Міністерство освіти і науки України
Львівський державний університет безпеки життєдіяльності
Національний університет "Львівська політехніка"

ЗАХИСТ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ

ТЕЗИ ДОПОВІДЕЙ
ІІ Міжвузівської науково-практичної конференції
студентів і курсантів

24 листопада 2017 р.

Державна служба України з надзвичайних ситуацій
Міністерство освіти і науки України
Львівський державний університет безпеки життєдіяльності
Національний університет "Львівська політехніка"

ЗАХИСТ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ

ТЕЗИ ДОПОВІДЕЙ
ІІ Міжвузівської науково-практичної конференції студентів і курсантів

24 листопада 2017 р.
м. Львів

Захист інформації в інформаційно-комунікаційних системах: збірник тез доповідей ІІ Міжвузівської науково-практичної конференції студентів і курсантів. – Львів: ЛДУ БЖД, 2017. – 65 с.

Організатори конференції:

Державна служба України з надзвичайних ситуацій
Міністерство освіти і науки України
Львівський державний університет безпеки життєдіяльності
Національний університет "Львівська політехніка"

У збірнику опубліковано матеріали конференції, на якій розглядалися питання захисту сучасних інформаційно-комунікаційних систем, а саме управління інформаційною безпекою, захист інформації в комп'ютерних мережах, технічний захист інформації та інформаційні технології.

Поштова адреса оргкомітету:
м. Львів, 79007, вул. Клепарівська, 35
Кафедра управління інформаційною безпекою
Контактні телефони: +380976132353
Електронна адреса: vsamotyj@gmail.com

Програмний комітет

Голова: **Андрій Кузик** – д.с.-г.н., професор, проректор Львівського державного університету безпеки життєдіяльності, полковник служби цивільного захисту

Співголова: **Володимир Самотий** – д.т.н., професор, завідувач кафедри управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності

Науково-організаційний комітет

Валерій Дудикевич – д.т.н., професор, завідувач кафедри захисту інформації Національного університету «Львівська політехніка»

Володимир Максимович – д.т.н., професор, завідувач кафедри безпеки інформаційних технологій Національного університету «Львівська політехніка»

Євген Мартин – д.т.н., професор, завідувач кафедри управління проектами, інформаційних технологій та телекомунікацій Львівського державного університету безпеки життєдіяльності

Леонід Мороз – д.т.н., доцент, професор кафедри управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності

Володимир Ромака – д.т.н., професор, професор кафедри захисту інформації Національного університету «Львівська політехніка»

Андрій Ренкас – к.т.н., доцент, начальник навчально-наукового інституту цивільного захисту Львівського державного університету безпеки життєдіяльності, полковник служби цивільного захисту

Ольга Меньшикова – к.ф.-м.н., доцент, заступник начальника навчально-наукового інституту цивільного захисту Львівського державного університету безпеки життєдіяльності з навчально-наукової роботи, полковник служби цивільного захисту

Андрій Лагун – к.т.н., доцент, заступник завідувача кафедри управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності

Олександр Придатко – к.т.н., заступник начальника кафедри управління проектами, інформаційних технологій та телекомунікацій Львівського державного університету безпеки життєдіяльності, майор служби цивільного захисту

Наталія Кухарська – к.ф-м.н., доцент, доцент кафедри управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності

Тарас Брич – к.т.н., доцент кафедри управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності

Марія Мандрона – к.т.н., доцент кафедри управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності

Орест Полотай – к.т.н., доцент кафедри управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності

Ростислав Гриник – викладач кафедри управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності, капітан служби цивільного захисту

Олег Вацлавик – викладач кафедри управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності.

ЗМІСТ

АЛГОРИТМІЗАЦІЯ ПРОЦЕСУ ІНТЕГРАЦІЇ СИСТЕМ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ В ПІДРОЗДІЛИ ДСНС УКРАЇНИ

Андрій Антонов, Назарій Бурак
Львівський державний університет безпеки життєдіяльності, м. Львів

Проведено аналіз сучасних систем електронного документообігу, які використовуються для організації діловодства у державних установах. Виділеного основні переваги та недоліки даних систем, та відмінності у функціоналі. На основі врахування специфіки роботи органів та підрозділів Державної служби України з надзвичайних ситуацій запропоновано алгоритм інтеграції зазначених систем у повсякденну діяльність.

Ключові слова: інформаційні технології, цивільний захист, системи електронного документообігу, контроль виконання документів, інтеграція.

Modern document management systems were analyzed, which are used for the organization of documents in government institutions. There were highlighted the main advantages and disadvantages of these systems. Also were shown differences in their functional possibilities. On the basis of work specifics of the State Service of Ukraine for Emergency Situations was proposed an algorithm for integrating these systems into the daily activities.

Key words: information technologies, civil defense, document management system, control of the documents execution, integration

Стрімкі темпи розвитку інформаційних технологій та телекомунікацій, їх інтеграція практично в усі сфери діяльності людини зумовлює автоматизацію значної частини робіт, пов'язаних із затратами ресурсів та матеріалів.

У сучасному ритмі життя суспільство повинне використовувати усі можливі засоби та заходи з метою зменшення використання ресурсів та пошук альтернатив їм. Саме на виконання однієї із таких гуманістичних місії і покликані системи електронного документообігу.

Відповідно до [1] ще з 2003 року в Україні на законодавчому рівні визнали необхідність використання систем такого типу.

Сьогодні автоматизація робіт з електронними документами набуває все більшого поширення. За даними дослідження компанії Siemens Business Services у 2011 р., продуктивність праці персоналу за сучасних умов при використання електронних документів зростає на 20–25 %. Саме тому автоматизація робіт документообігу, який відбувається в органах та підрозділах Державної служби України з надзвичайних ситуацій(ДСНС України), має важливе значення для підвищення рівня ефективності діяльності системи управління загалом[3].

Загальна схема роботи системи електронного документообігу у ДСНС України подано на рис.1

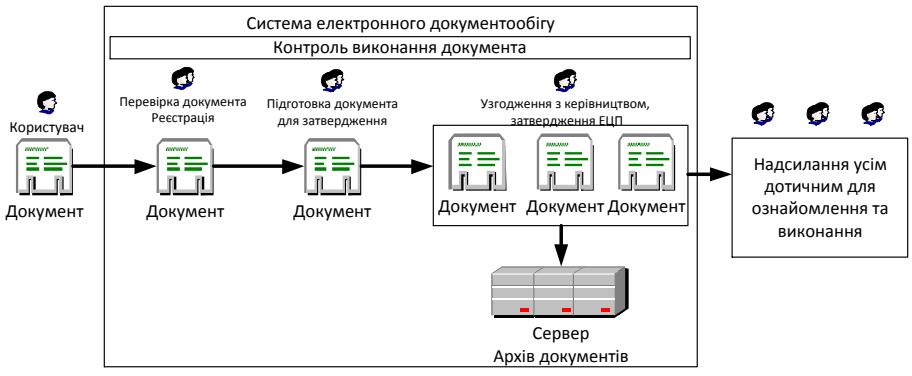


Рис 1. Типова структурна схема роботи системи електронного документообігу

Використання електронних документів значно полегшує дотримання систематизації та аналізу наявної службової інформації[2]. Це можливо забезпечити спеціальним програмними засобами, які дають змогу здійснити формування якісної електронної документації з усуненням різних видів прогалин, виконувати контроль процесів її виконання, збереження, пошуку та використання.

