролів є вибір чотирьох або більше випадкових слів і їх поєднання. Пароль **televisionfrogbootschurch** надійніший ніж **J0n@than#81**. Зверніть увагу, що, хоча другий пароль відповідає описаним вище правилам, програми зламу паролів дуже ефективні при визначенні цього типу пароля. Хоча багато політик створення паролів не дозволять використання першого пароля, **televisionfrogbootschurch**, він набагато надійніший ніж другий. Користувачу простіше його запам'ятати (особливо якщо він асоціюється з зображенням), він дуже довгий, і фактор випадковості ускладнює визначення такого пароля.

Використовуючи онлайн-інструмент для створення паролів, створіть паролі на основі загальної політики компанії щодо створення паролів, яка була описана вище.

a. Відкрийте веббраузер і перейдіть на http://passwordsgenerator.net

b. Виберіть параметри, які відповідають політиці вибору пароля

c. Згенеруйте пароль

Надайте відповідь на питання: Чи легко запам'ятати згенерований пароль?

_____

Використовуючи онлайн-інструмент для створення паролів, створіть паролі на основі випадкових слів. Зауважте, що оскільки слова з'єднані разом, вони не розглядаються як словникові слова.

d. Відкрийте веббраузер і перейдіть на http://preshing.com/20110811/xkcd-password-generator/

e. Згенеруйте новий пароль з випадкових слів, натиснувши **Generate Another!** у верхній частині вебсторінки.

Надайте відповідь на питання: Чи легко запам'ятати згенерований пароль?

_____

Частина 2: Безпечне зберігання паролів

Якщо користувач вирішить використовувати менеджер паролів, на першу характеристику надійного пароля можна не зважати, оскільки користувач завжди має доступ до менеджера паролів. Зверніть увагу, що деякі користувачі

довіряють свої паролі лише власній пам’яті. Менеджери паролів, як локальні, так і віддалені, використовують сховище паролів, яке може бути скомпрометоване.

Сховище менеджера паролів має бути надійно зашифроване і доступ до нього має жорстко контролюватися. За допомогою програм для мобільних телефонів та вебінтерфейсів, хмарні менеджери паролів надають своїм користувачам у будь-який час безперебійний доступ.

Популярним менеджером паролів є LastPass

Створіть пробний обліковий запис LastPass:

a. Відкрийте веббраузер і перейдіть на https://lastpass.com/

b. Натисніть **Start Trial** для створення пробного облікового запису.

c. Заповніть поля, як зазначено в інструкції.

d. Встановіть майстер-пароль. Цей пароль дає вам доступ до вашого облікового запису LastPass.

e. Завантажте та встановіть клієнта LastPass відповідно до своєї операційної системи.

f. Відкрийте клієнт і увійдіть до системи за допомогою майстер-пароля LastPass.

g. Дослідіть менеджер паролів LastPass.

Надайте відповідь на питання:

1. Коли ви додасте паролі до LastPass, де вони зберігаються?

2. Окрім вас, щонайменше, один інший суб’єкт має доступ до паролів. Хто цей суб’єкт?

3. Хоча зберігати всі Ваші паролі в одному місці може бути досить зручно, є недоліки у цьому підході. Як Ви думаєте, які недоліки?

Частина 3: Що тепер для Вас означає надійний пароль?

Використовуючи характеристики надійного пароля, наведені на початку цієї роботи, виберіть пароль, який легко запам’ятати, але важко вгадати. Складність паролів важлива, якщо вона не впливає на більш важливі вимоги, такі як придатність для легкого запам’ятовування.

Якщо використовується менеджер паролів, вимога до простоти запам’ятовування може бути скасована.

Короткий підсумок:

Обирайте пароль, який можете легко запам’ятати.

Обирайте пароль, який ніхто не зможе асоціювати з Вами.

Обирайте різні паролі та ніколи не використовуйте один і той самий пароль для різних сервісів. Складність паролів – це застосовна практика доти, доки не виникають проблеми з їх запам’ятовуванням.

КОНТРОЛЬНА РОБОТА ДО ТЕМИ 4

Ця контрольна робота охоплює матеріал теми. Вона призначена для надання додаткових можливостей попрактикувати навички та знання, подані у темі і підготовки до іспиту.

1. Як можуть користувачі, що працюють на комп'ютері, відкритому для спільного використання, приховати історію своїх вебпереглядів від інших працівників, які також можуть використовувати цей комп'ютер?

– для доступу до вебсайтів використовувати лише зашифроване з'єднання

– перезавантажити комп'ютер після закриття веббраузера

– використовувати веббраузер у режимі приватного (анонімного) перегляду

– перемістити завантажені файли у кошик

Пояснення

Коли користувач комп'ютера переглядає вебсторінку в приватному (анонімному) режимі, відбувається таке:

– відключаються файли cookie;

– тимчасові Інтернет-файли видаляються після закриття вікна;

– історія перегляду видаляється після закриття вікна.

використовувати веббраузер у режимі приватного (анонімного) перегляду

2. Як користувач може завадити іншим прослуховувати мережевий трафік під час роботи ПК через загальнодоступну точку доступу Wi-Fi?

– з'єднуватися з використанням служби VPN

– використовувати шифрування WPA2

– відключити Bluetooth

– створити сильні та унікальні паролі

Пояснення

Коли користувач з'єднується через зашифрований VPN-тунель у загальнодоступній мережі Wi-Fi, будь-які дані, що надсилаються або отримуються від користувача, залишатимуться нерозпізнаними.

з'єднуватися з використанням служби VPN

3. Чому пристрої IoT становлять більший ризик, ніж інші пристрої в мережі?

– більшість пристроїв IoT не отримують частого оновлення мікропрограми

– більшість пристроїв IoT не потребують підключення до Інтернету та не можуть отримувати нові оновлення

– для пристроїв IoT потрібні незашифровані бездротові з'єднання

– IoT-пристрої не можуть функціонувати в ізольованій мережі з єдиним підключенням до Інтернету

Пояснення

Пристрої IoT зазвичай використовують свою оригінальну прошивку та не отримують оновлення так часто, як ноутбуки, настільні комп'ютери та мобільні платформи.

більшість пристроїв IoT не отримують частого оновлення мікропрограми

4. Споживач хоче роздрукувати фотографії, що зберігаються на обліковому записі у хмарному сховищі використовуючи службу друку в Інтернеті третьої сторони. Після успішного входу в обліковий запис у хмарі клієнтові автоматично надають доступ до служби онлайн-друку третьої сторони. Що дозволило виконати цю автоматичну автентифікацію?

– користувач перебуває у незашифрованій мережі і пароль служби хмарного зберігання доступний для перегляду службі онлайн-друку

– інформація про обліковий запис для служби хмарного зберігання була перехоплена шкідливою програмою

– служба хмарного зберігання є довіреним програмним забезпеченням для служби онлайн-друку

– пароль, введений користувачем для служби онлайн-друку, аналогічний пароля, який використовується в службі хмарного зберігання

Пояснення

Відкрита авторизація (OAuth)- відкритий стандартний протокол, який дає змогу кінцевим користувачам отримувати доступ до сторонніх програм без застосування пароля користувача.

служба хмарного зберігання є довіреним програмним забезпеченням для служби онлайн-друку

5. Яке налаштування на бездротовому маршрутизаторі вважається нестандартним з точки зору безпеки бездротової мережі?

– активація бездротової безпеки

– застосування шифрування WPA2

– зміна стандартного SSID та пароля бездротового маршрутизатора

– заборона широкомовної трансляції SSID

Пояснення

Бездротовий маршрутизатор може бути налаштований таким чином, щоб заборонити передачу SSID, але ця конфігурація не вважається належною з точки зору безпеки бездротової мережі.

заборона широкомовної трансляції SSID

6. Яка технологія дає змогу користувачу уникнути витрат на обладнання та технічне обслуговування при створенні резервних копій даних?

– мережеве сховище (network attached storage)

– зовнішній жорсткий диск

– хмарний сервіс

– магнітна стрічка

Пояснення

Вартість зберігання у хмарі зазвичай залежить від обсягу необхідного місця для зберігання. Провайдер хмарного сервісу буде підтримувати обладнання, а користувач хмари матиме доступ до резервних даних.

хмарний сервіс

7. Який найкращий спосіб запобігти несанкціонованому використанню вашого Bluetooth?

– використовуйте Bluetooth лише під час під'єднання до відомого SSID

– завжди відключайте Bluetooth, коли він активно не використовується

– використовуйте Bluetooth лише для підключення до смартфона або планшета

– завжди використовуйте VPN під час з'єднання з Bluetooth

Пояснення

Bluetooth – це бездротова технологія, яку хакери можуть використовувати для прослуховування, встановлення віддаленого контролю доступу та поширення шкідливих програм. Користувач повинен вимикати Bluetooth, коли він не використовується.

завжди відключайте Bluetooth, коли він активно не використовується

8. Користувачеві важко запам'ятовувати паролі для декількох облікових записів у Інтернеті. Яке найкраще рішення варто спробувати користувачеві для вирішення цієї проблеми?

– повідомити паролі адміністратору мережі або комп'ютерному спеціалісту

– створити єдиний надійний пароль, який буде використовуватися для усіх облікових записів у Інтернеті

– записати паролі на папері й ретельно їх заховати

– зберегти паролі в централізованій програмі менеджера паролів

Пояснення

Менеджер паролів може використовуватися для зберігання та шифрування декількох паролів. Майстер-пароль може застосовуватися для захисту програмного забезпечення менеджера паролів.

зберегти паролі в централізованій програмі менеджера паролів

9. Який тип технології може запобігти зловмисному програмному забезпеченню відстежувати дії користувачів, збирати особисту інформацію та створювати небажані оголошення, що з'являються на комп'ютері користувача?

– антишпигунське ПЗ (antispyware)

– двофакторна автентифікація

– фаєрвол (брандмауер)

– менеджер паролів

Пояснення

Антишпигунське ПЗ (Antispyware) зазвичай встановлюється на машині користувача для сканування та видалення шкідливих програм, встановлених на пристрої.

антишпигунське ПЗ (antispyware)

10. Користувач працює в Інтернеті, використовуючи ноутбук та загальнодоступний WiFi у кафе. Що слід перевірити перш ніж підключитися до загальнодоступної мережі?

– чи веббраузер ноутбука працює у приватному режимі**?**

– чи ноутбук вимагає автентифікації користувача для спільного використання файлів і медіа**?**

– чи відімкнено адаптер Bluetooth на ноутбуці**?**

– чи встановлено на ноутбуці майстер-пароль для захисту паролів, що зберігаються у менеджері паролів**?**

Пояснення

Коли користувач під'єднується до загальнодоступної мережі, важливо знати, чи комп'ютер налаштований для спільного використання файлів і

мультимедіа, а також чи потрібна при цьому автентифікація користувача разом з шифруванням.

Чи ноутбук вимагає автентифікації користувача для спільного використання файлів і медіа

11. При зберіганні інформації на локальному жорсткому диску який спосіб захистить дані від несанкціонованого доступу?

– створення копії жорсткого диска

– двофакторна автентифікація

– видалення важливих файлів

– шифрування даних

Пояснення

Шифрування даних – це процес перетворення даних у форму, за якої лише довірена, уповноважена особа з секретним ключем або паролем може розшифрувати дані та отримати доступ до їх оригінального вигляду.

шифрування даних

12. Адміністратор мережі проводить тренінг для співробітників офісу про те, як створити надійний і ефективний пароль. Який пароль, найімовірніше, буде найважче вгадати або зламати злочинцеві?

– drninjaphd

– 10characters

– super3secret2password1

– mk$$cittykat104#

Пояснення

Обираючи надійний пароль:

– не використовуйте слова зі словника або імена будь-якою мовою

– не використовуйте поширені орфографічні помилки у словах зі словника

– не використовуйте назви комп'ютера або облікових записів

*– якщо це можливо, використовуйте спеціальні символи, такі як ! @ # $ % ^ & * ( )*

– використовуйте пароль з десяти або більше символів

mk$$cittykat104#

ДОДАТКОВІ РЕСУРСИ ТА ЗАВДАННЯ

Всі ваші пристрої можуть бути зламані

Використання електроніки в людському тілі перетворює тіло людини в кібермішень, як і будь-який комп'ютер або мобільний телефон. На конференції TEDx MidAtlantic в 2011 році Аві Рубін (Avi Rubin) пояснив, як хакери компрометують автомобілі, смартфони і медичні пристрої. Він попередив нас про зростаючу небезпеку «зламаного» світу. Для отримання додаткової інформації дивіться презентацію пана Рубіна за цим посиланням: https://www.ted.com/talks/avi_rubin_all_your_devices_can_be_hacked?subtitle=en

OnGuard Online

На цьому вебсайті представлена велика кількість інформації про те, як залишатися в безпеці в Інтернеті, наприклад, захищати комп'ютери, уникати шахрайства, бути обережно поводити себе онлайн і захищати дітей в Інтернеті. https://www.onguardonline.gov/

Національний інститут стандартів і технологій (National Institute of Standards and Technology, NIST)

Президент Обама видав виконавчий наказ 13636 (EO) «Покращення безпеки критично важливої інфраструктури». Відповідно до цього наказу NIST було доручено роботу із зацікавленими сторонами для розробки добровільних рамок, включаючи стандарти, керівні принципи і передові методи з метою зниження кіберризиків для критичної інфраструктури. Щоб дізнатися більше про це, а також фреймворк NIST, перейдіть за посиланням: https://www.nist.gov/cyberframework

Microsoft

Стаття, розміщена за посиланням https://www.microsoft.com/uk-ua/security/business/security-101/what-is-two-factor-authentication-2fa пояснює, як двофакторна автентифікація допомагає захищати дані користувача та забезпечує безпеку облікових записів через різноманітні методи автентифікації, зокрема SMS, біометричні дані та інші методи. Сторінка запрошує дізнайтися більше про Захисний комплекс Microsoft

На каналі YouTube можна знайти багато корисних відеороликів, які демонструють, як працюють методи 2FA, як налаштувати їх для вашого облікового запису та як вони забезпечують додаткову безпеку. Відеоролик «Двофакторна автентифікація. Що таке 2FA? Як включити двоетапну перевірку в Google?» є одним з найпопулярніших на каналі за тематикою двофакторної автентифікації. https://www.youtube.com/watch?v=ldof5C8Ls5c

ТЕМА 5. ШИФРУВАННЯ ТА ПРИХОВУВАННЯ ДАНИХ

У темі описуються криптографічні методи захисту інформації. Наведені історичні відомості виникнення та подальшого розвитку криптографії. Розглядаються проблеми використання криптостійких алгоритмів для ускладнення несанкціонованого доступу кіберзлочинців до захищеної інформації. Дається опис та поради щодо застосування сучасних алгоритмів шифрування.

Також у цій темі розкривається питання несанкціонованого доступу неавторизованих користувачів до об'єктів, обладнання та інших ресурсів організацій.

Окремим пунктом розглянуто Технології маскування та виявлення даних.

5.1. КРИПТОГРАФІЯ

Криптологія – це наука про створення і злам секретних кодів. Криптографія – це спосіб зберігання та передачі даних (рис.5.1), який дає змогу читати або обробляти ці дані тільки одержувачу, якому вони були призначені. Сучасна криптографія використовує обчислювально криптостійкі алгоритми, щоб ускладнити несанкціонований доступ кіберзлочинців до захищеної інформації.

Рис.5.1. Криптографічне повідомлення[50]

Захищеність даних забезпечує конфіденційність, тобто прочитати повідомлення зможе тільки одержувач, якому воно призначене. Сторони досягають цього шляхом шифрування. Шифрування – це процес кодування даних таким чином, щоб неавторизована третя сторона не змогла їх прочитати.

При використанні шифрування даних, відкритий текст називають звичайним або відкритим (plaintext або cleartext), а зашифровану версію – кодованим або криптограмою (ciphertext). Шифрування перетворює читабельне повідомлення з відкритим текстом в зашифрований текст, який є нечитабельним, замаскованим повідомленням. Розшифрування є зворотнім процесом. Для шифрування також потрібен ключ, який відіграє головну роль в шифруванні і розшифруванні повідомлення. Людина, яка володіє ключем, зможе розшифрувати криптограму і отримати відкритий текст.

[50] – https://encrypted-tbn0.gstatic.com/images?q=tbn:ANd9GcTj1yZ6N3tag-cc7k0S_0bzqwlbN8PU5ag_jGSAEkSCfb-A176i

В історії є приклади використання різних алгоритмів і методів шифрування. Алгоритм – це процес або формула, що використовуються для вирішення поставленої задачі. Кажуть, що Юлій Цезар використовував захищені повідомлення, які отримував, розмістивши два набори алфавіту поруч, і зсунувши один з них на певну кількість позицій. Як ключ використовувалася ця кількість позицій. За допомогою цього ключа він перетворював відкритий текст у зашифрований і тільки його полководці, у яких також був ключ, могли розшифрувати повідомлення. Цей метод називають шифром Цезаря.

Історія криптографії почалася в дипломатичних колах ще кілька тисяч років тому. Королівські гінці передавали зашифровані повідомлення до інших королівств. Іноді сусіди, які не брали участі у переписці, намагалися викрасти повідомлення, відправлені до ворожого королівства. Незабаром після цього, військові командири почали використовувати шифрування для захисту повідомлень.

Протягом століть різні методи шифрування, фізичні пристрої та допоміжні засоби використовувалися для шифрування і розшифровки текстів:

- Скитала (Scytale) (рис. 5.2);
- Шифр Цезаря;
- Шифр Віженера;
- Шифрувальна машина Enigma.

Рис. 5.2. Скитала[51]

І хоча ці методи використовувалися в різні епохи, кожен з них продовжує впливати на розвиток сучасних криптографічних систем. Всі методи шифрування використовують ключ для шифрування або розшифрування повідомлення. Ключ є важливим компонентом алгоритму шифрування. Надійність алгоритму шифрування напряму залежить від надійності ключа, який він використовує. Чим складніший ключ, тим більш безпечний алгоритм. Керування ключами є важливою частиною цього процесу.

Кожен метод шифрування використовує спеціальний алгоритм, який називають шифром, для шифрування і розшифрування повідомлень. Шифр – це низка чітко визначених кроків, які використовуються для шифрування/розшифрування повідомлень. Існує кілька способів створення зашифрованого тексту.

[51] – https://upload.wikimedia.org/wikipedia/commons/thumb/5/51/Skytale.png/1200px-Skytale.png

Транспозиція, або перестановка – літери міняють місцями (рис. 5.3).

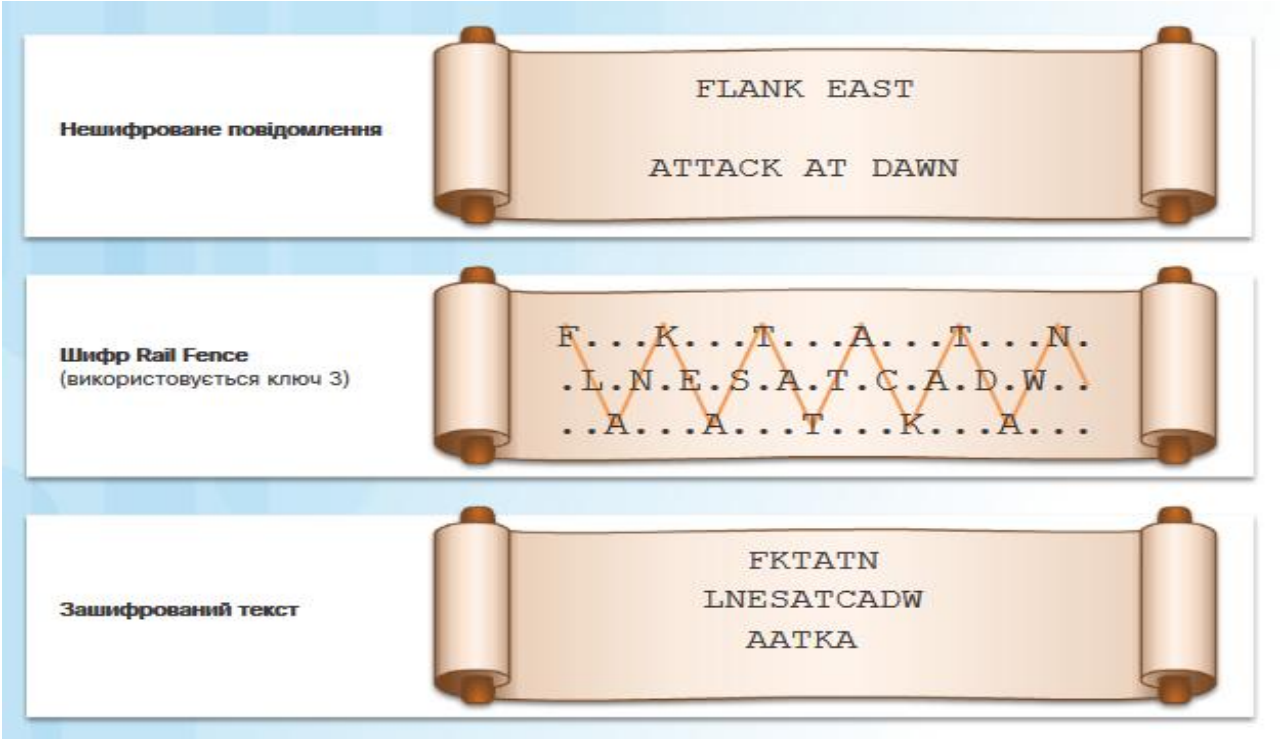


Рис. 5.3. Транспозиція, або перестановка[52]

Заміна або підстановка – літери замінені (рис. 5.4).

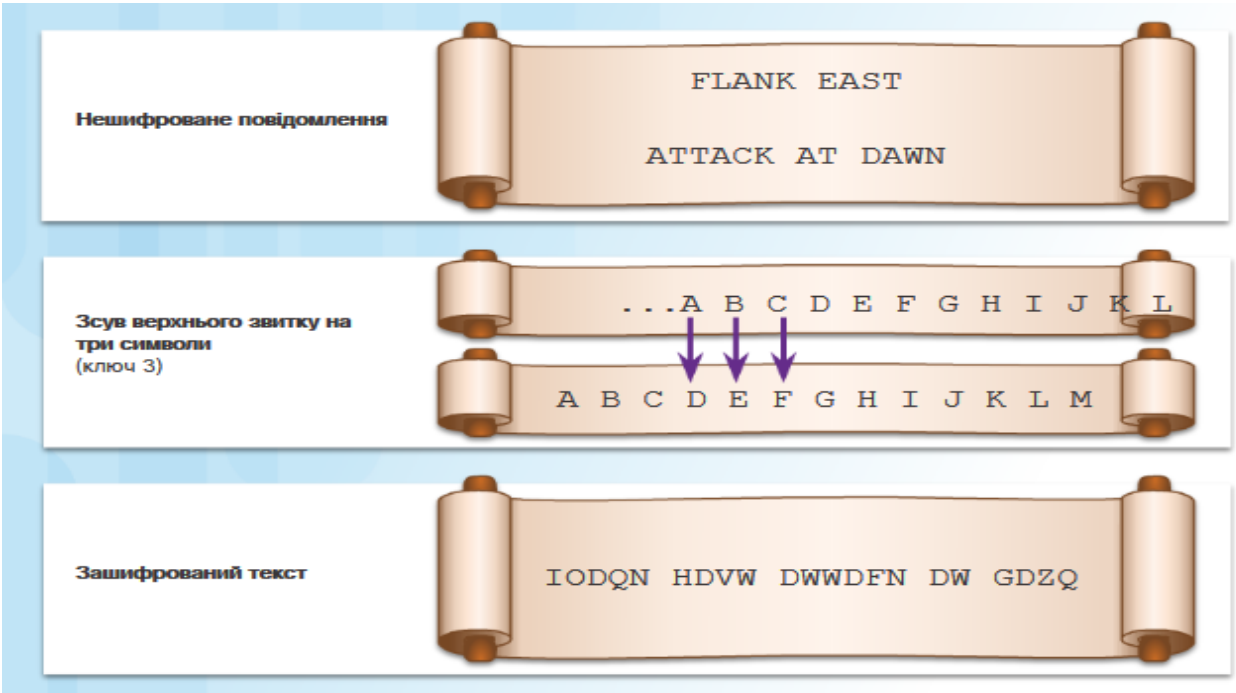


Рис. 5.4. Заміна або підстановка[53]

[52] – https://duchm72.files.wordpress.com/2015/07/20150721-1-4.png

[53] – за мотивами https://quantrimang.com/cong-nghe/he-thong-mat-ma-phan-2-dich-vu-mat-ma-190634

Схема одноразових шифроблокнотів (One-time pad) – відкритий текст в поєднанні з секретним ключем створює новий символ, який потім об’єднується з відкритим текстом для створення криптограми (рис. 5.5).

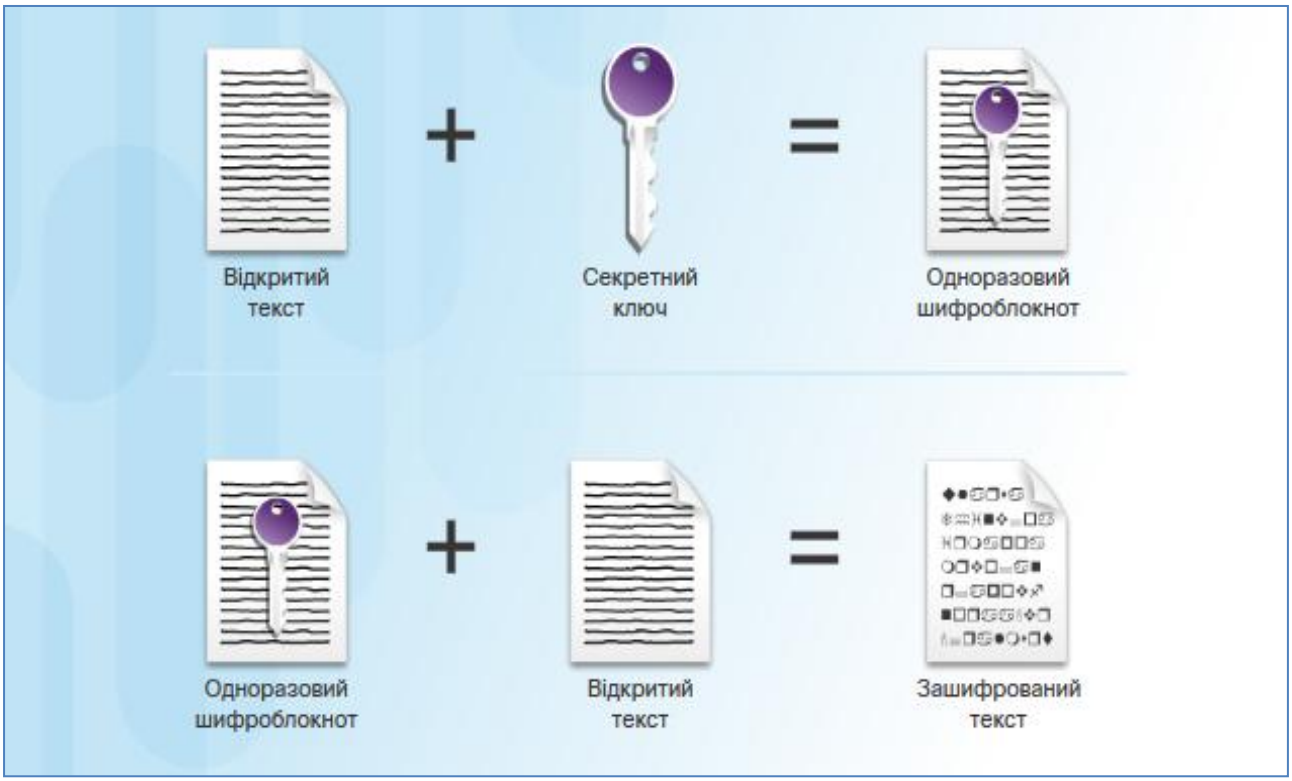


Рис. 5.5. Схема одноразових шифроблокнотів[54]

В старих алгоритмах шифрування, таких як шифр Цезаря або шифрувальна машина Enigma, конфіденційність забезпечувалася секретністю самого алгоритму. З розвитком технологій зворотне перетворення стало занадто легким, тому зараз використовують стійкі загальнодоступні алгоритми. При використанні більшості сучасних алгоритмів успішне розшифрування потребує знання відповідних криптографічних ключів. Це означає, що безпека шифрування полягає в секретності ключів, а не алгоритмів.

Деякі сучасні алгоритми шифрування як і раніше використовують транспозицію як частину алгоритму.

Керування ключами – найскладніший аспект проектування криптосистеми. Багато криптосистем зазнали краху через помилки в керуванні ключами. Всі сучасні криптографічні алгоритми містять обов’язкові процедури керування ключами. На практиці більшість атак на криптографічні системи спрямовані на систему керування ключами, а не на сам криптографічний алгоритм.

[54] – за мотивами https://interface31.ru/tech_it/assets_c/2016/11/introduction-to-cryptography-007-thumb-600xauto-7792.png

Криптографічне шифрування може забезпечити конфіденційність завдяки поєднання різних інструментів і протоколів.

Існує два підходи до підтримки безпеки даних при використанні шифрування. Перший – захистити алгоритм. Якщо безпека системи шифрування залежить від секретності самого алгоритму, то важливіше за все зберегти тайну алгоритму будь-якою ціною. Якщо хтось розкриє деталі роботи алгоритму, всім учасникам доведеться змінити алгоритм. Цей підхід не виглядає дуже надійним і керованим. Другий підхід – захистити ключі. В сучасній криптографії алгоритми є загальнодоступними. Секретність даних забезпечують криптографічні ключі. Криптографічні ключі – це паролі, які поступають на вхід алгоритму шифрування разом з даними, які необхідно зашифрувати.

Алгоритми шифрування поділяються на два класи:

Симетричні алгоритми використовують один і той самий заздалегідь відомий ключ (спільний ключ), іноді його називають парою секретних ключів, для шифрування і розшифрування даних. Як відправник, так і одержувач знають спільний ключ перед початком передачі будь-якого зашифрованого повідомлення. Симетричні алгоритми використовують один і той самий ключ для шифрування і розшифрування тексту. Алгоритми шифрування, які використовують спільний ключ, простіші і потребують менше обчислювальної потужності.

Асиметричні алгоритми шифрування – використовують один ключ для шифрування даних, а іншій ключ для розшифрування даних. Один з ключів є відкритим, а інший – закритим. В системі шифрування з відкритим ключем будь-яка людина може шифрувати повідомлення з використанням відкритого ключа одержувача, але тільки цей одержувач зможе розшифрувати його за допомогою свого закритого ключа. Сторони обмінюються захищеними повідомленнями без необхідності попереднього погодження спільного ключа. Асиметричні алгоритми більш складні. Ці алгоритми є ресурсоємними і більш повільними у виконанні.

5.2. СИМЕТРИЧНЕ ТА АСИМЕТРИЧНЕ ШИФРУВАННЯ

Симетричне шифрування

Симетричні алгоритми шифрування використовують один спільний ключ для шифрування і розшифрування даних. Цей метод також відомий як шифрування з закритим ключем.

Наприклад, Аліса і Боб живуть в різних місцях і хочуть обмінюватися секретними повідомленнями через поштову систему. Аліса хоче відправити Бобу секретне повідомлення.

Шифрування з закритим ключем використовує симетричний алгоритм. Аліса і Боб мають однакові ключі від одного замка. Обмін ключами відбувся до відправки будь-яких секретних повідомлень. Аліса пише секретне повідомлення і покладе його в маленьку коробку, яку закриє на замок. Вона відправляє коробку Бобу. Повідомлення всередині коробки у безпеці, поки вона йде через поштову систему. Коли Боб отримує коробку, він відкриває замок своїм ключем і виймає повідомлення. Боб може використати ті самі коробку і замок, щоб відправити секретну відповідь Алісі (рис. 5.6).

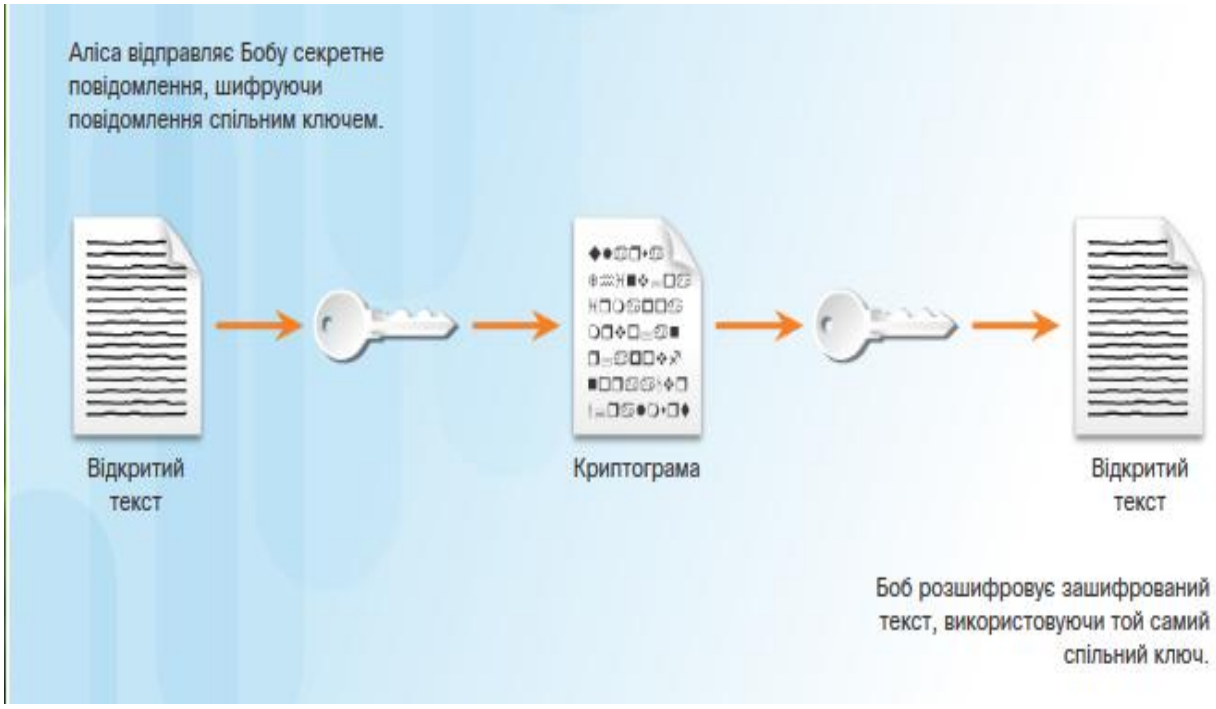


Рис. 5.6. Шифрування з закритим ключем[55]

Якщо Боб хоче поговорити з Керол, то йому потрібен новий спільний ключ для цього спілкування і він має тримати його в секреті від Аліси. Чим більша кількість людей, з якими Боб хоче спілкуватися приватно, тим більше ключів йому потрібно.

Найбільш поширеними типами криптографічних перетворень є блокові і потокові шифри. Ці методи відрізняються тим, як вони групують біти даних під час шифрування.

Блокові шифри

Блокові шифри перетворюють блок відкритого тексту фіксованої довжини в блок криптограми розміром 64 або 128 біт. Розмір блоку – це обсяг даних, які шифруються за один раз. Щоб розшифрувати цей зашифрований текст, застосуйте зворотне перетворення до блоку зашифрованого тексту, використовуючи той самий секретний ключ (рис. 5.7).

[55] – https://btu.edu.eg/wp-content/uploads/2020/03/Chapter-4-The-Art-of-Protecting-Secrets.pdf

Блочні шифри зазвичай характеризуються тим, що вихідні дані більші за вхідні, тому що розмір криптограми має бути кратним розміру блоку. Наприклад, стандарт шифрування даних (DES – Data Encryption Standard) є симетричним алгоритмом, який шифрує блоки 64-бітними фрагментами з використанням 56-бітного ключа. Для цього блоковий алгоритм бере дані по одному фрагменту за раз, наприклад, по 8 байтів, поки весь блок не буде заповнений. Якщо вхідних даних менше, ніж один повний блок, алгоритм додає штучні дані або пробіли, поки не використає всі 64 біти повністю.

Рис. 5.7. Блокове шифрування [56]

Потокові шифри

На відміну від блокових шифрів, потокові шифрують відкритий текст по одному байту або біту за один раз (рис. 5.8). Потокові шифри можна розглядати як блокові з розміром блоку в один біт. За допомогою потокового шифру перетворення цих менших одиниць відкритого тексту виконується по різному в залежності від їх розташування в потоці тексту, що шифрується. Потокові шифри можуть бути набагато швидшими, ніж блокові шифри, і зазвичай не збільшують розмір повідомлення, оскільки можуть шифрувати довільне число бітів.

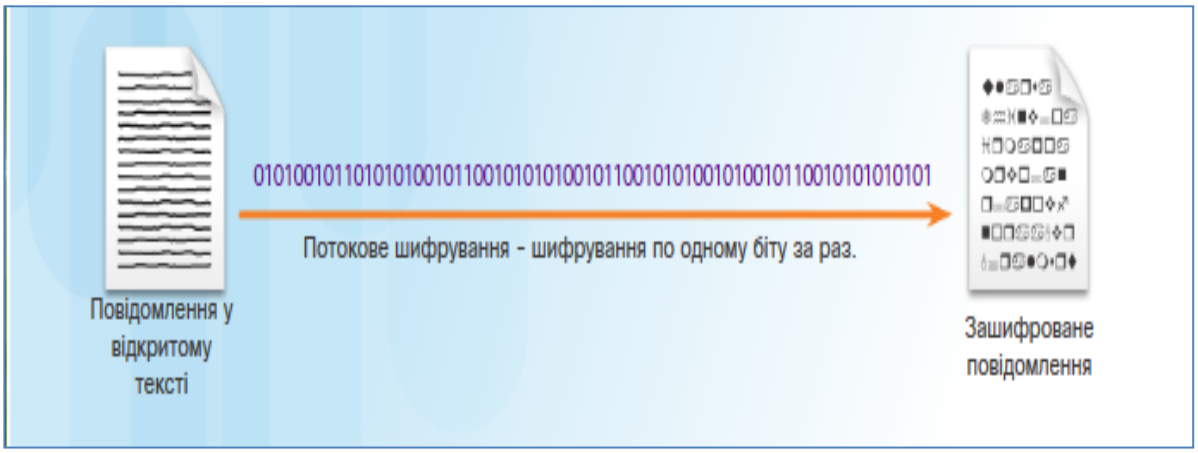


Рис. 5.8. Потокове шифрування[57]

[56, 57] – This figure was uploaded by researchgate.net

A5 – це потоковий шифр, який забезпечує конфіденційність голосового зв'язку і шифрує мобільний зв'язок. DES також можна використовувати в режимі потокового шифрування.

Складні криптографічні системи можуть комбінувати блочну та потокову обробку в одному процесі.

Багато криптографічних систем використовують симетричне шифрування. Розглянемо деякі з поширених криптографічних стандартів, які використовують симетричне шифрування:

3DES (Triple DES): Digital Encryption Standard (DES) – це симетричний блоковий шифр із 64-бітовим розміром блоку, який використовує 56-бітний ключ. В якості вхідних даних він приймає 64-бітний блок відкритого тексту, а на виході видає 64-бітний блок зашифрованого тексту. Алгоритм завжди працює з блоками однакового розміру і використовує як перестановки, так і заміни. Перестановка – це спосіб впорядкування всіх елементів набору.

Triple DES шифрує дані тричі і використовує інший ключ для хоча б одного з трьох проходів. Таким чином сумарний розмір ключа становить 112-168 біт. Алгоритм 3DES більш стійкий до атак, але набагато повільніший, ніж DES.

Цикл шифрування 3DES виглядає таким чином:

1. Дані шифруються першим проходом DES.
2. Дані дешифруються другим проходом DES.
3. Дані повторно шифруються третім проходом DES.

Для розшифровки криптограми використовується зворотній процес.

IDEA: Міжнародний алгоритм шифрування даних (The International Data Encryption Algorithm), який використовує 64-бітові блоки і 128-бітові ключі. IDEA виконує вісім циклів перетворень кожного з 16 блоків, які є результатом поділу кожного 64-бітного блоку. Алгоритм IDEA замінив DES і тепер використовується в PGP (Pretty Good Privacy). PGP – це програма, яка забезпечує конфіденційність і автентифікацію під час передачі даних. GNU Privacy Guard (GPG) є безкоштовною версією PGP з вільною ліцензією.

AES: Вдосконалений стандарт шифрування (The Advanced Encryption Standard) має фіксований розмір блоку 128 біт з розміром ключа 128, 192 або 256 біт. Національний інститут стандартів і технологій США (NIST) затвердив алгоритм AES в грудні 2001 року. Уряд США використовує AES для захисту секретної інформації.

AES – стійкий алгоритм, який використовує довші ключі. AES швидший за DES і 3DES, тому він використовується в рішеннях для програмних застосунків, а також в апаратному забезпеченні міжмережевих екранів та маршрутизаторах.

Серед інших блокових шифрів можна згадати Skipjack (розроблений NSA), Blowfish і Twofish.

Асиметричне шифрування

Асиметричне шифрування, також відоме як шифруванням з відкритим ключем, для шифрування використовує ключ, який відрізняється від ключа для розшифрування. Злочинець не може в прийнятні терміни обчислити ключ дешифрування, знаючи ключ шифрування і навпаки.

Якщо Аліса і Боб обмінюються секретними повідомленнями за допомогою шифрування з відкритим ключем, вони використовують асиметричний алгоритм. На цей раз Боб і Аліса не обмінюються ключами до відправки секретних повідомлень. Замість цього у Боба і Аліси є окремі замки з відповідними ключами. Якщо Аліса надсилає секретне повідомлення Бобу, вона має спочатку зв'язатися з ним і попросити його надіслати свій відкритий замок. Боб надсилає замок, але зберігає свій ключ. Коли Аліса отримує замок, вона пише своє секретне повідомлення і вкладає його в маленьку коробку. В ту ж коробку вона кладе свій відкритий замок, але залишає у себе свій ключ. Потім вона замикає коробку замком Боба. Коли Аліса закриє коробку, вона більше не зможе її відкрити, тому що у неї немає ключа до цього замка. Вона відправляє коробку Бобу, і, поки відправлення проходить через поштову систему, ніхто не зможе її відкрити. Коли Боб отримує коробку, він може відкрити її своїм ключем і отримати повідомлення від Аліси. Щоб відправити секретну відповідь, Боб кладе своє секретне повідомлення в коробку разом зі своїм відкритим замком і блокує коробку замком Аліси. Боб відправляє закриту коробку назад Алісі (рис. 5.9).