У сучасному арсеналі різнопланових систем електронного документообігу можна виділити такі системи як: «ДЕЛО», «ОРТіМА-WorkFlow», «Megapolis.Документообіг», ,

«Documentum», «АСКОД», «Док Проф», кожна з яких забезпечує певні функціональні призначення[4].

На основі проведеного аналізу зазначених систем електронного документообігу можна побудувати матрицю відповідності задекларованого функціоналу та потребам користувачів (Табл. 1.), де «+» – система повністю відповідає вимогам, «±» – система частково задовольняє вимоги та «–» – у системі відсутній даний функціонал.

Таблиця 1

Матриця покриття вимог користувачів функціоналом програмних засобів

Функції	Основні характеристики	Megapolis. Документообіг	OPTiMA-WorkFlow	Док Проф	АСКОД	Documentum	ДЕЛО
Робота з документами	Реєстрація	+	+	+	+	+	+
	Резолюція	+	+	+	+	+	+
	Контроль виконання	+	+	+	+	+	+
	Маршрутна карта	–	+	–	+	+	+
	Імпорт/Експорт	±	+	±	±	±	±
	Пошук	+	+	+	+	+	+
	Архів/Сервер зберігання	+/+	±/+	–/+	±/–	+/+	±/–

Використання спеціалізованого програмного забезпечення з метою автоматизації документообігу значно підвищить якість та ефективність, а основне – швидкість, обробки інформації, систематизацію та контроль за її виконанням. Програмне забезпечення такого типу дасть смогу зменшити використання природних ресурсів, особливо паперових, а від так і заощадить кошти та збереже екологію.

На основі виконаного дослідження можна зробити висновок, що, враховуючи специфіку діяльності та документації, для організації електронного документообігу в органах та підрозділах ДСНС України, зокрема і у вищих навчальних закладах служби цивільного захисту доцільно обрати одну із наступних програм: «Documentum», «Megapolis. Документообіг» або «OPTIMA-WorkFlow».

Література

1. Закон України «Про електронні документи та електронний документообіг» від 22 травня 2003 року № 851-IV із поправками. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/851-15.
2. Матвієнко О. Основи організації електронного документообігу: навчальний посібник / О. Матвієнко, М. Цивін. – К.: Центр навчальної літератури, 2008. – 112 с.
3. Наказ МВС України «Про затвердження Інструкції з організації контролю за виконанням документів у системі ДСНС» від 19 травня 2016р. № 387. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/en/z0865-16.
4. Перехрест Г. Впровадження електронного документообігу: огляд вітчизняних систем / Г. Перехрест// Довідник секретаря та офіс–менеджера. – 2007. – № 6. – С. 38–44.

DOCKER-ТЕХНОЛОГІЇ В ПОБУДОВІ МІКРОСЕРВІСІВ

Олег Андрушко, Микола Панасюк, Ігор Малець
Львівський державний університет безпеки життєдіяльності, Львів

Висвітлено складність командної роботи в процесі розробки програмних продуктів за умови віддаленого доступу. Доповнено існуючий багаж знань про технології контейнеризації в світлі особливостей використання Docker для побудови мікросервісів. Визначено особливості використання та основні переваги Docker-технологій в процесі побудови мікросервісів.

Ключові слова: контейнеризація, розробка мікросервісів, віртуалізація, Docker-технологія.

The problem of the complexity of teamwork in the process of developing software products with remote access is described. The existing knowledge of containerization technologies is supplemented in the light of the peculiarities of using Docker for creating microservices. The features of use and the main advantages of Docker-technologies in the process of building micro-services are determined.

Key words: containerization, development of microservice, virtualization, Docker-technology

Розробка серверних веб-додатків значно змінилася після дебюту Docker'а. Поява Docker спростила створення масштабованих та керованих додатків, побудованих за допомогою мікросервісів. Для кращого розуміння, що таке мікросервіс і як Docker допомагає їх реалізовувати, розглянемо приклад. Уявімо, що у команді веб-розробників працює три програмісти, які для створення одного й того ж додатку використовують різні операційні системи: macOS, Windows та Debian. Перш за все, кожне з перелічених середовищ вимагає окремих унікальних налаштувань. Крім того, розробники повинні встановити та налаштувати різні бібліотеки для своїх мов програмування. Неминучим є той факт, що бібліотеки та мови програмування конфліктуватимуть між різними середовищами. Додаймо ще сервери для тестування та виконання, після чого стає зрозумілим наскільки складно забезпечити однакові умови для всіх середовищ.

Зважаючи на окреслену проблему в роботі поставлено мету визначити особливості, переваги та недоліки використання Docker-технологій в процесі побудови мікросервісів.

Оскільки мікросервіси є автономними, незалежними прикладними блоками, кожен з яких виконує лише одну конкретну бізнес-функцію, їх можна розглядати як невеликі самостійні програми. Що станеться, коли створити десяток мікросервісів для одного додатку? І що, коли необхідно побудувати декілька мікросервісів з різними стеками технологій? Дуже швидко команда програмістів зіткнеться з багатьма перешкодами, оскільки розробники повинні керувати ще більшою кількістю середовищ, ніж у традиційному монолітному додатку.

Однак, існує рішення – використання мікросервісів та контейнерів для інкапсуляції кожного такого сервісу і Docker допомагає керувати цими контейнерами. Docker – це інструмент контейнерування, побудований на основі контейнерів Linux, для забезпечення простого керування контейнерними додатками. Далі розглянемо переваги Docker для розробки мікросервісів на основі аналізу процесів його використання.

Контейнерування, як альтернатива віртуалізації, завжди могло удосконалити спосіб створення додатків, а Docker, як інструмент контейнерування, часто порівнюється з віртуальними машинами.

Як відомо, віртуальні машини (VM) створені для оптимізації використання обчислювальних ресурсів. За умови запуску декількох віртуальних машин на одному сервері та розгортання кожного екземпляру програми на окремій віртуальній машині, забезпечуватиметься стабільне середовище для кожного екземпляра. Однак, на жаль, масштабуючи програму, швидко виникне проблема пов'язана з продуктивністю, оскільки VM споживають багато ресурсів.

Оскільки мікросервіси подібні до невеликих додатків потрібно розгортати мікроконтролери для власних віртуальних екземплярів (щоб забезпечити дискретне середовище). І слід погодитись з тим фактом, що присвоєння всієї віртуальної машини для розгортання лише невеликої частини додатку – не найефективніший варіант. Однак, за допомогою Docker можна зменшити втрати продуктивності та розгортати тисячі

мікросервісів на одному сервері, оскільки контейнер Docker вимагає набагато менше обчислювальних ресурсів, ніж віртуальні машини.

До цього моменту наш огляд зосереджувався на керуванні середовищами для одного додатка. Проте далі слід розглянути випадок розроблення двох різних проектів, або тестування двох різних версій того самого додатку. Конфлікти між версіями додатків або бібліотеками у цьому випадку неминучі, і підтримка двох різних середовищ на одній VM є складною задачею. Тут доречно задати питання: «Чим Docker кращий за віртуальні машини?». На відміну від роботи віртуальних машин, Docker не вимагає постійного створення нових середовищ, намагаючись уникнути конфліктів. Docker гарантує, що мікросервіси додатків працюватимуть у власних середовищах, які повністю відокремлені від операційної системи.

Завдяки Docker, перед командою розробників не виникає необхідності примусово працювати в ідентичних середовищах. Натомість, один розробник може створити стабільне середовище з усіма необхідними бібліотеками та мовами, після чого зберегти це налаштування в Docker Hub. Іншим розробникам залишається лише завантажити налаштування. Завдяки цій особливості Docker може заощадити багато часу.

Зважаючи на описані особливості використання Docker можна узагальнити основні переваги використання цієї технології:

- зменшення часу запуску (контейнер Docker запускається за лічені секунди, оскільки контейнер – це лише процес операційної системи. Запуск віртуальної машини з повною ОС може тривати декілька хвилин);
- швидке розгортання (не має необхідності створювати нове середовище. Членам команди веб-розробки потрібно лише завантажити образ Docker, щоб запустити його на іншому сервері);
- зручне керування та масштабування контейнерів (знищення та запуск контейнерів швидше ніж знищення і запуск віртуальної машини);
- використання обчислювальних ресурсів (можливість запуску більшої кількості контейнерів, ніж віртуальних машин на одному сервері);
- підтримка різних операційних систем (Docker працює під Windows, Mac, Debian та інші ОС).

Отже, використання мікросервісів та контейнерів вважається ефективним сучасним способом створення масштабованих та керованих веб-програм. У випадку не контейнеризації мікросервісу виникатимуть труднощі при їх розгортанні та керуванні. Саме тому, для уникнення будь-яких проблем під-час їх розгортання рекомендовано використання Docker. Окрім того, контейнерна система оркестрування надає можливість ефективно керувати комплексними докеризованими програмами.

Висновок: За результатами проведеного аналізу процесів використання Docker означено низку переваг, які полягають в оптимізації використання обчислювальних ресурсів, працездатності у відокремлених від ОС середовищах та можливості оркестрування комплексними програмами, що унеможливлює виникнення конфліктів між різними середовищами розробки під час побудови мікросервісів.

Література

1. Musaev A. A. The information infrastructure design of an educational organization using virtualization technologies / A. A. Musaev, S. M. Gazul, I. V. Anantchenko // Известия Санкт-Петербургского государственного технологического института (технического университета): Сб.науч.тр. Санкт-Петерберг : СПГТИ, 2014. – № 27(53). – С. 71-76.

2. Белоножко П. П. Свободные облачные аппаратно-программные платформы. Аналитический обзор / П. П. Белоножко, В. В. Белоус, Н. А. Куцевич, Д. А. Храмов // Науковедение: Интернет-журнал, 2016. – Том 8 (№6)

3. Docker – Build, Ship, and Run Any App, Anywhere. [Электронный ресурс]. – Доступ http://aws.amazon.com/ru/

НЕОБХІДНІСТЬ СТВОРЕННЯ КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

Валерія Войтович, Ростислав Гриник
Львівський державний університет безпеки життєдіяльності, м. Львів

In this work, the main task is to explain the need for a comprehensive information security system, to provide clear arguments and conclude.

Comprehensive information security system, security system, information resources.

Реалії сьогодення є такі, що інформацією потрібно не тільки володіти, але і вміти правильно та ефективно захищати. Інформація – це один з конструктивних ресурсів будь-якого підприємства, установи, організації тощо. Її слушне отримання, доцільне використання, належне зберігання та безпечна передача, відіграють кардинальну роль в роботі організації і т.д.

Напрацювання у сфері захисту інформації у нашій державі відбуваються довгий час і в посиленому темпі. За цей час накопичено значний досвід. На сьогоднішній день переважна кількість населення не вважає, що досить тільки провести на підприємстві ряд організаційних заходів, додати до складу автоматизованих систем певні технічні і програмні засоби - і цього буде достатньо для забезпечення безпеки інформаційних ресурсів.

Провідним напрямом пошуку нових шляхів захисту інформації є не тільки в створенні підходящих механізмів, а являє собою втілення регулярного процесу, втілюваного на всіх стадія життєвого циклу систем обробки інформації при комплексному використанні всіх наявних засобів захисту. За рахунок цього все фінансове забезпечення, засоби та методи, які використовуються для захисту інформації, найбільш раціональним чином об'єднуються в єдиний цілісний механізм - причому не тільки від зловмисників, але і від некомпетентних або недостатньо підготовлених користувачів і персоналу, а також позаштатних ситуацій технічного характеру.

Якраз на вирішення питань з ефективного захисту інформації, як від внутрішніх, так і від зовнішніх можливих загроз, націлено створення комплексної системи захисту інформації (КСЗІ) в автоматизованих системах: установ, підприємств, організацій тощо.

Що ж таке комплексна система захисту інформації ? Це відповідна система мір із захисту, зберіганню, шифруванню, моніторингу доступу до ресурсів та обміну ними. Вона забезпечує: захист інформації від будь-яких вірусних та хакерських загроз; безпечний доступ до зберігання ресурсів; цілісність даних при фізичній втраті або несправності матеріального носія; у разі пошкоджень відновлює інформаційну систему. Збереження конфіденційної інформації відбувається на віддаленому, спеціальному сервері. Доступ до якого контролюється і визначається безпосередньо, тільки керівництвом установи, підприємства, організації тощо, що потребує використання КСЗІ.

Але також є ряд проблем реалізації КСЗІ, а саме забезпечення надійного захисту, що знаходиться в системі інформації: виключення випадкового і навмисного отримання інформації сторонніми особами, розмежування доступу до пристроїв і ресурсів системи всіх користувачів, адміністрації і обслуговуючого персоналу. І другою не більш важливою проблемою є те, щоб система захисту не повинна створювати помітних незручностей користувачам в ході їх роботи з ресурсами системи.