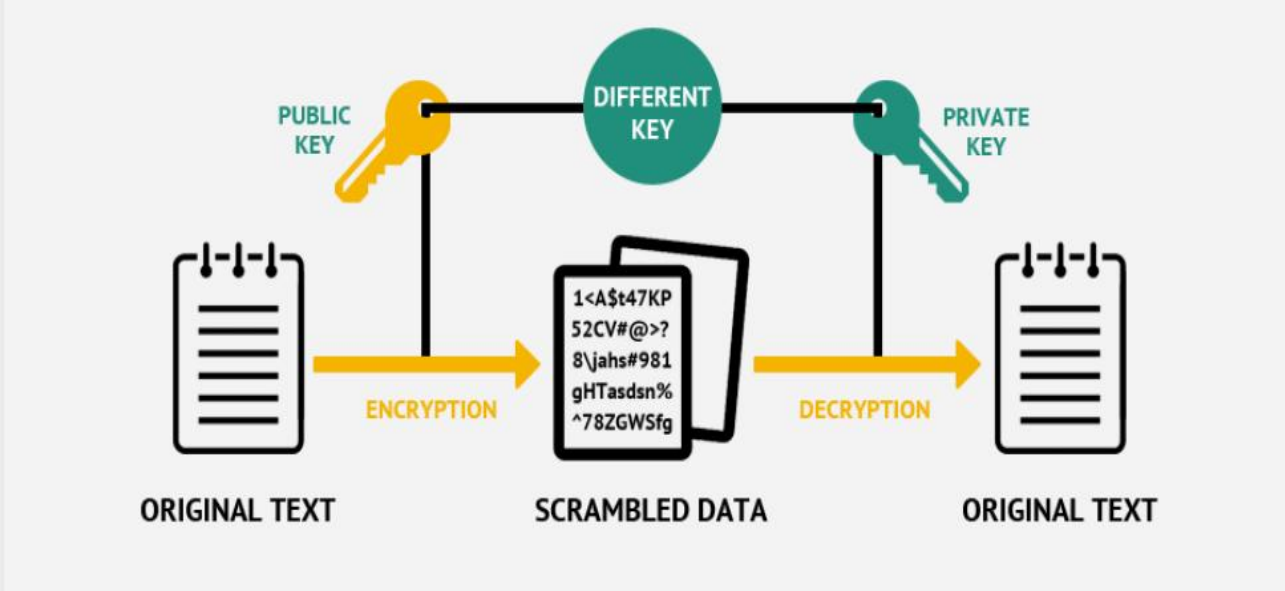


Рис. 5.9. Асиметричне шифрування[58]

[58] – https://www.hiclipart.com/free-transparent-background-png-clipart-fyxon

Наприклад, Аліса запитує і отримує відкритий ключ Боба. Аліса використовує відкритий ключ Боба для шифрування повідомлення з використанням узгодженого заздалегідь алгоритму. Аліса відправляє зашифроване повідомлення Бобу, а Боб використовує свій закритий ключ для дешифрування повідомлення.

Асиметричні алгоритми використовують відомі загальнодоступні формули. Пара незв'язаних ключів робить ці алгоритми безпечними. Розглянемо кілька асиметричних алгоритмів:

RSA Рівест-Шамір-Адлеман (Rivest-Shamir-Adleman) використовує добуток двох дуже великих простих чисел однакової довжини – від 100 до 200 цифр. Браузери використовують RSA для встановлення безпечного з'єднання.

Протокол Діффі-Хеллмана (Diffie-Hellman) забезпечує метод електронного обміну секретним ключем. Алгоритм Діффі-Хеллмана використовують такі захищені протоколи, як Secure Sockets Layer (SSL), Transport Layer Security (TLS), Secure Shell (SSH) та Internet Protocol Security (IPsec).

Схема Эль-Гамаля (ElGamal) лежить в основі державного стандарту США для цифрових підписів. Цей алгоритм є безкоштовним для використання, оскільки він не запатентований.

Еліптична криптографія (ECC) використовує еліптичні криві як частину алгоритму. У США Агентство національної безпеки використовує ECC для генерації цифрового підпису та обміну ключами.

5.3. ПОРІВНЯННЯ ТИПІВ ШИФРУВАННЯ

Керування ключами складається зі створення, обміну, зберігання, використання і заміни ключів, що використовуються в алгоритмі шифрування.

Керування ключами – найскладніша частина проектування криптосистеми. Багато криптосистем були зламані через помилки в керуванні ключами. На практиці більшість атак на криптографічні системи націлені на рівень керування ключами, а не на сам криптографічний алгоритм.

Існує кілька основних характеристик керування ключами, які потрібно враховувати:

- Генерація ключів;
- Перевірка ключів;
- Обмін ключами;
- Зберігання ключів;
- Час життя ключів;
- Скасування і знищення ключів.

Для опису ключів використовуються два терміни:

- **Довжина ключа (Key length)** – також називається розміром ключа, вимірюється в бітах.
- **Простір ключів (Keyspace)** – це кількість можливих варіантів ключів, які дає змогу генерувати конкретна довжина ключа.

Зі зростанням довжини ключа простір ключів збільшується експоненціально. Простір ключів алгоритму це набір усіх можливих значень ключа. Довші ключі більш надійні, проте вони також більш ресурсоємні. В просторі ключів практично кожного алгоритму є кілька слабких ключів, які дають змогу зловмиснику зламати шифр прискореним методом.

Важливо розуміти різницю між симетричними та асиметричними методами шифрування. Симетричні системи шифрування більш ефективні і можуть обробляти більше даних. Однак керування ключами у симетричних системах шифрування складніше. Асиметрична криптографія більш ефективна для захисту конфіденційності невеликих обсягів даних. Це робить більш безпечним обмін електронними ключами, який має невеликий обсяг даних. У той же час це не підходить для шифрування великих блоків даних.

Збереження конфіденційності важливе для даних, як під час зберігання, так і в процесі передавання. В обох випадках симетричному шифруванню надають перевагу через його швидкість і простоту алгоритму. Деякі асиметричні алгоритми можуть значно збільшити розмір зашифрованого об’єкта. Тому для даних, що передаються, використовуйте криптографію з відкритим ключем під час обміну секретним ключем, а потім симетричну криптографію для забезпечення конфіденційності відправлених даних.

Існує багато варіантів застосування як симетричних, так і асиметричних алгоритмів.

Токен, який генерує одноразові паролі, – це апаратний пристрій, у якому для генерації одноразового пароля застосовується криптографія. Одноразовий пароль – це автоматично згенерований цифровий або буквено-цифровий рядок символів, який автентифікує користувача тільки для однієї транзакції і тільки під час одного сеансу. Пароль змінюється приблизно кожні 30 секунд. Пароль сеансу відображається на дисплеї пристрою і користувач вводить його для входу.

В індустрії електронних платежів використовується алгоритм 3DES. Операційні системи використовують DES для захисту файлів користувача і системних даних за допомогою паролів. Більшість шифруваних файлових систем, таких як NTFS, використовують стандарт AES.

Алгоритми з асиметричним ключем використовуються у чотирьох протоколах:

- ***Інтернет-обмін ключами*** (Internet Key Exchange) (***IKE***), який є основним компонентом мереж VPN, що використовують протокол IPsec.
- ***Захищені роз'єми*** Secure Socket Layer (***SSL***), який є засобом реалізації криптографії у веббраузері.
- ***Захищена оболонка*** Secure Shell (***SSH***), який забезпечує захищений віддалений доступ до мережевих пристроїв.
- ***Висока конфіденційність*** Pretty Good Privacy (***PGP***), комп'ютерна програма, що забезпечує криптографічну конфіденційність і автентифікацію для підвищення безпеки електронної пошти.

VPN – це приватна мережа, яка використовує загальнодоступну мережу, зазвичай Інтернет, для створення безпечного каналу зв'язку. VPN з'єднує дві кінцеві точки, такі як два віддалених офіси через Інтернет, щоб створити з'єднання (рис. 5.10).

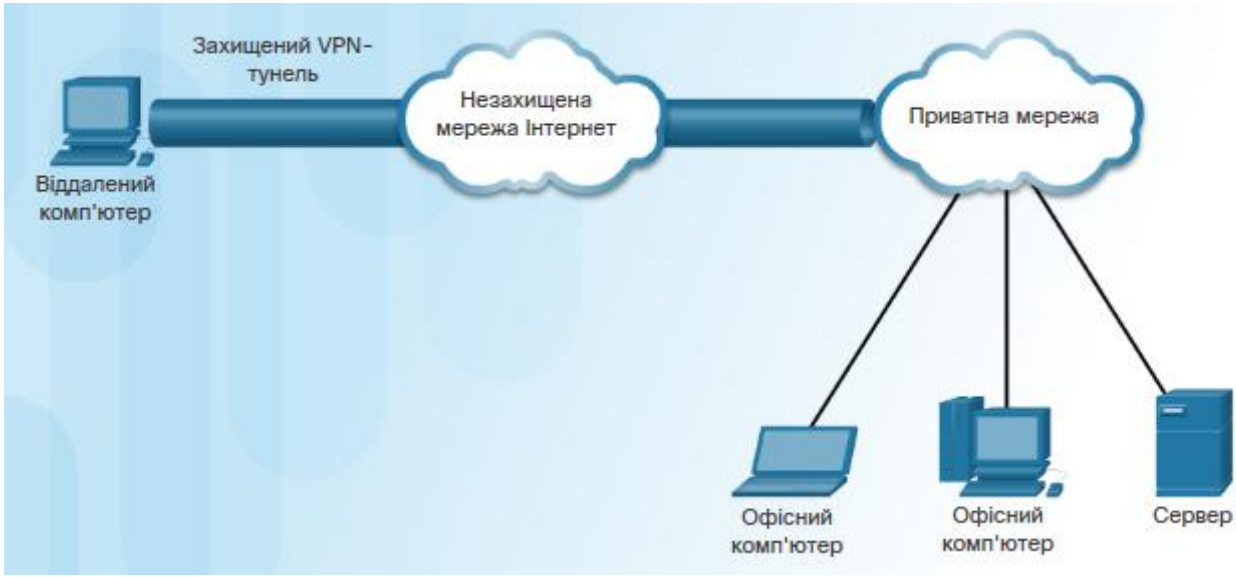


Рис. 5.10. Принципова схема створення безпечного каналу зв'язку через приватну мережу VPN[59]

Мережі VPN використовують IPsec. IPsec – це набір протоколів, розроблених для реалізації безпечних мережевих сервісів. Сервіси IPsec забезпечують автентифікацію, цілісність, контроль доступу та конфіденційність. За допомогою IPsec віддалені вузли можуть обмінюватися зашифрованою і перевіреною інформацією.

У багатьох організаціях виникає все більше проблем з даними, що використовуються. Під час використання дані більше не захищені, оскільки користувачу необхідно відкривати і змінювати їх.

[59] – This figure was uploaded by researchgate.net

В системній пам’яті можуть зберігатися конфіденційні дані, наприклад ключ шифрування. Якщо злочинці скомпрометують дані під час їх використання, вони будуть мати доступ до даних, які зберігаються та переміщуються.

5.4. КОНТРОЛЬ ДОСТУПУ

Контроль фізичного доступу – це розгорнуті реальні бар’єри, які мають запобігти прямому контакту з системами. Мета полягає в тому, щоб запобігти несанкціонованому фізичному доступу неавторизованих користувачів до об’єктів, обладнання та інших ресурсів організації.

Контроль фізичного доступу визначає ХТО, ДЕ і КОЛИ може увійти до яких приміщень (або вийти).

Приклади контролю фізичного доступу (рис.5.11 а) – і)[60]:

- Охоронці контролюють об’єкт.

Рис.5.11. Контроль доступу а)

Рис.5.11. Контроль доступу б)

- Паркани захищають периметр

- Детектори руху виявляють рухомі об’єкти.

Рис.5.11. Контроль доступу в)

Рис.5.11. Контроль доступу г)

Замки для ноутбуків захищають портативне обладнання.

[60] – This figures was uploaded by https://www.shutterstock.com/ru/search/security-cable-laptop

- Двері з замком запобігають несанкціонованому доступу.

Рис.5.11. Контроль доступу е)

- Сторожові собаки захищають територію.

Рис.5.11. Контроль доступу ж)

- Аварійна сигналізація виявляє вторгнення.

Рис.5.11. Контроль доступу д)

- Магнітні карти надають доступ до зон обмеженого доступу.

Рис.5.11. Контроль доступу є)

- Відеокамери здійснюють моніторинг об’єкту шляхом збору і запису зображення.

Рис.5.11. Контроль доступу з)

Тамбури-шлюзи (mantraps) дають змогу отримати доступ до захищеної зони після зачинення дверей під №1.

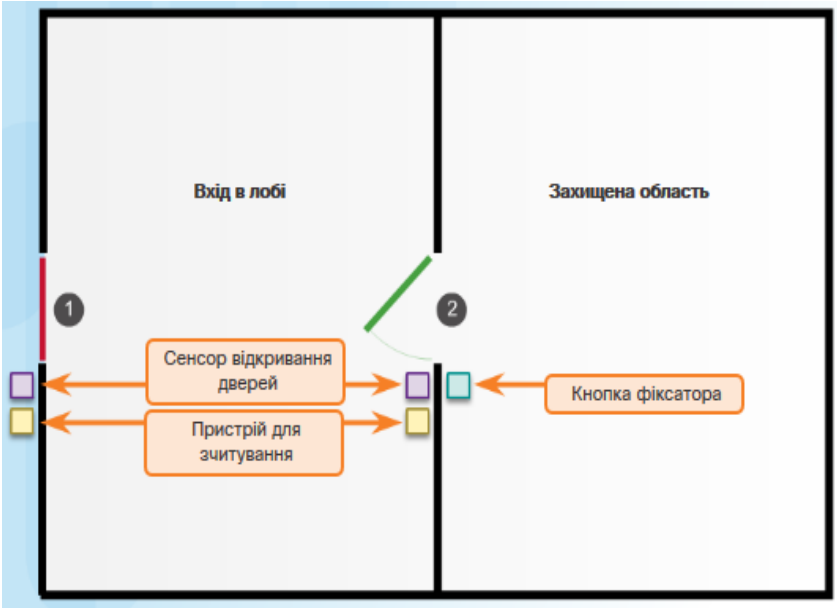


Рис.5.11. Контроль доступу і)

Розмежування логічного доступу забезпечують апаратні і програмні рішення для керування доступом до ресурсів та систем. Ці технологічні рішення включають інструменти та протоколи, які використовуються комп'ютерними системами для ідентифікації, автентифікації, авторизації та звітності.

До засобів логічного розмежування доступу відносять:

- Шифрування – це процес перетворення відкритого тексту на зашифрований текст.
- Смарткарти, які містять вбудований мікрочіп.
- Паролі – це захищені рядки символів.
- Біометричні дані – фізичні характеристики користувачів.
- Списки контролю доступу (Access Control Lists, ACL) визначають тип трафіку, який дозволений в мережі.
- Протоколи – це набір правил, які регулюють обмін даними між пристроями.
- Міжмережеві екрани – блокують небажаний мережевий трафік.
- Маршрутизатори з'єднують, як мінімум, дві мережеві інфраструктури.
- Системи виявлення вторгнень виконують моніторинг мережі на наявність підозрілих дій.
- Рівні відсікання (Clipping Levels) – є певними допустимими пороговими значеннями помилок до спрацювання сигналу тривоги.

Засоби адміністративного контролю доступу – це політики і процедури, визначені організацією для впровадження та забезпечення дотримання всіх аспектів контролю несанкціонованого доступу. Засоби адміністративного контролю зосереджені на персоналі і діловій практиці. До засобів адміністративного контролю відносять:

- політики – це твердження про наміри.
- процедури – докладні кроки, необхідні для виконання певних дій.

- практика найму співробітників – включає в себе кроки, що вживаються організацією для пошуку кваліфікованих співробітників.
- перевірка біографії – це вибіркова перевірка інформації про співробітників, яка включає інформацію з попередніх місць працевлаштування, кредитну історію та наявність судимостей.
- категоризація даних впорядковує дані за категоріями залежно від секретності.
- тренінги з питань безпеки інформують співробітників про політику безпеки, яка діє в організації.
- перевірки та ревізії дають змогу оцінити продуктивність роботи співробітника.

Обов'язкове розмежування доступу (Mandatory Access Control, MAC) обмежує дії, які суб'єкт може виконувати з об'єктом. Суб'єктом може бути користувач або процес. Об'єктом може бути файл, порт або пристрій вводу/виводу. Правило авторизації вказує, чи може суб'єкт отримати доступ до об'єкта.

Організації використовують MAC, якщо існують різні рівні секретності. У кожного об'єкта є мітка і у кожного суб'єкта є допуск. Система MAC обмежує доступ суб'єкта у відповідності до рівня секретності об'єкта та мітки користувача.

Наприклад, візьміть військову класифікацію з рівнями «Таємно» та «Цілком таємно». Якщо якийсь файл (об'єкт) вважається зовсім секретним, він класифікується (позначається) «Цілком таємно». Такий файл (об'єкт) можуть переглядати тільки співробітники (суб'єкти), у яких є допуск рівня "Цілком таємно". Механізм розмежування доступу повинен гарантувати, що співробітник (суб'єкт) з доступом тільки до секретної інформації ніколи не одержить доступу до файлу з міткою «Цілком таємно». Також користувач (суб'єкт) з доступом до інформації з грифом «Цілком таємно» не може змінити класифікацію файлу (об'єкта) з «Цілком таємно» на "Таємно". Крім того, користувач з доступом до інформації з грифом «Цілком таємно» не зможе відправити файл з міткою «Цілком таємно» користувачу з доступом тільки до інформації з грифом "Таємно".

Власник об'єкта визначає, чи дозволяти доступ до об'єкта з дискреційним розмежуванням доступу (Discretionary Access Control, (DAC). DAC відкриває або обмежує доступ до об'єкта, на основі рішення власника. Як випливає з назви, цей тип розмежування доступу є дискреційним (вибірковим), оскільки власник об'єкта з певними правами доступу може надавати ці ж права доступу іншому суб'єкту на власний розсуд.

У системах, що використовують дискреційне розмежування доступу, власник об'єкта може сам вирішувати, які суб'єкти будуть мати доступ до об'єкта і на якому рівні. Як показано на рисунку, одним з найпоширеніших методів є дозволи. Власник файлу може вказати, які конкретні дозволи (читання/ запис/ виконання) можуть мати інші користувачі.

Списки контролю доступу – є ще одним поширеним механізмом, що використовується для реалізації дискреційного розмежування доступу. У списках контролю доступу застосовуються правила для визначення дозволеного вхідного та вихідного трафіку в мережі.

Контроль доступу на основі ролей (Role-Based Access Control, (RBAC) працює залежно від ролі суб'єкта (рис.5.12). Ролі – це посадові обов'язки в організації. Конкретні ролі потребують певних дозволів для виконання певних операцій. Користувачі отримують дозволи у рамках своєї ролі.

Рис.5.12. Ролі[61]

RBAC може працювати в комбінації з DAC або MAC, застосовуючи відповідні політики. RBAC допомагає адмініструвати системи безпеки у великих організаціях з сотнями користувачів і тисячами можливих дозволів. Організації широко використовують RBAC для керування дозволами комп'ютерів усередині системи або застосунку. І вважають це найкращою практикою безпеки.

Під час контролю доступу на основі правил використовуються списки контролю доступу (ACL), які допомагають визначити, чи надавати доступ користувачу. В ACL міститься певна кількість правил, як показано на рисунку. Можливість надання доступу залежить від цих правил. Наприклад, одне з правил полягає в тому, що жоден співробітник не зможе отримати доступ до файлу платіжної відомості після завершення робочого дня або у вихідні.

Як і у випадку з MAC, користувачі не можуть змінювати правила доступу. Організації можуть комбінувати розмежування доступу на основі правил з іншими стратегіями для реалізації обмеження доступу. Наприклад, впровадження методів MAC може використовувати підхід, заснований на правилах.

В процесі ідентифікації застосовуються правила, що встановлені політикою авторизації. Суб'єкт запитує доступ до системного ресурсу.

[61] – https://www.shutterstock.com/ru/image-vector/managerial-level-role-illustration-281685752

Кожен раз, коли суб'єкт запитує доступ до ресурсу, засоби контролю доступу визначають, надавати чи забороняти доступ. Наприклад, політика авторизації визначає, які дії користувач зможе виконувати з ресурсом. Це дає змогу гарантувати безпеку та правильний доступ до чутливої інформації.

Унікальний ідентифікатор забезпечує правильний зв'язок між дозволеними діями і суб'єктами. Ім'я користувача – найбільш поширений метод, який використовується для ідентифікації користувача (рис.5.13). Ім'я користувача може бути буквено-цифровою комбінацією, персональним ідентифікаційним номером (PIN), смарт-картою або біометричними даними (відбитком пальця, скануванням сітківки або розпізнаванням голосу).

Рис.5.13. Логін[62]

Унікальний ідентифікатор гарантує, що система може ідентифікувати кожного окремого користувача, що дає змогу авторизованому користувачеві виконувати необхідні дії з конкретним ресурсом.

Політика кібербезпеки визначає, які засоби контролю ідентифікації слід використовувати. На основі ступеня чутливості інформації та інформаційних систем визначається, наскільки суворо має контролюватися доступ. Збільшення кількості випадків витоку даних змусило багато організацій посилити контроль ідентифікації. Наприклад, індустрія кредитних карт в Сполучених Штатах вимагає від всіх постачальників перейти на системи ідентифікації через смарт-карти.

Паролі, парольні фрази або PIN-коди є прикладами того, що знає користувач (рис.5.14). Паролі є найпопулярнішим методом, що використовується для автентифікації. Парольну фразу, код доступу, ключ доступу та PIN-код часто також називають паролями. Пароль – це послідовність символів, що використовується для підтвердження особи користувача. Якщо ці символи якимось чином пов'язані з користувачем (наприклад, містять ім'я, дату народження або адресу), кіберзлочинцям буде простіше підібрати його пароль.

Рис.5.14. Пароль[63]

[62], [63] – This figure was uploaded by shutterstock.com

У багатьох публікаціях рекомендується використовувати пароль довжиною не менше восьми символів. Не слід створювати занадто довгі паролі, які важко запам'ятати, або навпаки, настільки короткі, що вони стають вразливими для підбору. Паролі повинні містити комбінацію літер верхнього та нижнього регістрів, цифр та спеціальних символів. Користувачам слід використовувати різні паролі для різних систем. В іншому випадку, якщо злочинець зламає пароль користувача один раз, він отримає доступ до всіх його облікових записів. Менеджер паролів може допомогти користувачеві створювати та запам'ятовувати надійні паролі.

Смарт-карти, ключі-брелоки безпеки – це приклади того, що користувач має при собі (рис.5.15 – 5.17).

Смарт-карта безпеки. Смарткарта – це невелика пластикова картка розміром з кредитну, в яку вбудовано невеликий чіп. Чіп – це інтелектуальний носій даних, здатний обробляти, зберігати та захищати дані, що зберігаються. На смарткартах зберігається приватна інформація, наприклад номери банківських рахунків, інформація особистої ідентифікації, медичні записи та цифрові підписи. Смарткарти забезпечують автентифікацію та шифрування для захисту даних.

Рис.5.15. Смарт-карта[64]

Ключ-брелок безпеки – це невеликій пристрій, який можна прикріпити до зв'язки ключів. Він використовує процес, який називається двофакторною автентифікацією, що є більш безпечним, ніж комбінація імені користувача та пароля. Спочатку користувач вводить персональний ідентифікаційний номер (PIN-код). У випадку, якщо код введено правильно, на дисплеї ключа-брелока безпеки відобразиться номер. Це другий етап автентифікації, у якому користувач повинен ввести цей номер для входу на пристрій або до мережевої інфраструктури.

Рис.5.16. Ключ-брелок[64]

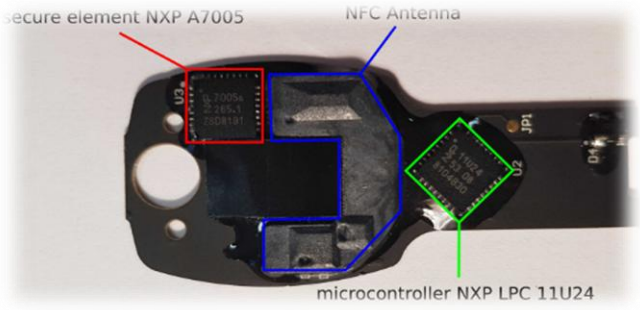


Рис.5.17. Електронні елементи ключа-брелока[64]

64 – https://stock.adobe.com/kz/search?k=%22password%20generator%22

Засоби контролю авторизації визначають, що користувач може і що не може робити в мережі після успішної автентифікації. Після того, як користувач підтвердить свою особистість, система перевіряє, до яких мережевих ресурсів користувач може отримати доступ і які дії користувач може виконувати з цими ресурсами. Авторизація відповідає на запитання: "Які права (читання, копіювання, створення, видалення) має користувач?"

Авторизація використовує набір атрибутів, який описує доступ користувача до мережевої інфраструктури. Система порівнює ці атрибути з інформацією, що міститься в базі даних автентифікації, визначає сукупність обмежень для цього користувача та передає її локальному маршрутизатору, до якого підключений користувач.

Авторизація виконується автоматично і не вимагає від користувачів додаткових дій після автентифікації. Авторизація має бути виконана одразу після успішної автентифікації користувача.

Визначення правил авторизації – це перший крок контролю доступу. Ці правила встановлює політика авторизації.

Групова політика визначає параметри авторизації на основі належності користувача до певної групи. Наприклад, всі співробітники організації мають магнітну карту, яка забезпечує доступ на об'єкт. Якщо посада працівника не вимагає доступу до серверної кімнати, його карта безпеки не дасть йому можливість туди увійти.

Політика на рівні повноважень визначає права доступу на основі статусу працівника в організації. Наприклад, лише старші працівники IT-відділу можуть заходити до серверної кімнати.

Рис.5.18. Засоби звітності[65]

Засоби звітності (рис.5.18) відстежують дії користувача та процесів, які стосуються внесення змін до системи, збирають цю інформацію і повідомляють дані про використання. Організація може використовувати ці дані для таких цілей, як аудит або виставлення рахунків. Зібрані дані можуть включати в себе: час входу користувача, відомості про успішні та невдалі спроби входу в систему, а також дані до яких мережевих ресурсів користувач звертався. Таким чином організація може відслідковувати дії, помилки та відхилення під час аудиту або розслідування.

[65] – https://www.shutterstock.com/ru/image-photo/responsibility-on-typewriter-223664218

Звітність забезпечується завдяки відповідним технологіям, політиці, процедурам та навчанню. З файлів журналу можна одержати детальну інформацію у відповідності з вибраними параметрами. Наприклад, в організації можуть переглядати журнал на предмет успішних або невдалих спроб входу в систему. Невдалі спроби входу в систему можуть свідчити про те, що злочинці намагалися зламати обліковий запис. Успішні спроби входу в систему показують, які користувачі використовували які ресурси системи та коли до них звертались. Наприклад, чи є нормальним для авторизованого користувача входити до корпоративної мережі о 3:00 ранку? Політики та процедури організації визначають, які дії слід фіксувати та яким чином створюються, перевіряються та зберігаються файли журналів.

Дотримання термінів зберігання даних, правил утилізації носіїв інформації та інших нормативних вимог сприяє належній звітності. Багато законів потребують здійснення спеціальних заходів для захисту різних типів даних. Ці закони стимулюють організацію до правильного способу обробки, зберігання та знищення даних. Відповідне навчання та обізнаність співробітників щодо корпоративних політик, процедур та пов'язаних з ними законів також посилюють відповідальність (рис.5.19).

Рис.5.19. Превентивний контроль[66]

Превентивні засоби означає запобіжні.

Превентивні засоби розмежування доступу запобігають небажаним або несанкціонованим діям. Для авторизованого користувача превентивне розмежування доступу означає обмеження. Призначення конкретних прав доступу користувачам в системі є прикладом превентивного контролю. Незважаючи на те, що користувач є авторизованим, система встановлює обмеження його прав, щоб запобігти можливим несанкціонованим діям. Міжмережевий екран, який блокує доступ до порту або сервісу, якими можуть скористатися кіберзлочинці, також є засобом превентивного контролю.

Стримувальний фактор є протилежним до заохочення. Заохочення стимулює людей чинити правильні дії, в той час як стримувальний фактор перешкоджає їм робити неправильні дії.

[66] – https://images.leadconnectorhq.com/image/f_webp/q_80/r_1200/u_https://storage.googleapis.com/msgsndr/43KkygQ5SY8zR4H6FHEa/media/66e0c6d97befbf21b3a1af29.png

Спеціалісти та організації, що займаються кібербезпекою, використовують стримувальні засоби для обмеження або мінімізації певних дій чи поведінки, але їх недостатньо для повного запобігання. Стримувальні засоби розмежування доступу перешкоджають одержанню несанкціонованого доступу до інформаційних систем та конфіденційних даних. Стримувальні засоби розмежування доступу перешкоджають атакам на системи, крадіжці даних та розповсюдженню шкідливого коду. Організації використовують стримувальні засоби розмежування доступу для підсилення дотримання політик кібербезпеки.

Стримувальні фактори застерігають потенційних кіберзлочинців проти вчинення злочину. На рисунку 5.20 представлені розповсюджені стримувальні засоби розмежування доступу, що використовуються в сфері кібербезпеки.

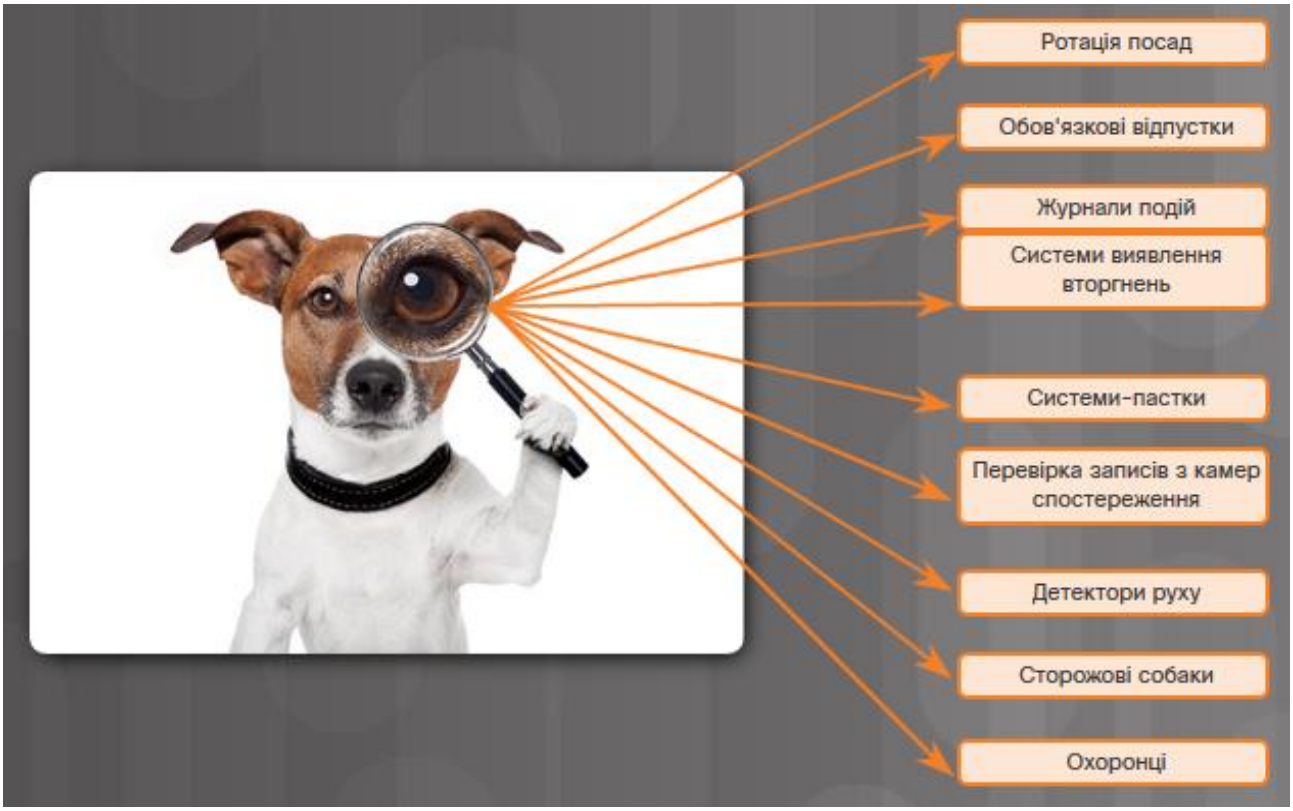


Рис. 5.20. Стримувальні засоби розмежування доступу[67]

Виявлення – це акт або процес виявлення чого-небудь. Ефективні механізми розкриття порушень дають змогу виявити різні типи несанкціонованих дій. Системи виявлення можуть бути дуже простими, наприклад, детектор руху або охоронець. А можуть бути більш складними, наприклад, система виявлення вторгнень (IDS). Всі ефективні механізми розкриття порушень мають кілька спільних рис: вони відслідковують незвичні або заборонені дії. Вони також надають методи реєстрації подій та оповіщення операторів системи про потенційний несанкціонований доступ.

[67] – https://stock.adobe.com/kz/search?k=%22password%20generator%22

Ефективні механізми розкриття порушень не запобігають чому-небудь, а працюють більше за фактом події.

Коригувальні заходи протидіють небажаним діям. Організації впроваджують коригувальні засоби розмежування доступу після того, як система зазнала загрози. Коригувальні заходи дають змогу відновити конфіденційність, цілісність та доступність системи. Вони також можуть повернути системи до нормального стану після несанкціонованих дій.

Відновлення – це повернення до нормального стану. Засоби відновлення розмежування доступу призначені для відновлення ресурсів, функцій і можливостей після порушення політики безпеки. Засоби відновлення можуть усунути пошкодження та запобігти збиткам у подальшому. Ці засоби мають більш розширені можливості в порівнянні з коригуючими засобами контролю та розмежування доступу.

Компенсація означає одержання чогось на заміну. Компенсувальні засоби розмежування доступу розширюють можливості інших засобів для більш суворого контролю за дотриманням політики безпеки.

Компенсувальні засоби можуть застосовуватись як заміна інших засобів, які неможливо використати в даних умовах. Наприклад, організація не має можливості тримати собаку для охорони, тому встановлює детектор руху з прожектором і звуком, що імітує гавкання собаки.

5.5. ПРИХОВУВАННЯ ДАНИХ

Технологія маскування даних захищає дані (рис.5.21), замінюючи конфіденційну інформацію на її неконфіденційну версію. Неконфіденційна версія виглядає як оригінал і виконує його функції. Це означає, що в бізнес-процесі можуть використовуватися неконфіденційні дані і немає необхідності змінювати додатки підтримки або системи зберігання даних. У більшості випадків використання маскування дає змогу обмежити поширення конфіденційних даних усередині IT-систем, шляхом заміни на сурогатні для тестування і аналізу.

Рис.5.21. Захищені дані[68]

[68] – https://img.freepik.com/premium-photo/interactive-digital-marketing-channels-illustration_66960-108.jpg?w=996

Інформація може маскуватися динамічно, якщо система або програма визначають запит користувача на одержання конфіденційної інформації як ризикований.

Маскування даних може замінити конфіденційні дані у невиробничих середовищах для захисту базової інформації.

Існує декілька методів маскування даних, які гарантують, що дані зберігають значення, але змінюються достатньо, щоб захистити їх конфіденційність:

- Підстановка замінює дані значеннями, які виглядають як достовірні для збереження анонімності записів.
- Перетасування створює набір даних заміщення з того ж набору даних, який користувач хоче замаскувати. Наприклад, цей метод добре підходить для фінансової інформації в тестовій базі даних.
- Обнулення застосовує нульове значення до обраного поля, що повністю запобігає моніторингу даних.

Стеганографія дає змогу приховати дані (повідомлення) в іншому файлі, такому як графічне зображення, аудіо або інший текстовий файл. Перевага стеганографії над криптографією полягає в тому, що приховане повідомлення не привертає до себе уваги. Наприклад, переглядаючи файл як в електронному, так і в друкованому вигляді зрозуміти, що рисунок містить приховане повідомлення, неможливо.

У приховуванні даних бере участь кілька компонентів. По-перше, є вбудовані дані, що є прихованим повідомленням. Текстовий контейнер (зображення, звук) приховує вбудовані дані, створюючи стеготекст (стегозображення, стегозвук). Стегоключ визначає процес приховування.

Підхід, який використовується для вбудовування даних в зображення-контейнер, використовує метод заміни молодших бітів (Least Significant Bits, LSB). У цьому методі використовують біти кожного пікселя у зображенні. Піксель – це основна одиниця програмування кольору в комп'ютерному зображенні. Колір конкретного пікселя – це суміш трьох кольорів: червоного, зеленого та синього (RGB). Три байти даних визначають колір пікселя (один байт для кожного кольору). Вісім бітів складають байт. 24-бітова система кольорів використовує всі три байти. Метод LSB використовує по одному біту з кожного компонента червоного, зеленого та синього кольорів. Кожен піксель може зберігати 3 біти.

Однією з літер у прихованому повідомленні є літера Т і вставка символу Т змінює лише два біти кольору. Людське око не здатне розпізнати зміни, внесені до молодших бітів. Результатом є прихований символ.

Загалом, достатньо змінити не більше половини бітів у зображенні, щоб ефективно приховати секретне повідомлення.

Соціальна стеганографія приховує інформацію, що знаходиться у всіх на очах. Для цього створюються повідомлення, скриту частину яких зможуть зрозуміти тільки посвячені у таємницю. Інші, хто просто прочитає повідомлення, не побачать прихованого послання. Підлітки в соціальних мережах використовують цю тактику для спілкування з найближчими друзями, при цьому всі інші, в тому числі батьки, не знають що насправді означає повідомлення. Так, наприклад, фраза "йдемо в кіно" може означати "похід на пляж".

Люди в країнах, де існує цензура засобів масової інформації, також використовують соціальну стеганографію, публікуючи повідомлення з завідомо неправильною орфографією або з прихованими посиланнями. По суті, вони спілкуються одночасно з різними аудиторіями.

Стеганаліз – це процес виявлення прихованої інформації. Метою стеганалізу є виявлення прихованих відомостей.

Структури, що повторюються в стегозображенні викликають підозру. Наприклад, диск може мати невикористані області, у яких приховується інформація. Утиліти для аналізу дисків можуть повідомляти про приховану інформацію в невикористаних кластерах пристроїв зберігання даних. Фільтри можуть перехоплювати пакети даних, що містять приховану інформацію в заголовках. Обидва ці методи використовують стеганографічні сигнатури.

Порівнюючи вихідне зображення зі стегозображенням, аналітик може візуально помітити структури, що повторюються.

Рис.5.22. Обфускація[69]

Обфускація даних – це практичне використання методів маскування даних та стеганографії в галузі кібербезпеки та кіберрозвідки. В результаті обфускації зміст повідомлення стає заплутаним, неоднозначним або важчим для розуміння. Система може навмисно кодувати повідомлення, щоб запобігти несанкціонованому доступу до конфіденційної інформації.

Технологія цифрових водяних знаків захищає програмне забезпечення від несанкціонованого доступу або модифікації. Технологія захисту програмного забезпечення за допомогою цифрових водяних знаків передбачає ін'єкцію у виконуваний код програми прихованого повідомлення, яке слугує доказом права власності.

[69] – https://ru.pinterest.com/pin/737323770213560150/

Приховане повідомлення є цифровим водяним знаком, за допомогою якого захищається програмне забезпечення. Якщо хтось спробує видалити цифровий водяний знак, то код стане непрацездатним.

Обфускація програмного забезпечення перетворює його у версію, еквівалентну оригіналу, але значно важчу для аналізу зловмисниками. Програма буде працювати, як раніше, але при спробі декомпіляції видаватиме незрозумілі результати.

ВИСНОВКИ

У розділі розглянуто основи криптографії, її методи, алгоритми шифрування та системи контролю доступу. Криптографія є ключовим інструментом захисту даних, який забезпечує конфіденційність, цілісність і автентифікацію інформації. Сучасні криптографічні системи базуються на симетричних і асиметричних алгоритмах, кожен із яких має свої переваги: симетричні алгоритми забезпечують високу швидкість, а асиметричні – зручність у керуванні ключами.

Важливу роль у криптографії відіграє управління ключами, оскільки більшість атак на криптографічні системи спрямовані саме на їх вразливості. Для захисту інформації застосовуються різні технології, зокрема шифрування, маскування даних, стеганографія, обфускація та цифрові водяні знаки. Маскування даних допомагає приховати конфіденційну інформацію у тестових середовищах, стеганографія дає змогу приховувати повідомлення у файлах, а обфускація ускладнює аналіз програмного забезпечення, зменшуючи ризики доступу до конфіденційних даних та інтелектуальної власності.

Контроль доступу забезпечується через фізичні, логічні та адміністративні засоби. Використання політик доступу, багаторівневих систем авторизації та звітності сприяє попередженню несанкціонованих дій. Методи, такі як дискреційний та обов’язковий контроль доступу, а також контроль на основі ролей, допомагають організаціям адаптуватися до різних рівнів загроз.

У темі також акцентується увага на важливості виявлення порушень і відновлення після інцидентів. Використання превентивних, стримуючих і коригуючих заходів сприяє зменшенню ризиків і захисту систем від кібератак.

Розвиток криптографії, обфускації та системи захисту даних є основою для підтримки безпеки в інформаційному просторі, що стає критично важливим в умовах цифрової трансформації.

ТЕРМІНИ І КОНЦЕПЦІЇ

1. ***AES (Advanced Encryption Standard)***

– сучасний шифр з блоком розміром 128 біт і ключами 128, 192 або 256 біт, що забезпечує високу швидкість і надійність.

2. ***Асиметричне шифрування (шифрування з відкритим ключем)***

– метод, де для шифрування використовується відкритий ключ, а для розшифрування – закритий.

3. ***Блокові шифри*** – метод шифрування, що обробляє фіксовані блоки даних (64 або 128 біт) за один раз.

4. ***DES (Data Encryption Standard)*** – старіший блоковий симетричний шифр з розміром блоку 64 біти. 3DES **(Triple DES)** – симетричний блоковий шифр, що шифрує дані тричі з різними ключами.

5. ***Керування ключами*** – процес створення, обмін, зберігання та захист криптографічних ключів.

6. ***Криптографія*** – метод зберігання та передачі даних, що забезпечує їх читання лише авторизованими одержувачами.

7. Криптосистема – система, що включає алгоритми шифрування, методи керування ключами та інші компоненти для забезпечення безпеки даних.

8. Криптологія – наука про створення та злам секретних кодів.

9. Криптографічний ключ – пароль, що використовується для шифрування і розшифрування даних.

10. Симетричні алгоритми шифрування – використовують один і той самий ключ для шифрування та розшифрування. Цей метод також відомий як шифрування з закритим ключем.

11. Транспозиція (Перестановка) – метод шифрування, що перемішує позиції символів у відкритому тексті.

12. Шифр Цезаря – метод шифрування, де алфавіт зсувається на певну кількість позицій як ключ шифрування.

13. Шифрування – процес перетворення відкритого тексту в зашифрований текст (криптограму), щоб забезпечити його безпеку.

14. Розшифрування – зворотний процес шифрування, що відновлює відкритий текст з криптограми.

15. Схема одноразових шифроблокнотів (One-time pad) – метод шифрування, що використовує випадкові ключі для кожного повідомлення.

16. Стеганографія – метод приховування інформації (повідомлень) в інших файлах, таких як графічні зображення, аудіо або текстові файли, так щоб вона була невидимою для стороннього спостерігача.

17. Обфускація – методи, що використовуються для заплутування інформації, щоб ускладнити несанкціонований доступ до конфіденційних даних.

ПРАКТИЧНЕ ЗАВДАННЯ 5.1. КРИПТОГРАФІЧНІ ПЕРЕТВОРЕННЯ

Цілі та задачі

Засвоїти базові криптографічні алгоритми шифрування і отримати навички їхнього використання

Частина 1: Здобуття навичок застосування методів базового шифрування (командна робота)

Частина 2: Шифрування та розшифрування повідомлень з застосуванням програмного онлайн-інструменту.

Необхідні ресурси

• ПК або мобільний пристрій з доступом до Інтернету

Довідкова інформація

З давніх часів люди прагнули захистити важливі повідомлення, і з розвитком суспільства методи шифрування ставали дедалі складнішими. Наука, що досліджує створення і злам шифрів, отримала назву криптологія**,** яка охоплює два основних напрями: криптографію (процес шифрування) і криптоаналіз (розкриття шифрів).

Різні алгоритми шифрування пропонують свої способи забезпечення секретності: від найпростіших до надскладних.

Розглянемо приклади базових шифрів. Вони розділяються на дві основні групи – шифри підстановки та шифри перестановки.

Шифри підстановки

- **Шифр Літорея**: відноситься до моноалфавітних шифрів. Це різновид шифру заміни, оскільки він базується на підстановці одних символів (літер) замість інших згідно з певними правилами.

У методі літери однієї групи (наприклад, приголосні) замінюються іншими літерами за визначеним ключем, тоді як голосні можуть залишатися незмінними.

Принцип роботи шифру (сценарій):

a) Визначається абетка.

b) Приголосні букви розподіляються у два ряди в певному порядку (секрет полягає у способі розташування).

c) При шифруванні одна літера замінюється іншою згідно зі встановленим правилом, тоді як голосні залишаються незмінними.

Приклад: Зашифруємо слово ПЕНЗЛИК, для випадку, коли голосні залишаються без зміни й маємо наступну таблицю заміни:

б	в	г	д	ж	з	к	л	м	н
щ	ш	ч	ц	х	ф	т	с	р	п

У цьому випадку слово "ПЕНЗЛИК" шифрується як "НЕПФСИТ", що нескладно виявити «ручним» аналізом.

2) Шифр RO1 (наприклад, RO1, RO13) є різновидом шифру Цезаря**.**

Шифр Цезаря **–** це класичний метод шифрування, в якому кожна літера замінюється на іншу, зміщену в алфавіті на фіксовану кількість позицій. RO у назві означає "rotate" (обертання), а число вказує, наскільки відбувається зміщення.

Так, RO1 означає зміщення на 1 позицію вправо (А → Б, Б → В, і т.д.), а ROT13 – популярний варіант із зміщенням на 13 позицій, який часто використовується для приховування тексту в простих випадках. Існують й варіанти зсуву вліво, наприклад, шифр RO-3.

Приклад шифру RO1 (зсув на 1 букву вправо)**:** фраза "НІЧ ЯКА МІСЯЧНА" перетворюється на "ОЇШ АЛБ НЇТАШОБ".

Застосування**:** Шифри заміни використовувались у військових повідомленнях (наприклад, шифри під час Першої світової війни). Проте з розвитком криптоаналізу ці шифри стали легко розкриватися, тому надалі використовувалися складніші методи.

Шифри перестановки (транспозиція)

Шифри перестановки – це методи шифрування, в яких символи відкритого тексту змінюють свій порядок відповідно до певного правила або ключа, але залишаються без заміни (інші символи не додаються).

Принцип**:** Літери початкового тексту переставляються, утворюючи шифротекст.

Приклад: Слово "ТАЄМНИЦЯ" може бути перетворено на "ЄТМАЦИНЯ" шляхом перестановки літер за певним шаблоном.

Шифри перестановки часто поєднують із іншими методами для ускладнення дешифрування. Наприклад, текст пишеться задом наперед або літери переставляються парами.

Приклад: "НЕСЕ ГАЛЯ ВОДУ" → "ЕН ЕС АГ ЯЛ ОВ УД".

Застосування**:** Шифри перестановки часто поєднують із іншими методами для ускладнення дешифрування.

ХІД ВИКОНАННЯ

Частина 1: Здобути навичок застосування методів базового шифрування

1. Ознайомитися з теоретичними відомостями до роботи. Здобути навички застосування методів найпростішого шифрування.
2. Розбитися на групи з 3-4-чоловік (голова та 3 шифрувальники).
3. Кожній групі виконати наступне:

- вибрати 3 повідомлення (фрази) з 4-5-слів;
- зашифрувати кожне окремим методом (літорея, ROTI та транспозиція);
- записати на «таємному» аркуші секрети свого шифру (не менш двох секретів для кожного шифру);
- записати кодовані повідомлення (Повідомлення 1, Повідомлення 2 та Повідомлення 3) та передати інший групі для розшифрування (код не надавати);
- отримати від іншої групи її зашифровані повідомлення та розшифрувати їх.

Час розшифрування повідомлення встановити близько 15 хвилин.

Частина 2: Шифрування та розшифрування повідомлень з застосуванням програмних онлайн-інструментів.

Інструмент Code Beautify (https://codebeautify.org/encrypt-decrypt) — це онлайн-інструмент для шифрування та дешифрування даних**.** Він підтримує різні криптографічні алгоритми, такі як Arcfour, Blowfish, Rijndael, Twofish, Xtea тощо. Крім того, користувачі можуть вибрати різні режими шифрування, наприклад CBC, ECB, CFB, CTR та інші.

Основні особливості:

- підтримка численних алгоритмів шифрування.
- різноманітні режими шифрування та дешифрування**.**
- простий інтерфейс, що дає змогу швидко працювати з даними.

Цей інструмент є корисним для розробників, аналітиків і користувачів, які працюють із конфіденційними даними та криптографією.

Виконайте наступне:

Крок 1

1.Ознайомтесь з інтерфейсом онлайн-інструменту Code Beautify.

2. Оберіть або сформуйте текст довжиною від 128 символів.

3. Оберіть агоритм шифрування Arcfour.

4. В полі «Enter Key» введіть ключ – Cybersecurity51

5. Опцію «Modes» оберіть «CBC».

4. В поле «Enter the Plain or Cipher Text» ведіть наступний текст обраного повідомлення й натісніть кнопку Encrypt (Зашифрувати).

Ознайомтесь з результатом – зашифрованим повідомленням. Повторіть експеримент з зашифрування декілька раз.

Яка максимальна довжина повідомлення є допустимою ? _____

Які зміни відбуваються на екрані при зміні вхідного повідомлення та його довжини? _____

Крок 2

Скопіюйте один з варіантів шифрованого тексту в буфер і проведіть такий експеримент:

- не змінюючи агоритму (Arcfour), ключа шифрування (Cybersecurity51) й опції «Modes» (CBC),

в поле «Enter the Plain or Cipher Text» ведіть текст з буфера (зашифроване повідомлення) й натісніть кнопку «Decrypt» (Розшифрувати).

Які зміни відбуваються на екрані при зміні вхідного повідомлення? _____

Крок 3

Повторіть експерименти з шифруванням/розшифруванням декілька разів, обираючі різні ключі, алгоритми шифрування й змінюючи режими.

Що відбудеться, якщо почергово змінювати опції дії, обрати інший алгоритм, інший ключ? _____

Який сенс виконуваних дій? _____

Продемонструйте кожну дію у звіті. Який висновок можна зробити з цих дій? Поясніть різницю між різними алгоритмами шифрування

ПРАКТИЧНЕ ЗАВДАННЯ 5.2. АЛГОРИТМ RSA

Цілі та задачі

Відпрацювання навичок шифрування в асиметричних криптосистемах, застосування схеми алгоритму RSA.

Частина 1: Здобуття навичок застосування методів базового шифрування (командна робота)

Частина 2: Шифрування та розшифрування повідомлень із застосуванням програмного онлайн-інструмента

Необхідні ресурси

• ПК або мобільний пристрій з доступом до Інтернету

Довідкова інформація

RSA – криптографічний система відкритого ключа, що забезпечує такі механізми захисту як шифрування і цифровий підпис (автентифікація – встановлення автентичності). Криптосистема RSA розроблена в 1977 році і названа на честь її розробників Ronald **Rivest**, Adi **Shamir** и Leonard **Adleman**.

Схема роботи алгоритму виглядає так (рис.5.23):

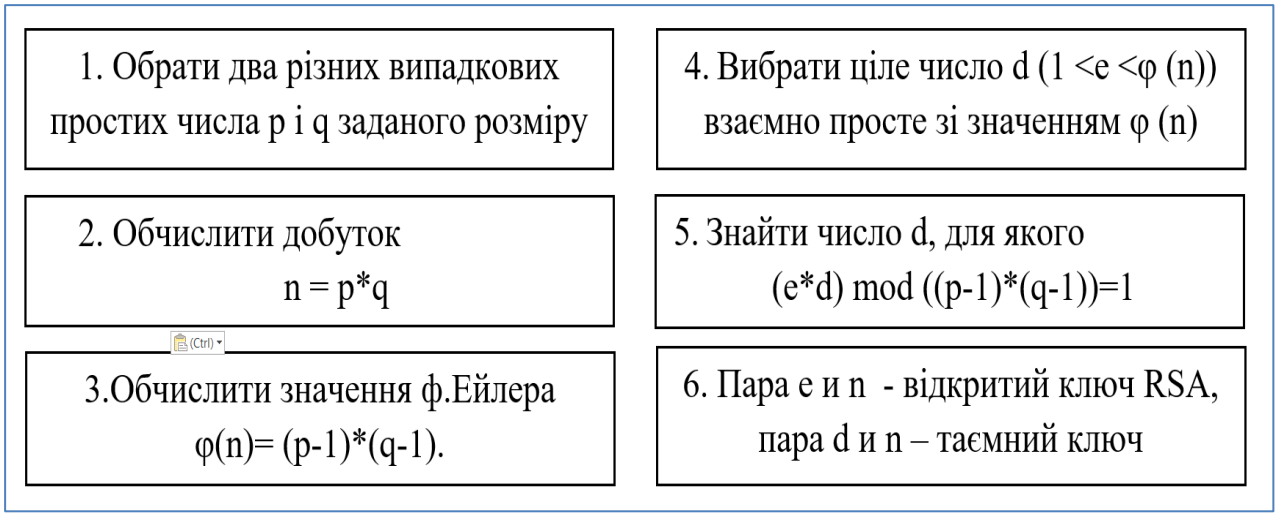


Рис.5.23. Схема роботи алгоритму RSA

Процес шифрування та дешифрування

Для того, щоб зашифрувати дані з відкритим ключем {e, n}, необхідно таке:

1) розбити текст, що буде зашифровано на блоки, кожен з яких може бути представлений у вигляді числа M (i) = 0,1,2 ..., n-1 (тобто тільки до n-1).

2) зашифрувати текст, що розглядається як послідовність чисел M(i) за формулою $P_a(i)=(M(I)^e) \bmod n$.

3) Щоб розшифрувати ці дані, використовуючи секретний ключ {d, n}, необхідно виконати зворотні обчислення: $M_a(i) = (P(i)^d) \bmod n$.

В результаті буде отримано безліч чисел M (i), які представляють собою вихідний текст.

Приклад роботи RSA

Зашифруємо й розшифруємо повідомлення "UKR" за алгоритмом RSA з застосуванням простих чисел p=11 и q=7 з використанням стандартного ASCII (англійська абетка).

Крок 1. Підбір відкритого й закритого ключів

1) Задано p=11 й q=7.
2) Визначаємо n= 11*7= 77.
3) Знайдемо φ(n) =(p-1)*(q-1)=60.
4) Рахуємо закритий ключ d як обернений до e за модулем φ(n), наприклад, візьмемо e=5.

Підбираємо d так, щоб (e*d) mod ((p-1)*(q-1))=1

(5*d) mod 60=1. Знаходимо, що d=13.

5) Відкритий ключ: (e=5, n=77)
6) Закритий ключ: (d=13, n=77)

Крок 2. Представлення вхідного тексту у числовому вигляді

Для RSA потрібно перекодувати кожну букву у числові значення. Конвертуємо слово "UKR" у числові значення, для чого використаємо Unicode (UTF-8):

"U" = 85
"K" = 75
"R" = 82

Крок 3. Шифрування

Застосовуємо RSA-шифрування й шифруємо кожен символ за формулою RSA:

$P_a(i)=(M(I)^e) \bmod n$,

де M — числове значення символу, e=5, n=77.

P1 = (85^5) mod 77 = 22;
P2 = (75^5) mod 77 = 43;
P3 = (82^5) mod 77 = 29;
Зашифроване повідомлення: 22, 43, 29.

Крок 4. Розшифрування

Для розшифрування застосовуємо закритий ключ {13,77}) і формулу $M_a(i) = (P(i)^d) \bmod n$.

M1=(22^13) mod 77 =85 = "U"
M2=(43^13) mod 77 =75 = "K"
M3=(29^13) mod 77 = 82 = "R"

Отримуємо розшифровані значення U = 85 (ASCII), K = 75 (ASCII), R = 82 (ASCII), = UKR

Дані розшифровані!

ХІД ВИКОНАННЯ

Ознайомтеся з теоретичними відомостями до роботи.

Закодуйте та розкодуйте з застосуванням алгоритму RSA слово, що є англомовною абревіатурою ваших Прізвища, Ім’я та по Батькові з застосуванням простих чисел p=3, q=13 та використанням стандартного ASCII.

Знайдіть інформацію про особливості застосування алгоритму. Включіть опис розрахунку за алгоритмом й знайдені відомості в звіт. Сформулюйте висновки до роботи

ДОДАТКОВІ РЕСУРСИ ТА ЗАВДАННЯ

Ознайомтесь з іншими інструментами, які мають схожі функції, що дають змогу ефективно працювати з шифруванням і криптографією.

1. **FreeFormatter – Online Encryption/Decryption Tools**

Інтуїтивний сервіс для шифрування/дешифрування, що підтримує різні алгоритми шифрування. **FreeFormatter** є корисним та зручним інструментом для швидкої обробки текстів та файлів у різних криптографічних форматах.

https://www.freeformatter.com

2. **CyberChef – The Swiss Army Knife of Encryption & Decryption**

Потужний інструмент для шифрування, дешифрування, перетворення даних тощо. Це потужний онлайн-інструмент для роботи з криптографією, шифруванням, дешифруванням та аналізом даних, який часто називають "швейцарським ножем для криптографії". Цей інструмент був створений британським агентством з кібербезпеки GCHQ і доступний для безкоштовного використання через веббраузер.

https://gchq.github.io/CyberChef/

3. **DCode – Online Cryptographic Tools**

Багатофункціональний сервіс для шифрування, дешифрування та роботи з криптографією. Він пропонує різноманітні інструменти для шифрування, дешифрування та аналізу криптографічних методів. DCode є популярним ресурсом серед криптографів, ентузіастів безпеки та тих, хто вивчає шифрування, оскільки надає широкий спектр інструментів для роботи з різними криптографічними алгоритмами.

https://www.dcode.fr/

Ці інструменти мають схожі функції, що дають змогу ефективно працювати з шифруванням і криптографією.

Який інструмент вам здався найбільш зручним? _____

Який вважаєте найбільш функціональним та застосовним для професійної роботи? _____

ТЕМА 6. ЗАБЕЗПЕЧЕННЯ ЦІЛІСНОСТІ ДАНИХ

Тема охоплює питання цілісності даних, зокрема процес хешування повідомлень. Описано основні алгоритми хешування, їхні характеристики та рекомендації щодо вибору. Висвітлені проблеми хешування, які можуть використовувати зловмисники, а також способи захисту. Окрім того, розглядається застосування цифрових підписів, підписання коду та сертифікатів, а також найбільш поширені алгоритми цифрового підпису. Особлива увага приділена забезпеченню цілісності баз даних.

Теоретичний матеріал доповнений практичними прикладами та додатковими поясненнями.

6.1. ВИДИ ЗАСОБІВ КОНТРОЛЮ ЦІЛІСНОСТІ ДАНИХ

В багатьох випадках необхідний механізм, який гарантує, що дані залишаються незмінними під час їх зберігання або передавання. Хешування – це інструмент, який забезпечує цілісність даних, використовуючи вхідні бінарні дані (повідомлення) і створюючи з них вихідні дані фіксованої довжини, які називають хеш-значенням або дайджестом (рис. 6.1, 6.2).

Рис. 6.1. Створення хеш-суми[70]

Рис. 6.2. Властивості хешування[71]

У системах хешування застосовуються криптографічно стійкі хеш-функції, які і забезпечують перевірку та гарантію цілісності даних. Вони також можуть застосовуватись для перевірки автентифікації.

[70], [71]- https://link.springer.com/book/10.1007/978-3-031-32959-3

Незашифровані паролі та ключі шифрування можна замінити відповідними хеш-функціями.

Це означає, що під час хешування одного і того ж пароля за допомогою конкретного алгоритму хешування, завжди буде одержано однаковий результат хеш-суми. Імовірність збігу хеш-сум є надзвичайно мізерною. Крім того, хеш функції є незворотніми – відновити вхідні дані за значенням хеш-суми дуже складно.

Кожен раз, коли дані змінюються, значення хеш-суми також змінюється. Через це криптографічні хеш-суми часто називають цифровими відбитками. Хеш-суми застосовують для того, щоб виявляти дублікати файлів даних, контроль зміни версії файлів та інші аналогічні задачі. Хешування допомагає запобігти випадковому або зловмисному пошкодженню або зміні даних. Хешування також є дуже ефективним. Хеш-сума як великого файлу, так і вміст всього диска під час хешування призводять до однакових за розміром результатів.

Хешування – це незворотня (одностороння) математична функція, яку відносно легко обчислити, але значно складніше знайти аргумент за її значенням. Незворотність функції можна навести, як аналог з меленою кавою. Легко змолоти кавові зерна, але майже неможливо відновити їх зі змелених кусочків.

Криптографічна хеш-функція має такі властивості:

- Вхідні дані можуть бути будь-якої довжини.
- Вихідні дані мають фіксовану довжину.
- Хеш-функція є одностороння і незворотна.
- З двох різних вхідних множин значень майже ніколи неможливо отримати однакові значення хеш-сум.

Хеш-функції дають змогу визначити, що дані змінились через помилку користувача або через збій в процесі передавання. Наприклад, відправник може переконатися, що повідомлення дійшло до одержувача без змін. Для цього передавальний пристрій обчислює хеш-суму повідомлення (відбиток фіксованої довжини).

Простий алгоритм хешування (8-бітна контрольна сума)

8-бітна контрольна сума є одним з перших алгоритмів хешування. Це є найпростіша форма хеш-функції. Під час розрахунку хеш-суми за цим алгоритмом 8-розрядна контрольна сума обчислює хеш, перетворюючи повідомлення в двійкові числа, а потім організовуючи рядок двійкових чисел в 8-бітові набори. Далі 8-бітові значення сумуються. Останній крок – перетворити результат у доповняльний код. Перетворення у доповняльний код відбувається таким чином: розряди двійкового числа інвертуються, після чого до числа додається одиниця. Це означає, що нулі перетворюються на одиниці, а одиниці

перетворюються на нулі. Останній крок – додати 1. Таким чином отримується 8-бітна хеш-сума.

1. Перетворіть повідомлення BOB в двійковий код з використанням таблиці кодів ASCII.

2. Перетворіть двійкові числа в шістнадцяткові.

3. Введіть шістнадцяткові числа в калькулятор (42 4F 42).

4. Натисніть кнопку **Calculate** (Обчислити) Результатом є хеш-сума **2D**

Спробуйте обчислити такі приклади:

SECRET = “S”=53 “E”=45 “C”=43 “R”=52 “E”=45 “T”=54

ХЕШ-СУМА = 3A

MESSAGE = “M”=4D “E”=45 “S”=53 “S”=53 “A”=41 “G”=47 “E”=45

ХЕШ-СУМА = FB

Сьогодні широко використовуються різні алгоритми хешування, серед яких популярними є MD5 та SHA, хоча через вразливості MD5 в криптографії його майже не застосовують.

Алгоритм Message Digest 5 (MD5)

Рон Рівест розробив алгоритм хешування MD5 і цей алгоритм використовується в Інтернеті для певного кола задач (рис.6.3). MD5 – це незворотня функція, яка дає змогу легко обчислити хеш із заданих вхідних даних, але робить складним обчислення вхідних даних за наявності лише значення хешу.

Рис.6.3. Хеш-захист[72]

MD5 формує 128-бітове значення хеш-суми. У 2012 році була реалізована атака шкідливим ПЗ Flame, яке скомпрометувало безпеку MD5. Автори ПЗ Flame використовували колізію MD5 для підробки сертифіката підпису коду Windows.

Алгоритм безпечного хешування (Secure Hash Algorithm, SHA)

У Національному інституті стандартів і технологій США (NIST) був розроблений алгоритм SHA, який включено у стандарт безпечного хешування (Secure Hash Standard, SHS). NIST опублікував SHA-1 в 1994 році. Сімейство алгоритмів SHA-2 замінило SHA-1, додавши чотири додаткові хеш-функції для створення сімейства SHA:

- SHA-224 (224 біт);
- SHA-256 (256 біт);
- SHA-384 (384 біт);
- SHA-512 (512 біт).

[72] – https://vsemedia.com/images/stories/code.jpg

SHA-2 – більш стійкіший алгоритм і він все частіше застосовується замість MD5. SHA-256, SHA-384 і SHA-512 є алгоритмами наступного покоління (рис. 6.4).

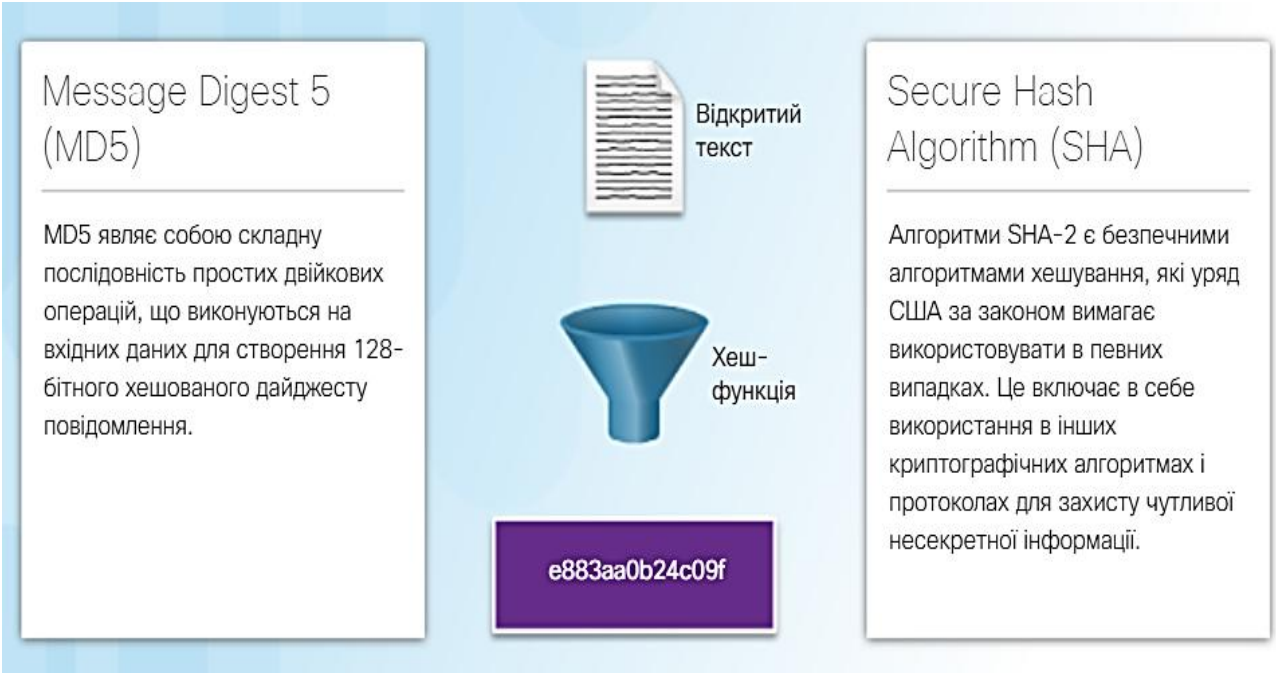


Рис. 6.4. Порівняння алгоритмів хешування MD5 і SHA-2[73]

За допомогою механізму перевірки цілісності можна переконатись, що дані та інформація не зазнали змін на шляху від відправника до одержувача. Впевненість у цілісності даних є важливою, коли користувач завантажує файл з Інтернету або під час криміналістичного дослідження цифрових носіїв.

Щоб перевірити цілісність всіх образів IOS, Cisco надає контрольні хеш-суми MD5 і SHA на вебсайті програмного забезпечення для завантаження. Користувач може порівняти значення MD5-дайджесту на сайті з дайджестом MD5 образу IOS, встановленого на пристрої. Якщо хеш-суми збігаються, користувач може бути впевненим в тому, що файл образу IOS було завантажено та встановлено у незміненому вигляді (рис. 6.5).

У сфері цифрової криміналістики хешування використовується для перевірки цифрових носіїв, що містять файли. Наприклад, експерт розраховує хеш-суму і створює побітну копію носія з файлами, формуючи таким чином цифровий клон. Потім експерт порівнює хеш-суму оригінального носія з хеш-сумою копії. Якщо значення хеш-сум збігаються, то копія ідентична оригіналу. Повна ідентичність бітів копії бітам оригіналу доводить незмінність. Спираючись на цю незмінність, можна відповісти на такі питання:

[73] – https://link.springer.com/book/10.1007/978-3-031-32959-3

Чи дійсно експерт має у своєму розпорядженні файли з оригінального носія?

- Чи можна стверджувати, що дані пошкоджені або змінені?
- Чи може експерт довести, що файли не пошкоджені?

Таким чином експерти можуть дослідити копії цифрових доказів не ризикуючи оригінальним носієм.

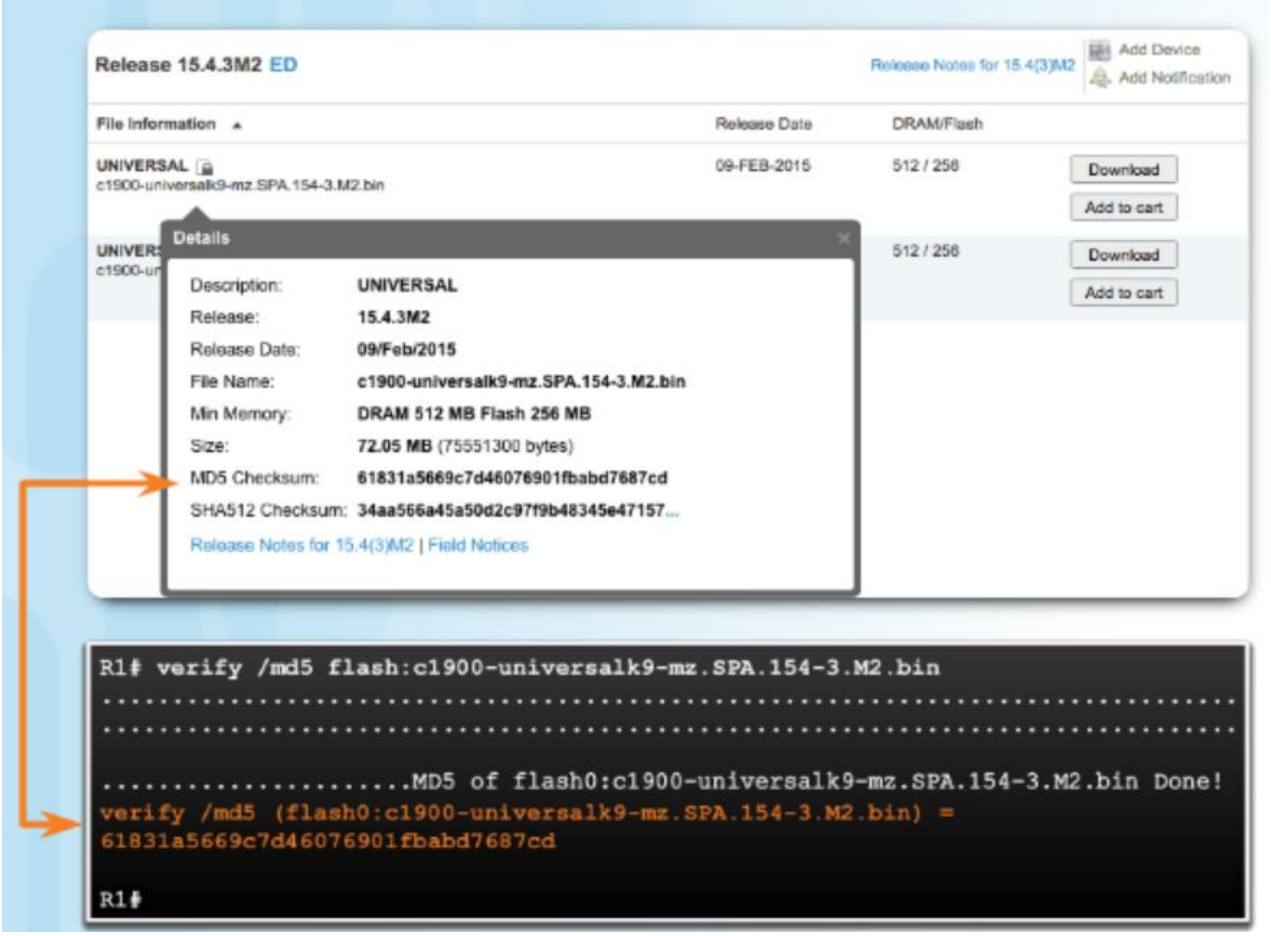


Рис. 6.5. Порівняння MD5-дайджестів з образом IOS[74]

Алгоритми хешувальння формують хеш-суму (цифровий відбиток) фіксованої довжини на основі вхідних даних будь-якого обсягу. Злочинець не зможе за допомогою лише хеш-суми, відновити вхідні дані. Якщо вхідні дані змінюються, це призводить до формування іншої хеш-суми. Такі властивості добре підходять і для захисту паролів. Паролі, що зберігаються у системі, повинні бути надійно захищені, але система також повинна мати можливість порівняти пароль, що вводиться під час входу, з тим, що зберігається у системі.

Система ніколи не записує пароль на жорсткий диск, вона зберігає тільки цифровий хеш.

[74] – This figure was uploaded by https://www.elektro.net/125855/anwendungen-von-hashing/

Криптографічні хеш-функції слід використовувати в таких цілях:

- Забезпечення підтвердження достовірності. У цьому випадку хеш-функція застосовується спільно з симетричним ключем автентифікації. Наприклад таким чином працюють протоколи IP Security (IPsec) або протоколи автентифікації маршрутизаторів.
- Автентифікацію шляхом генерації одноразових і односторонніх відповідей на запити протоколу автентифікації (рис. 6.6).
- Надання доказів перевірки цілісності повідомлень, зокрема тих, які використовуються в контрактах з цифровим підписом, і сертифікатах інфраструктури відкритого ключа (PKI), (такі сертифікати застосовуються, наприклад, для доступу до захищеного сайту з використанням браузера).

Рис. 6.6. Реєстрація облікового запису користувача і автентифікація[75]

При виборі алгоритму хешування рекомендується використовувати, як мінімум, SHA-256 або більш стійкі алгоритми, оскільки вони є в даний час найбільш безпечними. Уникайте використання SHA-1 і MD5 через виявлені в них серйозні вразливості безпеки. У промислових мережах слід застосовувати SHA-256 або більш стійкі алгоритми.

Хешування може виявити випадкові зміни, але воно не може запобігти навмисній зміні даних. Результат хешування не містить унікальної інформації, за допомогою якої можна було б однозначно визначити відправника.

[75] – https://link.springer.com/book/10.1007/978-3-031-32959-3

Це означає, що будь-хто може обчислити значення хеш-функції для будь-яких даних, якщо у нього є доступ до алгоритму потрібної хеш-функції. Наприклад, зловмисник може перехопити повідомлення, що передається через мережу, змінити його, перерахувати значення хеш-функції і додати до нового (підробленого) повідомлення. Приймаючий пристрій перевірятиме тільки те значення хешу, яке додане до повідомлення. Тому хешування вразливе для атак типу «людина посередині» і не захищає переданих даних.

Щоб одержати хеш-код, для входу в систему, зловмисник повинен вгадати пароль. Дві найбільш популярні атаки, що використовуються для зламування паролів, – це атаки перебору за допомогою словників та атака грублої сили (brute-force attacks) (рис.6.7).

Атака методом перебору за допомогою словника використовує файл, який містить розповсюджені слова, фрази і паролі. Файл має розраховані хеші. Така атака порівнює хеш-суми у файлі з значенням хешу пароля. Якщо хеш збігається, зловмисник дізнається групу потенційно правильних паролів.

Рис.6.7. Атака[76]

Атака грубої сили намагається використовувати будь-яку можливу комбінацію символів для заданої довжини пароля. Такі атаки вимагають потужних обчислювальних ресурсів, але якщо наявний великий запас часу, то цей метод виявить пароль зі стовідсотковою точністю. Тому паролі повинні бути досить довгими, щоб зробити час, необхідний для виконання атаки занадто довгим для успішності атаки. Хешування паролів ускладнює зловмисникам задачу вгадування паролів.

Сіль

Додавання солі під час хешування забезпечує більш надійний захист пароля (рис. 6.8). Якщо у двох користувачів однаковий пароль, вони також будуть мати однакові значення хешів паролів. Сіль, яка є випадковим рядком символів, додається до пароля перед хешуванням. Це створює різний хеш-результат для двох паролів. База даних зберігає як хеш, так і сіль. Хеш-суми однакових паролів відрізняються, тому що сіль в кожному випадку є різною.

[76] – https://www.shutterstock.com/ru/image-photo/green-screen-computer-monitor-displays-connected-352183106 https://www.shutterstock.com/ru/image-photo/dictionary-attack-1716533

В якості солі використовується випадкове число, тому сіль не обов’язково тримати у секреті.

Додавання солі не дає змоги зловмисникові використовувати атаку перебору за словником, щоб спробувати вгадати пароль. Крім того, наявність солі також не дає змоги використовувати таблиці пошуку і таблиці веселки, щоб зламати хеш.

Рис. 6.8. Додавання солі до хешу[77]

Криптографічно стійкий генератор псевдовипадкових чисел (Cryptographically Secure Pseudo-Random Number Generator, CSPRNG) – кращий вибір для генерування солі.

Такий генератор генерує випадкове число, яке має високий ступінь випадковості і абсолютно непередбачуване, тому воно забезпечує криптографічну стійкість (рис. 6.9).

Впроваджуючи механізм додавання солі необхідно дотримуватись таких рекомендацій:

- Формувати унікальну сіль для кожного пароля користувача.
- Ніколи не використовувати одну і ту ж сіль багаторазово.
- Довжина солі повинна бути рівною довжині вихідного значення хеш-функції.
- Завжди виконуйте хешування на сервері в вебзастосунку.

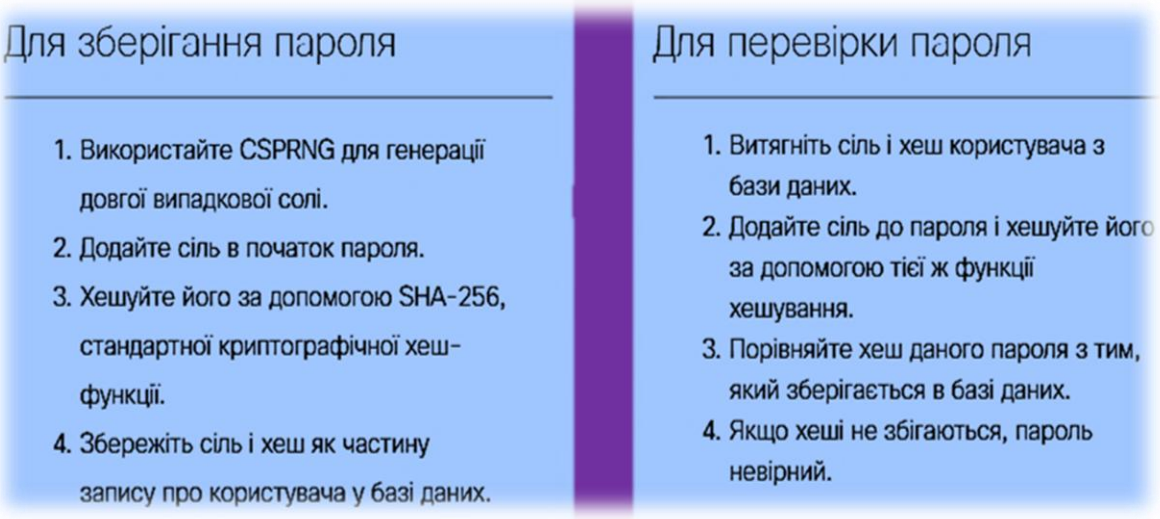


Рис. 6.9. Рекомендації для збереження та перевірки пароля[78]

[77] – https://www.shutterstock.com/ru/image-vector/salt-shaker-seasoning-line-art-vector-361658537

Таблиці пошуку

У таблицях пошуку зберігаються попередньо обчислені хеш-суми паролів, які взяті з відповідних словників, а також самі ці паролі. За допомогою таблиць пошуку можна перевіряти сотні хеш-сум за секунду.

Реверсивні таблиці пошуку

За допомогою таких таблиць кіберзлочинці реалізують атаку методом грубої сили або перебором за допомогою словника з перевіркою великої кількості хеш-сум без попередньо побудованої таблиці пошуку. Використовуючи викрадену базу даних облікових записів, зловмисник створює таблицю пошуку, яка містить список хеш-сум усіх правильних паролів та список користувачів. Зловмисник хешує кожен ймовірний пароль і за допомогою таблиці пошуку, отримує список користувачів, паролі яких збіглися з ймовірними. Така атака є ефективною, оскільки багато користувачів має однакові паролі.

Веселкові таблиці

Веселкові таблиці, у порівнянні зі звичайними таблицями пошуку, мають менший об’єм. Скорочення об’єму досягається шляхом зменшення швидкості зламу. Скоротивши об’єм таблиці, зловмисник може перевірити більшу кількість хеш-сум використовуючи однаковий об’єм пам’яті.

Веселкові таблиці — це класичний метод для злому хешованих паролів, але їх ефективність знижується завдяки сучасним методам безпеки, таким як сіль та повільні хеш-функції.

Захист можна також підсилити за допомогою методу розтягнення ключа. Розтягнення ключа робить роботу хеш-функції дуже повільною, що знижує ефективність атаки, роблячи високопродуктивне обладнання, яке може обчислювати мільярди хешів за секунду, менш ефективним.

Наступний рівень захисту від атак методом грубої сили, або атаки з допомогою словника забезпечується поєднанням секретного ключа і хеш-суми. У такій схемі тільки той, хто знає хеш-суму, може перевірити пароль. Одним із способів зробити це – включити секретний ключ в хеш-суму, використовуючи спеціальний алгоритм хешування, який називається кодом автентифікації повідомлень з використанням хеш-функцій (Keyed-hash Message Authentication Code, HMAC або KHMAC). HMAC використовує додатковий секретний ключ у якості вхідних даних для хеш-функції. Використання HMAC дає змогу не тільки перевірити цілісність даних, але й забезпечує автентифікацію.

[78] – https://pt.linkedin.com/pulse/arte-de-garantir-integridade-parte-1-tipos-controle-idal%C3%A9cio-silva

HMAC використовує спеціальний алгоритм, який об’єднує криптографічну хеш-функцію з секретним ключем (рис. 6.10).

Рис. 6.10. Алгоритм хешування HMAC[79]

Тільки відправник і одержувач знають секретний ключ, а результат хеш-функції залежить як від вхідних даних, так і від секретного ключа. Таким чином, лиш той, хто знає секретний ключ, може обчислити коректну хеш-суму функції HMAC. Ця властивість дає можливість запобігти атаці типу «людина посередині» і забезпечує автентифікацію джерела даних.

Розглянемо приклад, коли відправник хоче гарантувати, що повідомлення залишаться незмінними під час передавання і хоче надати одержувачу можливість автентифікації джерела даних.

Пристрій, що передає, вводить дані (наприклад, інформацію про оплату для Террі Сміта у $100 і секретний ключ) на вхід алгоритму хешування і обчислює відбиток, або хеш-суму HMAC фіксованої довжини. Одержувач отримує автентифікований відбиток, прикріплений до повідомлення (рис. 6.11).

Приймаючий пристрій відділяє відбиток від повідомлення і використовує повідомлення у відкритому тексті у поєднанні з секретним ключем в якості вхідних даних для тієї ж функції хешування. Якщо приймаючий пристрій обчислює відбиток, рівний відправленому відбитку, повідомлення одержано в незмінному вигляді. Крім того, одержувач може бути впевненим у походженні повідомлення, тому що тільки відправнику відомий спільний секретний ключ. Функція HMAC підтвердила достовірність повідомлення.

HMAC також можна використовувати для автентифікації Інтернет-користувачів. На багатьох вебсервісах використовують базову автентифікацію, у якій ім’я користувача і пароль передаються у незашифрованому вигляді. Якщо ж автентифікація відбувається з використанням механізму HMAC, то користувач зобов’язаний передати ідентифікатор приватного ключа і хеш-суму HMAC. Сервер знаходить приватний ключ користувача та обчислює хеш-суму HMAC. Обчислена сервером хеш-сума повинна збігтися з хеш-сумою HMAC, яка була одержана від користувача.

[79] – https://link.springer.com/book/10.1007/978-3-031-32959-3

За допомогою функції HMAC проводиться автентифікація джерела кожного з пакетів та перевірка цілісності даних в VPN-мережах, що базуються на протоколі IPsec.

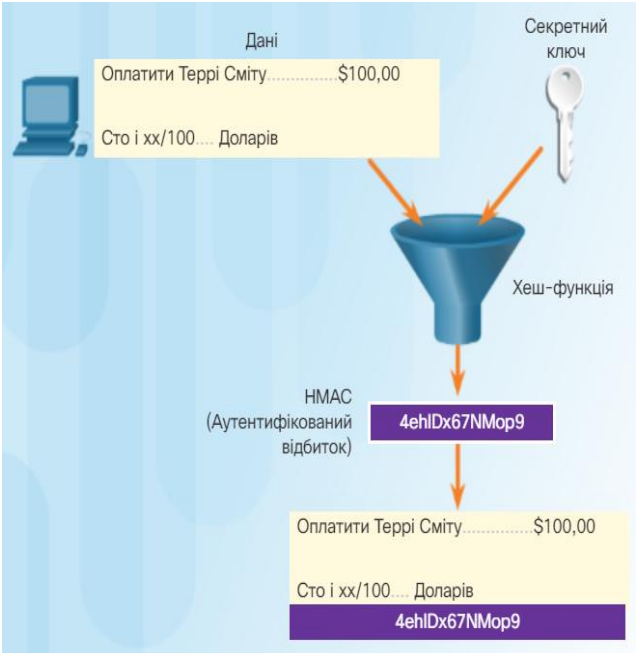


Рис. 6.11. Створення значення HMAC[80]

Продукти Cisco використовують хешування для автентифікації об’єктів, перевірки цілісності і достовірності даних:

- Маршрутизатори Cisco IOS під час роботи використовують схему, аналогічну HMAC: в повідомлення про оновлення протоколу маршрутизації додається автентифікаційна інформація за допомогою секретного ключа.
- Шлюзи та клієнти IPsec перевіряють цілісність та достовірність пакетів використовуючи алгоритми хешування, зокрема MD5 і SHA-1 в режимі HMAC.
- Образи програмного забезпечення Cisco, які розміщені на сайті Cisco.com, містять контрольну суму на основі MD5, щоб клієнти могли перевіряти цілісність завантажених образів.