Головна мета створення системи КСЗІ - її надійність. Надійність захисту інформації домірна системності. При не скоординуванні між собою окремих складових, ризик «проколів» в технології захисту збільшується.

По-перше, необхідність комплексних рішень полягає в об'єднанні в одне ціле локальних систем захисту інформації (СЗІ), при цьому вони повинні функціонувати в єдиній «зв'язці». Як локальних СЗІ можуть бути розглянуті, наприклад, види захисту інформації (правова, організаційна, інженерно-технічна).

По-друге, необхідність комплексних рішень обрунтована призначенням самої системи. Система повинна об'єднати логічно і технологічно всі складові захисту. Але з її сфери випадають питання повноти цих складових, вона не враховує всіх факторів, які надають або можуть впливати на якість захисту. Наприклад, система включає в себе об'єкти захисту, а всі вони включені чи ні - це вже поза межами системи.

Тому якість, надійність захисту залежать не тільки від видів складових системи, алеі від їх повноти, яка забезпечується при врахуванні всіх чинників і обставин, що впливають на захист. Саме повнота всіх складових системи захисту, що базується на аналізі таких факторів і обставин, є другим призначенням комплексності.

При цьом повинні враховуватіся всі чинники вразлівості інформації, потенційно можливі загрози її безпеці, охоплюватися всі необхідні об'єкти захисту, використовуватись всі можливі види, методи й засоби захисту.

По-третє, тільки при комплексному підході система може забезпечувати безпеку всієї сукупності інформації, що підлягає захисту, і при будь-яких обставинах. Це означає, що повинні захищатися всі носії інформації, у всіх компонентах її збору, зберігання, передачі і використання, в усі час і при всіх режимах функціонування систем обробки інформації.

У той же час комплексність не виключає, а, навпаки, передбачає диференційований підхід до захисту інформації, в залежності від складу її носіїв, видів таємниці, до яких віднесена інформація, ступеня її конфіденційності, засобів зберігання і обробки, форм і умов проявлення вразливості, каналів та методів несанкціонованого доступу до важливої інформації.

Таким чином, значиміть комплексного рішення, щодо захисту інформації складається:

— в інтеграції локальних систем захисту;

— в забезпеченні повноти всіх складових системи захисту;

— в забезпеченні всеосяжність захисту інформації.

На сьогодні існує забезпечення захисту інформації є безперервний процес, який заключається безпочередньо в контролі захисту, виявленні вразливих місць системи захисту, аргументація та реалізація ефективної систем захисту. Виходячи з цього, можна сформулювати наступне визначення: «Компексна система захисту інформації - система, повно і всебічно охоплює всі предмети, процеси і фактори, які забезпечують безпеку всієї інформації, що захищається».

Література

1. Дубов, Дмитро Володимирович. "Стратегічні аспекти кібербезпеки України." Стратегічні пріоритети 4 (2013): 29.

2. В.В. Домарев. Безпека інформаційних технологій. Методологія створення систем захисту. - К .: ТОВ "ДС", 2001. 688 с.

3. Гриник, Р. О. Дослідження проблем захисту сучасного кіберпростору України / Р. О. Гриник, М. В. Маржан // Актуальні задачі та досягнення у галузі кібербезпеки : матеріали Всеукр. наук.-практ. конф., м. Кропивницький, 23–25 листоп. 2016 р. – Кропивницький : КНТУ, 2016. – С. 30–31.

РЕАЛІЗАЦІЯ ЛІНІЙНОГО ТА ДИФЕРЕНЦІАЛЬНОГО КРИПТОАНАЛІЗУ БЛОКОВОГО ШИФРУ

Олег Гевак, Андрій Лагун
Львівський державний університет безпеки життєдіяльності, м. Львів

Розглянуто методи криптоаналізу блокових симетричних шифрів, зокрема повного перебору ключів, статистичний, зустрічі посередині, бумеранга, лінійний та диференціальний криптоаналіз, slide-атака. Проведено дослідження стійкості блокового шифру на основі мережі Фейстеля з використанням розроблених прикладних програм для методів лінійного та диференціального криптоаналізу.

Ключові слова: криптографія, блоковий шифр, ключ, атака, відкритий текст, шифротекст, лінійний та диференціальний криптоаналіз.

Were considered such cryptanalysis methods of modern block ciphers as full searching of keys, statistic method, meeting in the middle, boomerang, linear and differential cryptanalysis, slide-attack. Also was researched the stability of block cipher based on the Feistel network with usage the designed software for the linear and differential cryptanalysis.

Keywords: cryptography, block cipher, key, attack, plaintext, ciphertext, linear and differential cryptanalysis.

Криптографія дає можливість перетворити інформацію таким чином, що її прочитання (відновлення) можливо тільки при знанні ключа. Шифрування – це перетворювальний процес в якому вихідний текст, що називається відкритим текстом, замінюється шифрованим текстом. Розшифрування - зворотний процес до шифрування. На основі ключа шифрований текст перетвориться у вхідний.

Метою атаки алгоритму шифрування є знаходження відкритого тексту, маючи криптотекст, або не маючи ключа шифрування, пошук власне ключа шифрування. Залежно від типу вхідних даних зловмисника криптографічні атаки поділяють на дві категорії:

- пасивне прослуховування каналу, по якому передаються зашифровані повідомлення – атака з відомим криптотекстом – є найбільш складною, але і водночас найбільш доступною та реалістичною;
- атака з використанням пристрою шифрування, які бувають поділяються на атаки з відомим відкритим текстом; атаки з вибраним відкритим текстом; адаптивні атаки з вибором відкритого тексту; атаки з вибором криптотексту та адаптивні атаки з вибором криптотексту.

Для розкриття криптографічного алгоритму використовуються такі ресурси як кількість інформації та час для здійснення атаки, а також пам’ять, що необхідна для збереження інформації при атаці.

Поява нових криптоалгоритмів призводить до розробки нових методів їх зламування. Розглянемо коротко існуючі на даний момент методи аналізу блокових шифрів.

Метод повного перебору передбачає перебір всіх можливих варіантів ключа шифрування. Для пошуку ключа розміром в n біт існує 2^n варіантів ключа.

Задачею статистичного методу є розробка алгоритмів, що визначають невідомий ключ чи частину ключа. Використовується процедура статистичної класифікації для пошуку невідомого параметра за доступними випадковими спостереженнями.

Метод зустрічі посередині базується на парадоксі днів народження.

Лінійний криптоаналіз є комбінацією пошуку лінійних статистичних аналогів для рівнянь шифрування, статистичного аналізу відкритих та криптотекстів, а також методів узгодження та перебору.

Диференціальний криптоаналіз працює з парами криптотексту, що мають деяку відмінність.