Примітка: Термін "об’єкт" означає пристрій або систему всередині організації.

6.2. ЦИФРОВІ ПІДПИСИ

Рукописні підписи і печатки на документах підтверджують авторство. Цифрові підписи можуть забезпечувати ті ж функції.

Внести зміни у незахищений цифровий документ дуже легко. Цифровий підпис дає змогу визначити, чи редагувався документ після його підпису користувачем. Цифровий підпис (digital signature) – це математичний метод, який використовується для перевірки достовірності та цілісності повідомлення, цифрового документа або програмного забезпечення.

Електронний цифровий підпис (ЕЦП) є криптографічним механізмом. Він створюється за допомогою приватного ключа користувача, що дає змогу перевірити його дійсність за допомогою відповідного публічного ключа, забезпечуючи таким чином захист від підробки, та підтверджує походження даних.

[80] – https://link.springer.com/book/10.1007/978-3-031-32959-3

У багатьох країнах цифрові підписи мають таку ж юридичну силу, як і документ, підписаний вручну (рис.6.12). Електронний підпис, що стоїть під електронним контрактом, договором або будь-яким іншим документом, який у паперовому вигляді потребує рукописного підпису, має повну юридичну силу. Для вирішення задач, що пов'язані з юридичним захистом та регулюванням, передбачені та ведуться відповідні журнали подій, відстежують історію змін у електронному документі.

Рис.6.12. Юридична сила ЕЦП[81]

Цифровий підпис допомагає встановити справжність, цілісність і неможливість відмови (невідхильність). Цифрові підписи мають характерні властивості на яких побудовано механізм автентифікації об'єкта і перевірки цілісності даних.

Цифрові підписи є альтернативою механізму HMAC.

Під відхиленням розуміють відмову від авторства. Невідхильність – це спосіб гарантувати, що відправник повідомлення або документа не може відмовитись у надсиланні, а одержувач не може відмовитись у отриманні повідомлення або документа.

Наявність цифрового підпису гарантує, що відправник електронним способом підписав повідомлення або документ. Кожен з користувачів має унікальний цифровий підпис, тому той, хто створив підпис під документом, не зможе пізніше заперечувати свого авторства.

В основі цифрових підписів є асиметрична криптографія. Алгоритм відкритого ключа, такий як RSA, генерує два ключі: один закритий, інший відкритий. Ці ключі математично пов'язані між собою.

Аліса хоче відправити Бобу електронний лист, у якому міститься важлива інформація про вихід нового продукту на ринок. Боб повинен бути абсолютно впевненим, що повідомлення прийшло саме від користувача Аліса і доставлене в незмінному вигляді.

Аліса створює повідомлення та дайджест (хеш-суму) повідомлення. Вона шифрує дайджест повідомлення своїм закритим ключем.

[81] – https://www.avest.com.ua/wp-content/uploads/2021/01/kep-2048x1226.jpg

Аліса пов’язує повідомлення, зашифрований дайджест повідомлення і відкритий ключ для створення підписаного цифровим підписом документа. Одержаний результат Аліса відправляє Бобу (рис. 6.13).

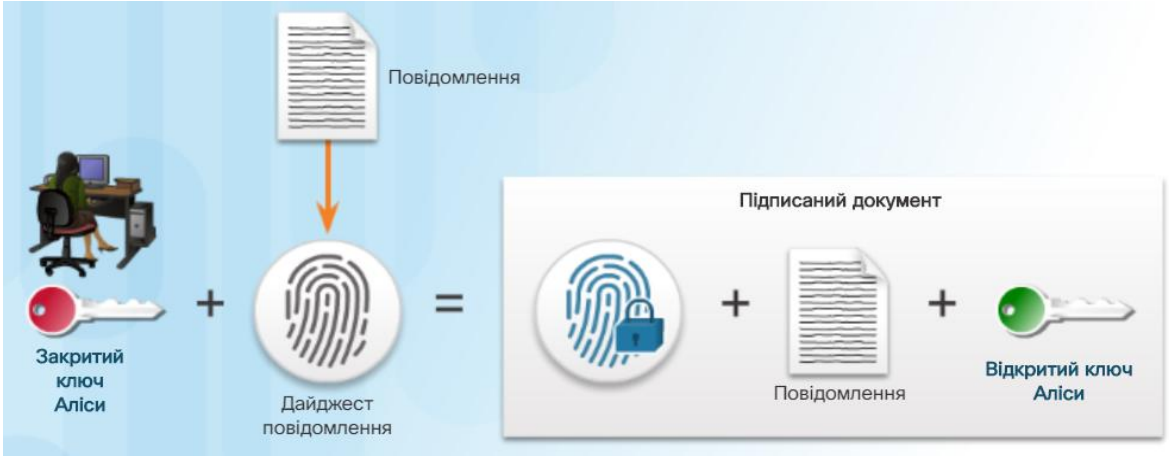


Рис. 6.13. Аліса відправляє підписаний документ[82]

Боб отримує повідомлення і читає його. Щоб переконатися, що повідомлення прийшло від Аліси, він створює дайджест повідомлення. Він бере зашифрований дайджест повідомлення, отриманий від Аліси, і розшифровує його за допомогою відкритого ключа Аліси. Боб порівнює дайджест повідомлення, отриманий від Аліси, з тим, який він створив. Якщо вони збігаються, Боб знає, що може довіряти отриманим даним і що ніхто не підробляв повідомлення (рис. 6.14).

Рис. 6.14. Боб читає документ і порівнює дайджест повідомлення[83]

Замість підписування всього документа можна підписати тільки його хеш-суму. Така схема підвищує ефективність та спрощує задачі, пов’язані з перевіркою цілісності та забезпечення сумісності. Впровадивши в організації систему електронного документообігу, що відповідає усім юридичним вимогам, можна повністю відмовитись від паперових документів та та традиційних печаток. Нижче наводяться два приклади використання цифрових підписів:

Приклад 1. Підписання коду – використовується для перевірки цілісності виконуваних файлів, що завантажуються з вебсайту постачальника. Підписання коду також використовує підписані цифрові сертифікати для автентифікації і перевірки аутентичності вебсайту.

[80,81] – This figure was uploaded by slideshare.net

Приклад 2. Цифрові сертифікати – використовуються для перевірки організації або окремого користувача, а також для автентифікації вебсайту постачальника і встановлення зашифрованого з'єднання для обміну конфіденційними даними (рис.6.15).

Найбільш поширеними є три алгоритми цифрового підпису – Digital Signature Algorithm (DSA), Rivest-Shamir-Adleman (RSA) і Elliptic Curve Digital Signature Algorithm (ECDSA). Всі три алгоритми містять механізми створення та перевірки цифрових підписів. Ці алгоритми функціонують на основі асиметричного шифрування з використанням відкритих ключів. Робота з цифровими підписами базується на двох операціях:

1. Генерація ключа.
2. Перевірка ключа.

Обидві операції потребують шифрування і розшифрування ключів.

Алгоритм DSA базується на складності обчислень дискретних логарифмів. У багатьох країнах алгоритм DSA використовують у державному секторі для створення цифрових підписів. Можливості алгоритму DSA обмежуються формуванням та перевіркою цифрового підпису.

Рис.6.15. Цифровий підпис[84]

RSA є найбільш поширеним алгоритмом шифрування з відкритим ключем, з тих, які використовуються сьогодні. RSA створено в 1977 році. Названий на честь авторів: Рона Ривеста, Аді Шаміра і Леонарда Адлемана. В основі RSA лежить асиметричне шифрування. RSA можна використовувати не тільки для роботи з цифровими підписами, а також і для шифрування повідомлення.

DSA працює швидше, ніж RSA, в якості підпису для цифрового документа. Алгоритм RSA краще підходить для ситуацій, коли крім вимог підпису і перевірки електронних документів необхідне ще й шифрування повідомлень.

Як і більшість криптографічних систем, алгоритм RSA базується на двох математичних компонентах: модульній арифметиці і задачі факторизації великих цілих чисел.

[84] – https://www.vecteezy.com/free-vector/space-draw?page=64

ECDSA – відносно новий алгоритм цифрового підпису, який поступово замінює RSA. Його перевага полягає в тому, що він може використовувати набагато менші розміри ключа при такому ж рівні безпеки і потребує значно менших об’ємів обчислень, ніж RSA.

Алгоритм ECDSA широко використовується в новітніх криптографічних системах, таких як блокчейн (Bitcoin використовує ECDSA для підписів транзакцій).

6.3. ЦИФРОВІ СЕРТИФІКАТИ

Цифровий сертифікат - це аналог електронного паспорта. Він дає змогу користувачам, хостам і організаціям безпечно обмінюватися інформацією через Інтернет. Цифровий сертифікат підтверджує автентичність користувача, який надсилає повідомлення (рис. 6.16). Цифрові сертифікати також можуть забезпечити конфіденційність для одержувача за допомогою засобів шифрування відповіді.

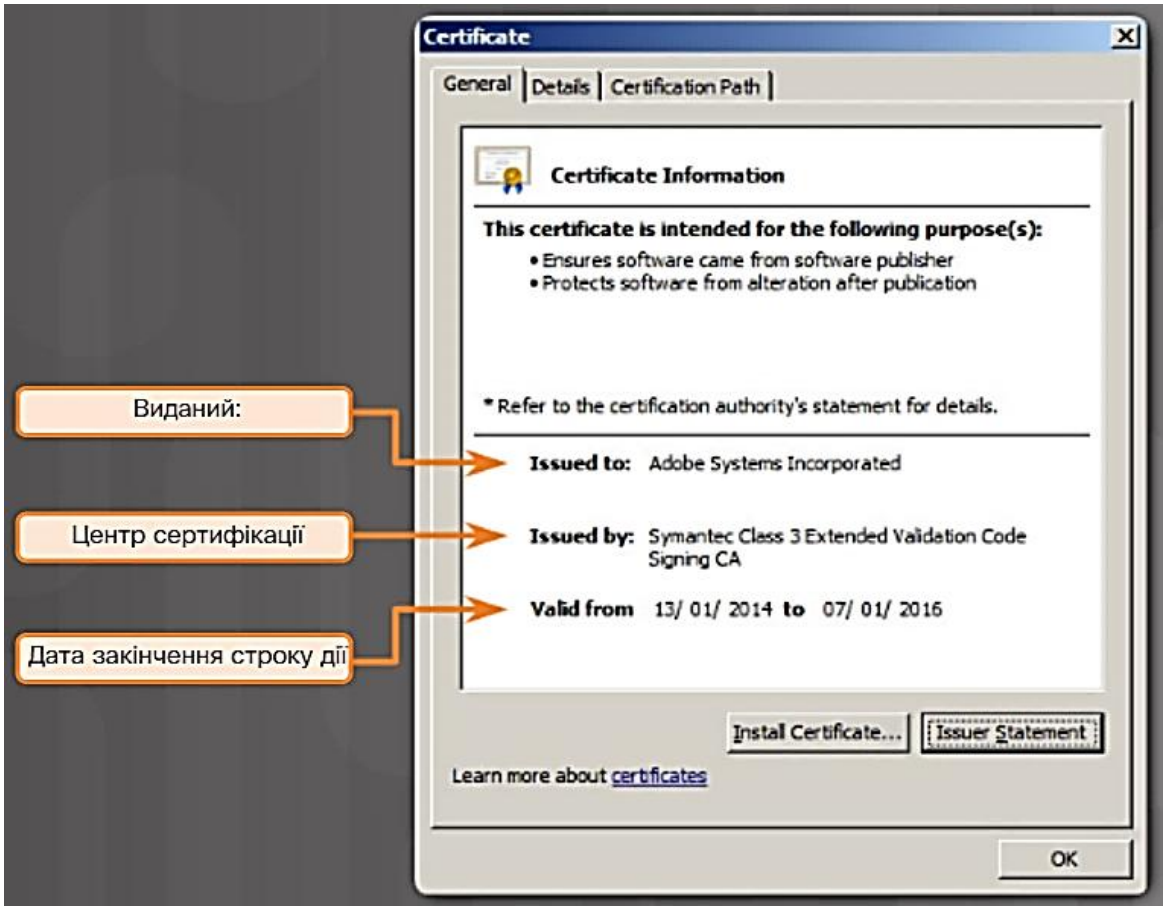


Рис. 6.16. Цифровий сертифікат[85]

[85] – https://xakep.ru/wp-content/uploads/2017/09/137634/image4.png

Цифрові сертифікати схожі на фізичні сертифікати. Наприклад, паперовий сертифікат Cisco Certified Network Associate Security (CCNA-S) містить відомості про те кому, ким (джерело сертифікатів) і на який тармін видано цей сертифікат (рис. 6.17).

Цифрові сертифікати використовують криптографічні ключі для підпису й шифрування даних, що забезпечує їхню цілісність та захист від підробок. Це гарантує надійність переданої інформації.

Щоб зрозуміти, як використовувати цифровий сертифікат, розглянемо приклад. Користувач Боб підтверджує замовлення у користувача Аліса. Вебсервер Аліси використовує цифровий сертифікат для захисту транзакції (рис. 6.18).

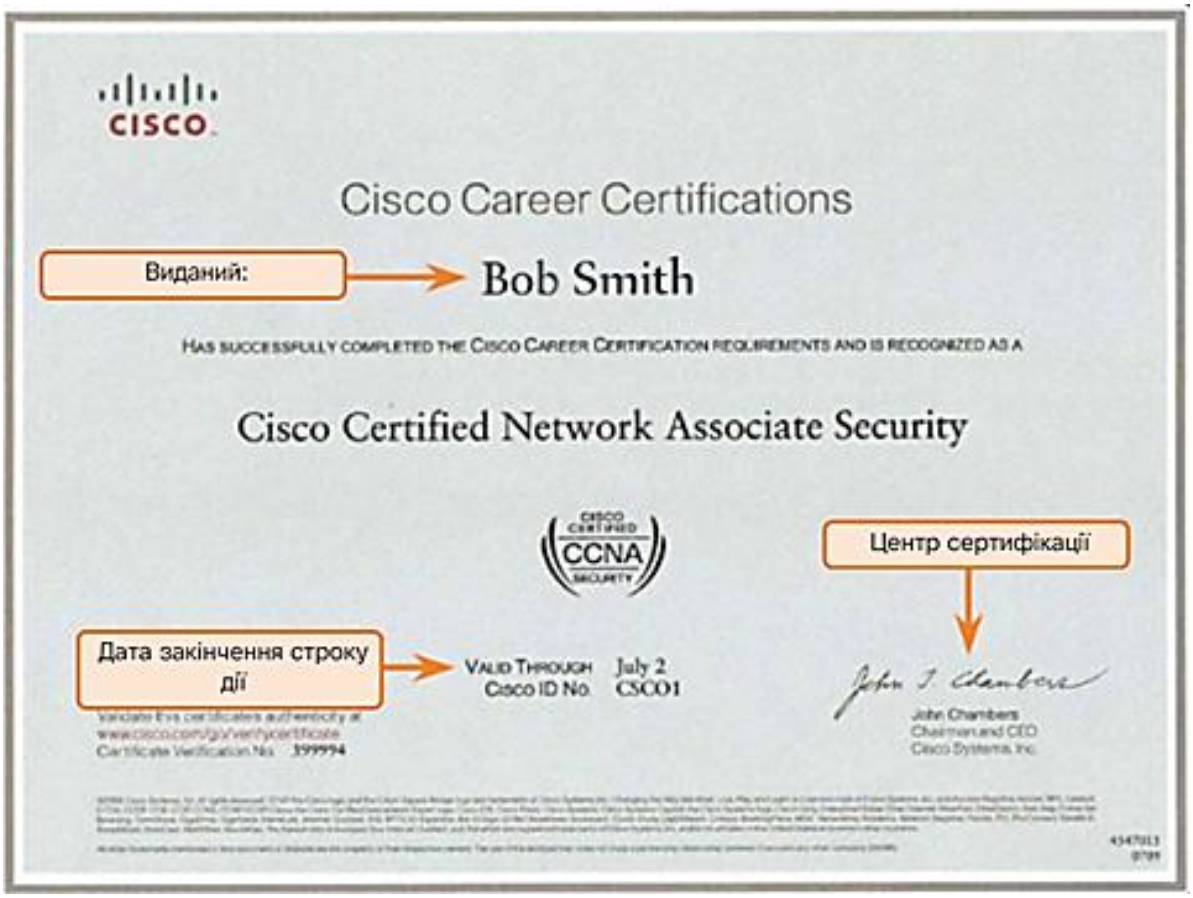


Рис. 6.17. Паперовий сертифікат IT компанії Cisco[86]

Крок 1: Користувач Боб переходить на вебсайт користувача Аліса. Успішно встановивши безпечне з'єднання, браузер, як правило, відображає значок замка в рядку стану безпеки.

Крок 2: Вебсервер Аліси надсилає цифровий сертифікат в браузер користувача Боб.

[86] – https://www.spc-trigger.com/files/CDCNIDS.jpg

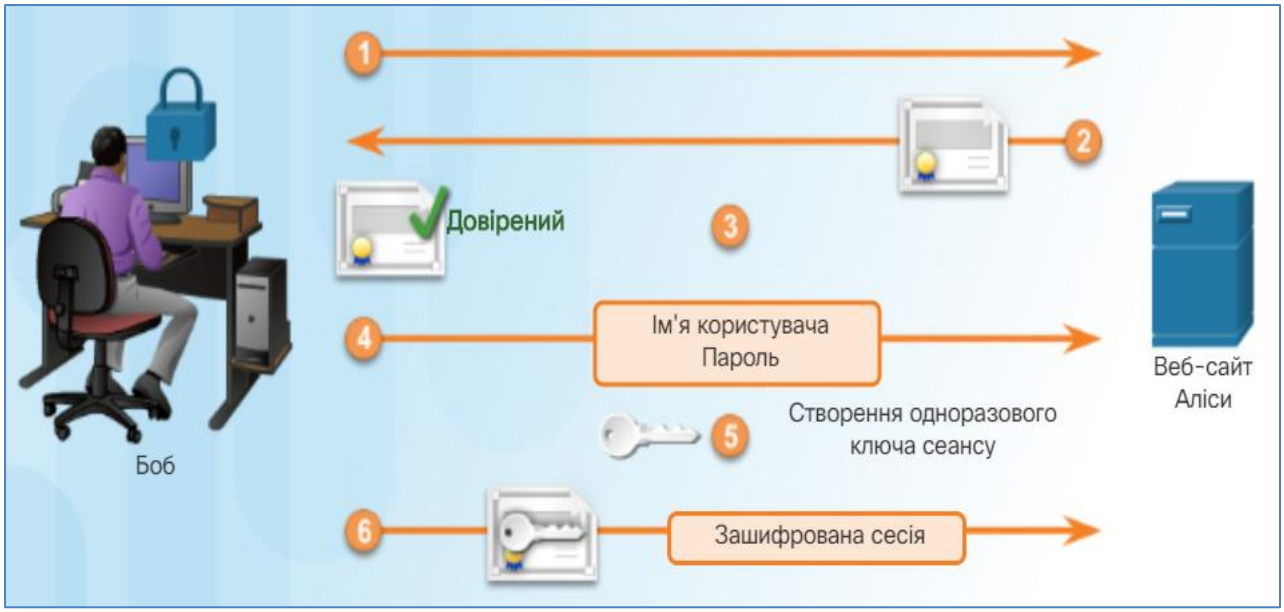


Рис. 6.18. Використання цифрового сертифіката[87]

Крок 3: Браузер Боба перевіряє сертифікат, що зберігається в налаштуваннях браузера. Транзакція може бути продовжена тільки за наявності довіреного сертифіката.

Крок 4: Користувач Боб ще має пройти автентифікацію і ввести пароль. Після успішної автентифікації створюється захищене з'єднання між комп'ютером Боба і вебсервером Аліси.

Крок 5: Веббраузер Боба створює унікальний одноразовий ключ сеансу.

Крок 6: Веббраузер Боба використовує відкритий ключ вебсервера, що відповідає сертифікату вебсервера для шифрування сеансу. В результаті тільки вебсервер Аліси може читати транзакції, відправлені з браузера Боба.

Підхід, який потребує багатократної взаємної ідентифікації усіх сторін в Інтернеті, є незручним. Тому сторони погоджуються довіряти нейтральній третій стороні. Передбачається, що третя сторона ретельно проводить перевірку учасників, що бажають одержати посвідчення. Після такої ретельної перевірки, третя сторона видає посвідчення, яке важко підробити. З цього моменту усі учасники, які довіряють цій третій стороні, просто приймають посвідчення, які видає ця третя сторона.

Наприклад, Аліса подає заяву для отримання водійських прав. У цьому процесі вона представляє документи, що засвідчують її особу (свідоцтво про народження, посвідчення особи з фотографією та ін.) у відповідний державний орган. Державний орган перевіряє особистість Аліси і допускає її пройти екзамен для одержання водійського посвідчення.

[87] – This figure was uploaded by slideshare.net

Після успішного завершення екзамену державний орган видає Алісі водійське посвідчення. Пізніше Алісі потрібно перевести в готівку банківський чек. Після пред'явлення чека, працівник банку запитує в неї посвідчення, яке засвідчує її особу. Банк, оскільки він довіряє державному органу, який видав документ, приймає цей документ у якості посвідчення особи під час переведення грошей з чека в готівку (рис. 6.19).

Центр сертифікації (CA) функціонує аналогічно державному органу в попередньому прикладі. CA видає цифрові сертифікати, для автентифікації організацій і користувачів. Ці сертифікати також використовують для підписування та перевірки цілісності повідомлень. Якщо цифровий сертифікат має стандартну структуру, його зможе прочитати та інтерпретувати будь-яка система, незалежно від його видавця (рис.6.20).

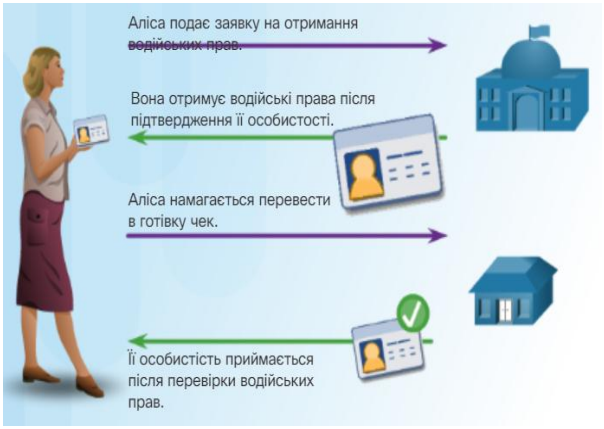


Рис. 6.19. PKI аналогія з водійськими правами[88]

Рис. 6.20. Інформація, що має міститися в цифровому сертифікаті за стандартом X.509

[88] – This figure was uploaded by slideshare.net

X.509 є стандартом для інфраструктури відкритих ключів (public key infrastructure, PKI) для керування цифровими сертифікатами. PKI – це політики, ролі і процедури, необхідні для створення, поширення, використання, зберігання та відкликання цифрових сертифікатів, а також керування ними. Згідно із стандартом X.509, цифрові сертифікати повинні містити стандартну інформацію.

Браузери і застосунки виконують обов'язкову валідацію (перевірку) сертифіката, щоб переконатись, що він є дійсний. Сертифікат відкритого ключа підтверджує, що відкритий ключ належить відповідній особі.

Перевірка включає в себе такі три процеси (рис. 6.21):

– дослідження сертифіката – прослідковується шлях сертифікації, з перевіркою кожного сертифіката, починаючи з сертифіката кореневого джерела сертифікатів (CA);

– перевірку шляху – вибір сертифіката емітента (CA) для кожного сертифіката у ланцюжку;

– перевірку на відкликання – дає змогу переконатись у тому, що сертифікат не був відкликаний; якщо сертифікат відкликаний, то під час цієї перевірки встановлюється причина відкликання.

Рис. 6.21. Процес валідації[89]

Суб'єкт отримує сертифікат для відкритого ключа від комерційного CA. Сертифікат є частиною ланцюжка сертифікатів, яку також називають ланцюжком довіри. Кількість сертифікатів в ланцюжку залежить від ієрархічної структури CA.

Є автономний кореневий центр сертифікації і підлеглий центр сертифікації в мережі. Причиною застосування дворівневої структури є те, що механізм підписування за стандартом X.509 дає змогу спростити усунення наслідків несанкціоного доступу. Якщо є автономний центр сертифікації, то він може підписати новий сертифікат для хоста в мережі. Якщо б автономний центр сертифікації був відсутнім, то довелося б встановлювати новий сертифікат корневого CA на кожному клієнтському комп'ютері, телефоні або планшеті.

[89] – This figure was uploaded by slideshare.net

6.4. ЦІЛІСНІСТЬ БАЗ ДАНИХ

Бази даних – це ефективний спосіб зберігання, вилучення та аналізу даних. Об’єми даних, які збираються, зростають, як і степінь їх конфіденційності, кількість баз даних збільшується і спеціалісти із забезпечення кібербезпеки відіграють значну роль у їх захисті.

Базу даних можна розглядати як електронну шафу-картотеку. Під терміном "цілісність даних" розуміють точність, узгодженість і надійність даних, що зберігаються в базі даних. Відповідальність за забезпечення цілісності даних лежить на тих, хто проектує, розробляє та керує експлуатацією баз даних.

Є чотири правила або обмеження цілісності даних.

Правило 1. Цілісність об’єктів: Кожен рядок повинен мати унікальний ідентифікатор, що називається первинним ключем.

Правило 2. Цілісність доменів: Всі дані, що зберігаються в стовпці, повинні відповідати одному і тому ж формату і відповідати єдиному спільному визначенню.

Правило 3. Цілісність посилань: Зв’язки між таблицями повинні залишатися незмінними. Тому користувач не може видалити запис, який пов’язаний з іншим записом.

Правило 4. Визначена користувачем цілісність: Набір правил, визначених користувачем, які не відносяться до жодної з інших категорій. Наприклад, клієнт робить нове замовлення. Спочатку перевіряється, чи це новий клієнт. Якщо це так, то додаємо нового клієнта до таблиці клієнтів.

Введення даних в систему частіше за все здійснюють користувачі. Відповідні засоби контролю допомагають забезпечити коректність даних, які вводяться (рис.6.22).

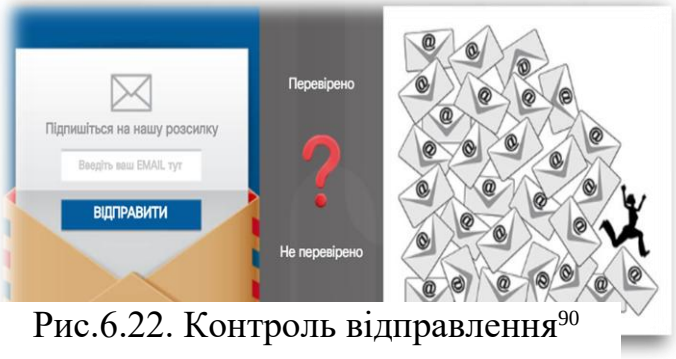


Рис.6.22. Контроль відправлення[90]

Керування введенням даних за допомогою випадаючих списків

Введення даних на основі таблиці за допомогою випадаючих списків замість того, щоб вводити дані вручну. Наприклад, можна стандартизувати ввід місця розташування, застосувавши випадаючий список, що формується на основі бази даних системи поштової адресації США.

[90] – This figure was uploaded by slideshare.net

Засоби контролю перевірки значень у полях даних

Ці засоби встановлюють правила для базової перевірки коректності введення значень у полях даних й приклади правил наведено нижче.

- Обов'язковість введення даних (введення неможливо закінчити, якщо в обов'язкових полях не будуть міститись дані.
- Маска введення (дає змогу виключити введення некоректних даних та забезпечити єдиний формат даних, наприклад, для номерів телефону).
- Додатні значення грошових сум.
- Діапазони даних (гарантують, що користувач не зможе ввести дані за межами заданого діапазону, наприклад, дата народження, не може бути введена як 01-18-1820).
- Обов'язкове затвердження іншою особою (наприклад, обов'язкове узгодження з другою або третьою особою у випадках, коли працівник банку отримує запит на зарахування або зняття з рахунку, на суму, що перевищує вказане обмеження).
- Ліміт на кількість змінених записів (наприклад, якщо кількість змінених записів перевищує заданий ліміт за певний проміжок часу, то система заблокує обліковий запис користувача до тих пір, поки менеджер не визначить, чи є ці транзакції правомірними).
- Відстеження незвичної поведінки (система блокується, коли виявляє аномальну активність).

Правило валідації перевіряє чи дані відповідають параметрам, які визначені конструктором бази даних. Правило валідації допомагає забезпечити повноту, правильність і узгодженість даних. Критерії, що використовуються під час валідації, включають такі критерії:

- розмір – перевіряє кількість символів в елементі даних;
- формат – перевіряє відповідність даних заданому формату;
- узгодженість – перевірка узгодженості у зв'язаних елементах даних;
- діапазон – перевіряє, що дані перебувають в межах між мінімальним і максимальним значенням;
- контрольна цифра – використання додаткових обчислень для створення контрольної цифри, що призначена для виявлення помилок.

Перевірка типу даних – найпростіший метод перевірки правильності даних, який дає змогу переконатись у тому, що дані введені користувачем є потрібного типу (рис.6.23). Наприклад, номер телефону не може містити інших символів крім цифр. В базах даних передбачено три типи даних: ціле число, стрічка і десяткові дроби.

Бази даних часто є основною мішенню для хакерів через високу концентрацію у них важливої інформації. Одним із поширених методів атак є SQL-ін'єкція**,** яка дає змогу зловмисникам виконувати несанкціоновані запити до

Рис.6.23. Аномалія[91]

бази даних, змінюючи або вилучаючи дані. Для захисту баз даних необхідно впроваджувати механізми фільтрації вводу, регулярні оновлення системи та обмеження привілеїв доступу користувачів. Одним з найбільш важливих аспектів забезпечення цілісності бази даних є контроль над процесом введення даних. Відсутність такого контролю стає причиною багатьох вразливостей. Багато відомих атак реалізуються через некоректне введення в базу даних. Такі атак можуть привести до зависання або інших порушень у роботі застосунків, а також до витоку конфіденційної інформації.

Наприклад, користувач підписується на розсилання новин, заповнюючи форму у вебзастосунку. Програма-застосунок бази даних автоматично генерує і відправляє підтвердження через електронну пошту. Одержавши електронне повідомлення з посиланням для підтвердження підписки, кіберзлочинці модифікують URL-адресу цього розсилання. Наприклад, змінюють ім’я користувача, адресу електронної пошти або статус підписки. Електронне повідомлення повертається назад на сервер, на якому працює програма-застосунок бази даних. Якщо вебсервер не перевіряє відповідність адреси електронної пошти або іншої облікової інформації, тим даним, які були введені в форму, то у базу даних потрапляє некоректна інформація. Хакери можуть автоматизувати цю атаку і таким чином внести тисячі некоректних записів в базу даних з інформацію про підписників.

Під виявленням аномалій розуміють виявлення неочікуваних признаків та поведінку даних. До таких признаків відносять значення, які різко виділяються, винятки, відхилення та інші аномальні прояви в різноманітних застосунках баз даних. Виявлення і перевірка аномалій є важливим контрзаходом або захистом з визначення шахрайства. Завдяки виявленн. аномалій у базах даних можна розпізнати шахрайські операції з кредитними картками та страховими полісами. Засоби виявлення аномалій у базі даних також можуть допомогти запобігти значним руйнуваннням або зміні даних.

Під перевіркою даних на аномалії мають на увазі тестові запити або зміни даних, коли система виявляє незвичайні або несподівані явища. Прикладом аномалії можуть бути запити транзакцій для однієї і тієї ж кредитної картки з віддалених один від одного регіонів за дуже короткий період часу. Якщо запит на транзакцію з Нью-Йорка відбувається о 10:30 ранку, а другий запит надходить з Чикаго о 10:35 ранку, то система запускає перевірку другої транзакції.

[91] – https://st2.depositphotos.com/1005979/8328/i/950/depositphotos_83286172-stock-photo-outlier-unqiue-different.jpg

Інший приклад – зміна адрес електронної пошти в незвичайно великій кількості записів бази даних. Адреси електроної пошти застосовуються під час організації DoS-атак, тому їх зміна у сотнях записів бази даних може вказувати на те, що зловмисник використовує корпоративну базу даних як інструмент для організації DoS-атаки.

Базу даних можна розглядати як електронну шафу-картотеку. Належна підтримка файлової системи є першочерговим завданням забезпечення достовірності та практичної цінності даних в базі даних. База даних складається з таблиць, записів, полів та даних в кожному з полів. Для забезпечення цілісності файлової системи бази даних, користувачі повинні дотримуватись певних правил. Цілісність об'єкта – це правило цілісності, в якому говориться, що кожна таблиця повинна мати первинний ключ і що стовпець або стовпці, вибрані як первинний ключ, повинні бути унікальними і не містити порожніх значень (NULL). Null в базі даних означає, що значення відсутні або невідомі. Цілісність об'єкта дає змогу належним чином організувати дані в записах.

Іншою важливою концепцією є взаємозв'язок між різними "системами картотек" або таблицями. Механізм забезпечення цілісності посилань базується на зовнішніх ключах. Зовнішній ключ в одній таблиці посилається на первинний ключ у другій таблиці (рис. 6.24).

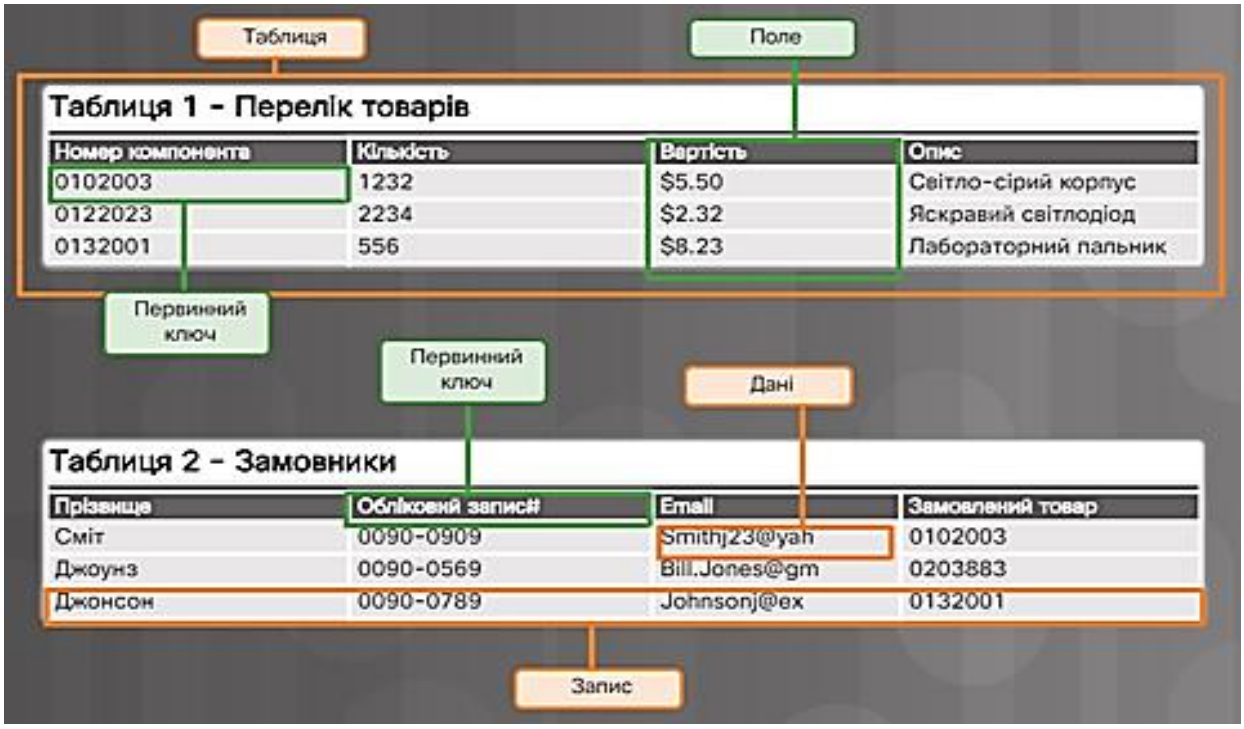


Рис. 6.24. Взаємозв'язок між таблицями (посилання зовнішнього ключа в одній таблиці на первинний ключ у другій таблиці)

Первинний ключ унікальним чином ідентифікує сутності (рядки) в таблиці (рис. 6.25). Цілісність посилань – це правило, за допомогою якого підтримується цілісність зовнішніх ключів.

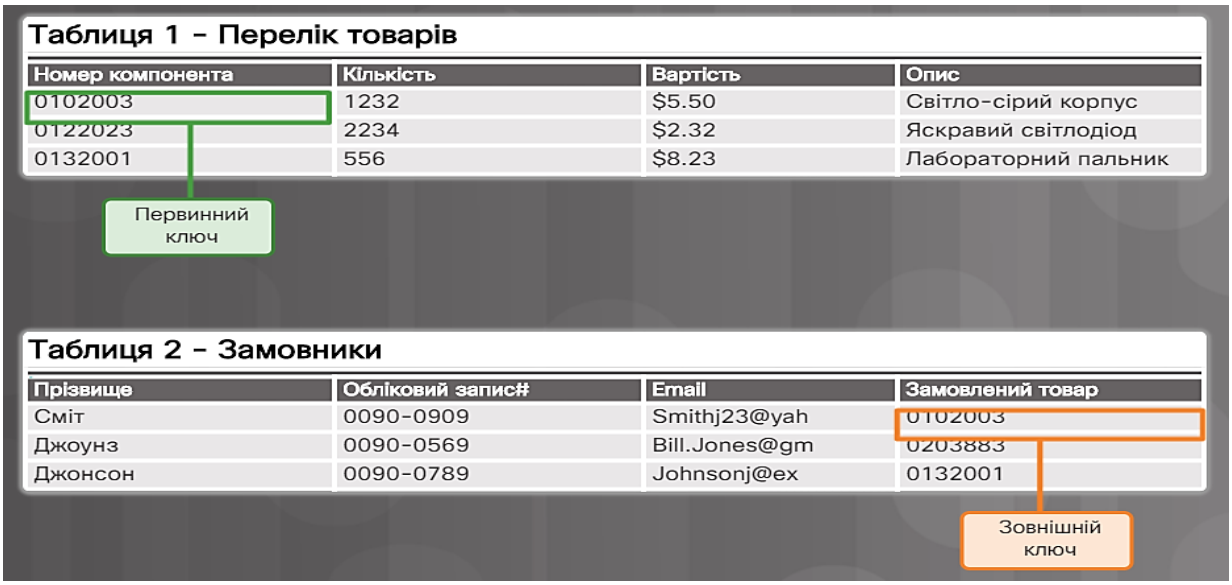


Рис. 6.25. Взаємозв’язок між таблицями
(ідентифікація первинним ключем рядка в таблиці)

Цілісність доменів гарантує, що всі елементи даних в стовпці потрапляють в певний набір допустимих значень. Кожен стовпець у таблиці має певний набір значень, наприклад, набір чисел для номерів кредитних карток, номерів соціального страхування або адрес електронної пошти (таблиця 6). Обмеження на значення кожного такого стовпця (атрибуту), забезпечує цілісність доменів. Правило цілісності доменів може зводитись до вибору правильного типу даних, довжини і/або формату даних для стовпця.

Таблиця 6. Забезпечення цілісності домену завдяки обмеженням атрибуту

SSN 243-27-3361	• Повинен містити дев'ять цифр • Формат xxx-xx-xxxx • Вводиться або змінюється лише клієнтом • Вимагає підтвердження
Номер кредитної карти 4539 4769 0728 4479	• Повинен містити шістнадцять цифр • Формат xxxx-xxxx-xxxx-xxxx • Вводиться або змінюється лише клієнтом • Вимагає підтвердження
Email адреса tortor@odio.com	• Повинна містити не більше 128 символів • Формат xxxx@xxxx.xxx • Вводиться або змінюється лише клієнтом • Перевіряється за допомогою відповіді через електронну пошту

ВИСНОВКИ

Тема 6 охоплює ключові аспекти забезпечення цілісності даних, які є основою надійності інформаційних систем. Цілісність даних забезпечується шляхом хешування, цифрових підписів, сертифікатів та контролю баз даних.

Хешування виступає як базовий механізм перевірки цілісності, що дає змогу виявити зміни в даних. Криптографічні хеш-функції, такі як SHA-256, демонструють високу стійкість до атак і є стандартом у сучасних системах. Використання солі під час хешування підвищує захист паролів, запобігаючи атакам грубої сили та застосуванню веселкових таблиць.

Цифрові підписи і сертифікати забезпечують перевірку автентичності джерела даних, гарантують їх незмінність і підтверджують авторство. Впровадження сертифікаційних механізмів, заснованих на інфраструктурі відкритих ключів (PKI), дає змогу створювати безпечні з'єднання та захищати електронні комунікації.

Цілісність баз даних підтримується через встановлення правил, таких як цілісність об'єктів, доменів, посилань та користувацьких обмежень. Ці заходи знижують ризики порушення даних і допомагають запобігати аномаліям у введенні. Методи виявлення аномалій є ефективними інструментами боротьби з шахрайством і забезпечення стабільності даних.

Загалом, тема підкреслює важливість комплексного підходу до забезпечення цілісності даних, інтеграції технічних та організаційних заходів, а також використання сучасних технологій для захисту інформації. Це сприяє зменшенню ризиків і підвищує довіру до інформаційних систем у цифрову епоху.

ТЕРМІНИ І КОНЦЕПЦІЇ

Ця вправа призначена для того, щоб ви могли практикувати важливі терміни та концепції, викладені в темі.

1. Атака грубої сили (brute-force)

– метод злому паролів шляхом перебору всіх можливих комбінацій.

2. Веселкові таблиці (Rainbow Tables)

–попередньо обчислені таблиці значень хеш-функцій, які використовуються для швидкого відновлення паролів шляхом пошуку їх відповідників у хешованій формі. Вони є ефективним інструментом для атаки на хеші паролів.

3. Виявлення аномалій

– процес ідентифікації незвичних або неочікуваних поведінкових характеристик у даних.

4. DoS-атака (Denial-of-Service)

– вид атаки, спрямований на порушення доступності сервісів шляхом перевантаження системи.

5. Домен цілісності

– набір правил, які обмежують допустимі значення в межах одного стовпця бази даних.

6. ECDSA (Elliptic Curve Digital Signature Algorithm)

– алгоритм цифрового підпису, який використовує еліптичні криві для зменшення розміру ключів при збереженні високого рівня безпеки.

7. Зовнішній ключ

– атрибут таблиці, який посилається на первинний ключ іншої таблиці для забезпечення цілісності посилань.

8. HMAC (Keyed-Hash Message Authentication Code)

– механізм автентифікації, який використовує хеш-функції спільно із секретним ключем для забезпечення цілісності та достовірності даних.

9. Криптографічна хеш-функція

– математична функція, яка генерує хеш-значення для будь-якого набору даних і є односторонньою та незворотною.

10. MD5

–алгоритм хешування, який приймає на вхід дані будь-якого розміру і генерує на виході 128-бітові хеші, але має вразливості до атак.

11. Первинний ключ

– унікальний ідентифікатор запису в таблиці бази даних.

12. Повільні хеш-функції

– спеціальні криптографічні функції, які спроектовані таким чином, щоб їх обчислення займало значно більше часу порівняно зі звичайними хеш-функціями. Основною метою використання повільних хеш-функцій **є** захист паролів та інших чутливих даних від атак, що базуються на переборі **або** використанні попередньо обчислених таблиць (rainbow tables).

13. PKI (Public Key Infrastructure)

– інфраструктура відкритих ключів, що забезпечує створення, поширення, зберігання та відкликання цифрових сертифікатів.

14. ***SQL-ін'єкція***

— вид атаки на бази даних, при якій зловмисник вставляє шкідливий SQL-код у запит, що виконується додатком. Це дає змогу йому отримати

несанкціонований доступ до даних, змінити або видалити їх, а також виконати інші небажані дії. Вразливість виникає через некоректну обробку введених користувачем даних, які інтегруються у SQL-запит без належної перевірки чи фільтрації.

15. SHA (Secure Hash Algorithm)

– сімейство алгоритмів хешування, що забезпечують більшу стійкість порівняно з MD5.

16. Сіль (Salt)

– випадковий рядок символів, який додається до даних перед хешуванням для підвищення безпеки.

17. Хешування

– процес обчислення унікального дайджесту (хеш-суми) фіксованої довжини для перевірки цілісності вхідних даних.

18. Цілісність даних

– забезпечення точності, узгодженості та надійності інформації під час її зберігання або передачі.

19. Цифровий відбиток

– результат роботи хеш-функції, який представляє унікальне значення для вхідних даних.

20. Цифровий підпис

– криптографічний механізм, який підтверджує достовірність, цілісність і неможливість відмови від авторства електронних документів.

21. Цифровий сертифікат

– електронний документ, що підтверджує автентичність власника та забезпечує шифрування даних для безпечного обміну інформацією.

22***. Цілісність бази даних***

– правила та методи забезпечення точності, узгодженості та надійності даних у базі.

ПРАКТИЧНЕ ЗАВДАННЯ 6.1. ЗАСТОСУВАННЯ ХЕШУ

Цілі завдання

Дослідити принципи та методи порівняння даних за допомогою хеш-функцій, використати програму хешування для перевірки цілісності даних.

Довідкова інформація/Сценарій

Важливо виявляти, пошкодження або підміну даних. Програма хешування може бути використана щоб перевірити, чи змінилися дані, чи вони залишилися незмінними. Програма хешування виконує хеш-функцію на даних або файлі та повертає значення (як правило, набагато коротше). Є багато різних хеш-функцій, деякі дуже прості, а деякі достатньо складні. Коли однакова хеш-функція виконується з однаковими даними, то значення, що повертається, завжди однакове. Якщо з даними відбуваються будь-які зміни, то повернене значення хешу буде іншим.

Необхідні ресурси

ПК з доступом до Інтернету.

ХІД ВИКОНАННЯ

Крок 1: Підготовка інформації

Підготуйте інформацію, на основі якої буде створюватися файл для подальшого хешування

Крок 2: Виклик Hash генератора

Відкрийте веббраузер і перейдіть за посиланням

https://tools.sochka.com/md5-sha1-hashing.html

Повинно відкритися вікно Hash генератора (рис.6.26).

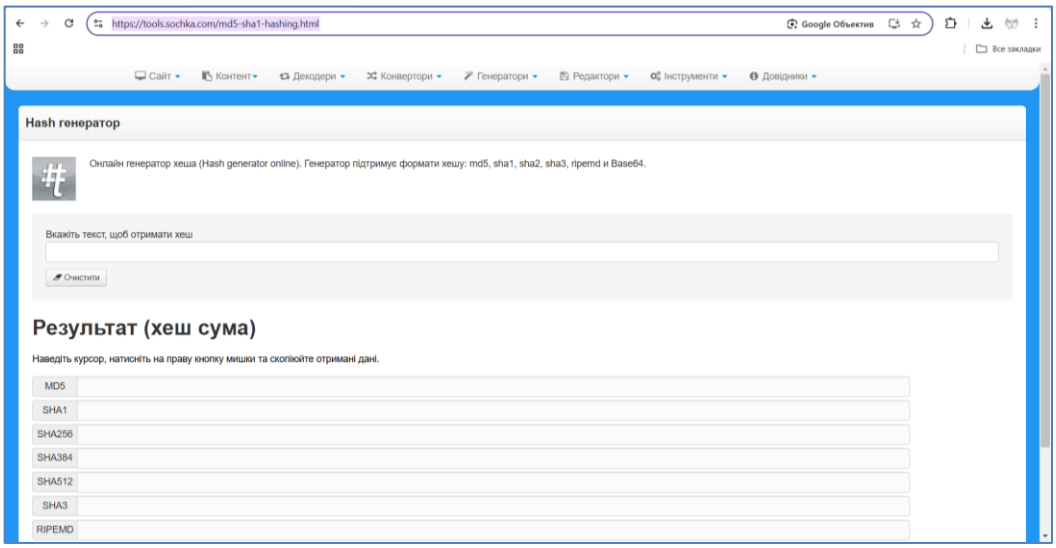


Рис. 6.26. Вікно Hash генератора

Крок 3: Введіть текст, щоб отримати хеш, обчисліть його

Вкажіть вигляд екрана зі сформованими хешами, надайте пояснення щодо отриманої картини.

a) Що означає рядок з написом MD5?
b) Що означають рядки з написами SHA1, SHA256, SHA384, SHA512, SHA3?
c) Які значення в них знаходяться?
d) Зверніть увагу, що багато типів хеш-функцій створюють хеш різної довжини. Чому?

Крок 4: Внесіть мінімальну зміну в інформацію, що хешується (додайте один символ).

Обчисліть новий хеш. Зафіксуйте його копіями екранів.

Поясніть різницю в отриманих результатах.

Крок 5: Внесіть багатозначну зміну у інформацію, що хешується

Повторіть процедуру зміни вхідного повідомлення 5-разово. Змінюйте довжину повідомлення, кількість і тип символів, що додаються або прибираються.

Останнім експериментом повторіть хешування першого повідомлення.

e) Які значення сформовані в рядку MD5? Як вони змінювались?
f) Які значення отримані поряд з іншими функціями? Як впливала на отримані результати зміна інформації в рядку вводу тексту?
g) Чи отримали в останньому експерименті хеш, еквівалентний першому? Про що це свідчить?
h) Розкажіть про алгоритми хешування, опишіть їхні переваги та недоліки.

Крок 6. Сформулюйте висновки.

ПРАКТИЧНЕ ЗАВДАННЯ 6.2. ВИКОРИСТАННЯ ЕЦП

Цілі завдання

Зрозуміти концепції цифрового підпису.

Частина 1: Продемонструвати використання цифрових підписів.

Частина 2: Продемонструвати перевірку цифрового підпису.

Довідкова інформація / Сценарій

Цифровий підпис – це математичний метод, який використовується для перевірки автентичності та цілісності цифрового повідомлення. Цифровий підпис є еквівалентом рукописного підпису. Цифрові підписи можуть бути набагато більш безпечними. Мета цифрового підпису полягає в тому, щоб запобігти підробці та інперсоніфікації цифрових повідомлень. У багатьох країнах, включаючи Сполучені Штати, цифрові підписи мають таке ж юридичне значення, як і традиційні форми підписаних документів. Уряд Сполучених Штатів тепер публікує електронні версії бюджетів, законів і законопроектів Конгресу з цифровими підписами.

Необхідні ресурси

ПК або мобільний пристрій з доступом до Інтернету

ХІД ВИКОНАННЯ

ЧАСТИНА 1: ВИКОРИСТАННЯ ЦИФРОВИХ ПІДПИСІВ

У цій частині ви будете використовувати вебсайт для перевірки підпису документа між Алісою і Вами. Аліса і Ви використовуєте одну пару закритих і відкритих ключів RSA. Кожен з вас використовує свій закритий ключ для підписання юридичного документа (таблиця 1п). Потім ви відправляєте документи один одному. І Аліса, і Ви можете перевірити підпис один одного відкритим ключем. Ви також повинні домовитися про спільну відкриту експоненту для розрахунку.

Таблиця 1п. Відкритий і закритий ключі RSA

Відкритий ключ RSA	d94d889e88853dd89769a18015a0a2e6bf82bf356fe14f251fb4f5e2df0d9f9a94a68a30c428b39e3362fb3779a497eceaea37100f264d7fb9fb1a97fbf621133de55fdcb9b1ad0d7a31b379216d79252f5c527b9bc63d83d4ecf4d1d45cbf843e8474babc655e9bb6799cba77a47eafa838296474afc24beb9c825b73ebf549
Закритий ключ RSA	47b9cfde843176b88741d68cf096952e950813151058ce46f2b048791a26e507a1095793c12bae1e09d82213ad9326928cf7c2350acb19c98f19d32d577d666cd7bb8b2b5ba629d25ccf72a5ceb8a8da038906c84dcdb1fe677dffb2c029fd8926318eede1b58272af22bda5c5232be066839398e42f5352df58848adad11a1
Відкрита експонента	10001

Крок 1: Підпишіть документ

Аліса підписує юридичний документ і відправляє його Вам з використанням відкритих і закритих ключів RSA (рис.6.27), показаних в таблиці вище. Тепер Вам доведеться перевірити цифровий підпис Аліси, щоб довіряти справжності електронного документа.

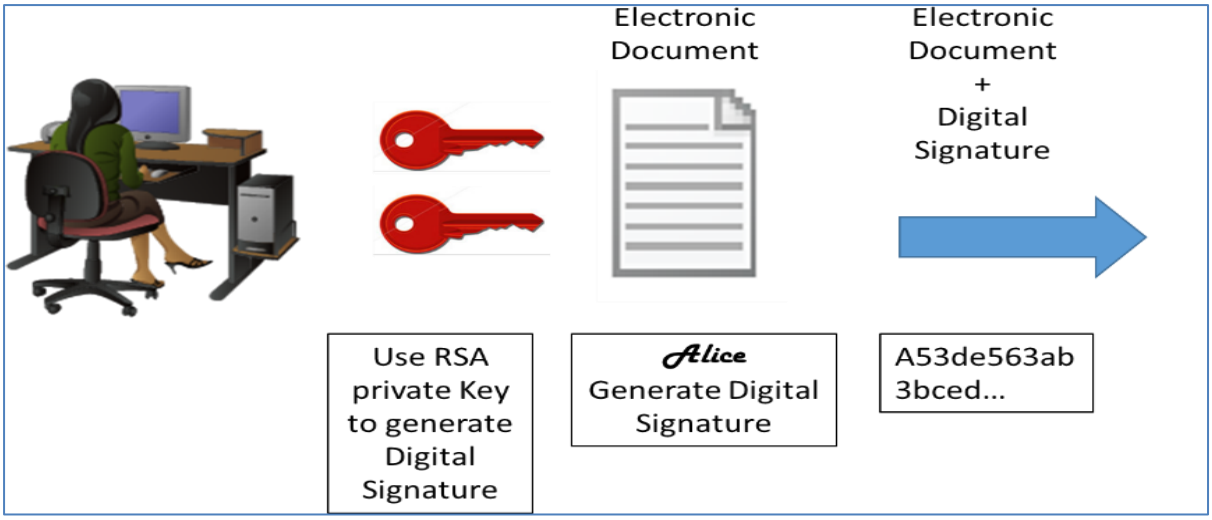


Рис.6.27. Перевірка підпису документа[92]

Крок 2: Перевірте цифровий підпис

Ви отримує документ з цифровим підписом, показаним в таблиці 2п.

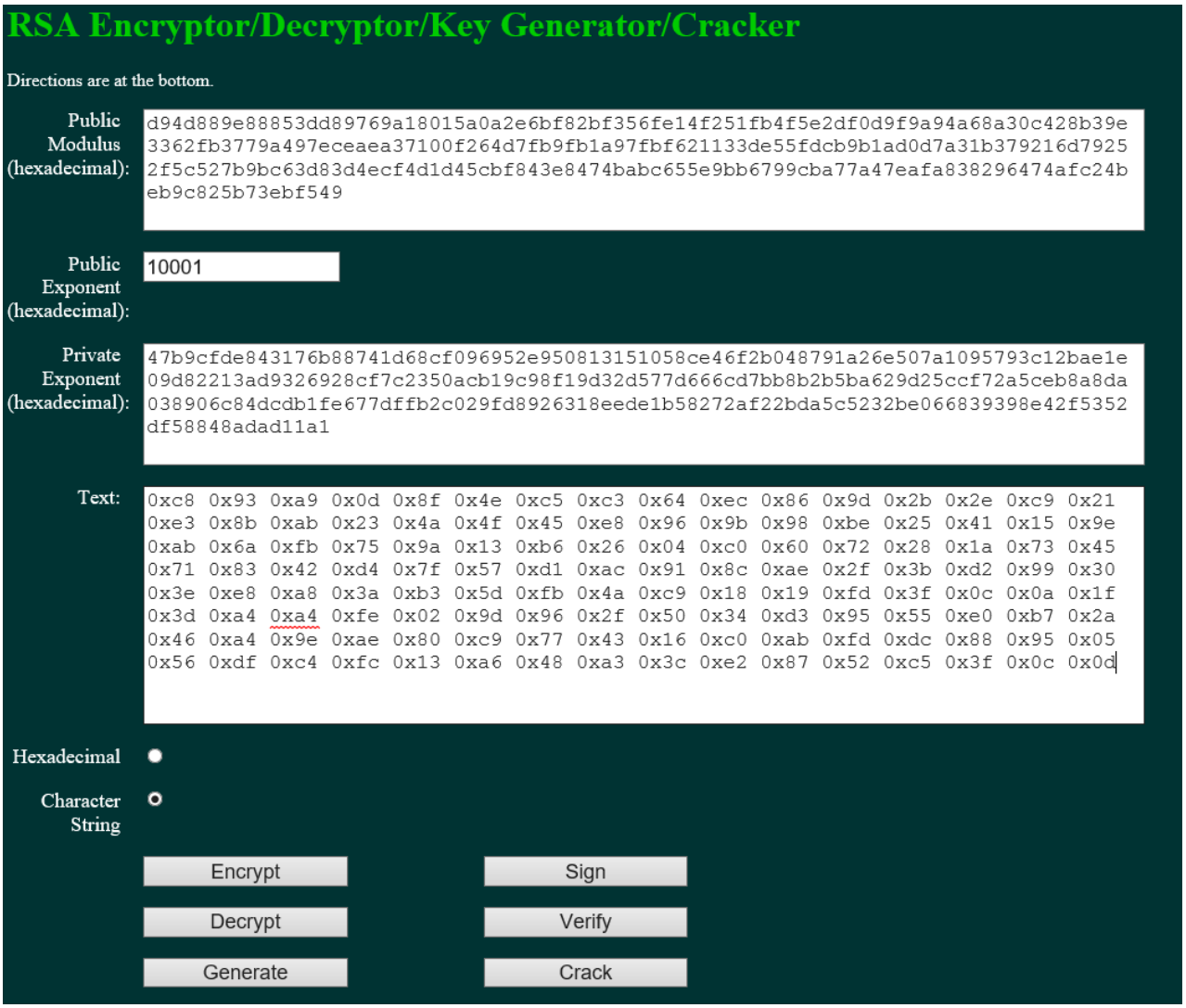
Таблиця 2п Цифровий підпис Аліси

Цифровий підпис Аліси
0xc8 0x93 0xa9 0x0d 0x8f 0x4e 0xc5 0xc3 0x64 0xec 0x86 0x9d 0x2b 0x2e 0xc9 0x21 0xe3 0x8b 0xab 0x23 0x4a 0x4f 0x45 0xe8 0x96 0x9b 0x98 0xbe 0x25 0x41 0x15 0x9e 0xab 0x6a 0xfb 0x75 0x9a 0x13 0xb6 0x26 0x04 0xc0 0x60 0x72 0x28 0x1a 0x73 0x45 0x71 0x83 0x42 0xd4 0x7f 0x57 0xd1 0xac 0x91 0x8c 0xae 0x2f 0x3b 0xd2 0x99 0x30 0x3e 0xe8 0xa8 0x3a 0xb3 0x5d 0xfb 0x4a 0xc9 0x18 0x19 0xfd 0x3f 0x0c 0x0a 0x1f 0x3d 0xa4 0xa4 0xfe 0x02 0x9d 0x96 0x2f 0x50 0x34 0xd3 0x95 0x55 0xe0 0xb7 0x2a 0x46 0xa4 0x9e 0xae 0x80 0xc9 0x77 0x43 0x16 0xc0 0xab 0xfd 0xdc 0x88 0x95 0x05 0x56 0xdf 0xc4 0xfc 0x13 0xa6 0x48 0xa3 0x3c 0xe2 0x87 0x52 0xc5 0x3f 0x0c 0x0d

Скористайтесь посиланням https://www.nmichaels.org/rsa.py, щоб використати онлайн-інструмент RSA для перевірки справжності цифрового підпису Аліси (таблиця 3п).

[92] – This figure was uploaded by link.springer.com

Таблиця 3п. Онлайн-інструмент цифрового підпису



a) Скопіюйте і вставте відкриті і закриті ключі з таблиці 1 у поля Public Modulus і Private Exponent на сайті, як показано на рисунку вище.

b) Переконайтеся, що значення Public Exponent дорівнює 10001.

c) Вставте цифровий підпис Аліси з Таблиці 2 в поле з написом на вебсайті, як показано вище.

d) Тепер Ви можете перевірити цифровий підпис, натиснувши кнопку Verify знизу вебсайту. Чий підпис ідентифіковано?

Крок 3: Створіть підпис для відповіді

Ви отримує і перевіряє електронний документ і цифровий підпис Аліси. Тепер Ви створюєте електронний документ і генеруєте свій власний цифровий підпис, використовуючи закритий ключ RSA в таблиці 1.

Ви посилаєте Алісі електронний документ і цифровий підпис.

Крок 4: Перевірте цифровий підпис

a) Скопіюйте і вставте відкриті і закриті ключі з таблиці 1 вище у поля Public Modulus і Private Exponent на сайті, як показано на рисунку вище.

b) Переконайтеся, що значення Public Exponent дорівнює 10001.

c) Вставте Ваш цифровий підпис з таблиці варіантів в поле з написом на вебсайті, як показано вище.

d) Тепер Аліса може перевірити цифровий підпис, натиснувши кнопку Verify знизу вебсайту. Чий підпис ідентифіковано?

ЧАСТИНА 2: СТВОРІТЬ СВІЙ ВЛАСНИЙ ЦИФРОВИЙ ПІДПИС

Тепер, коли ви бачите, як працюють цифрові підписи, ви можете створити свій власний цифровий підпис.

Крок 1: Створіть нову пару RSA-ключів

a) Перейдіть на інструмент вебсайту і створіть новий набір відкритих і закритих ключів RSA.

b) Видаліть вміст полів з написами Public Modulus, Private Modulus і Text. Просто використовуйте мишу, щоб виділити текст і натисніть клавішу delete на клавіатурі.

c) Переконайтеся, що поле «Public Exponent» має значення 10001.

d) Створіть новий набір ключів RSA, натиснувши кнопку Generate в правому нижньому кутку вебсайту.

e) Скопіюйте нові ключі в таблицю 4п.

Таблиця 4п. Нові ключі RSA

Відкритий ключ	
Закритий ключ	

Тепер введіть своє повне ім'я в таблицю 5п та поле з написом Text і натисніть Sign.

Таблиця 5п. Персональний цифровий підпис

Персональний цифровий підпис	

ЧАСТИНА 3: ОБМІНЯЙТЕСЯ І ПЕРЕВІРТЕ ЦИФРОВІ ПІДПИСИ

Тепер ви можете використовувати цей цифровий підпис.

Крок 1: Обміняйтеся вашими новими відкритими і закритими ключами в Таблиці 5 з вашим партнером по лабораторній роботі.

a) Запишіть відкриті і закриті ключі RSA свого партнера з його Таблиці 4п.

b) Запишіть обидва ключа в таблицю нижче (Таблиці 6п).

Таблиця 6п. Ключі RSA партнера по лабораторній роботі

Відкритий ключ	
Закритий ключ	

c) Тепер обміняйтеся цифровими підписами з Таблиці 5п. Запишіть цифровий підпис в Таблицю 7п.

Таблиця 7п. Цифровий підпис

Цифровий підпис партнера по лабораторній роботі	

Крок 2: Перевірте цифровий підпис партнера по лабораторній роботі

a) Щоб підтвердити цифровий підпис свого партнера, вставте його або її відкриті і закриті ключі до відповідних полів, помічених Public and Private modulus на вебсайті.

b) Тепер вставте цифровий підпис в поле з написом Text.

c) Тепер перевірте його або її цифровий підпис, натиснувши кнопку verify.

d) Що відображається в текстовому полі?

У висновку поясніть мету і сферу застосування цифрових підписів.

ТЕМА 7. ЗАХИСТ ОРГАНІЗАЦІЙ ВІД КІБЕРАТАК В УМОВАХ ВІЙНИ ТА ПОВСЯКДЕННІЙ ДІЯЛЬНОСТІ

Ця тема охоплює деякі технології та процеси, що використовуються фахівцями з кібербезпеки для захисту мережі, обладнання та даних організації (рис.7.1). Спочатку коротко описуються різні типи міжмережевих екранів, пристроїв безпеки та програмного забезпечення, які на цей час використовуються, а також найкращі рекомендації щодо їх застосування.

Рис.7.1. Підготовка атаки[93]

Далі в цій темі пояснюється, що таке бот-мережі, ланцюг кібервбивства (kill chain), захист на основі аналізу поведінки та особливості використання NetFlow для моніторингу мережі.

У третій частині теми обговорюється підхід компанії Cisco до кібербезпеки, а саме група швидкого реагування CSIRT та збірка сценаріїв з безпеки (security playbook). Коротко розглядаються інструменти, які використовують експерти з кібербезпеки для виявлення мережевих атак та їх запобігання.

7.1. СКАНУВАННЯ ПОРТІВ

Сканування портів – це процес зондування комп'ютера, сервера або іншого мережевого пристрою для виявлення відкритих портів. В мережах кожному застосунку, запущеному на пристрої, призначається ідентифікатор, який називається номером порта. Саме завдяки використанню цього номера на обох кінцях сеансу зв'язку необхідні дані передаються до потрібного застосунку. Сканування портів може використовуватися зі зловмисною метою як розвідувальний інструмент для ідентифікації операційної системи та служб, що працюють на комп'ютері або іншому пристрої. А також цей підхід застосовується мережевим адміністратором для перевірки політик безпеки в мережі.

З метою оцінки ефективності міжмережевого екрану та безпеки портів у вашій комп'ютерній мережі, ви можете використовувати такий інструмент сканування портів, як Nmap, для пошуку всіх відкритих портів (рис. 7.2).

[93] – https://www.shutterstock.com/ru/image-vector/two-businessman-computer-laptop-send-email-355094873

Оскільки сканування портів може розглядатися як попередник мережевої атаки, не слід випробовувати його без дозволу на публічних серверах в Інтернеті або в мережі компанії.

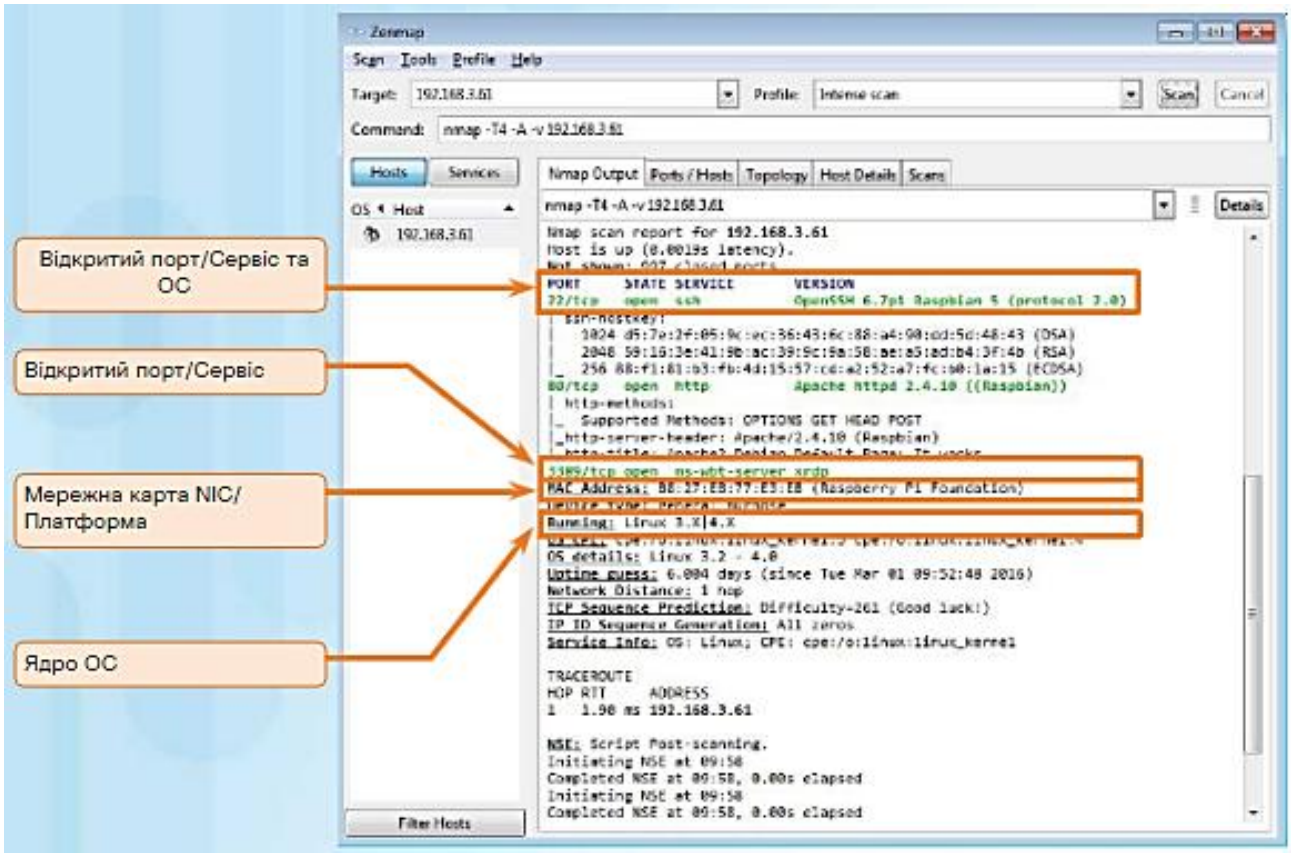


Рис. 7.2. Результати сканування портів за допомогою Nmap

Щоб виконати сканування портів на комп’ютері у вашій локальній домашній мережі за допомогою Nmap, завантажте та запустіть таку програму як, наприклад, Zenmap, вкажіть цільову IP-адресу комп’ютера, який ви хочете просканувати, виберіть стандартний профіль сканування та натисніть Сканувати. Після сканування Nmap повідомлятиме про всі активні служби (наприклад, вебсервіси, поштові служби тощо) та номери портів. Результатом сканування портів зазвичай, може бути одна з трьох відповідей:

- ***Open або Accepted*** – хост відповів, вказуючи на те, що ця служба прослуховує порт.
- ***Closed, Denied або Not Listening*** – хост відповів, що з’єднання з портом будуть відхилені.
- ***Filtered, Dropped або Blocked*** – не було відповіді від хоста.

Щоб виконати сканування портів вашої мережі з зовнішньої мережі, ви маєте ініціювати сканування поза межами мережі. Це передбачає запуск Nmap для сканування портів вашого міжмережевого екрану або публічної IP-адреси маршрутизатора. Щоб визначити вашу публічну IP-адресу, використовуйте

пошукову систему, таку як Google, із запитом "Яка моя IP-адреса?". Пошукова система поверне перелік ресурсів для визначення вашої публічної IP-адреси.

Щоб запустити сканування шести найбільш популярних портів для вашого домашнього маршрутизатора або міжмережевого екрану, перейдіть до онлайн-сканера портів (Nmap Online Port Scanner) за адресою: https://hackertarget.com/nmap-online-port-scanner/ та задайте свою публічну IP-адресу в полі вводу*: IP address to scan…* і натисніть кнопку *Quick Nmap Scan*. Якщо є відповідь *open* для будь-якого з портів: 21, 22, 25, 80, 443 або 3389, то, швидше за все, на вашому маршрутизаторі або міжмережевому екрані увімкнена переадресація портів і ви у своїй приватній мережі використовуєте сервери, як показано на рисунку 7.3.

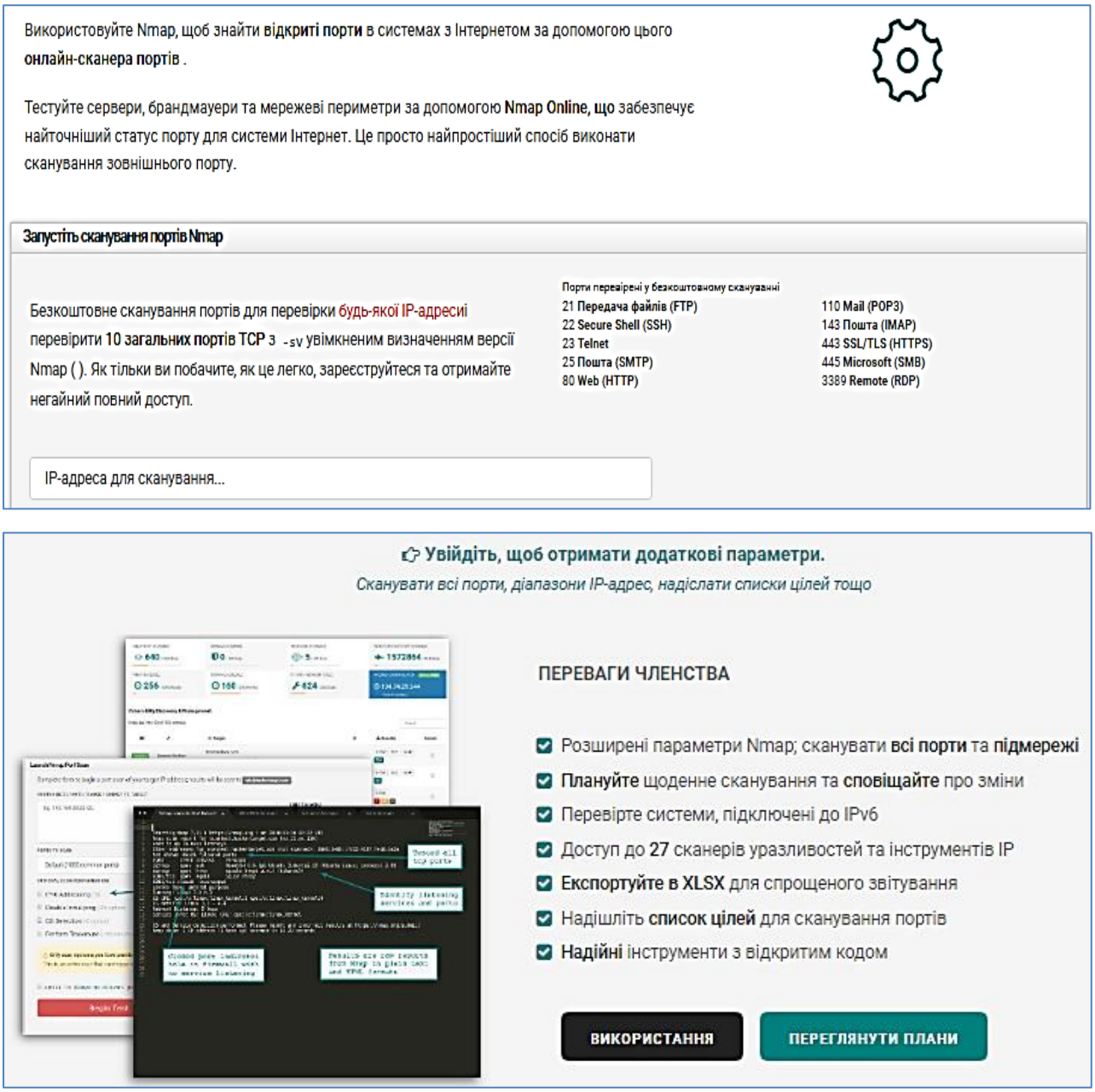


Рис. 7.3. Онлайн-сканер портів Nmap

Шість випадків використання онлайн-сканера портів

Визначте статус брандмауерів на основі хоста та мережі

Розуміння результатів онлайн-сканування Nmap покаже, чи є брандмауер: shodan.io. Пошуковик знаходить мільйони погано налаштованими міжмережевими екранами на щоденній основі.

Перевірте протоколювання брандмауера та IDS

Запустіть дистанційне сканування вашої інфраструктури, щоб перевірити, чи ваш моніторинг безпеки працює належним чином. Перегляньте реєстрацію брандмауера та сповіщення системи виявлення вторгнень.

Знайдіть відкриті порти на хмарних віртуальних серверах

У 2016 році тисячі баз даних MongoDB були скомпрометовані, а дані витікали через те, що сервер був налаштований на прослуховування через Інтернет-інтерфейс. Використовуючи онлайн-сканер портів, можна швидко ідентифікувати брандмауер хоста з погано налаштованими отворами або службами.

Виявлення несанкціонованих змін брандмауера

Коли зміни бази правил брандмауера потребують схвалення ради змін. Заплановане сканування портів Nmap може швидко визначити зміни брандмауера, які не пройшли процедуру затвердження змін.

Не всі брандмауери добре працюють з IPv6

У міру розгортання IPv6 важливо зрозуміти, чи має інтерфейс IPv6 такий же рівень захисту, як і існуючі адреси IPv4. Багато віртуальних серверів (VPS) розгорнуті з увімкненим IPv6 за замовчуванням. Ви перевірили своє?

Усунення несправностей мережевих служб

Вас підштовхують до впровадження нової послуги. Менеджери кажуть, що це не їхня проблема, а адміністратор брандмауера вказує пальцем на розробників. Іноді вам просто потрібно знати, чи відкритий порт і чи хтось його слухає.

Щоб розпочати сканування портів онлайн сканером Nmap потрібно зробити лише три кроки.

Крок 1. Заповніть форму; введення адреси або імені хоста цілі

Введіть загальнодоступну IP-адресу або ім’я хосту, до яких можна отримати доступ із зовнішнього Інтернету. Ви повинні мати дозвіл на сканування цілі. Онлайн-сканування портів Nmap також можна виконувати за списком дійсних цільових адрес; просто додайте цілі, розділені комами або у вигляді списку з розривами рядків.

Скануйте одну IP-адресу або ім’я хосту. Приклад: 192.168.1.1 example.com.

Сканувати діапазон IP-адрес Приклад: 192.168.1.0/24 192.168.1.1-50

Вибравши опцію **Об'єднати звіт,** учасники можуть вибрати отримання єдиного звіту, який містить підсумкову таблицю кількох запитуваних цілей NMAP, а також повні результати, представлені в одному файлі (рис.7.4).

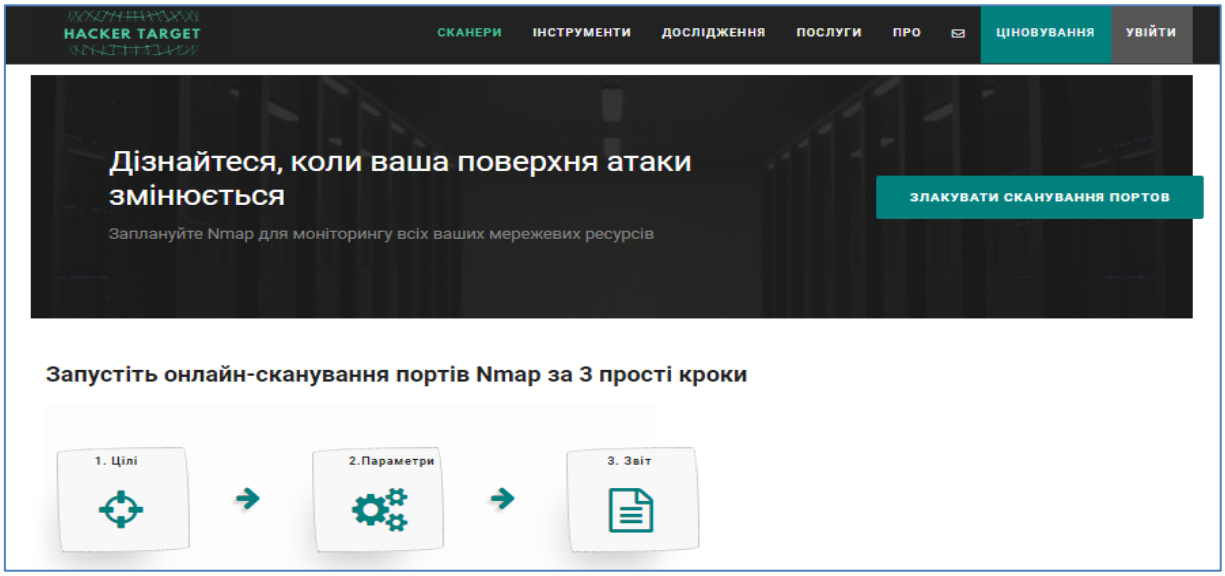


Рис.7.4. Рекомендації

Крок 2. Вирішіть, які порти ви хочете сканувати

Виберіть параметр порту на основі стандартних параметрів Nmap; За замовчуванням, Швидке сканування (-F) або Сканування всіх портів 65535 на IP-адресі. Сканування всіх портів – найточніший спосіб виявити кожну службу прослуховування. Для всебічної перевірки конфігурації брандмауера потрібне повне сканування всіх портів. Зауважте, що повне сканування може тривати від 20 хвилин до кількох годин залежно від мережі.

Також доступне сканування загальних портів UDP, а також користувацька опція конфігурації порту, де ви можете вибрати підмножину конкретних портів (udp або tcp).

Можна вказати додаткову конфігурацію:

- Протокол за замовчуванням – IPv4, виберіть параметр Протокол, щоб увімкнути IPv6 (параметр nmap –6)
- Пінг виконується за замовчуванням, щоб переконатися, що система відповідає, виберіть опцію, щоб вимкнути ping (параметр nmap –Pn)
- Увімкніть виявлення ОС, щоб перевірити версію операційної системи (параметр nmap –O)
- Виконайте необов'язковий метод Traceroute, використовуючи результати сканування портів, щоб знайти найбільш точний метод (опція nmap --traceroute)

Крок 3. Останнім кроком є просто запуск сканування портів

Фактичний час сканування буде значно відрізнятися залежно від цільової мережі та кількості портів, які скануються.

Результати Nmap будуть доставлені на вашу зареєстровану електронну адресу після завершення сканування порту. Результати також доступні на **інформаційній панелі учасників** для завантаження. Покращуйте свій робочий процес звітування про безпеку за допомогою простої у використанні опції експорту в XLSX для всіх відкритих портів. Створення підсумкових звітів для кількох профілів сканування та/або мереж.

Зразок результатів від Nmap Online

Налаштування за замовчуванням виконуватимуть сканування портів за допомогою тесту на основі TCP SYN. Це стандартне сканування портів Nmap (-sS) з увімкненим визначенням версії (nmap -sV). Будь-які інші вибрані додаткові параметри будуть включені.

Результати надсилаються на електронну адресу зареєстрованих користувачів. Результати сканування доступні у форматі простого тексту та HTML (рис. 7.5).

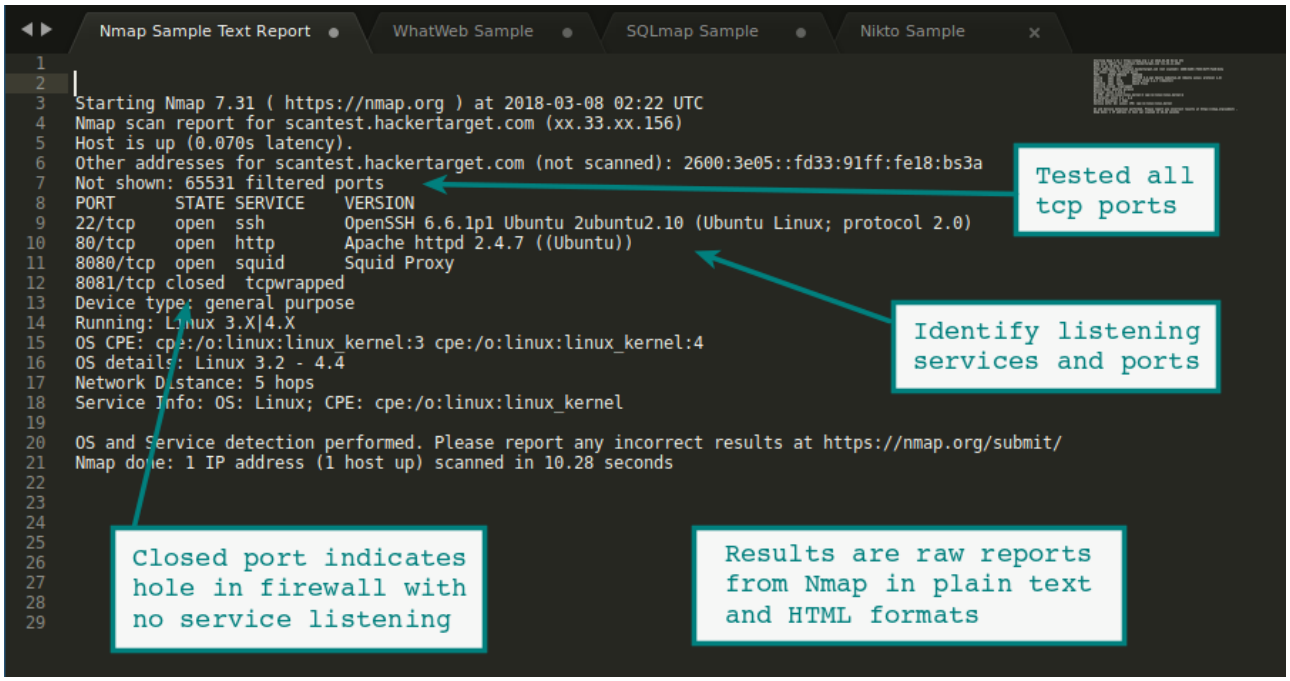


Рис. 7.5. Відображення результатів сканування портів інструментом Nmap

Про програмне забезпечення сканера портів Nmap

Nmap – це сканер мережевих портів, який перевіряє мережеве підключення між різними хостами та службами. Брандмауери, ACL маршрутизатора та інші фактори можуть вплинути на мережеве підключення.

Спочатку Nmap був простим, але потужним інструментом, який дозволяв сканувати мережі або окремі хости, щоб визначити, чи працюють служби та чи є брандмауер. Сучасні версії Nmap мають розширені можливості, включаючи

вбудовану мову сценаріїв (NSE), яка може виконувати безліч додаткових перевірок щодо будь-яких служб, які виявлено відкритими. Цей постійно зростаючий список скриптів штовхнув Nmap у сферу швидкого легкого сканера вразливостей.

Завантажте Nmap сьогодні з сайту https://insecure.org/ (рис.7.6), він доступний у версіях для Windows і Linux / FreeBSD. Zenmap – це графічний інтерфейс для тих, кому не зручно працювати з командним рядком. Під час встановлення Nmap я закликаю вас завантажувати з вихідного коду, оскільки він постійно вдосконалюється та надбудовується. Дистрибутиви Linux не завжди матимуть останню версію в сховищі пакунків.