Метод бумеранга є посиленим варіантом диференціального криптоаналізу і використовує чотири (а не два, як у диференціальному аналізі) відкритих тексти та відповідних їм криптотексти.

Особливістю слайд-атаки є незалежність від кількості раундів алгоритму до якого вона застосовується, проте раунди алгоритму повинні бути ідентичними.

Для застосування атаки з використанням лінійного криптоаналізу необхідно здійснити кілька підготовчих етапів. Для початку, необхідно знайти ймовірності всіх лінійних апроксимацій. Для кожної з пар значення на вході та виході sBox, перебираючи всі можливі значення відкритого тексту на вході будується таблиця ймовірностей переходу вхідного значення маски у вихідне значення.

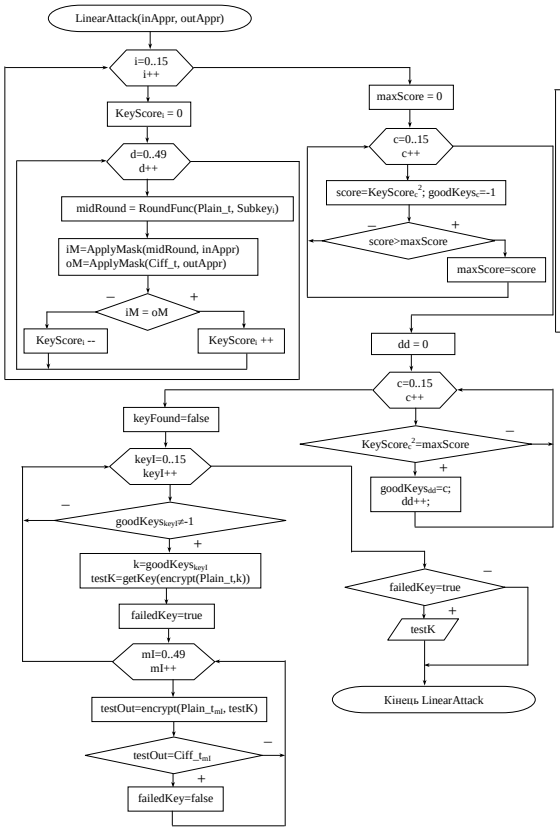


Рис. 1. Алгоритм лінійного криптоаналізу

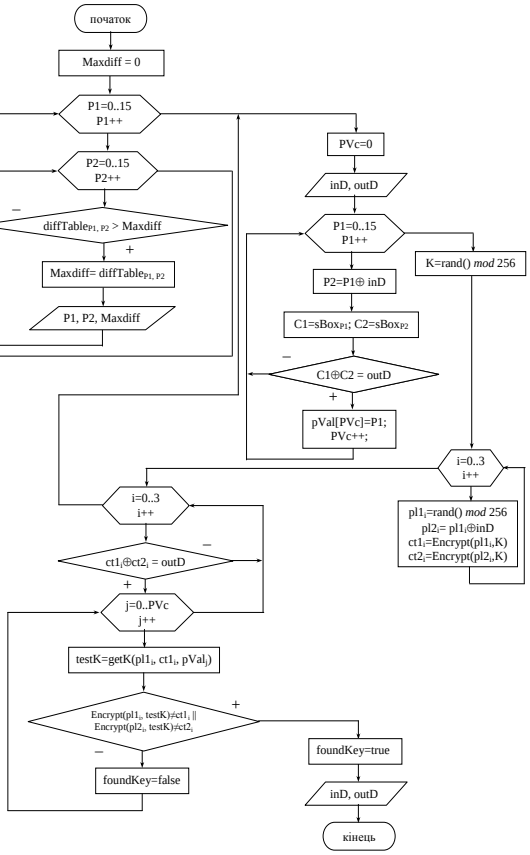


Рис.2. Алгоритм диференціального криптоаналізу

На цьому підготовчий етап завершений. Далі відбувається безпосередньо атака на криптоалгоритм. Блок-схему алгоритму, що реалізує лінійний криптоаналіз наведено на рис. 1. Алгоритм складається з наступних кроків:

- обирається одна з найбільш ймовірних апроксимацій;

- здійснюється пошук можливих варіантів ключа. Відбувається підрахунок випадків коли ключ задовольняє значення апроксимації;

- виділяються ключі з максимальним значенням випадків коли ключ задовольняв обрану апроксимацію;

- виконуючи перебір виділених ключів відбувається пошук ключа для другого раунду;

- з раундових ключів формується ключ шифрування, який перевіряється на усьому існуючому матеріалі. В разі успіху, робимо припущення що це і є істинний ключ шифрування.

При атаці з використанням диференціального криптоаналізу першим кроком є побудова та аналіз таблиці диференціалів криптоалгоритму. Будь-який з диференціалів цієї таблиці може бути використаний для здійснення найбільш успішної атаки.

Атака відбувається так (рис. 2).

- для атаки обираємо пару, що є різницею на вході та виході функції sBox;

- генеруємо певну кількість матеріалу, що складається з пар (P1, P2) – (C1, C2);

- пошук раундового ключа –вибираються, так звані, «хороші» пари, які задовольняють обрану пару відмінностей і для «хорошої» пари відбувається перевірка того чи задовольняє знайдений ключ існуючий матеріал.

- якщо ключ задовольняє всі пари з існуючого матеріалу, то робимо припущення, що знайдений ключ і є ключем шифрування, якщо ні – продовжуємо пошук «хорошої» пари.

Література

1. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы и исходные тексты на языке Си / Б. Шнайер. – Триумф, 2002. – 816 с.

2. Брилюк Д. В. Подход к созданию трудноанализируемых шифров / Д. В. Брилюк. – 2000.

3. Ковтун В. Ю. Введение в криптоанализ. Криптоанализ симетричных криптосистем: блочные шифры / В. Ю. Ковтун. – Санкт-Петербург: «БХВ-Петербург». – 2009.

СИСТЕМИ КОНТРОЛЮ ДОСТУПУ НА ОБ'ЄКТ

Надія Джур, Орест Полотай
Львівський державний університет безпеки життєдіяльності, м.Львів

Розглянемо основні системи контролю доступу та як вони працюють, елементи системи та де їх можна застосовувати, тобто сфери їх використання. Описано пристрої які здійснюють контроль доступу на об'єкт, що охороняється та який елемент системи виконує основну функцію. Показано систему контролю доступу на об'єкт Winkhaus та що вона в себе включає.

Ключові слова:система контролю доступу, електронні системи.

Consider the main access control systems and how they work, the elements of the system and where they can be used, that is, the scope of their use. Described devices that control the access to the protected object and which element of the system performs the main function. The system of access control for the Winkhaus object and its inclusion includes.

Key words: access control system, electronic systems.