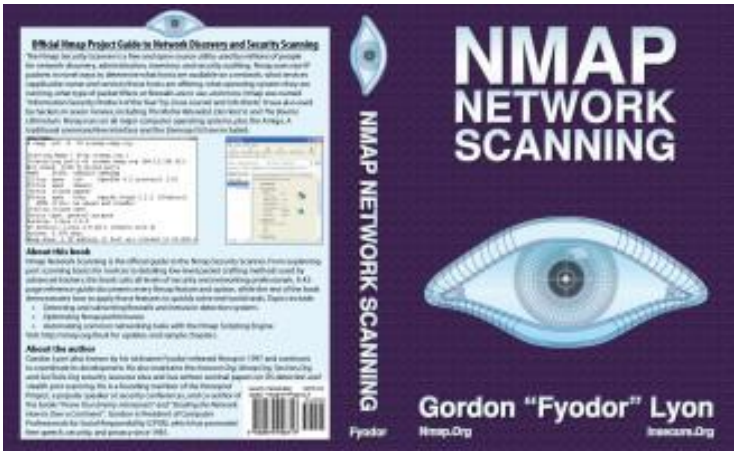


Рис.7.6. Завантажте Nmap

7.2. ПРИСТРОЇ БЕЗПЕКИ

На сьогодні не існує єдиного пристрою безпеки або технології, які б дозволили вирішити всі проблеми мережевої безпеки. Через наявність безлічі пристроїв та програмних інструментів захисту важливо, щоб вони працювали разом. Пристрої безпеки найбільш ефективні, коли вони є частиною системи.

Пристрої безпеки можуть бути автономними пристроями, такими як маршрутизатор або міжмережевий екран, платою, яку можна встановити до мережевого пристрою, або модулем із власним процесором та кешованою пам'яттю. Засоби безпеки також можуть бути реалізовані програмно та запускатись на мережевому пристрої. Пристрої безпеки поділяються за категоріями:

Міжмережеві екрани

Міжмережевий екран (фаєрвол, брандмаурер) – ключовий елемент системи кібербезпеки, що забезпечує моніторинг і контроль трафіку між довіреною мережею (наприклад, внутрішньою корпоративною) і зовнішніми ресурсами, такими як Інтернет. Це умовна стіна, яка призначена для запобігання поширенню вогню з однієї частини будівлі в іншу. Як показано на рисунку 7.7, в комп'ютерних мережах міжмережевий екран використовується для контролю або фільтрації повідомлень, яким дозволено входити/виходити до/з пристрою або мережі. Фаєрвол може встановлюватися на одному комп'ютері з метою його захисту (фаєрвол на базі хоста – host-based firewall), або він може бути

автономним пристроєм, який захищає комп'ютери та всі інші пристрої у мережі (мережевий фаєрвол – network-based firewall).

З роками, комп'ютерні та мережеві атаки стали більш витонченими, тому були розроблені нові типи міжмережевих екранів для задоволення різних потреб у процесі захисту мережі. Нижче наведено перелік найбільш поширених типів міжмережевих екранів:

- ***Фаєрвол мережевого рівня (Network Layer Firewall)*** – фільтрування на основі IP-адрес джерела та отримувача.
- ***Міжмережевий екран транспортного рівня (Transport Layer Firewall)*** – фільтрування на основі портів відправника й отримувача, та фільтрування на основі станів з'єднання.

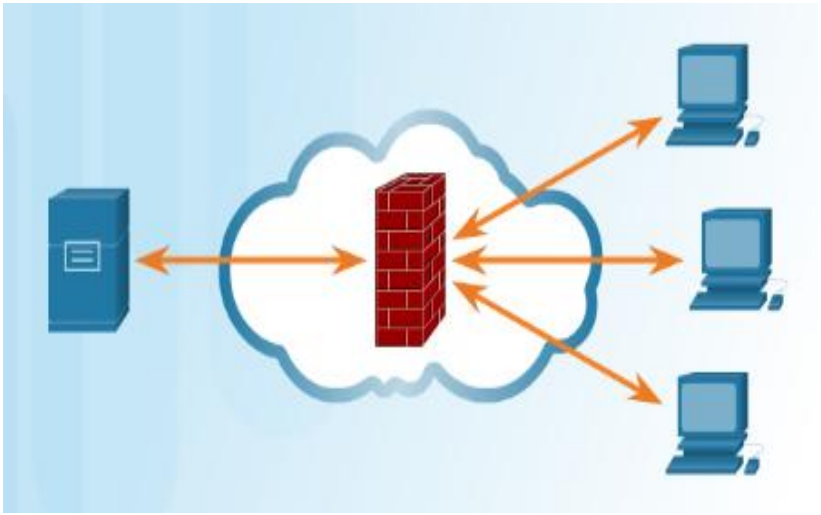


Рис. 7.7. Робота міжмережного екрану[94]

- ***Міжмережевий екран прикладного рівня (Application Layer Firewall)*** – фільтрування на основі типу застосунку, програми або сервісу.
- ***Міжмережевий екран на основі контексту (Context Aware Application Firewall)*** – фільтрування на основі користувача, пристрою, ролі, типу застосунку та профілю загроз.
- ***Проксі-сервер (Proxy Server)*** – фільтрування вмісту вебзапитів, таких як URL-адреса, домен, соцмережі тощо.
- ***Зворотний проксі-сервер (Reverse Proxy Server)*** – розміщується перед вебсерверами і захищає, приховує, розвантажує та розподіляє доступ до вебсерверів.
- ***NAT-міжмережевий екран (Network Address Translation (NAT) Firewall)*** – приховує або маскує приватні адреси хостів у мережі.
- ***Фаєрвол на базі хоста (Host-based Firewall)*** – фільтрація портів та викликів системних служб на одному комп'ютері.

Firewalls (міжмережеві екрани) – міжмережеві екрани Cisco нового покоління (Cisco Next Generation Firewalls) підтримують усі можливості маршрутизатора ISR, а також надають розширені функції керування та аналітики в мережі. Cisco Adaptive Security Appliance (ASA) з можливостями міжмережевого екрана зображено на рисунку 7.8.

[94] – https://link.springer.com/book/10.1007/978-3-031-32959-3

Рис. 7.8. Міжмережеві екрани Cisco[95]

Routers (Маршрутизатори) – маршрутизатори Cisco з інтегрованими сервісами (Integrated Services Router – ISR), зображені на рисунку 7.9, окрім самої маршрутизації виконують багато функцій міжмережевого екрана, включно з фільтрацією трафіку, можливістю запуску системи запобігання вторгненням (Intrusion Prevention System, IPS), шифрування та VPN-тунелювання.

Рис. 7.9. Маршрутизатори Cisco[96]

IPS – IPS пристрої Cisco нового покоління (Cisco Next Generation IPS), показані на рисунку 7.10, призначені для запобігання вторгненням.

Рис. 7.10. IPS пристрої Cisco[97]

VPN – пристрої безпеки Cisco оснащені технологіями віртуальної приватної мережі (Virtual Private Network, VPN) для сервера і клієнта. Ця технологія розроблена для безпечного зашифрованого тунелювання.

95,96,97 - https://www.cisco.com/c/ru_ua/index.html

Malware/Antivirus – Cisco Advanced Malware Protection (AMP) постачається на маршрутизаторах Cisco нового покоління, міжмережевих екранах, пристроях IPS, пристроях безпеки для Web та електронної пошти, а також може встановлюватися як ПЗ на комп'ютерах.

Інші пристрої безпеки – до цієї категорії належать засоби захисту web та електронної пошти, пристрої дешифрування, сервери керування доступом клієнтів та системи контролю безпеки.

7.3. КІБЕРАТАКИ ТА ЇХНЄ ВИЯВЛЕННЯ

Еволюція кіберзагроз та інструменти захисту (рис.7.11)

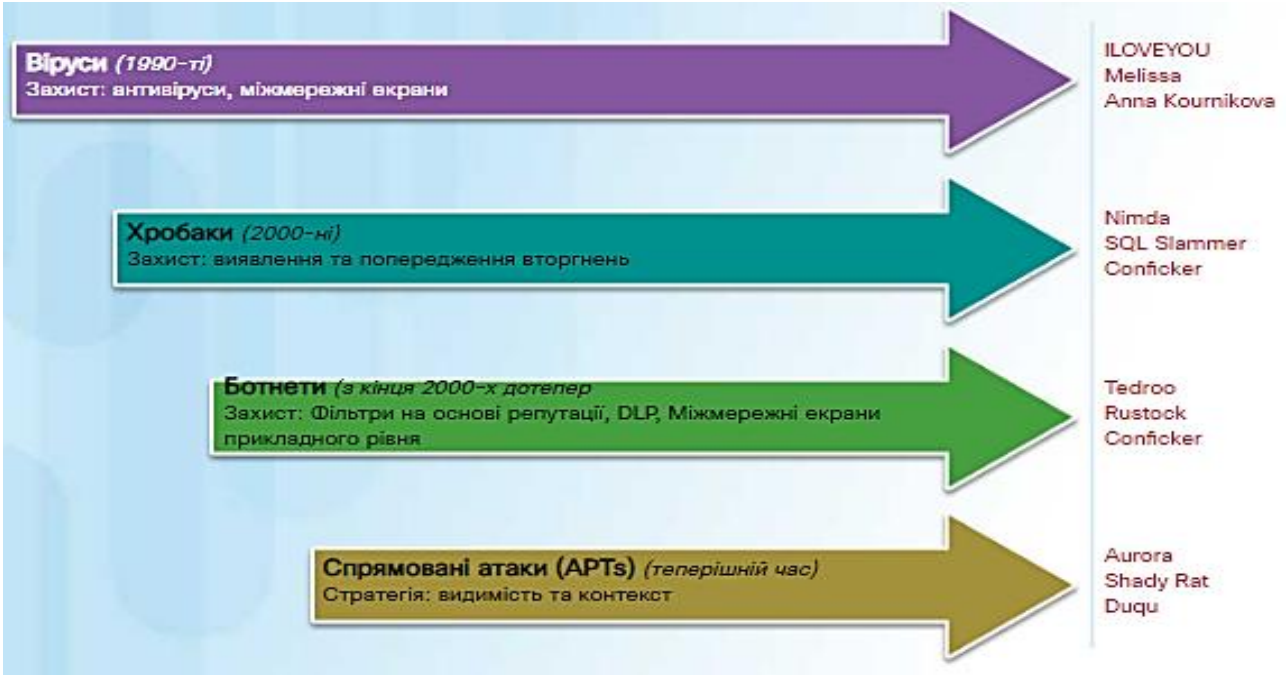


Рис.7.11. Еволюція кіберзагроз[98]

Виявлення атак у реальному часі

Програмне забезпечення не є досконалим. Атака нульового дня (zero-day attack) виникає, коли зловмисник намагається використовувати вразливості у частині коду програми, перш ніж їх виправить розробник. Витонченість та кількість атак нульового дня сьогодні зростає, тому шанси зловмисників досягнути цілі високі, а успішність захисту тепер вимірюється тим, наскільки швидко мережа зможе відреагувати на атаку.

[96] – https://www.researchgate.net/profile/Md-Miah-107/publication/356918824/figure/fig9/AS:1099479348461595@1639147712692/Figure-Behavior-Based-Security_W640.jpg

Найкращим сценарієм було б виявлення атак по мірі їх розгортання у реальному часі та припинення їх негайно або протягом кількох хвилин. На жаль, багато компаній та організацій сьогодні не здатні виявити атаки впродовж кількох днів чи навіть місяців після їх появи. Швидка ідентифікація та аналіз подій є критично важливими для мінімізації шкоди від атак та забезпечення стабільності систем.

Сканування у реальному часі від периметра до кінцевих вузлів мережі – Виявлення атак у реальному часі потребує активного зондування на наявність атак за допомогою міжмережевого екрана та мережевих пристроїв IDS/IPS. Також для виявлення шкідливих програм слід використовувати клієнт/серверне програмне забезпечення нового покоління з під'єднання до глобальних онлайн-центрів аналізу загроз. Сьогодні активні пристрої сканування та програмне забезпечення повинні виявляти аномалії мережі, використовуючи аналіз з урахуванням контексту та на основі поведінки.

DDoS-атаки та реагування в режимі реального часу – DDoS – це одна з найбільших загроз, яка потребує виявлення та реакції у реальному часі. Як показано на рисунку 7.12, від атак DDoS надзвичайно важко захиститись, оскільки пакети-нападники, що виглядають як дозволений трафік, надходять від сотень або тисяч підставних хостів-зомбі. Для багатьох компаній та організацій регулярні атаки DDoS порушують роботу інтернет-серверів і негативно впливають на доступність мережі. Тому можливість виявлення та реагування на атаки DDoS в режимі реального часу має вирішальне значення.

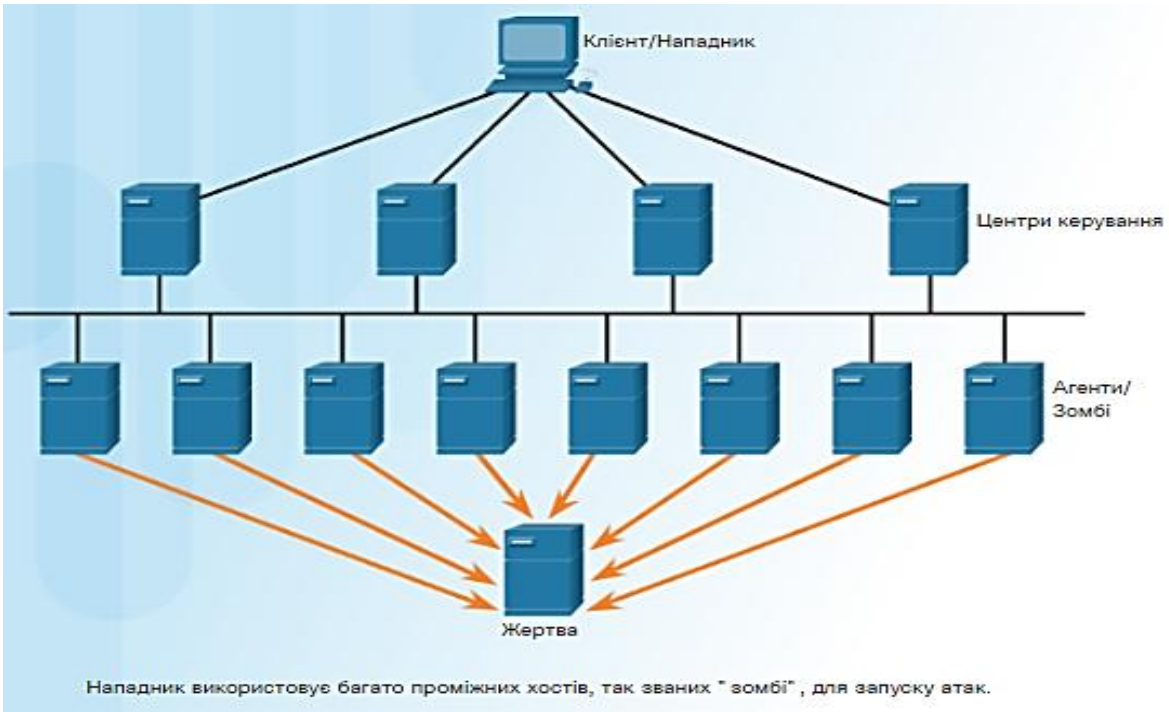


Рис. 7.12. Розподілені атаки відмови в обслуговуванні DDoS[99]

[99] – https://ictechnotes.blogspot.com/2011/07/network-security-acl.html

Як забезпечити захист від постійних атак нульового дня, а також розвинутих цільових загроз (advanced persistent threats – APT), які викрадають дані протягом тривалого часу? Одним із рішень може бути використання на рівні підприємства сучасних засобів для виявлення зловмисного ПЗ в режимі реального часу.

Мережеві адміністратори повинні постійно моніторити мережу на наявність ознак шкідливого ПЗ або шаблонів поведінки, які вказують на присутність APT. Cisco пропонує систему вдосконаленого захисту від шкідливого ПЗ (Advanced Malware Protection – AMP), яка аналізує мільйони файлів і зіставляє їх із сотнями мільйонів інших проаналізованих зразків шкідливих програм. Це забезпечує глобальну оцінку шкідливих атак, серій зловмисних операцій і їх поширення.

Ефективність таких систем залежить від постійного оновлення баз даних загроз та їх адаптації до нових видів шкідливого програмного забезпечення.

AMP – це клієнт/серверне програмне забезпечення, яке розгортається як окремий сервер на кінцевих точках або на інших мережевих пристроях безпеки. На рисунку наведені переваги архітектури Сітки Безпеки AMP (AMP Threat Grid) (рис. 7.13).

Рис. 7.13. Переваги рішення AMP Threat Grid[100]

Для ефективного захисту від сучасних кіберзагроз підприємствам необхідно впроваджувати комплексні рішення, що включають постійний моніторинг мережі, аналіз поведінки шкідливого програмного забезпечення та використання інноваційних систем захисту, таких як AMP.

[100] – https://www.cisco.com/c/ru_ua/index.html

Ботнет

Ботнет – це група ботів, з'єднаних через Інтернет, та контрольованих одним зловмисником або групою. Бот-комп'ютер зазвичай заражається в наслідок відвідування вебсайту, відкривання вкладення електронної пошти або через заражений медіафайл.

Ботнет може налічувати десятки або навіть сотні тисяч ботів. Ці боти можуть активуватися для розповсюдження шкідливого програмного забезпечення, запуску DDoS-атак, розповсюдження спаму через електронну пошту або виконання атаки підбору пароля методом "грубої сили". Ботнети зазвичай контролюються командами з центру керування.

Кіберзлочинці часто за окрему плату здають в аренду ботнети третім особам для зловмисних цілей.

На рисунку 7.14 показано, як використовується фільтр трафіку ботнетів для інформування спільноти безпеки у всьому світі про місцезнаходження ботнетів.

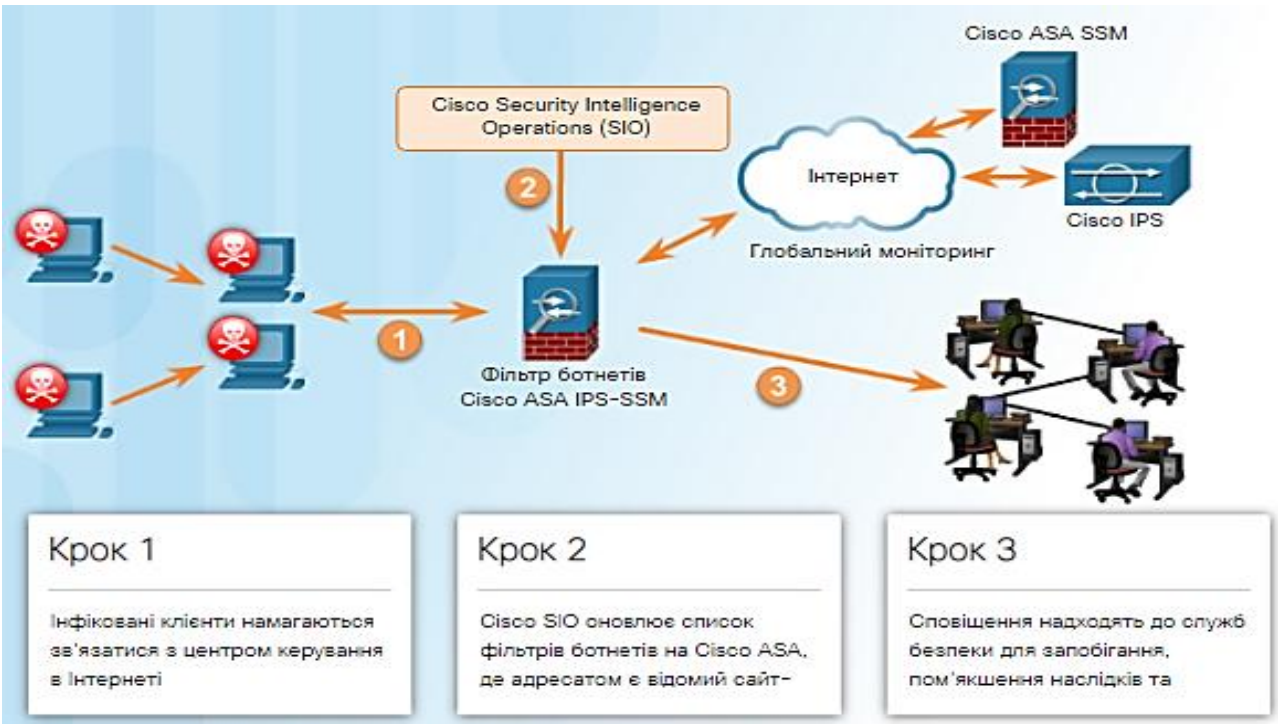


Рис. 7.14. ASA, як фільтр Ботнет трафіку[101]

Отже, боротьба з ботнетами потребує використання сучасних технологій для виявлення та блокування їх активності, а також глобальної співпраці у сфері кібербезпеки для зниження ризиків та захисту користувачів від потенційних загроз.

[101] – https://www.cisco.com/c/ru_ua/index.html

Ланцюг кібервбивства (проникнення в кіберзахист)

У кібербезпеці поняття «ланцюг кібервбивства» (Kill Chain) означає етапи атаки на інформаційні системи.

Розроблений корпорацією Lockheed Martin, як структура системи безпеки для виявлення та реагування на інциденти, ланцюг кібервбивства складається з таких етапів (рис. 7.15):

Етап 1. Розвідка – нападник збирає інформацію про ціль.

Етап 2. Озброєння – нападник створює експлойт та готує засоби для відправки на ціль.

Етап 3. Доставка – нападник відправляє на ціль експлойт і шкідливе навантаження електронною поштою або в інший спосіб.

Етап 4. Експлуатація – експлойт виконується.

Етап 5. Встановлення – на стороні жертви встановлюється зловмисне програмне забезпечення та чорні ходи (backdoors).

Етап 6. Керування та контроль – віддалене керування жертвою здійснюється через канал керування та контролю або сервер.

Етап 7. Дія – нападник виконує шкідливі дії, такі як крадіжка інформації, або запускає додаткові атаки на інші пристрої в мережі, повторно застосовуючи етапи Kill Chain.

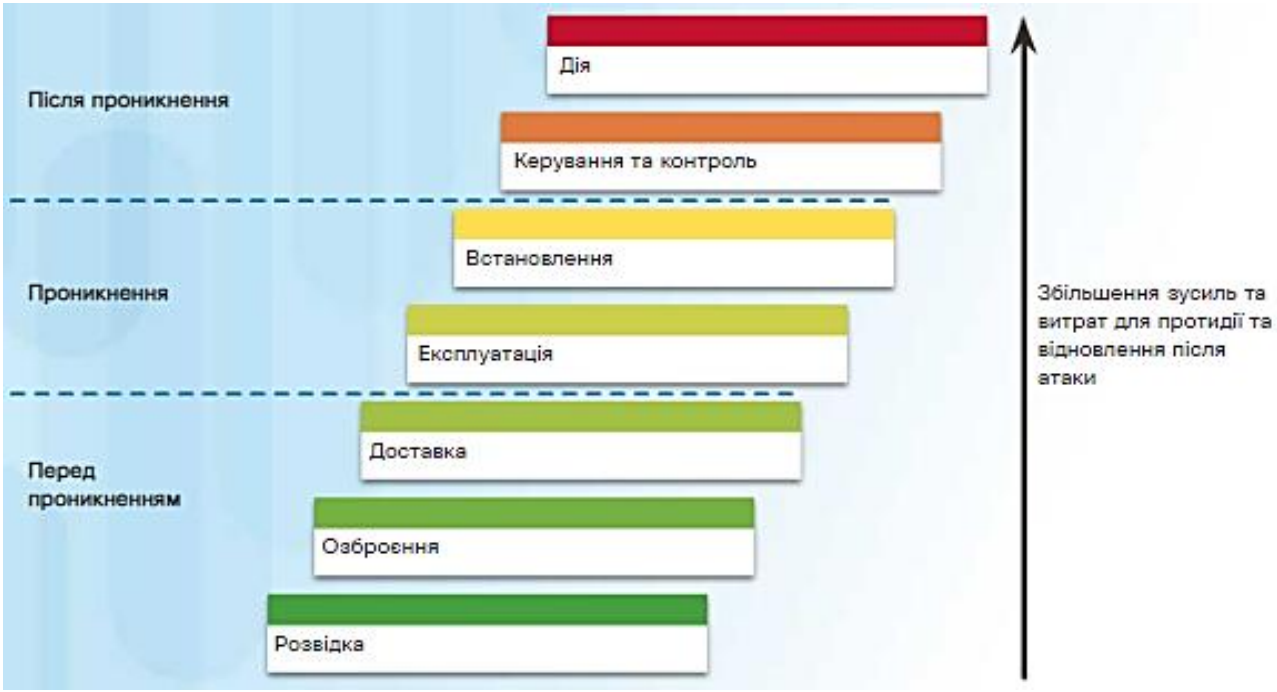


Рис. 7.15. Ланцюг кібервбивства (Cyber Kill Chain)

Для захисту від ланцюга кібервбивства, засоби мережевої безпеки створюються для протидії атаці на кожному з її етапів. Виходячи з поняття

ланцюга кібервбивства, потрібно відповісти на такі питання про засоби захисту компанії:

- Які ознаки атаки на кожному з етапів Kill Chain?
- Які інструменти безпеки необхідні для виявлення ознак нападу на кожному з етапів?
- Чи існують слабкі місця у здатності компанії виявляти атаку?

Компанія Lockheed Martin стверджує, що розуміння етапів Kill Chain дозволило їм встановити захисні перепони, сповільнити хід атаки і, зрештою, запобігти втраті даних. На рисунку показано, як кожен з етапів Kill Chain веде до збільшення зусиль та витрат для протидії атакам та відновлення системи після атак.

Безпека на основі аналізу поведінки

Безпека на основі аналізу поведінки (Behavior-based security) – це форма виявлення загроз, яка не покладається на відомі сигнатури загроз, а замість цього використовує інформаційний контекст для виявлення аномалій в мережі. Виявлення загроз на основі аналізу поведінки передбачає перехоплення та аналіз потоку трафіку між користувачем у локальній мережі та локальним або віддаленим пунктом призначення. Аналіз цих повідомлень дає змогу виявити контекст та моделі поведінки, які можуть бути використані для виявлення аномалій. При використанні такого методу можна помітити наявність атаки через зміну звичної поведінки.

- ***Пастки для хакерів (Honeypots)*** – це інструмент виявлення загроз на основі аналізу поведінки, який спочатку заманює зловмисника, використовуючи передбачувані моделі поведінки нападника. Після потрапляння хакера до пастки, адміністратор мережі може захопити трафік, записати та проаналізувати поведінку зловмисника. Це дає адміністратору можливість вивчити стратегію зловмисника і покращити захист.
- ***Архітектура рішення Cisco's Cyber Threat Defense*** – це архітектура безпеки, яка використовує виявлення на основі аналізу поведінки та індикаторів атаки для забезпечення більшої прозорості, контексту і контролю. Мета полягає в тому, щоб знати, хто організував, що то за атака, де і коли вона відбувалася та яким чином. Для досягнення зазначеної мети ця архітектура безпеки використовує багато технологій захисту.

Технологія NetFlow

Технологія NetFlow використовується для збору інформації про дані, що проходять через мережу. Інформацію, що надає NetFlow, можна порівняти з телефонним рахунком за ваш мережевий трафік. Вона показує вам, які користувачі та пристрої є у вашій мережі, а також коли і як ці користувачі та пристрої отримували доступ до неї. NetFlow – важлива технологія для виявлення кібератак, яка базується на аналізі поведінки. Комутатори, маршрутизатори і

міжмережеві екрани, оснащені NetFlow, можуть повідомляти інформацію щодо входу, виходу та транзиту даних у мережі. Інформація надсилається до колекторів NetFlow, які збирають, зберігають та аналізують записи NetFlow.

Як показано на рисунку 7.16, NetFlow спроможний збирати інформацію за багатьма параметрами про те, як дані переміщуються мережею.

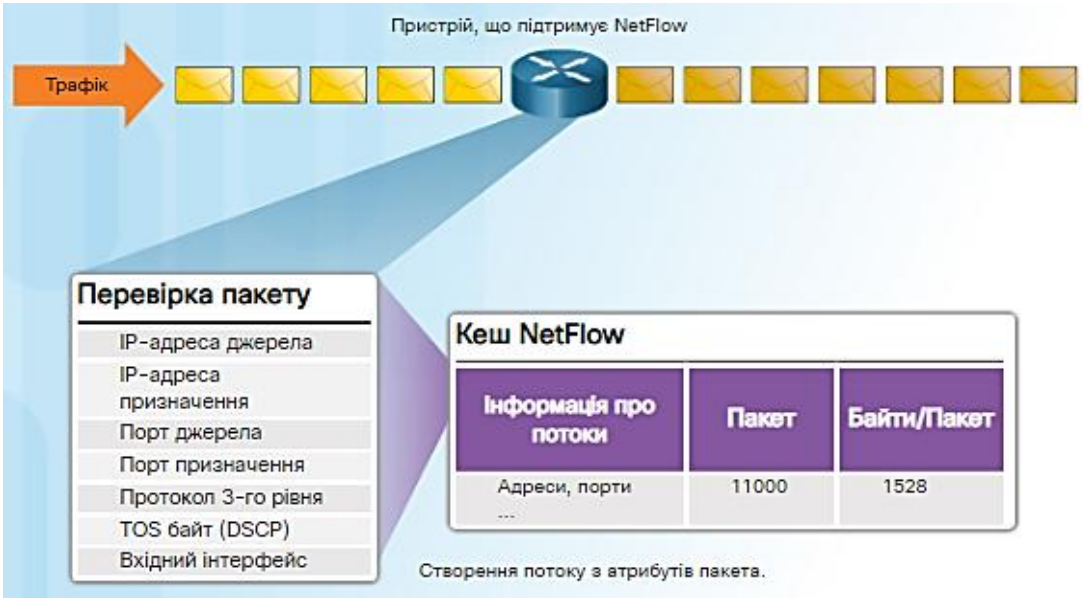


Рис. 7.16. Створення потоку в NetFlow[102]

Завдяки цьому NetFlow може визначити еталонні шаблони поведінки, спираючись на понад 90 різних параметрів.

Організації CSIRT

Як показано на рисунку 7.17, багато великих організацій мають групи реагування на інциденти з комп'ютерної безпеки (CSIRT, Computer Security Incident Response Team) для отримання, аналізу та реагування на повідомлення про інциденти в області комп'ютерної безпеки. Команда зазвичай включає фахівців із мережевої безпеки, аналітиків та експертів із програмного забезпечення, які працюють спільно для забезпечення безперебійної роботи організації.

Рис. 7.17. IT компанії що мають штатні групи реагування на інциденти

[102] – https://the-purple.team/netflow_protocol/

Основними завданнями CSIRT є оперативна відповідь на загрози, мінімізація наслідків атак, відновлення систем після інцидентів і запобігання подібним ситуаціям у майбутньому.

Основна місія CSIRT полягає в тому, щоб забезпечити недоторканість даних, систем і самої компанії, шляхом проведення комплексних розслідувань інцидентів з комп'ютерної безпеки.

Як показано на рисунку 7.18, щоб запобігти інцидентам з безпеки, Cisco CSIRT надає профілактичну оцінку загроз, план пом'якшення наслідків, аналіз тенденцій інцидентів та огляд архітектури безпеки.

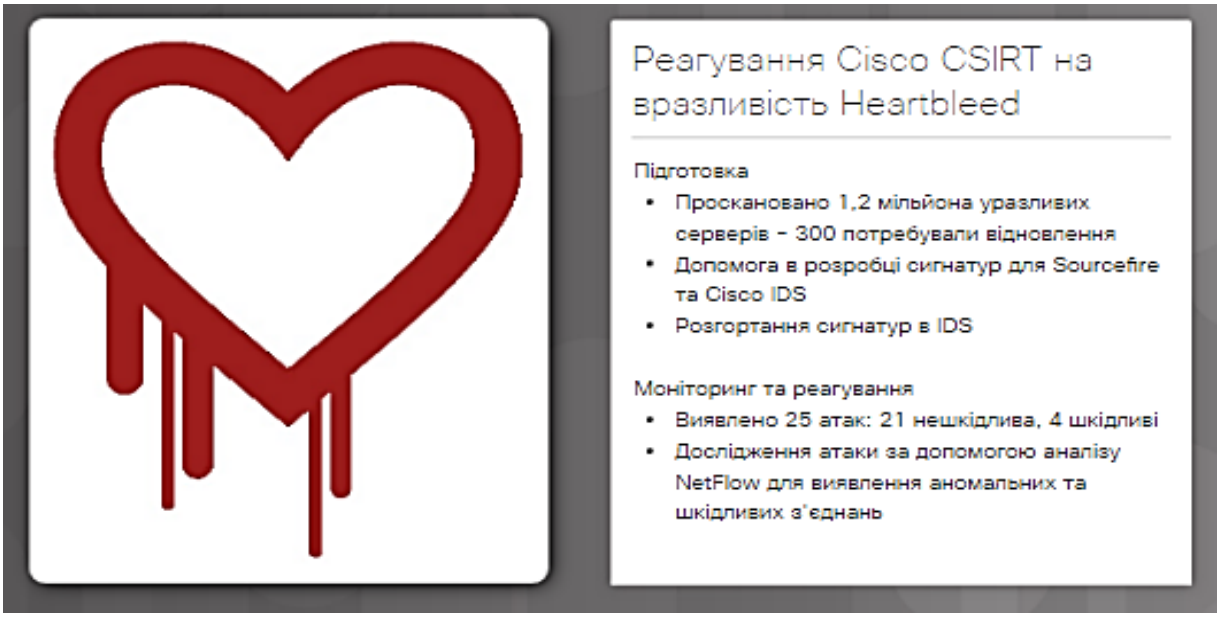


Рис. 7.18. Превентивні заходи щодо запобігання інцидентам з безпеки від Cisco CSIRT

Cisco CSIRT співпрацює з Форумом груп реагування на інциденти з кібербезпеки та захисту (Forum of Incident Response and Security Teams – FIRST), National Safety Information Exchange (NSIE), Defense Security Information Exchange (DSIE) та DNS Operations Analysis and Research Center (DNS-OARC).

Існують державні та публічні організації CSIRT, такі як відділ CERT Інституту програмного забезпечення в університеті Карнегі-Меллона, які допомагають організаціям та державним CSIRT розвивати, застосовувати та вдосконалювати свої можливості з керування інцидентами.

CSIRT— це команда реагування на інциденти кібербезпеки, яка займається виявленням, аналізом та усуненням кіберзагроз і інцидентів у комп'ютерних системах, але CSIRT також сприяє обміну інформацією про загрози між організаціями та вдосконалює заходи захисту на основі отриманих даних.

Збірка сценаріїв з організації захисту

Технології постійно змінюються. Це означає, що і кібератаки також розвиваються. Постійно виявляються нові вразливості та методи нападу. Безпека стає важливою проблемою для бізнесу, оскільки порушення безпеки мають серйозні наслідки для його репутації і ведуть до фінансових втрат. Атаки націлені на критичні мережі і конфіденційні дані. Організації повинні мати плани з підготовки до можливого зламу, його ліквідації та відновлення після нього.(рис.7.19)

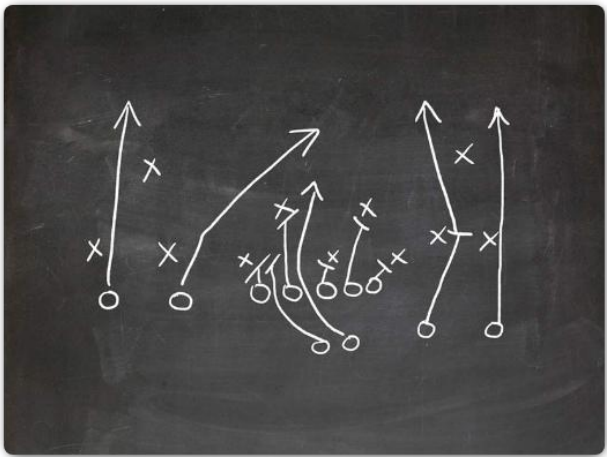


Рис.7.19. Розробка сценаріїв захисту[103]

Найкращий спосіб підготуватися до порушення безпеки – це запобігти йому. В організації мають бути керівництва щодо виявлення ризиків кібербезпеки для систем, активів, даних, захисту системи шляхом проведення навчання охоронців і персоналу та якнайшвидшого виявлення порушень кібербезпеки. При виявленні порушень безпеки необхідно вжити відповідних заходів для зменшення їх впливу та шкоди. План реагування повинен бути гнучким з різними варіантами дій під час атаки. Після того, як порушення буде усунуто, а скомпрометовані системи і служби будуть відновлені, заходи безпеки і процеси мають бути оновлені з урахуванням отриманного досвіду.

Вся ця інформація має бути додана до збірки сценаріїв з оргацізації захисту. Збірка сценаріїв з організації захисту – це набір повторюваних запитів (звітів) щодо джерел даних інцидентів, які дають можливіть їх виявити та відреагувати на них. В ідеалі збірка сценаріїв з організації захисту має допомогати у виконанні таких дій:

- Виявлення пристроїв, заражених зловмисним ПЗ.
- Виявлення підозрілої активності в мережі.
- Виявлення невдалих спроб автентифікації.
- Опис та розуміння вхідного та вихідного трафіку.
- Надання зведеної інформації, включно з тенденціями, статистикою та метриками.
- Забезпечення зручного та швидкого доступу до статистики та метрик.
- Співставлення подій з усіх відповідних джерел даних.

[103] – https://www.shutterstock.com/ru/image-photo/football-play-strategy-drawn-out-on-137165630

Ось деякі з інструментів, що використовуються для запобігання та виявлення інцидентів:

- **SIEM (Security Information and Event Management)** – Система керування інформаційною безпекою та подіями безпеки – це програмне забезпечення, яке збирає з пристроїв безпеки в мережі та аналізує попередження (alerts), журнали та інші дані, отримані в реальному часі та в минулому.
- **DLP (Data Loss Prevention Software)** – програмне забезпечення для запобігання втратам даних – це програмна або апаратна система, яка призначена для запобігання крадіжці конфіденційних даних або їх несанкціонованому передаванню за межі мережі. Система DLP може зосередитися на авторизації доступу до файлів, обміні даними, копіюванні даних, моніторингу активності користувачів тощо. Системи DLP призначені для моніторингу і захисту даних в трьох різних станах: дані у використанні, дані при передачі та дані в стані спокою. Дані у використанні (data in-use) орієнтовані на клієнта, дані при передачі (data in-motion) – це дані, які переміщуються мережею, а дані в стані спокою (data at-rest) – це ті, що зберігаються.
- **Cisco ISE (Identity Services Engine) та TrustSec** – регулюють доступ до мережевих ресурсів шляхом створення політик контролю доступу на основі ролей, що дає змогу розмежовувати доступ до мережі (гості, користувачі мобільних пристроїв, співробітники) без додаткових ускладнень (рис.7.20). Класифікація трафіку ґрунтується на ідентифікаційних даних користувача або пристрою.

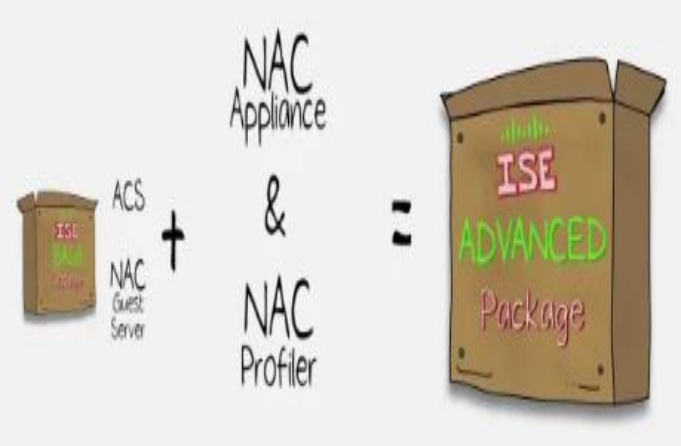


Рис.7.20. CIsco ISE

Системи IDS та IPS

На рисунку 7.21 зображена система виявлення вторгнень (Intrusion Detection System, IDS), яка може бути окремим мережевим пристроєм або одним з кількох інструментів на сервері чи міжмережевому

Рис. 7.21 – Система виявлення вторгнень (IDS)[104]

[104] – https://www.cisco.com/web/ANZ/cpp/refguide/hview/security/asa.html

екрані, який сканує трафік відповідно до бази даних правил або сигнатур у пошуках шкідливих атак. При виявленні відповідності правилам або сигнатурам IDS реєструє виявлення атаки та створює попередження для мережевого адміністратора. Система виявлення вторгнень не запобігає атакам, оскільки не вживає ніяких дій при виявленні інциденту. Завдання IDS – виключно виявлення, реєстрація та створення попередження.

Сканування, яке виконує IDS, уповільнює роботу мережі (відоме як латентність). Щоб запобігти затримці у мережі, IDS зазвичай розміщують офлайн (в автономному режимі), окремо від звичайного мережевого трафіку. Дані копіюються або віддзеркалюються комутатором, а потім пересилаються до IDS для проведення аналізу в режимі офлайн (рис.7.22). Існують також інструменти IDS, які можна встановлювати поверх операційної системи комп'ютера, наприклад Linux або Windows.

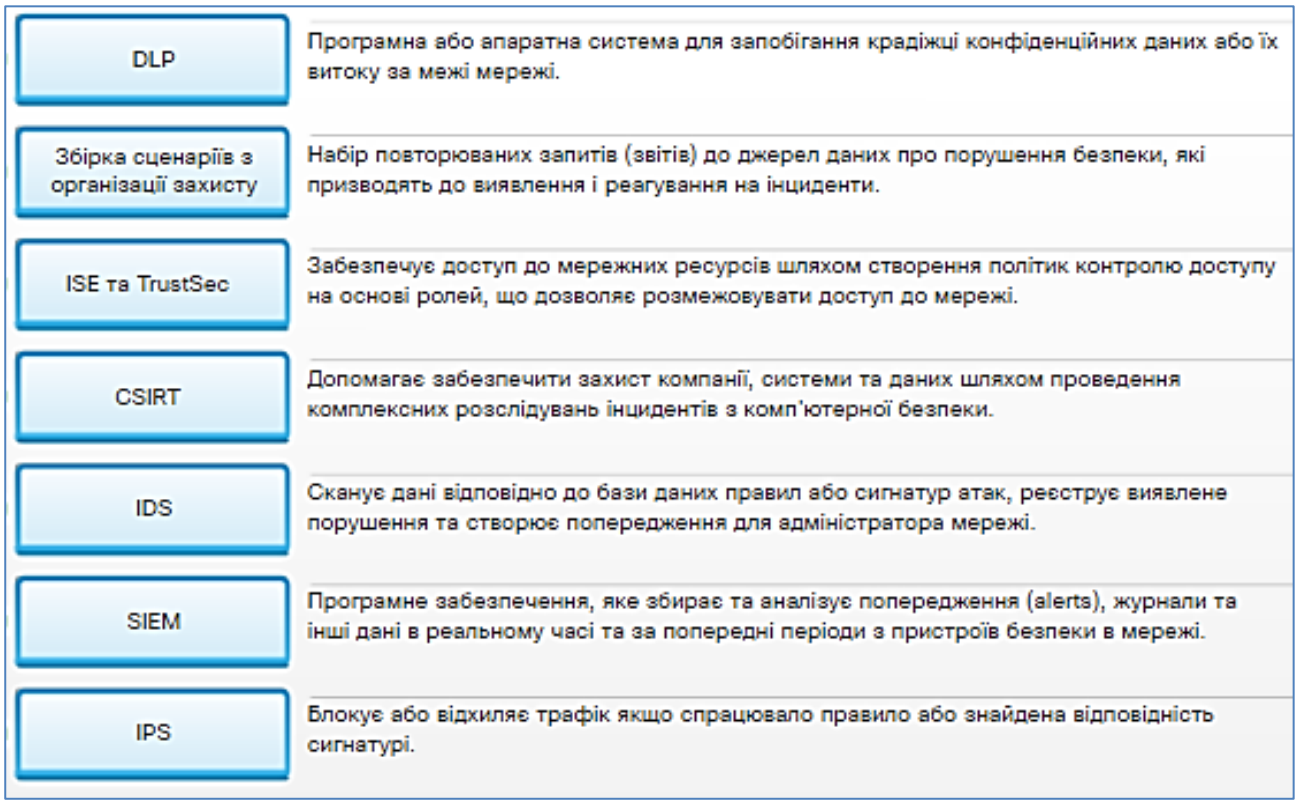


Рис. 7.22. Системи запобігання і виявлення інцидентів

Система запобігання вторгненням (Intrusion Prevention System, IPS) має можливість блокувати або відхиляти трафік на основі спрацювання правила або відповідної сигнатури. Однією з найбільш відомих систем IPS/IDS є Snort. Комерційна версія Snort – це Cisco's Sourcefire. Sourcefire має можливість у реальному часі виконувати аналіз трафіку і портів, ведення журналів, пошук і зіставлення контенту, а також виявлення спроб зондування, атак і сканування портів. Це рішення також інтегрується з іншими сторонніми інструментами для створення звітності, аналізу логфайлів та продуктивності.

7.4. ПРАКТИКИ БЕЗПЕКИ. ОРГАНІЗАЦІЇ З КІБЕРБЕЗПЕКИ. СЕРТИФІКАЦІЯ

Фахівці з кібербезпеки повинні частіше співпрацювати з колегами. Міжнародні технологічні організації часто спонсорують семінари і конференції. Ці організації часто підтримують мотивацію спеціалістів у сфері кібербезпеки.

У світі, переповненому кіберзагрозами, є значна потреба в кваліфікованих та досвідчених фахівцях з інформаційної безпеки. IT-індустрія встановила стандарти для фахівців з кібербезпеки для отримання професійних сертифікатів, що підтверджують навички та рівень знань.

CompTIA Security+

Security+ – програма, що спонсорується асоціацією виробників комп'ютерної техніки (Computer Technology Industry Association, CompTIA), сертифікує компетенцію IT-адміністраторів у забезпеченні інформаційної безпеки. Тест Security+ охоплює найбільш важливі принципи забезпечення безпеки мережі і керування ризиками, включаючи проблеми, пов'язані з хмарними обчисленнями.

EC-Council Certified Ethical Hacker (CEH)

Сертифікований етичний хакер (Certified Ethical Hacker) – ця сертифікація середнього рівня стверджує, що спеціалісти з кібербезпеки, які мають цей сертифікат, володіють навичками та знаннями з різних методів хакерства. Ці фахівці з кібербезпеки використовують ті ж навички та методи, що і кіберзлочинці для виявлення вразливостей систем і точок доступу до них.

SANS GIAC Security Essentials (GSEC)

Сертифікація SANS GSEC (SANS – SysAdmin, Audit, Network, Security; GSEC – Security Essentials Certification) є гарним вибором для першого сертифіката для фахівця з кібербезпеки, який може продемонструвати розуміння термінології і концепцій безпеки і володіє навичками і знаннями, необхідними для реалізації забезпечення безпеки. Програма SANS GIAC пропонує ряд додаткових сертифікатів в сферах адміністрування безпеки, експертиз та аудиту.

(ISC)^2 Certified Information Systems Security Professional (CISSP)

Сертифікація CISSP (сертифікований спеціаліст з інформаційної безпеки) – це незалежна сертифікація для фахівців з кібербезпеки з великим досвідом в технічному та управлінському планах. Вона також офіційно схвалена Міністерством оборони США (U.S. Department of Defense, DoD) і є загальновизнаною галузевою сертифікацією у сфері безпеки.

ISACA Certified Information Security Manager (CISM)

Спеціалісти, що відповідають за керування, розробку і контроль систем інформаційної безпеки на рівні підприємства або ті, хто розробляє кращі методи

забезпечення безпеки, можуть претендувати на CISM. Власники цих документів володіють передовими навичками керування ризиками у сфері безпеки.

Багато державних та експертних організацій опублікували рекомендації щодо передових практик безпеки. До них належать:

- **Оцінка ризиків** – розуміння цінності того, що ви захищаєте, допоможе вам виправдати витрати на безпеку.
- **Створення політики безпеки** – розробіть політику, яка чітко окреслює корпоративні правила, обов'язки та очікування.
- **Заходи з фізичної безпеки** – обмежте доступ до комунікаційних шаф, серверних кімнат, а також забезпечте дотримання норм протипожежної безпеки.
- **Ретельна перевірка персоналу** – при прийомі на роботу необхідно належним чином вивчати анкетні дані та минуле співробітників.
- **Створення і перевірка резервних копій** – регулярно виконуйте резервне копіювання та перевіряйте можливість відновлення даних з них.
- **Підтримка виправлень і оновлень системи безпеки** – регулярно оновлюйте операційні системи і програмне забезпечення серверів, клієнтів і мережевих пристроїв.
- **Використання засобів контролю доступу** – налаштуйте ролі і рівні привілеїв користувачів, а також надійну автентифікацію.
- **Регулярна перевірка реагування на інциденти** – сформуйте команду реагування на інциденти та випробовуйте сценарії реагування на надзвичайні ситуації.
- **Впровадження інструменту моніторингу, аналізу та керування мережею** – виберіть рішення для моніторингу безпеки, яке поєднується з іншими технологіями.
- **Впровадження мережевих пристроїв безпеки** – використовуйте нове покоління маршрутизаторів, міжмережевих екранів та інших пристроїв безпеки.
- **Впровадження комплексного рішення для захисту кінцевих вузлів** – використовуйте корпоративні версії антивірусів та програм для захисту від усіх видів шкідливого ПЗ.
- **Навчання користувачів** – навчайте користувачів та співробітників процедурам безпеки.
- **Шифрування даних** – шифруйте всі конфіденційні дані компанії, включно з електронною поштою.

Деякі найбільш корисні рекомендації містяться в репозиторіях організацій, наприклад, в Ресурсному центрі комп'ютерної безпеки Національного інституту стандартів та технологій США (NIST), як показано на рисунку 7.23.

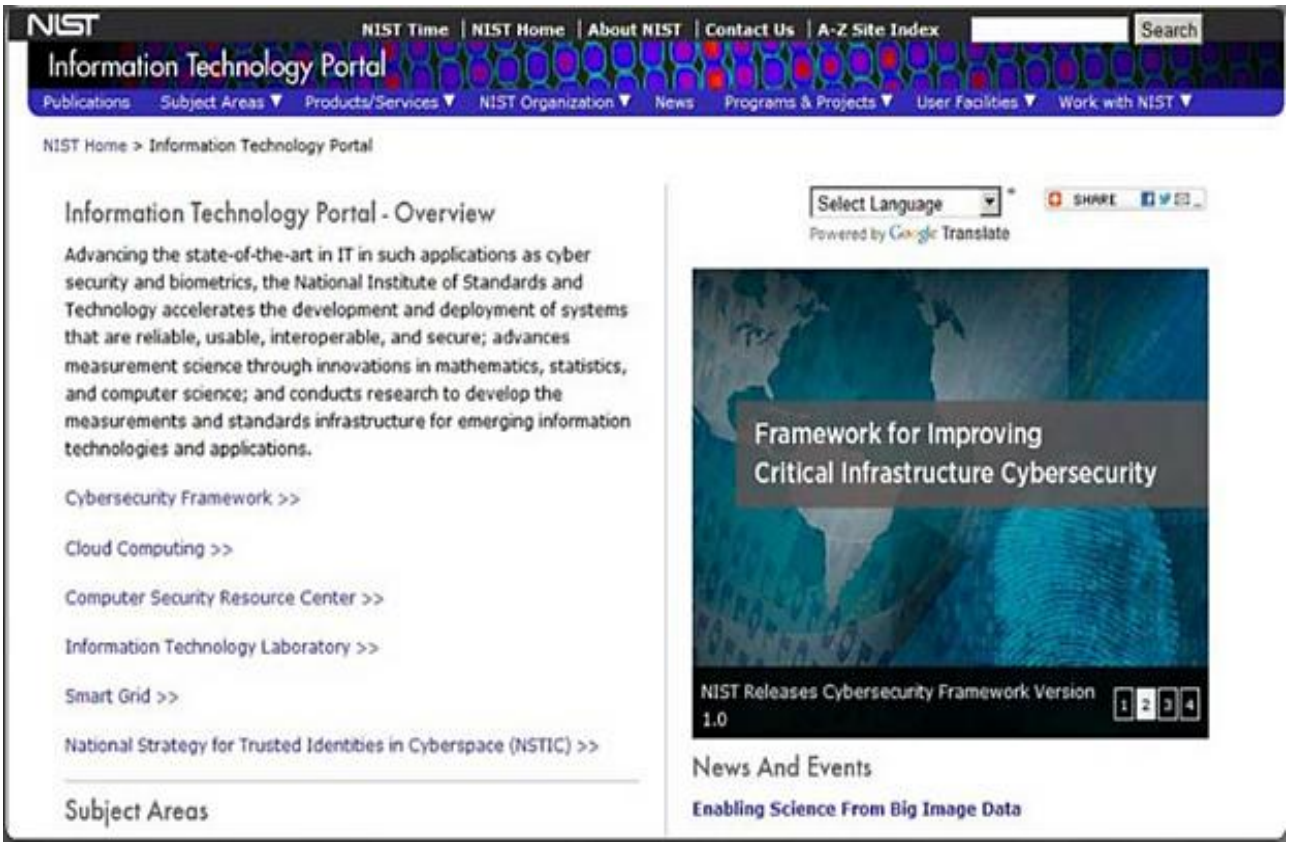
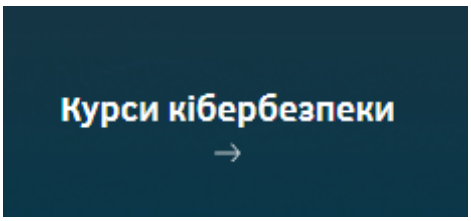


Рис. 7.23. Репозиторій ресурсного центру комп'ютерної безпеки Національного інституту стандартів та технологій США (NIST)

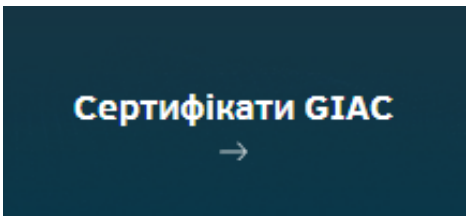
Однією із найбільш відомих і шанованих організацій з навчання кібербезпеки є Інститут SANS.

Про Інститут SANS

Започаткована в 1989 році як кооператив для лідерів у сфері інформаційної безпеки, постійна місія SANS полягає в наданні професіоналам у галузі кібербезпеки практичних навичок та теоретичних знань, що спрямовані на підвищення рівня безпеки у сучасному світі. Організація сприяє цим зусиллям через високоякісні навчальні програми, сертифікаційні курси, стипендіальні академії, спеціалізовані освітні програми, кібердіапазони та інші ресурси, що відповідають індивідуальним потребам кожного професіонала. Завдяки дослідженням, даним та співпраці з провідними експертами у сфері кібербезпеки, SANS забезпечує необхідний освітній рівень та підтримку як для окремих осіб, так і для організацій.



Від кіберосновів до стратегій лідерства SANS пропонує понад 60 практичних курсів, які допомагають кіберфахівцям будь-якого рівня отримати практичні навички.



Сертифікати GIAC забезпечують найвищу та найсуворішу гарантію знань і навичок кібербезпеки, доступ до промислових, державних та військових організацій у всьому світі (рис.7.24).

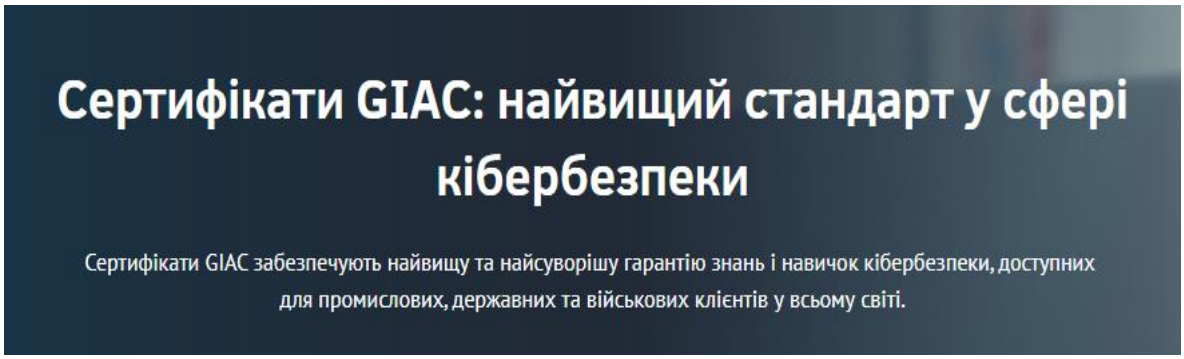


Рис.7.24. Найвищий стандарт у сфері кібербезпеки

Зони фокусування сертифікації GIAC, які відповідають сучасним тенденціям та потребам галузей (рис.7.25)

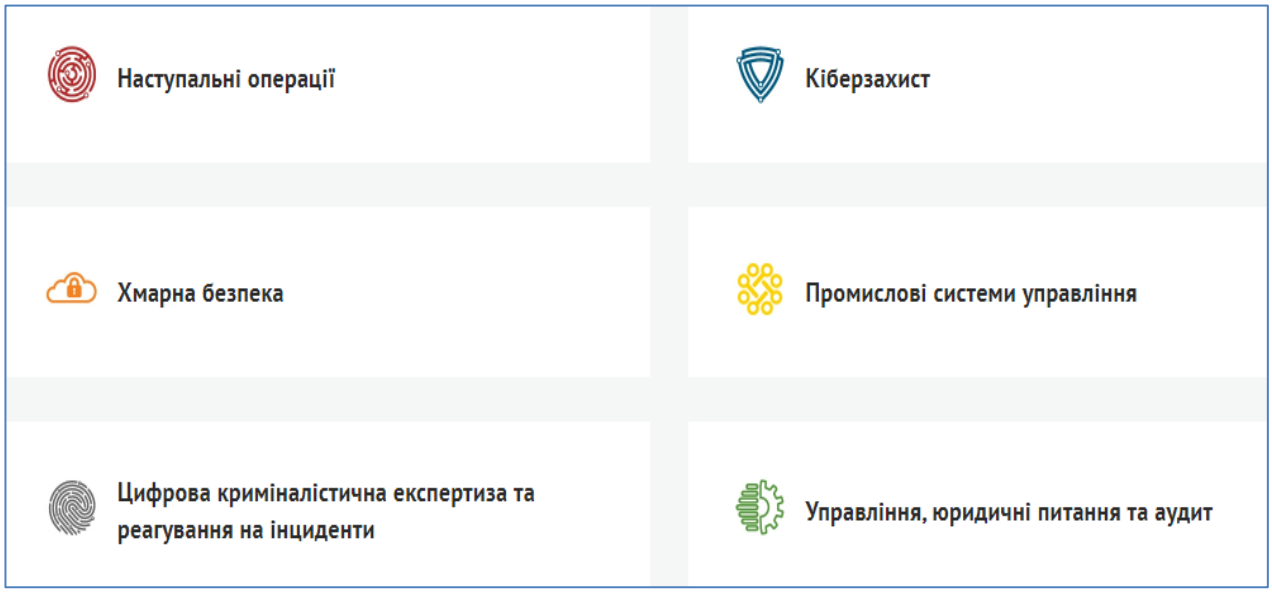


Рис.7.25. Зони фокусування сертифікації GIAC

Сертифікати операторів червоної команди

Сертифікати GIAC для наступальних операцій охоплюють критичні області та вузькоспеціалізовані способи використання, гарантують, що професіонали добре володіють основними наступальними здібностями. Сертифікати GIAC (рис.7.26, рис.7.27) підтверджують, що у вас є знання та навички, необхідні для роботи зі спеціалізованими командами розробників червоного, фіолетового та експлуатаційного кольору.

Рис.7.26. Емблема[105]

Рис.7.27. Сертифікати Red Team Operations

Сертифікований оператор GIAC (GCIH)

Сертифікація GIAC Incident Handler підтверджує здатність фахівця виявляти, реагувати та вирішувати інциденти комп'ютерної безпеки, використовуючи широкий спектр основних навичок безпеки. Власники сертифікатів GCIH мають знання, необхідні для управління інцидентами безпеки, розуміння загальних методів атак, векторів та інструментів, а також уміння захищатися від таких атак і реагувати на них, коли вони трапляються.

GIAC Enterprise Vulnerability Assessor (GEVA)

GIAC Enterprise Vulnerability Assessor – це провідна сертифікація, спрямована на перевірку технічних навичок оцінки вразливостей і перевірених часом практичних підходів для забезпечення безпеки в масштабах підприємства.

Сертифікований GEVA-фахівець зможе керувати загрозами, всебічно оцінювати вразливості та розробляти енергійну захисну стратегію з першого дня.

GIAC Python Coder (GPYC)

Сертифікація GIAC Python Coder (GPYC) підтверджує розуміння фахівцем основних концепцій програмування, а також здатність писати й аналізувати робочий код за допомогою мови програмування Python. Власники сертифікації GPYC продемонстрували знання звичайних бібліотек Python, створюючи власні інструменти, збираючи інформацію про систему чи мережу, взаємодіючи з вебсайтами та базами даних, а також автоматизуючи тестування.

Сертифікати хмарної безпеки

Рис.7.28. Захист хмари[105]

Безпека хмари (рис.7.28) зараз є важливою в нашій глобальній інфраструктурі. Сертифікати хмарної безпеки GIAC (рис.7.29) розроблені, щоб допомогти вам освоїти практичні кроки, необхідні для захисту систем і програм у хмарі від найнебезпечніших загроз. Від безпеки вебдодатків і автоматизації DevOps до тестування на проникнення в хмарі – у сценаріях загальнодоступної, багатохмарної та гібридної хмари – у нас є облікові дані, необхідні як професіоналам, так і організаціям для забезпечення хмарної безпеки на будь-якому підприємстві.

Рис.7.29. Сертифікати Cloud Security Techniques

GIAC Cloud Security Essentials (GCLD)

Сертифікація GCLD підтверджує здатність лікаря-практика застосовувати профілактичні, детективні та реакційні методи для захисту цінних хмарних робочих навантажень.

GIAC Cloud Security Automation (GCSA)

Сертифікація GCSA охоплює хмарні послуги та сучасні методи DevSecOps, які використовуються для більш безпечного створення та розгортання систем і програм.

Сертифікований GIAC захисник вебдодатків (GWEB)

Сертифікація GIAC Web Application Defender дає змогу кандидатам продемонструвати володіння знаннями та навичками безпеки, необхідними для боротьби з поширеними помилками вебдодатків, які призводять до більшості проблем із безпекою. Успішний кандидат матиме практичний досвід використання сучасних інструментів для виявлення та запобігання помилок перевірки введення, міжсайтових сценаріїв (XSS) та ін'єкції SQL, а також глибоке розуміння автентифікації, контролю доступу та керування сеансами, їх слабкі сторони та як їх найкраще захистити. Сертифіковані GIAC захисники вебдодатків (GWEB) володіють знаннями, навичками та здібностями для захисту вебдодатків, а також розпізнавання та пом'якшення недоліків безпеки в існуючих вебдодатках.

GIAC Public Cloud Security (GPCS)

Сертифікація GPCS підтверджує здатність лікаря-практика захищати хмару як у загальнодоступних, так і в багатохмарних середовищах. Сертифіковані GPCS професіонали знайомі з нюансами AWS, Azure і GCP і мають навички, необхідні для захисту кожної з цих платформ.

Цифрова криміналістична експертиза та сертифікати реагування на інциденти

Потрібна інтуїція та спеціальні навички, щоб знайти приховані докази та полювати на невловимі загрози (рис. 7.30). Сертифікати GIAC з цифрової криміналістичної експертизи та реагування на інциденти охоплюють здібності, необхідні фахівцям DFIR (рис.7.31), щоб досягти успіху в своїй справі, підтверджуючи, що професіонали можуть виявляти зламані системи, визначати, як і коли відбулося порушення, розуміти, що

Рис.7.30. Експертиза[105]

зловмисники прийняли або змінили, а також успішно локалізувати та усувати інциденти. Підтримуйте свої знання щодо виявлення загроз і боротьби з ними в актуальному стані – а свою робочу роль – у безпеці – завдяки сертифікатам DFIR.

Рис.7.31. Поглиблені сертифікати

GIAC Battlefield Forensics and Acquisition (GBFA)

Сертифікація GBFA демонструє, що особа навчена та кваліфікована щодо правильного збору, отримання та швидкого аналізу сортування багатьох форм зберігання даних.

GIAC Advanced Smartphone Forensics (GASF)

Популярність мобільних пристроїв у нашій роботі та особистому житті стає все більш широкою та складною. Обсяг і тип даних, які передають ці пристрої, як-от списки контактів, електронна пошта, робочі документи, SMS-повідомлення, зображення, історія перегляду в Інтернеті та конкретні дані програми, роблять їх важливими для особи, яка носить пристрій, і дає змогу отримати багате джерело даних. для проведення судово-медичних експертиз.

Сертифікований судовий експерт GIAC (GCFE)

Сертифікація GIAC Certified Forensic Examiner (GCFE) підтверджує знання практикуючого спеціаліста з комп'ютерного криміналістичного аналізу з акцентом на основні навички, необхідні для збору та аналізу даних з комп'ютерних систем Windows. Власники сертифікатів GCFE мають знання, навички та вміння проводити типові розслідування інцидентів, включаючи електронне виявлення, криміналістичний аналіз та звітність, отримання доказів,

криміналістичну експертизу браузера та відстеження діяльності користувачів і програм у системах Windows.

Сертифікати кіберзахисту

Рис.7.32. Емблема 2[105]

Кіберзахисники відіграють важливу роль у забезпеченні безпеки підприємства. Захист від атак (рис.7.32) можливий лише за наявності правильного набору навичок і впевненості у своїх силах і здібностях своєї команди. Сертифікати GIAC Cyber Defense (рис.7.33) охоплюють весь спектр захисту і зосереджені на двох сферах: основи кіберзахисту та синя команда. Незалежно від того, чи є ваші потреби на рівні для початківців, просунутих чи для спеціалізованої сфери захисту, GIAC має повноваження, необхідні для захисту вашої організації від останніх загроз.

Рис.7.33. Сертифікати кіберзахисту

GIAC Open Source Intelligence (GOSI)

Сертифікація GOSI підтверджує, що фахівці-практики мають міцну основу в методології та структурі OSINT і добре обізнані у зборі даних, звітності та аналізі цілей.

Сертифікований GIAC адміністратор безпеки Windows (GCWN)

Сертифікація GIAC Certified Windows System Administrator (GCWN) підтверджує здатність лікаря-практика захищати клієнти та сервери Microsoft

Windows. Власники сертифікації GCWN мають знання та навички, необхідні для налаштування та керування безпекою операційних систем і програм Microsoft, зокрема: PKI, IPSec, групова політика, AppLocker, DNSSEC, PowerShell та захист Windows від шкідливих програм і постійних зловмисників.

Архітектура захисту GIAC (GDSA)

Сертифікація GDSA доводить, що спеціалісти-практики можуть розробити та впровадити ефективну комбінацію мережевих та орієнтованих на дані контролю, щоб збалансувати запобігання, виявлення та реагування.

Сертифікований GIAC Security Operations Certified (GSOC)

Сертифікація GSOC підтверджує здатність лікаря-практика захищати підприємство, використовуючи основні інструменти та методи реагування на інциденти Blue Team. Сертифіковані GSOC професіонали добре володіють технічними знаннями та ключовими концепціями, необхідними для управління операційним центром безпеки (SOC).

Сертифікований аналітик GIAC (GCIA)

Сертифікація GIAC Intrusion Analyst підтверджує знання спеціаліста з моніторингу мережі та хосту, аналізу трафіку та виявлення вторгнень. Власники сертифікатів GCIA мають навички, необхідні для налаштування та моніторингу систем виявлення вторгнень, а також для читання, інтерпретації та аналізу мережевого трафіку та відповідних файлів журналів.

Сертифікація постійного моніторингу GIAC (GMON)

Сертифікація GIAC Continuous Monitoring (GMON) підтверджує здатність лікаря-практика запобігати вторгненням і швидко виявляти аномальну активність. Володарі сертифікації GMON продемонстрували знання обґрунтованої архітектури безпеки, моніторингу безпеки мережі, безперервної діагностики та пом’якшення наслідків, а також безперервного моніторингу безпеки.

Сертифікований аналітик GIAC (GCDA)

Сертифікація GCDA підтверджує, що людина вміє збирати, аналізувати та тактично використовувати сучасні мережеві та кінцеві джерела даних для виявлення зловмисної чи несанкціонованої діяльності.

---

[105] – https://stock.adobe.com/kz/search?k=%22password%20generator%22

Сертифікати промислових систем управління

Рис.7.34. Емблема 3 [105]

Атаки на інфраструктуру промислового контролю відбуваються все частіше і частіше. Системам управління по всьому світу потрібні сильні команди інформаційної безпеки, які стоять за ними, щоб гарантувати, що ці загрози не досягнуть успіху (рис. 7.34). Сертифікати системи промислового контролю GIAC охоплюють те, що потрібно знати фахівцям ICS: як захищати критичні промислові системи та реагувати на інциденти, які неминуче виникнуть. Отримавши сертифікацію в ICS (рис.7.35), ви підтверджуєте свою здатність захищати важливу інфраструктуру, а також свою цінність для робочого місця.

Рис.7.35. Сертифікати промислових систем управління

Глобальний спеціаліст із промислової кібербезпеки (GICSP)

GICSP об’єднує IT, інженерію та кібербезпеку, щоб гарантувати безпеку промислових систем управління від проектування до виходу з експлуатації. Ця унікальна сертифікація промислової системи керування, яка не стосується виробників, орієнтована на практикуючих спеціалістів, є результатом спільної роботи GIAC та представників глобального галузевого консорціуму, що включає організації, які розробляють, розгортають, експлуатують та/або підтримують інфраструктуру промислової автоматизації та систем керування. GICSP оцінить базовий рівень знань і розуміння серед різноманітних спеціалістів, які розробляють або підтримують системи керування та поділяють відповідальність за безпеку цих середовищ.

Захист критичної інфраструктури GIAC (GCIP)

Сертифікація GCIP підтверджує, що фахівці, які отримують доступ, підтримують та обслуговують критичні системи, мають розуміння нормативних вимог NERC CIP, а також практичні стратегії впровадження.

Відповідь GIAC та промисловий захист (GRID)

Сертифікація GRID призначена для професіоналів, які хочуть продемонструвати, що вони можуть виконувати стратегії активного захисту, специфічні та відповідні для мережі та систем промислової системи керування (ICS). Від кандидатів вимагається продемонструвати розуміння підходу Active Defense, атак, характерних для ICS, і того, як ці атаки дають змогу використовувати стратегії пом'якшення наслідків. Кандидати також повинні продемонструвати розуміння стратегій та фундаментальних методів, характерних для основних предметів із фокусом ICS, таких як моніторинг безпеки мережі (NSM), цифрова криміналістична експертиза та реагування на інциденти (DFIR).

ВИСНОВКИ

На початку теми було описано деякі технології та процеси, що використовують експерти з кібербезпеки для захисту мережі, обладнання та даних організацій, включно з типами міжмережевих екранів, пристроями безпеки та програмним забезпеченням.

Сканування портів є важливим процесом для виявлення відкритих портів і активних служб на мережевих пристроях. Воно може використовуватися як мережевими адміністраторами для перевірки безпеки мережі, так і зловмисниками для пошуку вразливостей.

Також було розглянуто ботнети, ланцюг кібервбивства, безпеку на основі аналізу поведінки та використання NetFlow для моніторингу мережі.

Пристрої безпеки є ключовими елементами захисту мережі та можуть бути як апаратними, так і програмними рішеннями. До них належать міжмережеві екрани**,** маршрутизатори**,** системи запобігання вторгненням (IPS)**,** VPN та антивірусні рішення. Сучасні пристрої, такі як рішення Cisco, поєднують у собі функції фільтрації трафіку, шифрування, моніторингу загроз та управління безпекою, що забезпечує комплексний захист мережевої інфраструктури. В заключній частині пояснено підхід Cisco до кібербезпеки, включно з групою швидкого реагування CSIRT та що таке збірка сценаріїв з організації захисту. Коротко розглянуто інструменти, які спеціалісти з кібербезпеки використовують для виявлення і запобігання мережевим атакам, у тому числі SIEM, DLP, Cisco ISE та TrustSec, а також системи IDS і IPS.

ТЕРМІНИ І КОНЦЕПЦІЇ

Ця вправа призначена для того, щоб ви могли практикувати важливі терміни та концепції, викладені в темі.

1. Сканування портів

- процес зондування комп'ютера, сервера або іншого мережевого хоста з метою знаходження відкритих портів. Використовується для перевірки безпеки, виявлення вразливостей та діагностики мережевих проблем. Прикладом інструменту для сканування є **Nmap**

2. Фаєрвол (брандмауер)

- захищає мережу, контролюючи, який трафік дозволений для входу, а також для виходу. Це мережевий пристрій або програмне забезпечення, що контролює та фільтрує вхідний і вихідний трафік відповідно до заданих правил безпеки. Основна функція – захист мережі від несанкціонованого доступу та загроз.

ПРАВДА ЧИ БРЕХНЯ.

1. Сьогодні існують єдині пристрої безпеки, які будуть вирішувати всі потреби мережевої безпеки в організації

- БРЕХНЯ.

4. Ця атака порушує функціонування служб, пригнічуючи сервери і мережеві пристрої фіктивним трафіком

- DDoS.

5. Тип заходів безпеки, які обмежують доступ до телекомунікаційних шаф, місць розташування серверів, а також системи пожежогасіння

- фізична безпека.

6. Правда чи брехня. Ботнет може налічувати десятки тисяч ботів або навіть сотні тисяч

- ПРАВДА.

7. Концептуальний план етапів атаки на інформаційні системи

- вбивчий ланцюг (Kill Chain).

8. Пристрій безпеки, який має можливість блокувати або відхиляти трафік на основі позитивного правила або відповідності сигнатурі

- IPS / IDS.

9. Інструмент, який використовується для збору інформації про дані, що проходять через мережу

- NetFlow.

ПРАКТИЧНЕ ЗАВДАННЯ 7.1. МОДЕЛЬ ЗБІРКИ СЦЕНАРІЇВ

Використання моделі збірки сценаріїв (Playbook Model)

У складній мережі дані, зібрані з різних інструментів моніторингу, можуть легко перевищити можливості їх обробки. У цій вправі ви створите свій власний playbook для організації та документування даних моніторингу.

Перейдіть за цим посиланням, щоб краще зрозуміти playbook:

https://blogs.cisco.com/security/using-a-playbook-model-to-organize-your-information-security-monitoring-strategy/

Створіть свій власний playbook, склавши три основні розділи:

- Ідентифікатор звіту і тип звіту з назвою.
- Постановка задачі.
- Аналіз результатів.

Hacking On a Dime

Сайт Hacking on Dime пояснює, як використовувати інструмент nmap для збору інформації про цільову мережу.

https://hackonadime.blogspot.com/2011/05/information-gathering-using-nmap-and.html

Примітка: **nmap –** надзвичайно популярний і потужний сканер портів, випущений в 1997 році. Спочатку він був створений тільки для Linux; проте пізніше був перенесений на численні платформи, включаючи Windows і Mac OS X. Як і раніше розповсюджується безкоштовно; для отримання додаткової інформації дивись https://nmap.org/.

КОНТРОЛЬНА РОБОТА ДО ТЕМИ 7

Ця контрольна робота охоплює матеріал теми. Вона призначена для надання додаткових можливостей попрактикувати навички та знання, подані у темі і підготовки до Іспиту.

1. Який інструмент може ідентифікувати шкідливий трафік, порівнюючи вміст пакета з відомими сигнатурами атаки?

– Nmap
– Zenmap
– NetFlow
– IDS

Пояснення

IDS або система виявлення вторгнення – це пристрій, який може сканувати пакети та порівнювати їх з набором правил або сигнатурами атак. Якщо пакети відповідають сигнатурам атаки, IDS може створювати сповіщення та зареєструвати виявлення у log-файлі.

IDS

2. Який останній етап схеми Ланцюга кібервбивства (Cyber Kill Chain)?

– збирання інформації про жертву
– зловмисні дії
– дистанційне керування пристроєм-жертвою
– створення зловмисного навантаження

Пояснення

Вбивчий ланцюг (Cyber Kill Chain) описує фази послідовного розгортання кібератаки. Він складається з таких фаз:

– розвідка;
– озброєння;
– доставка;
– застосування;
– інсталяція;
– команда і контроль;
– дії над жертвою.

Загалом, ці фази виконуються послідовно. Проте, під час атаки деякі етапи можуть виконуватися одночасно, особливо в разі залучення декількох нападників або цілих груп.

зловмисні дії

3. Який протокол використовується у рішенні Cisco Cyberthreat Defense для збору інформації про трафік, який передається мережею?

– NetFlow
– NAT
– Telnet
– HTTPS

Пояснення

NetFlow використовується як для збору інформації про трафік, що проходить через мережу, так і для формування звіту на центральному колекторі.

NetFlow

4. Який інструмент може здійснювати аналіз трафіку та портів у режимі реального часу, а також дає змогу виявити сканування портів, атаки з ідентифікації та переповнення буфера?

– Snort
– Netflow
– Nmap
– SIEM

Пояснення

Snort – це система захисту від вторгнення (IPS) з відкритим кодом, яка здатна здійснювати аналіз трафіку та портів у режимі реального часу, реєстрацію пакетів, пошук та відповідність контенту, а також виявлення, атак зондування, сканування портів, ідентифікації та атак на переповнення буферів.

Snort

5. Який тип атаки перериває роботу сервісів, навантажуючи мережеві пристрої фіктивним трафіком?

– сканування портів (port scans)
– нульовий день (zero-day)
– атака грубої сили (brute force)
– DDoS

Пояснення

DDoS або розподілена відмова в обслуговуванні – це атака, яка використовується для порушення роботи служб, шляхом перевантаження мережевих пристроїв фіктивним трафіком.

DDoS

Response Team, CSIRT)

Щоб дізнатися більше про групу CSIRT та її склад, перейдіть за цим посиланням:

https://tools.cisco.com/security/center/emergency.x?i=56#3

Cisco Web Security Appliance

Cisco Web Security Appliance (WSA) – це рішення «все-в-одному», яке поєднує в собі захист від зловмисного ПЗ підвищеної складності, моніторинг і контроль додатків, прийнятні політики використання, аналітичні звіти і безпечний мобільний доступ на єдиній платформі. Для отримання додаткової інформації про WSA відвідайте це посилання:
https://www.cisco.com/c/en/us/products/security/web-security-appliance/index.html

Фільтри репутації Cisco IronPort Email Security Appliance

Фільтри репутації Cisco IronPort забезпечують захист від спаму для вашої електронної пошти. Діючи як перша лінія захисту, ці фільтри видаляють до 80 відсотків вхідного спаму на рівні з'єднання. Для отримання додаткової інформації про фільтри репутації Email Security Appliance (ESA) відвідайте це посилання:
https://www.cisco.com/en/US/prod/vpndevc/ps10128/ps10154/rep_filters_index.html

Cisco Cyber Threat Defense

Рішення Cisco для захисту від кіберзагроз фокусується на найскладніших, небезпечних загрозах інформаційної безпеки, які ховаються в мережах протягом декількох місяців або років, викрадаючи важливу інформацію і порушуючи роботу. Для виявлення цих загроз рішення виявляє підозрілі моделі мережого трафіку. Потім рішення надає контекстну інформацію про атаку, користувачів, ідентифікаційні дані та інше – усе відображається на єдиній інформаційній панелі. Для отримання додаткової інформації перейдіть за цим посиланням:

https://www.cisco.com/en/US/netsol/ns1238/index.html

Приклад використання системи запобігання вторгненням (мережевий варіант)

Системи запобігання вторгненням (Intrusion prevention systems, IPS) є важливою частиною стратегії поглибленого захисту Cisco. Існують дві основні реалізації IPS: розгортання IPS на периметрі і розгортання IPS в мережі. Щоб дізнатися більше про необхідність використання обох моделей розгортання для захисту мережевого трафіку, ознайомтеся з прикладом використання за цим посиланням:

https://www.cisco.com/web/about/ciscoitatwork/security/csirt_network-based_intrusion_prevention_system_web.html

ТЕМА 8. ЧИ ГОТОВІ ВИ ПОВ'ЯЗАТИ СВОЄ МАЙБУТНЄ З КІБЕРБЕЗПЕКОЮ?

Тема охоплює правові та етичні питання, що виникають при роботі у сфері кібербезпеки. Також тут обговорюються навчальні та кар'єрні шляхи в галузі кібербезпеки.

Сторінка Місток талантів Мережевої академії (The Networking Academy Talent Bridge page) на сайті netacad.com у розділі Ресурси (Resources) надає достатньо інформації про те, як скласти гарне резюме або підготуватися до співбесіди.

8.1. ПРАВОВІ ПРОБЛЕМИ КІБЕРБЕЗПЕКИ

Для ефективного захисту від атак професіонали з кібербезпеки повинні мати такі ж навички, що і хакери, особливо хакери у чорних капелюхах. Відмінність хакера від професіонала з кібербезпеки полягає в тому, що професіонал з кібербезпеки повинен працювати у правовому полі.

Рис.8.1. Глобальний альянс з кібербезпеки

Персональні юридичні питання

Ви навіть не повинні бути працівником, щоб потрапити під дію законів про кібербезпеку. У вашому приватному житті ви можете мати можливість та навички для зламу комп'ютера чи мережі іншої людини. Є стара приказка: "Просто тому, що ти можеш, не означає, що ти повинен". Візьміть це до уваги. Більшість хакерів, знають вони про це чи ні, залишають по собі сліди, які можуть відслідковувати кіберспеціалісти.

Фахівці з кібербезпеки розвивають в собі багато навичок, які можна використати з добрими чи злими намірами. Ті, хто використовує свої навички у

правовому полі для захисту інфраструктури, мереж та конфіденційності, завжди користуються великим попитом.

Корпоративні правові питання

У більшості країн є закони про кібербезпеку. Вони можуть мати відношення до критичної інфраструктури, мереж та конфіденційності корпоративних і персональних даних. Підприємства повинні дотримуватися цих законів.

У контексті кібербезпеки корпоративні правові питання стосуються відповідальності компаній за дотримання законодавчих вимог та захист даних клієнтів, партнерів і співробітників. Компанії зобов'язані забезпечувати відповідність своїх внутрішніх процесів нормам законів про захист даних, таких як GDPR у Європі або CCPA у США. Це включає впровадження політик конфіденційності, заходів безпеки для запобігання витокам інформації та регулярні аудити для виявлення вразливостей.

У деяких випадках, якщо ви порушите закони про кібербезпеку під час виконання вашої роботи, то може бути покарана компанія, а ви можете втратити свою роботу. В інших випадках ви можете бути притягнуті до відповідальності, одержати штрафні санкції, а можливо навіть засуджені.

Загалом, якщо ви не впевнені в тому, що певна дія або поведінка є законною, то припускайте, що вона незаконна і не робіть цього. Ваша компанія може мати юридичний відділ або хтось із відділу кадрів зможе відповісти на ваші запитання, перш ніж ви зробите щось незаконне.

Міжнародне право та кібербезпека

Сфера законів про кібербезпеку значно новіша, ніж сама кібербезпека. Як згадувалося раніше, у більшості країн діють свої закони і їхня кількість буде зростати.

Міжнародне право у сфері кібербезпеки є відносно новим і спрямоване на створення спільних правил для боротьби з кіберзагрозами на глобальному рівні. Основними викликами є узгодження національних інтересів, суверенітету та принципів співпраці між державами. Документи, такі як Будапештська конвенція про кіберзлочинність, стали першим кроком до регулювання міжнародних злочинів у кіберпросторі, проте їх ратифікували не всі країни. Окрім цього, виникає питання відповідальності держав за кібератаки, які здійснюються з їх території. Важливу роль у міжнародній кібербезпеці відіграють ООН та інші організації, які працюють над розробкою норм і стандартів для запобігання конфліктам у кіберпросторі та захисту критичної інфраструктури

8.2. ЕТИЧНІ ПИТАННЯ КІБЕРБЕЗПЕКИ

Крім роботи у рамках закону, фахівці з кібербезпеки повинні також демонструвати етичну поведінку.

Персональні етичні питання

Людина може діяти неетично і не підлягати обвинуваченню, штрафам або тюремному ув'язненню. Це може статись тому, що формально дія могла бути законною. Але це не означає, що така поведінка є прийнятною. Етичність поведінки досить легко визначити. Неможливо перерахувати усі приклади неетичної поведінки, які може продемонструвати особа, що володіє навичками з кібербезпеки. Нижче наведено всього два приклади.

Запитайте у себе:

- Чи хотів би я виявити, що хтось зламав мій комп'ютер і змінив зображення на моїй сторінці у соціальній мережі?
- Чи хотів би я дізнатись, що IT-технік, якому я довірив налаштувати мою мережу, розповів колегам особисту інформацію про мене, яку він виявив під час роботи у моїй мережі?

Якщо хоча б на одне з цих запитань ви відповіли "ні", то не робіть цього іншим.

Корпоративні етичні питання

Етика – це правила поведінки, які іноді застосовуються як закони. У сфері кібербезпеки існує безліч питань, які не охоплюються законами. Це означає, що робити щось формально законне не завжди є етичною справою. Оскільки багато чого у сфері кібербезпеки не регулюється (або ще не було охоплено) законодавством, багато професійних IT-організацій створили кодекси етики для людей у своїй галузі. Нижче наведено список з трьох організацій, які мають кодекси етики:

- Інститут кібербезпеки (CyberSecurity Institute, CSI) опублікував етичний кодекс.
- Асоціація безпеки інформаційних систем (Information Systems Security Association, ISSA) має кодекс етики.
- Асоціація фахівців з інформаційних технологій (Association of Information Technology Professionals, AITP) має як етичний кодекс, так і стандарти поведінки.

Cisco має команду, що завжди дотримується принципу етичного ведення бізнесу. Перейдіть за посиланням, щоб прочитати про це більше. На сайті розміщено Кодекс ділової поведінки Cisco (Cisco's Code of Business Conduct) у вигляді електронної книги та PDF-файлу. В обох файлах є "Дерево етичних рішень", яке показано на рисунку 8.2.