У нашому сучасному світі зловмисників так багато, що, мабуть, кожна розсудлива людина стикається з тим, щоб захистити себе, своїх рідних і своє майно. І найпростішим захистом в таких випадках є створення системи контролю доступу до своїх будинків та квартир.

Найчастіше люди потребують контролю доступу до нерухомості або до їх матеріальних цінностей.

Системи контролю доступом являють собою комплекс програмно-апаратних технічних пристроїв безпеки, які здійснюють управління доступом, реєстрацію входів і виходів всіх суб'єктів, обмеження входу та виходу.

Системи контролю доступу організовуються з метою розмежування доступу самих різних суб'єктів і об'єктів на територію через точки входу та виходу: двері, ворота, пропускні пости.

Системи контролю й керування доступом можуть бути виконані у вигляді локального рішення (наприклад, на одні вхідні двері) або мережевих систем з можливістю охоплення великої кількості приміщень і різних входів та виходів. Кожна конкретна система контролю доступу підбирається виходячи з вимог користувачів і поставлених завдань перед системою.

Локальні системи контролю та управління доступом найчастіше використовуються для особистої безпеки, коли потрібно контролювати один центральний вхід до приміщення або невелику кількість входів.

Мережеві системи контролю і управління доступом найчастіше використовують для безпеки офісів та цілих будинків, де розташована велика кількість приміщень і дверей.

Організовуючи систему контролю доступу на об'єкті необхідно розглянути які елементи системи необхідно встановити. Головні завдання реалізовуються за допомогою пристроїв, що представлені в таблиці 1.

Таблиця 1

Головні елементи системи контролю доступу на об'єкт

Перегороджуючі пристрої для установки на двері	Перегороджуючі пристрої для установки на проходах та проїздах	Зчитувачі
1.електролямки	1.турнікети	1.контролери
2.електромагнітні замки	2.шлюзові кабіни	2.ідентифікатор
3.електромеханчні замки	3.ворота і хвіртки	3.картка
	4.шлагбауми	4.брелок
		5.біометричні зчитувачі

Саме ці пристрої і здійснюють контроль доступу на об'єкт, що охороняється. Більше того вони здатні максимально виключити вплив людського фактора на цей процес і організувати стандартне управління доступом до об'єкта.

Серед низки систем, що призначені для організації контролю доступу, варто відзначити нову систему, що має назву Winkhaus та одну із багатьох її систем для захисту нашого майна. Winkhaus має дві електронні системи: система замикання blueSmart та система доступу blueChip.

Система blueSmart від Winkhaus – це представник останнього покоління електронних систем доступу. Вона вдало поєднує сучасний дизайн та вміння керувати доступом у будівлях зі складною організаційною структурою.

Ця автономна бездротова система працює за допомогою віртуальної мережі. Вона складається із вбудованих електронних компонентів, які, взаємодіючи один з одним, здійснюють обробку інформації та передають інформацію до інших компонентів системи. В результаті, дозвіл або відмова в доступі та інші команди, що пов'язані з системою, виконуються стабільно, надзвичайно легко і дуже швидко.

Технологія дозволяє здійснювати контроль доступу та керувати автоматизованими системами в адміністративних будівлях, готелях, лікарнях, спортивних комплексах, будинках для літніх людей, школах та навіть в аеропортах.

Рис.1 Циліндр blueSmart

Рис.2 Зчитувач blueSmart

Рис.3 Ключ blueSmart

Рис.4 Зчитувач blueSmart

Рис.5 Подвійний регулятор циліндра blueSmart

Отже, можна зробити висновок, що системи контролю доступу зараз дуже багато та щодня вдосконалюється і все для того , щоб захистити наше майно та покращити життя людині в світі технологій.

Література

1.[Електронний ресурс]. – Доступний з https://www.winkhaus.com

2.Барсуков, В.С. Сучасні технології безпеки / В.С. Барсуков, В.В. Водолазський. - М.: Нолидж, 2009. - 496 с.

ОСНОВИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Роман Дибач, Олександр Белей
Львівський навчально-науковий інститут ДВНЗ «Університет банківської справи», м.Львів

Інформаційна безпека є однією із суттєвих складових частин національної безпеки країни, її забезпечення завдяки послідовній реалізації грамотно сформульованої національної інформаційної стратегії в значній мірі сприяла б забезпеченню досягнення успіху при вирішенні задач у політичній, військово-політичній, військовій, соціальній, економічній та інших сферах державної діяльності.

Ключові слова: інформаційна безпека, інформаційна культура, інформація, забезпечення, охорона, загроза, суспільство, держава, особа.

Information security is one of the essential components of the national security of the country, ensuring its success by solving problems in the political, military-political, military, social, economic and other spheres of state activity through the consistent implementation of a well-formulated national information strategy that greatly contribute to the achievement of success.

Keywords: informational security, information culture, information, provision, protection, threat, society, state, person.

Масове впровадження нових технічних засобів, на основі яких здійснюється інформатизація у всьому світі, робить прозорими державні кордони і формує нові геополітичні парадигми у розумінні глобальних соціально-технічних систем. Міжнародна інформаційна сфера стає не тільки однією з важливих сфер співробітництва, а й середовищем конкуренції між окремими особами, державами, міждержавними політичними та економічними угрупуваннями. Електронно-комунікаційна інфраструктура, як і інші інформаційні ресурси, стає об’єктом міждержавної боротьби за світове лідерство або об’єктом недобросовісної конкуренції у підприємницькій діяльності чи інших суспільних інформаційних відносинах.

Все це зумовлює необхідність формування такого аспекту інформаційної культури, як культура інформаційної безпеки, культура організації інформаційної безпеки. Зазначений аспект розвитку інформаційної культури набуває відображення у такій прикладній науковій дисципліні, як теорія організації (тектологія) інформаційної безпеки.

Цікавою є думка відомого українського дослідника проблем інформаційної безпеки Р. Л. Калюжного, який вважає, що інформаційна безпека є видом суспільних інформаційних правовідносин щодо створення, підтримки, охорони та захисту бажаних для людини, суспільства і держави безпечних умов життєдіяльності; суспільних правовідносин, пов'язаних із створенням, розповсюдженням, зберіганням та використанням інформації.

У суспільних відносинах із застосуванням комп’ютерних інформаційних систем питання інформаційної безпеки широко висвітлюється у спеціальній літературі. Сьогодні критична маса науково-практичних знань щодо розвитку суспільних інформаційних відносин у такому аспекті дає змогу сформувати на теоретичному рівні елементи загальної теорії організації інформаційної безпеки в умовах формування інформаційного суспільства.

Мета інформаційної безпеки – режимно-секретне інформаційне забезпечення діяльності держави, галузі, підприємства, особистості.