Навіть якщо ви не працюєте в Cisco, питання та відповіді, знайдені в цьому дереві рішень, можна легко застосувати на вашому робочому місці. Як і в юридичних питаннях, якщо ви сумніваєтесь, чи може дія або поведінка бути неетичною, або припускаєте, що це неетично, не робіть цього. Можливо, є хтось у відділі кадрів або юридичному відділі вашої компанії, хто може прояснити вашу ситуацію, перш ніж ви зробите те, що вважатиметься неетичним.

Пошукайте в Інтернеті інші організації зі сфери IT, які мають кодекси етики. Спробуйте знайти, що у них є спільного.

Рис. 8.2. Принцип дії під час вирішення етичних дилем у сфері кібербезпеки

Корпоративна етика у сфері кібербезпеки передбачає відповідальне використання технологій і дотримання моральних принципів у процесі роботи. Це стосується як захисту даних, так і ставлення до колег, клієнтів та конкурентів. Наприклад, фахівці з кібербезпеки не повинні використовувати свої знання для несанкціонованого доступу до інформації чи отримання особистої вигоди.

Спільними рисами кодексів етики IT-організацій є чесність, конфіденційність, повага до прав інших та прозорість у діях. Важливо також уникати конфлікту інтересів та повідомляти про потенційні загрози або порушення, навіть якщо це може бути складним рішенням. Дотримання етичних

стандартів допомагає не лише зміцнити репутацію компанії, а й підтримувати довіру з боку клієнтів та партнерів

8.3. ВАКАНСІЇ У ГАЛУЗІ КІБЕРБЕЗПЕКИ

Багато підприємств в різних галузях промисловості та бізнесу наймають фахівців з кібербезпеки. Існує декілька пошукових онлайн-систем, які допоможуть вам знайти потрібні вакансії у галузі кібербезпеки:

- ITJobMatch – Пошукова система ITJobMatch спеціалізується на пошуку різноманітних вакансій у IT по всьому світу.
- Monster – це пошукова система для вакансій усіх типів. Посилання спрямовує безпосередньо на вакансії, пов’язані з кібербезпекою.
- CareerBuilder – також є пошуковою системою для всіх типів вакансій. Посилання спрямовує безпосередньо на вакансії, пов’язані з кібербезпекою.

Це лише три з багатьох вебсайтів пошуку вакансій. Навіть якщо ви тільки починаєте свою освіту в галузі IT та кібербезпеки, використання систем пошуку роботи – це зручний спосіб дослідити, які види вакансій популярні у всьому світі.

Залежно від вашого інтересу до кібербезпеки, для вас можуть бути доступні різні види вакансій, і вони можуть вимагати наявності навичок, які підтверджуються спеціалізованими сертифікатами. Наприклад, тестувальник вторгнення, також відомий як хакер у Білому капелюсі, шукає та використовує вразливості в додатках, мережах та системах. Щоб стати тестувальником вторгнення, вам потрібно отримати досвід роботи на інших IT-посадах, як адміністратор систем безпеки, адміністратор мережі та системний адміністратор. Кожна з цих вакансій потребує специфічного набору навичок, які допоможуть вам стати цінним співробітником компанії.

Сподіваємося, що цей курс став для вас поштовхом до вивчення IT та кібербезпеки і до побудови подальшої успішної кар’єри!

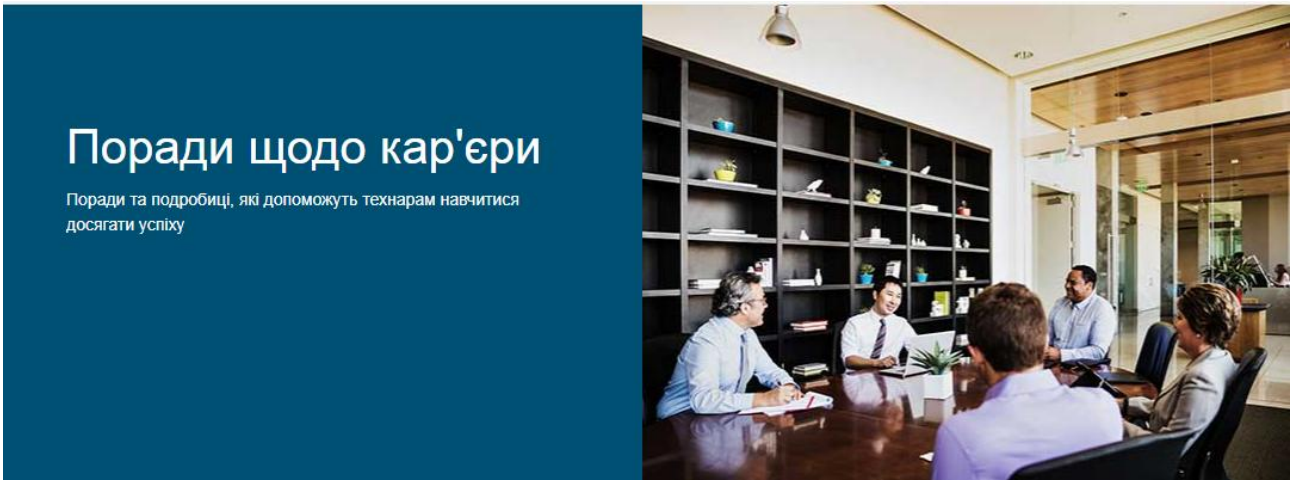


Рис. 8.3. Поради та подробиці

Основні навички

Окрім технічних навичок, щоб досягти успіху як технолог, вам також потрібен цілісний набір нетехнічних навичок, які користуються попитом роботодавців у всьому світі. Це основні навички, пов’язані з вашим успіхом як професіоналом, незалежно від вашої галузі чи посади.

Мережа, подача заявок та співбесіди

Щоб отримати роботу, потрібно представити себе в професійній формі, отримати поради та поради щодо того, як здивувати роботодавців.

Як отримати досвід

Досвід є однією з найбільших проблем для отримання роботи. Вивчіть методи отримання досвіду, а також поясніть їх роботодавцям.

Поради щодо сертифікації

Отримання сертифікації Cisco може бути досить складним процесом, навчіться підготуватися до успіху. Зрозумійте, як сертифікати вписуються у ваші загальні кар’єрні цілі та як втілити їх у реальність.

ВИСНОВКИ

Ця тема розпочинається з обговорення правових та етичних питань, з якими зазвичай стикаються професіонали зі сфери кібербезпеки. Також у ній представлені освітні та кар’єрні шляхи для тих, хто бажає стати професіоналом з кібербезпеки. Запропоновано зовнішні сайти для пошуку вакансій.

Слід підкреслити, що правові та етичні питання відіграють ключову роль у сфері кібербезпеки. Професіонали з кібербезпеки повинні мати навички, подібні до хакерів, але діяти виключно в межах правового поля. Корпоративна відповідальність передбачає дотримання законів про захист даних, таких як GDPR чи CCPA, щоб уникнути штрафів та репутаційних втрат.

Міжнародне право у кібербезпеці, попри свою новизну, сприяє створенню глобальних норм для боротьби з кібератаками, однак існують виклики, пов’язані з суверенітетом держав. Етична поведінка фахівців є не менш важливою, оскільки формально законні дії не завжди є морально прийнятними. Дотримання кодексів етики допомагає підтримувати довіру клієнтів та зміцнювати репутацію компаній. Кар'єра у кібербезпеці потребує поєднання технічних та нетехнічних навичок, а також професійного розвитку через отримання досвіду та сертифікацій.

КОНТРОЛЬНА РОБОТА З ЕТИКИ ДО ТЕМИ 8

Ця контрольна робота охоплює матеріал теми. Вона призначена для надання додаткових можливостей попрактикувати навички та знання, подані у темі і підготовки до Іспиту.

1. Під час зустрічі з відділом маркетингу представник IT-відділу розглядає особливості майбутнього продукту, який буде випущений в наступному році.

– неетично

– етично

2. Алісія - співробітниця компанії, втратила свою корпоративну перепустку. Вона поспішає на зустріч і не має часу відвідати відділ кадрів, щоб отримати тимчасову перепустку. Ви надаєте їй свою перепустку, доки вона не зможе отримати заміну.

– неетично

– етично

Пояснення

Співробітники ніколи не повинні передавати свої перепустки іншому працівнику, незалежно від ситуації або знайомства з ним. Коли ви не контролюєте ваші облікові дані, ви не знаєте, як і для чого вони використовуються.

неетично

3. Співробітник, перебуваючи у ресторані разом із друзями, описує захопливу нову відеогру, яка розробляється в компанії, в якій він працює. Етично чи ні поводиться працівник компанії?

– неетично

– етично

Пояснення

Неетично поширювати конфіденційну ідеєю щодо продукту до початку його випуску. Опис гри для групи друзів за межами компанії може призвести до витоку ідеї і поставити під загрозу випуск нового продукту.

неетично

4. Співробітник вказує на недоліки дизайну нового продукту менеджеру відділу.

– неетично

– етично

Пояснення

І працівник, і менеджер разом працюють в одному відділі тієї ж компанії, тому така поведінка буде етичною.

етично

5. Працівника звільнено після п’ятнадцяти років роботи в одній компаній. Протягом тижня його наймає інша компанія. У новій компанії співробітник ділиться документами та ідеями щодо продуктів, які він пропонував у попередній компанії.

– етично

– неетично

Пояснення

Незважаючи на те, що працівник був звільнений, він, ймовірно, підписав договір про нерозголошення (Non-Disclosure Agreement(NDA)) з попередньою компанією. Будь-яка робота або оригінальна ідея, розроблена в компанії, незважаючи на те, хто її запропонував, залишається власністю компанії. Залежно від рівня тяжкості порушення, це може призвести до судових позовів.

неетично

ДОДАТКОВІ РЕСУРСИ ТА ЗАВДАННЯ

Cisco Learning Network

На сайті Cisco Learning Network ви можете дізнатися про потенційні можливості кар’єрного росту, отримати навчальні матеріали для сертифікаційних іспитів і налагодити контакти з іншими студентами та експертами в області мереж. Для отримання додаткової інформації перейдіть за цим посиланням:

https://learningnetwork.cisco.com

Навчання і сертифікація

Інформацію щодо навчання та останніх сертифікацій Cisco можна знайти в розділі «Навчання і сертифікація» на вебсайті Cisco:

https://www.cisco.com/web/learning/training-index.html

Інформація про кар’єру і зарплату

Тепер, коли ви пройшли всі модулі, прийшов час подумати про кар’єру і зарплату в сфері мережевих технологій. Нижче наведені два посилання на сайти, що містять списки вакансій і потенційну зарплату. В Інтернеті є багато таких сайтів. **Happy Monday** – платформа, яка публікує статті про кар'єру в IT та кібербезпеці, включаючи інформацію про обов'язки та рівень оплати праці для різних позицій.

https://happymonday.ua/chym-zajmayetsya-security-specialist?utm_source=chatgpt.com

Сертифікати CompTIA

Асоціація промислових обчислювальних технологій (http://www.comptia.org) пропонує кілька популярних сертифікатів, включаючи Security +. Це відео від CompTIA фокусується на кібербезпеці.

https://www.youtube.com/watch?v=up9O44vEsDI

СПИСОК ЛІТЕРАТУРИ

1. Азаренкова Г. М. Аналіз моделювання і управління ризиком (в схемах та прикладах): навчальний посібник / Г. М. Азаренкова. – Львів : "Новий світ – 2000", 2024. – 240 с.
2. Бобало Ю. Я. Стратегічна безпека системи “об’єкт – інформаційна технологія” : монографія / Ю.Я. Бобало, В.Б. Дудикевич, Г.В. Микитин Г. В. Львів : Видавництво Львівської політехніки, 2020. – 260 с.
3. Бобало Ю.Я. Інформаційна безпека : навчальний посібник / Ю. Я. Бобало, І. В. Горбатий, М. Д. Кіселичник, А. П. Бондарєв, С. С. Войтусік, А. Я. Горпенюк, О. А. Нємкова, І. М. Журавель, Б. М. Березюк, Є. І. Яковенко, В. І. Отенко, І. Я. Тишик. Львів : Видавництво Львівської політехніки, 2019. –580 с.
4. Бобровський О. М., Коваленко В. Г. Основи криптографії та управління ключами / О.М. Бобровський, В.Г. Коваленко. Київ: Національний університет оборони України, 2018. – 250 с.
5. Богуш В.М. Технічний захист інформації: навчальний посібник в 2 ч. Ч. 1: Основи технічного захисту інформації / В.М.Богуш, В. Д. Бровко, О.С.Кобус, В.Д. Козюра. Київ: Видавництво Ліра-К, 2022. – 286с.
6. Верес О.М. Проектування баз даних у середовищі MS ACCESS 2010 : навчальний посібник / О. М. Верес, І. В. Рішняк. Львів : Видавництво Львівської політехніки, 2016. – 232 с.
7. Гарасимчук О. І. Комплексні системи санкціонованого доступу : навчальний посібник / Гарасимчук О. І. та ін. Львів: Видавництво Львівської політехніки, 2010. – 212 с.
8. Гребенюк А.М. Г 79 Основи управління інформаційною безпекою: навч. посібник / А.М. Гребенюк, Л.В. Рибальченко. Дніпро: Дніпроп. держ. унт внутріш. справ, 2020. – 144 с.
9. Дудикевич В.Б. Забезпечення інформаційної безпеки держави : навчальний посібник / В. Б. Дудикевич, І. Р. Опірський, П. І. Гаранюк, В. С. Зачепило, А. І. Партика. Львів : Видавництво Львівської політехніки, 2017. – 204 с.
10. Євсеєв С. П. Кібербезпека: криптографія з Python : навчальний посібник / С. П. Євсеєв, О. В. Шматко, О. Г. Король. – Харків: Видавництво "Новий Світ-2000", 2024. – 120 с.
11. Іваненко Л. П. Криптографічний захист інформації: методи та управління ключами / Л. П. Іваненко, С. В. Гринь. Львів: Львівський національний університет імені Івана Франка, 2021. – 300 с.
12. Коробейнікова Т.І. Технології захисту локальних мереж на основі мережевого обладнання CISCO : навч. пос. / Т. І. Коробейнікова, С. М. Захарченко. – Л.: Вид-во Львівської політехніки, 2021. – 232с.

13. Лужецький В. А. Захист персональних даних. Навчальний посібник / Лужецький В. А., Войтович О. П., Дудатьєв А. В. – Вінниця ВНТУ, 2013. – 246 с.
14. Мельник Р. А. Програмування вебзастосувань (фронт-енд та бек-енд) : навчальний посібник. Львів : Видавництво Львівської політехніки, 2018. – 248 с.
15. Нестеренко Г. Інформаційна безпека: курс лекцій. Київ: НАУ, 2022. 102 с.
16. Остроухов В.В. Інформаційна безпека. Підручник / В. В. Остроухов, М. М. Присяжнюк, О. І. Фармагей, М. М. Чеховська та ін.; під ред. В. В. Остроухова – К.: Видавництво Ліра-К, 2021. – 412 с.
17. Павлиш В. А. Основи інформаційних технологій і систем : підручник / В. А. Павлиш, Л. К. Гліненко, Н. Б. Шаховська. Львів : Видавництво Львівської політехніки, 2018. – 620 с.
18. Сенів М. М. Безпека програм та даних : навчальний посібник / М.М.Сенів, В. С. Яковина. Львів : Видавництво Львівської політехніки, 2015. 256 с.
19. Сєров Ю. О. Соціальні комунікації в мережі Internet: навчальний посібник / Ю.О. Сєров, С.С. Федушко. Львів : Видавництво Львівської політехніки, 2017. – 236 с.
20. Сукач Ю.Г. Захист об’єктів та проведення відновлювальних робіт у надзвичайних ситуаціях: Частина І. Навчальний посібник / Ю.Г. Сукач, Р.Л. Ткачук.– Львів: Видавництво —Растр, 2017. – 464с.
21. Тарнавський Ю.А. Безпека інформаційних систем [Електронний ресурс]: підручник для студ. спеціальності 122 «Комп’ютерні науки», освітня програма «Цифрові технології в енергетиці». – Київ : КПІ ім. Ігоря Сікорського, 2023. – 161 с.
22. Титова Н.М. Інформаційна безпека та кібербезпека держави: навчальний посібник / Н.М,Титова, Н.М. Рідей, В.П. Настрадін, М.М.Присяжнюк, С.М. Мамченко, С.В.Артюх, Р.О.Яворська. Київ: Видавництво Ліра-К, 2023. – 224с.
23. Химиця Н.О. Інформаційна діяльність в органах державної влади та управління : навчальний посібник. Львів : Видавництво Львівської політехніки, 2014. 148 с.
24. Хорошко В.О. Проєктування комплексних систем захисту інформації : підручник / В. О. Хорошко, І. М. Павлов, Ю. Я. Бобало, В. Б. Дудикевич, І. Р. Опірський, Л. Т. Пархуць. Львів : Видавництво Львівської політехніки, 2020. – 320 с.
25. Katz, Jonathan, Lindell, Yehuda (2024). Introduction to Modern Cryptography (3rd ed.). CRC Press. 521 p., https://www.cs.umd.edu/~jkatz/imc.html
26. Yevseiev S. Synergy of building cybersecurity systems: monograph / S. Yevseiev, V. Ponomarenko, O. Laptiev, O. Milov and others. – Kharkiv: PC TECHNOLOGY CENTER, 2021. – 188 p.

27. Yevseiev S. (2023) Models of socio-cyber-physical systems security: monograph / S. Yevseiev, Yu. Khokhlachova, S. Ostapov, O. Laptiev and others. – Kharkiv: PC TECHNOLOGY CENTER, 2023. – 168 p.
28. Stallings, W. (2017). Cryptography and Network Security: Principles and Practice (7th ed.). Upper Saddle River, NJ: Pearson Education.
29. Yevseiev S. Modeling of security systems for critical infrastructure facilities: monograph / S. Yevseiev, R. Hryshchuk, K. Molodetska, M. Nazarkevych and others. – Kharkiv: PC TECHNOLOGY CENTER, 2022. – 196 p.

Стандарти та Законодавча база

30. ДСТУ 3396.0-96. Захист інформації. Основні положення. [Електронний ресурс] — Режим доступу: https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=69172
31. ДСТУ 3996.1-96. Захист інформації. Порядок проведення роботи. [Електронний ресурс] — Режим доступу: https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=69173
32. Закон України «Про електронні документи та електронний документообіг», редакція від 31.12.2023 р. [Електронний ресурс] — Режим доступу: https://zakon.rada.gov.ua/laws/show/851-15#Text
33. Закон України «Про електронний цифровий підпис», редакція від 07.11.2018 р. [Електронний ресурс] — Режим доступу: https://zakon.rada.gov.ua/laws/show/852-15#Text
34. Закон України «Про захист інформації в інформаційно-комукаційних системах», редакція від 28.06.2024 р. [Електронний ресурс] — Режим доступу: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text
35. Закон України «Про захист персональних даних», редакція від 27.04.2024 р. [Електронний ресурс] — Режим доступу: https://zakon.rada.gov.ua/laws/show/2297-17#Text
36. Закон України «Про основи національної безпеки України», редакція від 08.07.2018 р. [Електронний ресурс] — Режим доступу: https://zakon.rada.gov.ua/laws/show/964-15#Text
37. Наказ Державної служби соціального зв'язку та захисту інформації України Про затвердження Порядку координації діяльності органів державної влади, органів місцевого самоврядування, військових формувань, підприємств, установ і організацій незалежно від форм власності з питань запобігання, виявлення та усунення наслідків несанкціонованих дій щодо державних інформаційних ресурсів в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах, редакція від 10.01.2023 р.

[Електронний ресурс] — Режим доступу: https://zakon.rada.gov.ua/laws/show/z0603-08#Text

38. Наказ Державної служби соціального зв’язку та захисту інформації України Наказ Адміністрації Держспецзв'язку від 15.01.2021 № 23 "Про затвердження Методичних рекомендацій щодо категоризації об’єктів критичної інфраструктури" [Електронний ресурс] — Режим доступу: https://cip.gov.ua/ua/news/nakaz-administraciyi-derzhspeczv-yazku-vid-15-01-2021-23-pro-zatverdzhennya-metodichnikh-rekomendacii-shodo-kategorizaciyi-ob-yektiv-kritichnoyi-infrastrukturi
39. ДСТУ ISO/IEC 27000: 2019 provides the overview of information security management systems (ISMS). нформаційні технології. Методи захисту. Системи керування інформаційною безпекою. Огляд і словник термінів (*ISO/IEC 27000:2018*, IDT) [Електронний ресурс] — Режим доступу: https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=85795
40. ДСТУ ISO/IEC 27005:2023 Інформаційна безпека, кібербезпека та захист конфіденційності. Настанова керування ризиками інформаційної безпеки (ISO/IEC 27005:2022, IDT), [Електронний ресурс] — Режим доступу: https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=104400
41. Регламент європейського парламенту і ради (ЄС) 2019/881 від 17 квітня 2019 року «Про Агентство Європейського Союзу з питань мережевої та інформаційної безпеки (ENISA) та про сертифікацію кібербезпеки інформаційно-комунікаційних технологій» , а також про скасування Регламенту (ЄС) № 526/2013 (Акт про кібербезпеку) Електронний ресурс] — Режим доступу: Regulation - 2019/881 - EN - EUR-Lex
42. Директива Європейського Парламенту про безпеку мережі та інформаційних систем (Директива NIS) Directive - 2016/1148 - EN - EUR-Lex
43. Регламент (ЄС) 2016/679 Європейського парламенту та Ради від 27 квітня 2016 р. про захист фізичних осіб щодо обробки персональних даних та про вільне переміщення таких даних, а також про скасування Директиви 95/46/ЄС (Загальне положення про захист персональних даних) Regulation - 2016/679 - EN - gdpr - EUR-Lex

ДОДАТОК 1. ОСНОВНІ СЕРВІСИ GOOGLE

Сервіси Google

- Google Статистика пошуку – дає змогу дізнатись найбільш популярні, а також швидше за все набирали популярність запити в заданий відрізок часу.
- Google AdSense – сервіс контекстної реклами, що дає змогу заробити господарям сторінок з великою відвідуваністю. Програма автоматично доставляє текстові та графічні оголошення, розраховані на вебсайт і його зміст. Застосовується й для блогів чи відео на YouTube.
- Google Ads – сервіс контекстної реклами, працює з ключовими словами.
- Google Alerts – відправлення на пошту результатів пошуку із заданою періодичністю.
- Google Analytics – безкоштовний сервіс, який дає змогу власникам ресурсів отримувати докладну інформацію про трафік, поведінку користувачів, джерела відвідувань і ефективність маркетингових кампаній.
- Google Arts & Culture – інтерактивно-представлені популярні музеї світу, платформа, що надає доступ до колекцій мистецтва, культурних об'єктів і історичних пам'яток.
- Google App Engine – платформа для створення та хостингу масштабованих вебзастосунків на серверах компанії Google.
- Google Apps – сервіс для використання служб Google разом зі своїм доменом.
- Google Merchant Center (раніше Google Base) – дає змогу власникам контенту поміщати структуровану інформацію в сховище, автоматично отримуючи можливість пошуку за цією інформацією.
- Blogger – це сервіс для ведення блогів, що дає змогу тримати на своєму хостингу не тільки програмне забезпечення, а всю інформацію: записи, коментарі та персональні сторінки в СУБД на серверах Google.
- Google Bookmarks – дає змогу відзначати сайти закладками, додавати до них ярлики та примітки. По ярликах і приміток можна робити пошук, закладки зберігаються на сервері і доступні з будь-якого комп’ютера.
- Google Calendar – онлайновий сервіс для планування зустрічей, подій і справ з прив’язкою до календаря. Можливо спільне використання календаря групою користувачів. Крім того, сервіс інтегрований з Gmail.
- Google Classroom – безкоштовний веб сервіс створений Google для шкіл з метою спрощення створення, поширення і класифікації завдань безпаперовим шляхом. Основна мета сервісу - прискорити процес поширення файлів між викладачами і студентами.

- Google Cloud Print – технологія, за допомогою якої принтер підключається до інтернету, що дає змогу ряду користувачів роздруковувати документи віддалено.
- Google Correlate – сервіс, який дає змогу дізнатися, які запити часто роблять разом із заданим.
- Google Custom Search – дає змогу веброзробникам інтегрувати пошук Google в їхні вебзастосунки, також частиною набору інструментів, що стосуються "спеціального пошуку" від Google.
- Google Документи – веборієнтований застосунок для роботи з документами, що допускає спільне використання документа. Зараз замінений на Google Drive.
- Google Directory (раніше Catalogs) – вміст мережі, впорядковані за тематичним категоріях. Закрився.
- Google Dictionary – сервіс для перекладу окремих слів на інші мови.
- Google Drive – хмарне сховище від Google з можливістю онлайн (в браузері) просмотру файлів різного типу (у тому числі й файлів фотошопу). Пропонує 15 Гб вільного місця.
- Google Finance – сайт-агрегатор біржової інформації.
- Gmail – безкоштовна електронна пошта з великим обсягом місця для зберігання повідомлень (понад 10,1 Гб), з доступом по POP3 і зручним вебінтерфейсом. Також є OpenID-провайдером для всіх служб Google.
- Google Groups – архів конференцій Usenet.
- Google Лабораторія – інкубатор ідей для нових сервісів, призначений для тестування інтерфейсу тощо
- Google Maps – набір карт, побудованих на основі безкоштовного картографічного сервісу.
- Google Maps API – інтерфейс, що дає змогу вбудовувати карти на зовнішні сайти за допомогою JavaScript.
- Google Mars – карти Марса.
- Google Moon – карти місяця.
- Google Mobile – інтерфейс для використання застосунків Google за допомогою мобільних пристроїв.
- Google Новини – автоматично створюваний новинний сайт, на якому зібрані заголовки більш ніж з 400 джерел новин по всьому світу: схожі статті групуються, а потім показуються згідно з особистими інтересами кожного читача.
- Google Ngram Viewer – дає змогу вивести у вигляді графіка статистику вживання тих чи слів у російській, англійській, німецькій, французькій, іспанській, єврейській чи китайській літературі протягом заданого відрізка часу.
- Google Picasa Web – персональні галереї фотографій.

- Google Play – магазин застосунків від Google, що дає змогу власникам пристроїв з операційною системою Android встановлювати і купувати різні застосунки (власникам Android-пристроїв зі Сполучених Штатів і Росії також доступне придбання на Google Play книжкових видань, музики і фільмів).
- Google Public Data Explorer – публічні дані та прогнози від ряду міжнародних організацій та наукових установ.
- Google Public DNS – альтернативний DNS-сервер Google.
- Google Talk – програма для обміну миттєвими повідомленнями (на основі протоколу XMPP) і інтернет-телефон.
- Google Search History – історія пошукових запитів користувача.
- Google Sites – безкоштовний хостинг, який використовуєвікі-технологію.
- Google Translate – система статистичного машинного перекладу слів, текстів, фраз, вебсторінок між будь-якими парами мов.
- Google Trends – частотність обраного пошукового запиту.
- Google Voice – передача голосу по протоколу VoIP.
- Google Webmasters – інструменти для вебмайстрів.
- Picnik – онлайн-сервіс для редагування фотографій. Закрито в 2012 році.
- YouTube – відеохостинг.
- Google One Pass – онлайн-магазин, де видавці можуть продавати доступ до контенту.
- Google+ – соціальна мережа
- Google Keep – багатофункціональний сервіс для збереження текстових нотаток, списків, голосових заміток і зображень. Підтримує організацію нотаток за кольорами та мітками, а також можливість їх спільного використання, дає змогу користувачам ставити нагадування за допомогою геолокації або часу..
- **Google Lens** – сервіс для розпізнавання об'єктів за допомогою камери смартфона. Може визначати текст, рослини, тварин, товари та інші об'єкти для пошуку в Google.
- **Google Fit** – платформа для моніторингу фізичної активності, здоров'я та фітнесу користувача. Працює з мобільними пристроями та розумними годинниками.
- **Google Stadia** – хмарна платформа для потокового ігрового сервісу, що дає змогу грати в сучасні відеоігри без потужного обладнання.
- **Google Podcasts** – сервіс для прослуховування, підписки та управління подкастами на мобільних пристроях і вебплатформах.
- **Google Forms** – сервіс для створення анкет, опитувань і тестів, з можливістю аналізу зібраних даних у Google Sheets.

Спеціальний пошук Google

- Google Book Search – повнотекстовий пошук по книгах, оцифрованих компанією Google (понад 10 мільйонів книг з найбільших бібліотек США).
- Google Custom Search – сервіс для створення власної системи пошуку на основі пошукової системи Google.
- Google Shopping – сервіс для пошуку товарів у різних інтернет-магазинах, який дає змогу користувачам порівнювати ціни, переглядати пропозиції та здійснювати покупки. Спочатку він був доступний тільки в США та Канаді, але наразі працює у багатьох країнах світу, зокрема в Європі, Австралії, Індії та інших регіонах.
- Hackser Style Google – інтерфейс пошуку мовою Leet.
- Google Images – сервіс пошуку картинок в пошуковій системі Google.
- Special Searches – пошук на спеціалізованих сайтах (BSD, Linux, Mac OS X і Microsoft).
- Google Patents Search – пошук по патентах серед понад 7 мільйонів доступних в базі даних.
- Google Scholar – сервіс для пошуку наукових джерел: статей, книг, дисертацій, опублікованих різними науковими організаціями та професійними спільнотами.
- Google Suggest – частина пошуку Google, технологія автозаповнення рядка пошукового запиту на основі загальної статистики найпопулярніших запитів.
- Google Video – сервіс для пошуку, перегляду і збереження відео.
- Телефонна книга – служба Google, яка дає змогу знайти телефонні номери і адреси, опубліковані в загальнодоступних джерелах. Результати пошуку з адресної книги Google з'являються над іншими результатами при введенні певних типів запитів (імені, прізвища, міста і т. д.).
- Мовні інструменти – інструмент, що дає змогу використовувати Google на безлічі різних мов.
- Калькулятор – сервіс для розрахунків, вбудований в рядок пошуку. Наприклад, якщо задати пошук рядка 900+600*2-(3+1), то буде виданий відповідь 2096, а також інтернет-сторінки, де такий рядок може зустрічатися. Сервіс знає безліч математичних функцій, вміє дотримуватися пріоритету операцій.
- Конвертер валют – дає змогу швидко і зручно перевести одну валюту в іншу. Наприклад, 600 USD in UAH – скільки буде $600 в гривнях.

ДОДАТОК 2. ПРАКТИЧНІ РЕКОМЕНДАЦІЇ ЩОДО ПРОТИДІЇ ЗЛАМУ ПАРОЛІВ

Щоб запобігти зламу ваших паролів за допомогою соціальної інженерії, грубої сили або атаки за словником, а також захистити ваші онлайн-облікові записи, рекомендуємо:

1. Не використовуйте один і той самий пароль, таємне запитання та відповідь для кількох важливих облікових записів.

2. Використовуйте пароль, який містить не менше 16 символів, принаймні одну цифру, одну велику літеру, одну малу літеру та один спеціальний символ.

3. Не використовуйте імена своїх рідних, друзів або домашніх тварин у своїх паролях.

4. Не використовуйте у своїх паролях поштові індекси, номери будинків, номери телефонів, дати народження, ідентифікаційні картки, номери соціального страхування тощо.

5. Не використовуйте слова зі словника у своїх паролях.

Приклади надійних паролів: ePYHc~dS*)8$+V-', qzRtC{6rXN3N\RgL, zbfUMZPE6`FC%)sZ.

Приклади слабких паролів: qwert12345, Gbt3fC79ZmMEFUFJ, 1234567890, 987654321, nortonpassword.

6. Не використовуйте два або більше подібних паролів, більшість символів яких однакові, наприклад, ilovefreshflowersMac, ilovefreshflowersDropBox, оскільки якщо один із цих паролів вкрадено, це означає, що всі ці паролі вкрадені.

7. Не використовуйте в якості паролів щось, що можна клонувати (але ви не можете змінити), як-от відбитки пальців.

8. Не дозволяйте вашим веббраузерам (FireFox, Chrome, Safari, Opera, IE, Microsoft Edge) зберігати ваші паролі, оскільки всі паролі, збережені у веббраузерах, можна легко розкрити.

9. Не входьте до важливих облікових записів на чужих комп'ютерах або при підключенні до загальнодоступної точки доступу Wi-Fi, Tor, безкоштовного VPN або вебпроксі.

10. Не надсилайте конфіденційну інформацію в Інтернеті через незашифровані (наприклад, HTTP або FTP) з'єднання, оскільки повідомлення в цих з'єднаннях можна перехопити з дуже невеликими зусиллями. Ви повинні використовувати зашифровані з'єднання, такі як HTTPS, SFTP, FTPS, SMTPS, IPSec, коли це можливо.

11. Під час подорожі ви можете зашифрувати свої інтернет-з'єднання, перш ніж вони залишать ваш ноутбук, планшет, мобільний телефон або маршрутизатор. Наприклад, ви можете налаштувати приватну VPN з такими протоколами, як WireGuard (або IKEv2, OpenVPN, SSTP, L2TP через IPSec) на своєму власному сервері (домашній комп'ютер, виділений сервер або VPS) і підключитися до нього. Крім того, ви можете налаштувати зашифрований SSH-тунель між комп'ютером і власним сервером і налаштувати Chrome або FireFox на використання проксі-сервера socks. Тоді, навіть якщо хтось захопить ваші дані під час їх передачі між вашим пристроєм (наприклад, ноутбуком, iPhone, iPad) і вашим сервером за допомогою сніфера пакетів, вони не зможуть вкрасти ваші дані та паролі із зашифрованих потокових даних.

12. Наскільки надійний мій пароль? Можливо, ви вважаєте, що ваші паролі дуже надійні, їх важко зламати. Але якщо хакер вкрав ваше ім'я користувача та хеш-значення MD5 вашого пароля з сервера компанії, а райдужна таблиця хакера містить цей хеш MD5, ваш пароль буде швидко зламано.

Щоб перевірити надійність ваших паролів і дізнатися, чи знаходяться вони в популярних райдужних таблицях, ви можете конвертувати свої паролі в хеші MD5 за допомогою генератора хешування MD5, а потім розшифрувати паролі, надіславши ці хеші до онлайнової служби розшифровки MD5. Наприклад, ваш пароль «0123456789A», й, використовуючи метод грубої сили, комп'ютеру може знадобитися майже рік, щоб зламати ваш пароль, але якщо ви розшифруєте його, надіславши його хеш MD5 (C8E7279CD035B23BB9C0F1F954DFF5B3) на вебсайт, як багато часу необхідно, щоб зламати його? Ви можете провести тест самостійно.

13. Рекомендується змінювати паролі кожні 10 тижнів.

14. Рекомендується запам'ятати кілька основних паролів, зберегти інші паролі в текстовому файлі та зашифрувати цей файл за допомогою 7-Zip, GPG або програмного забезпечення для шифрування диска, наприклад BitLocker, або керувати своїми паролями за допомогою програмного забезпечення для керування паролями.

15. Шифруйте та створюйте резервні копії своїх паролів у різних місцях, то якщо ви втратили доступ до свого комп'ютера чи облікового запису, ви зможете швидко відновити свої паролі.

16. Увімкніть двоетапну автентифікацію, коли це можливо.

17. Не зберігайте критичні паролі в хмарі.

18. Отримайте доступ до важливих вебсайтів (наприклад, Paypal) безпосередньо із закладок, інакше уважно перевірте його доменне ім'я. Перед

введенням пароля бажано перевірити популярність вебсайту за допомогою панелі інструментів Alexa, щоб переконатися, що це не фішинговий сайт.

19. Захистіть свій комп'ютер за допомогою брандмауера та антивірусного програмного забезпечення, заблокуйте всі вхідні з'єднання та всі непотрібні вихідні з'єднання за допомогою брандмауера. Завантажуйте програмне забезпечення лише з авторитетних сайтів і перевіряйте контрольну суму MD5 / SHA1 / SHA256 або підпис GPG інсталяційного пакета, коли це можливо.

20. Зберігайте операційні системи (наприклад, Windows 7, Windows 10, Mac OS X, iOS, Linux) і веббраузери (наприклад, FireFox, Chrome, IE, Microsoft Edge) на ваших пристроях (наприклад, Windows PC, Mac PC, iPhone, iPad, планшет Android) оновлюйте, встановивши останнє оновлення безпеки.

21. Якщо на вашому комп'ютері є важливі файли, і інші можуть отримати доступ до них, перевірте, чи є апаратні клавіатурні реєстратори (наприклад, бездротова клавіатура), програмні кейлоггери та приховані камери, коли ви вважаєте, що це необхідно.

22. Якщо у вашому домі є маршрутизатори WIFI, то можна дізнатися паролі, які ви ввели (у будинку вашого сусіда), виявивши жести ваших пальців і рук, оскільки сигнал WIFI, який вони отримали, змінюється, коли ви рухаєте пальцями та руки. У таких випадках ви можете використовувати екранну клавіатуру для введення паролів. Це було б безпечніше, якби ця віртуальна клавіатура (або програмна клавіатура) щоразу змінювала розкладку.

23. Коли ви залишаєте їх, заблокуйте свій комп'ютер і мобільний телефон.

24. Зашифруйте весь жорсткий диск за допомогою VeraCrypt, FileVault, LUKS або подібних інструментів, перш ніж помістити на нього важливі файли, і фізично знищити жорсткий диск ваших старих пристроїв, якщо це необхідно.

25. Отримайте доступ до важливих вебсайтів у приватному режимі чи в режимі анонімного перегляду або використовуйте один веббраузер для доступу до важливих вебсайтів, використовуйте інший для доступу до інших сайтів. Або перейдіть на неважливі вебсайти та встановіть нове програмне забезпечення у віртуальній машині, створеній за допомогою VMware, VirtualBox або Parallels.

26. Використовуйте принаймні 3 різні адреси електронної пошти, використовуйте першу для отримання електронних листів з важливих сайтів і програм, таких як Paypal і Amazon, використовуйте другу для отримання електронних листів з неважливих сайтів і програм, використовуйте третю (з іншого постачальника послуг електронної пошти, наприклад Outlook і GMail), щоб отримувати ваш електронний лист зі скиданням пароля, коли перший (наприклад, Yahoo Mail) зламано.

27. Використовуйте принаймні 2 різні номери телефону, НЕ повідомляйте іншим номер телефону, який ви використовуєте для отримання текстових повідомлень з кодами підтвердження.

28. Не натискайте посилання в електронному листі чи SMS-повідомленні, не скидайте свої паролі, натискаючи їх, за винятком того, що ви знаєте, що ці повідомлення не підроблені.

29. Нікому не повідомляйте свої паролі в електронній пошті.

30. Можливо, одне з програмного забезпечення чи додатка, яке ви завантажили чи оновили, було змінено хакерами. Ви можете уникнути цієї проблеми, не встановлюючи це програмне забезпечення чи додаток у перший раз, за винятком того, що вони опубліковані, щоб усунути діри в безпеці. Натомість можна використовувати вебдодатки, які є більш безпечними та портативними.

31. Будьте обережні, користуючись онлайн-інструментами вставки та інструментами захоплення екрана, не дозволяйте їм завантажувати ваші паролі в хмару.

32. Якщо ви вебмайстер, не зберігайте паролі користувачів, таємні запитання та відповіді у вигляді простого тексту в базі даних, замість цього вам слід зберігати хеш-значення (SHA1, SHA256 або SHA512) цих рядків. Рекомендується створити унікальний випадковий рядок солі для кожного користувача. Крім того, непогано зареєструвати інформацію про пристрій користувача (наприклад, версію ОС, роздільну здатність екрана тощо) і зберегти для них підсолені хеш-значення, а потім, коли він/вона спробує ввійти з правильним паролем, але його/її пристрій інформація НЕ збігається з попередньою збереженою, дозвольте цьому користувачеві підтвердити свою особу, ввівши інший код підтвердження, надісланий через SMS або електронну пошту.

33. Якщо ви розробник програмного забезпечення, вам слід опублікувати пакет оновлень, підписаний закритим ключем за допомогою GnuPG, і перевірити його підпис відкритим ключем, опублікованим раніше.

34. Щоб забезпечити безпеку вашого бізнесу в Інтернеті, вам слід зареєструвати власне доменне ім’я та налаштувати обліковий запис електронної пошти з цим доменним іменем, тоді ви не втратите обліковий запис електронної пошти та всі свої контакти, оскільки ви можете розміщувати свою пошту будь-де, ваш обліковий запис електронної пошти не може бути вимкнено постачальником послуг електронної пошти.

35. Якщо сайт покупок в Інтернеті дає змогу здійснювати оплату лише за допомогою кредитних карток, вам слід використовувати віртуальну кредитну картку.

36. Закрийте веббраузер, коли виходите з комп'ютера, інакше файли cookie можуть бути легко перехоплені невеликим USB-пристроєм, що дозволить обійти двоетапну перевірку та увійти до свого облікового запису за допомогою вкрадених файлів cookie на інших комп'ютерах.

37. Не довіряйте та видаляйте погані сертифікати SSL зі свого веббраузера, інакше ви НЕ зможете забезпечити конфіденційність і цілісність з'єднань HTTPS, які використовують ці сертифікати.

38. Зашифруйте весь системний розділ, інакше вимкніть файл підкачки та функції глибокого сну, оскільки ваші важливі документи можна знайти у файлах pagefile.sys та hiberfil.sys.

39. Щоб запобігти атакам методом грубого входу на ваші виділені сервери, сервери VPS або хмарні сервери, ви можете встановити програмне забезпечення для виявлення та запобігання вторгненням, наприклад LFD (Daemon Failure Login) або Fail2Ban.

40. Якщо це можливо, використовуйте хмарне програмне забезпечення, а не встановлюйте програмне забезпечення на свій локальний пристрій, оскільки все більше і більше атак на ланцюжок поставок, які встановлюють шкідливі програми або оновлення на ваш пристрій, щоб вкрасти ваші паролі та отримати доступ до абсолютно секретних даних.

41. Рекомендується генерувати контрольні суми MD5 або SHA1 всіх файлів на вашому комп'ютері (за допомогою програмного забезпечення, наприклад MD5Summer) і зберігати результат, а потім перевіряти цілісність ваших файлів (і знаходити троянські файли або програми з вставленим бекдором) щодня порівнюючи їх контрольні суми з результатом, збереженим раніше.

42. Кожна велика компанія повинна впровадити та застосувати систему виявлення вторгнень на основі штучного інтелекту (включаючи засоби виявлення аномалій поведінки мережі).

43. Дозволити лише IP-адресам, які внесені до білого списку, підключатися до важливих серверів і комп'ютерів або входити на них.

НАВЧАЛЬНЕ ВИДАННЯ

Ткачук Ростислав Львович
Маслова Наталія Олександрівна
Івануса Андрій Іванович

ОСНОВИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Навчальний посібник

Літературний редактор Галина Падик

Технічний редактор, верстка
та відповідальний за випуск: Ростислав Ткачук

Підписано до друку 19.11.2025 р.
Формат 60×84/16 Гарнітура Times New Roman
Друк цифровий. Папір офсетний.
Ум. друк. арк. 15,11 Обл. вид. арк. 11,49

Друк ЛДУБЖД
79007, м. Львів, вул. Клепарвська, 35
тел./факс. 032 233 24 79
e-mail: vnr@ldubgd.edu.ua
Свідоцтво суб'єкта видавничої справи
ДК №7249 від 09.02. 2021 р.