Основні характеристики інформаційної безпеки:

- доступність – можливість за прийнятний час отримати шукану інформаційну послугу будь-яким суб’єктом виконавчої влади;
- цілісність – актуальність і несуперечливість інформації, її захищеність від руйнування і несанкціонованої зміни;
- конфіденційність – захист від несанкціонованого ознайомлення.

Проблема інформаційної безпеки розглядається у трьох основних аспектах:

- захист інформації;
- контроль за національним інформаційним простором;
- достатнє інформаційне забезпечення державних і недержавних органів, громадських, приватних організацій.

Контроль за національним інформаційним простором включає заходи щодо мінімізації збитків від здійснення підривних психологічних операцій як іноземними державами, так і внутрішніми організаціями.

Елементи інформаційної безпеки:

- доступність (можливість за визначений час отримати необхідну інформаційну послугу);

- цілісність (актуальність і несуперечливість інформації, її захищеність від руйнування і несанкціонованої зміни);
- конфіденційність (захист від несанкціонованого доступу).

Одним із видів національної безпеки є інформаційна безпека України (серед інших видів такої безпеки – політична, економічна, військова, екологічна, міжнародна, соціальна, регіональна).

Інформаційна безпека України – передбачений Конституцією захист політичних, державних, громадських інтересів країни, загальнолюдських і національних цінностей.

Основні законодавчі акти з питань регулювання інформаційної безпеки України: «Про інформацію», «Про державну статистику», «Про науково-технічну інформацію», «Про національний архівний фонд і архівні установи», «Про державну таємницю», «Про захист інформації в автоматизованих системах».

Одним із проектів, що має безпоседнє відношення до забезпечення інформаційної безпеки в Україні, є «Цифрова адженда України – 2020», що виступає в ролі короткострокового та початкового інструмента розвитку та стимулювання внутрішніх ринків споживання, впровадження та виробництва «цифрових» технологій на найближчі три роки. Вона містить бачення трансформації економіки від «аналогової» до «цифрової», заходи щодо імплементації відповідних стимулів для «цифровізації» суспільно-економічного життя, освіти, медицини і т. д., виклики та інструменти розвитку «цифрової» інфраструктури, набуття громадянами «цифрових» компетенцій, а також визначає критичні сфери та проекти «цифровізації» країни.

Активне забезпечення інформаційної безпеки спрямовано на завчасне виявлення й попередження загроз. Це може досягатися шляхом проведення заходів щодо з'ясування планів, цілей, сил і засобів конфронтуючої соціальної системи, а також застосування протидії деструктивним акціям на етапі їхньої підготовки.

Для розв'язання конфліктів різного масштабу останнім часом все частіше використовується інформаційна сфера, яка породжує таке явище, як інформаційне протиборство, що характеризується, з одного боку, впливом на системи добування, оброблення, поширення та зберігання інформації противника, а з іншого – застосуванням заходів захисту своїх подібних систем від деструктивного й керуючого впливу. Інформаційне протиборство здійснюється між різноманітними видами соціальних суб'єктів (особистостей, суспільств, держав), проте цілий ряд таких конфліктних взаємодій має певні відносно стійкі ознаки, які в сукупності утворюють окремі форми протиборства – інформаційну війну, інформаційний тероризм, інформаційну злочинність.

Інформаційна безпека не може розглядатися лише як окремий стан. Безперечно, що це є як властивістю та атрибутом інформаційного суспільства, так і діяльністю та результатом діяльності людини, спрямованої на забезпечення певного рівня безпеки в інформаційній сфері.

Інформаційна безпека має враховувати майбутнє, а отже, вона не є станом, а становить собою процес. Таким чином, інформаційну безпеку слід розглядати крізь органічну єдність ознак, таких як стан, властивість, а також управління загрозами і небезпеками, за якого забезпечується обрання оптимального шляху їх усунення і мінімізації впливу негативних наслідків.

Отже, інформаційна безпека являє собою одне з найважливіших понять у науці і різних сферах людської діяльності. Сутність і комплексність цього поняття виявляється характером сучасного інформаційного суспільства.

Література

1.Важливість інформаційної безпеки [Електронний ресурс]. – Режим доступу: https://itua.com.ua/uk/security – Назва заголовку з екрану.

2.Інформаційна безпека [Електронний ресурс]. – Режим доступу: http://www.ukr.vipreshebnik.ru/entsiklopediya/55-i/1943-informatsijna-bezpeka.html – Назва заголовку з екрану.

3.Інформаційна безпека в Україні [Електронний ресурс]. – Режим доступу: http://jure.in.ua/tema-9-informatsijna-bezpeka/ – Назва заголовку з екрану.

4.Кібербезпека та інформаційна безпека [Електронний ресурс]. – Режим доступу: http://ko.com.ua/kiberbezpeka_chi_informacijna_bezpeka_120068 – Назва заголовку з екрану.

5.Поняття і зміст інформаційної безпеки [Електронний ресурс]. – Режим доступу: http://pidruchniki.com/16850303/ politologiya/ponyattya_zmist_informatsiynoyi_bezpeki – Назва заголовку з екрану.

6.Цифрова адженда України. Проект [Електронний ресурс]. – Режим доступу: https://www.slideshare.net/tsnua/ss-72226573 – Назва заголовку з екрану.

БЕЗПЕКА ДАВАЧІВ У ФІЗИЧНОМУ ПРОСТОРІ КІБЕРФІЗИЧНИХ СИСТЕМ

Валерій Дудикевич, Галина Микитин, Андрій Ребець
Національний університет «Львівська політехніка», м. Львів

Проаналізовано структуру комплексної системи безпеки (КСБ) фізичного простору (ФП) кіберфізичної системи (КФС): давач – загроза – профіль безпеки – технологія захисту.

Ключові слова: кіберфізична система, фізичний простір, давачі, комплексна система безпеки, загрози, профілі безпеки, технології захисту.

The complex security system (CSS) structure of a physical space (PS) of a cyber-physical system (CPS) (sensor – threat – security profile – defense technology) was analyzed.

Keywords: cyber-physical system, physical space, sensors, complex security system, threats, security profiles, defense technologies.

Стратегія кібербезпеки України визначає як один з пріоритетних напрямків захист інформаційних процесів на об'єктах критичної інфраструктури, в яких моніторинг та управління здійснюється за допомогою інформаційно-комунікаційних технологій, зокрема КФС на рівні кібернетичного і фізичного просторів та комунікаційного середовища. Фізичний простір КФС, представлений давачами, забезпечує відбір інформації з фізичного середовища для подальшого її передавання комунікаційним середовищем до кібернетичного простору, який забезпечує контроль та управління відповідно до цих даних. Існує необхідність забезпечити роботоздатність ФП кіберфізичної системи, тому актуальними є питання безпеки та достовірності даних, отриманих від давачів.

Широке застосування у фізичному просторі КФС мають давачі на основі мікроелектромеханічних систем (МЕМС). МЕМС – це технології і пристрої, що поєднують в собі мікроелектронні і мікромеханічні компоненти. У структурі КФС МЕМС-давачі представлені на рівні ФП і призначені для виконання таких задач: реєстрація даних про стан об'єктів та середовища; реєстрація подій для роботи систем безпеки; проведення вимірювань для екологічного моніторингу; збір даних для прийняття рішень на всіх етапах роботи КФС; попередження аварійних ситуацій; вимірювання фізичних величин. За функціональним призначенням давачі поділяються на: акселерометри, призначені для вимірювання величини зміни швидкості (прискорення) в метрах на секунду в квадраті (м/с^2) або джі (g); магнітометри, які вимірюють магнітну індукції в теслах (Тл); гіроскопи, для вимірювання швидкості обертання (кутової швидкості) в градусах за секунду (°/с) або радіанах за секунду (рад/с); барометри, які вимірюють атмосферний тиск в паскалях (Па); гігрометри, призначені для вимірювання відносної вологості навколишнього середовища у %; давачі температури, які вимірюють температуру навколишнього середовища в градусах Цельсія (°С), градусах Фаренгейта (°F) та кельвінах (К); давачі освітленості, для вимірювання інтенсивності видимого світла в люксах (лк); давачі наближення, призначені для вимірювання відстані до об'єкта в сантиметрах (см). Стандарт IEEE 2700-2014 визначає основні вимоги до параметрів МЕМС-давачів. Зокрема, у табл. 1. наведені вимоги до параметрів МЕМС-акселерометрів.

Таблиця 1

Вимоги щодо параметрів МЕМС-акселерометрів

Параметр	Одиниця вимірювання	Розподіл		
		Мінімум	Типовий	Максимум
Діапазон вимірювань	g (9,81 м/с^2)	-3σ	$\pm FSB/2$	$+3\sigma$
Цифрова розрядність	біт	-	2^n біт	-
Нульове зміщення	мg	-3σ	$\overline{X}$	$+3\sigma$
Чутливість	g/*LSB*			
Затримка даних	мкс			
Шум	мg (*RMS*)	-3σ	X_{RMS}	$+3\sigma$

Розглянемо структуру КСБ фізичного простору КФС, яка дозволить реалізувати захищений і достовірний відбір даних від давачів і, відповідно, безпечне функціонування кіберфізичної системи. Для давачів характерні такі класи загроз відповідно до методики STRIDE як модифікація даних (tampering with data – T) та відмова в обслуговуванні (denial of service – D). У табл. 2 представлені технології захисту ФП кіберфізичної системи у контексті створення структури комплексної системи безпеки: давач ФП– загроза – профіль безпеки – технологія захисту.

Таблиця 2

Комплексна система безпеки ФП кіберфізичної системи: технології захисту

Клас загроз ФП: методика STRIDE	T (модифікація даних)	D (відмова в обслуговуванні)
Загрози	• модифікація показів	• перебої електроживлення; • перевищення порогових значень; • апаратні відмови
Технології захисту	• механізм здійснення контрольних вимірювань	• дублювання давача; • аварійне вимкнення давача; • самодіагностика
Профілі захисту	• Intrusion Detection System Sensor Protection Profile V1.3 (2007.07.25) (Профіль захисту для давачів системи виявлення вторгнень)	
Нормативне забезпечення	• IEEE 2700-2014 Standard for Sensor Performance Para-meter Definitions (Стандарт визначення параметрів продуктивності давачів); • IEC 62047- Series. Part 1-22. Micro-Electromechanical Devices – MEMS (Мікроелектромеханічні пристрої – МЕМС. Частина 1-22)	

Для забезпечення цілісної безпеки давачів у ФП необхідно вирішити такі задачі:

• забезпечення цілісності (Ц) – дані не можуть бути модифіковані неавторизованим користувачем або процесом під час їх зберігання, передавання і обробки; жоден компонент системи не може бути видалений, модифікований або доданий в обхід або порушуючи політику безпеки);

• забезпечення доступності (Д) – можливість використання ресурсу чи системи відповідно до правил, встановлених політикою безпеки, не очікуючи довше заданого проміжку часу.

• забезпечення гарантованості (Г) – дотримання сукупності вимог, серед яких формулювання і коректна реалізація функціональності, адекватний захист та достатня стійкість і надійність системи.

Вирішення задач цілісної безпеки забезпечують відповідні послуги безпеки на основі технологій захисту інформації згідно структури “задача безпеки – послуга безпеки – технологія захисту інформації”, яка для фізичного простору, представленого МЕМС-давачами має вигляд: Ц – відновлення безпечного стану – завадостійке кодування; Д – управління доступом – RAC; Г – політика стримування – RAC.

Розглянуто КСБ МЕМС-давачів фізичного простору КФС на рівні структури “давачі ФП – загроза STRIDE – профіль безпеки – технологія захисту ” відповідно до нормативного забезпечення.

Література

1. Указ Президента України “Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року “Про Стратегію кібербезпеки України”” від 15.03.2016 № № 96/2016. – [Електронний ресурс]. – Режим доступу: http://zakon5.rada.gov.ua/laws/show/96/2016

ОСОБЛИВОСТІ ЗАХИСТУ PROXY-СЕРВЕРА, ЯК ОДИН ІЗ СПОСОБІВ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ РОЗПОДІЛЕНИХ ІНФОРМАЦІЙНИХ СИСТЕМ

Наталія Думич, Орест Полотай
Львівський державний університет безпеки життєдіяльності, м.Львів

Описано основне призначення та суть розподіленої системи. Показано механізми захисту розподіленої системи. Описано особливості та призначення proxy-сервера. Описано основні функції програмного забезпечення для організації захищеності proxy-з'єднань.

Ключові слова: proxy-сервер, розподілена система.

The main purpose and essence of the distributed system are described. The mechanisms of protection of the distributed system are shown. Describes the features and purpose of the proxy server. The main functions of the software for the organization of security of proxy connections are described.

Keywords: proxy server, distributed system.

Під розподіленою системою розуміють набір незалежних комп'ютерів, що представлені користувачам, як єдина об'єднана система. Мається на увазі, що всі машини в системі автономні, а користувачі вважать, що мають доступ до єдиної системи. Прикладом розподіленої системи може служити локальна обчислювальна мережа (ЛОМ).

На сьогоднішній день гостро постає питання безпеки інформації при обміні даними під час взаємозв'язку між ЛОМ та небезпечним середовищем – мережею Інтернет. Тим не менш, розповсюдження Інтернету та активне використання online-серверів приймає масовий характер. Відправлення документів, спілкування чи здійснення фінансових операцій засобами Інтернету стає щоденною потребою. І кожен раз потрібно впевнитись, що, наприклад, дані про засоби оплати та ваш рахунок гарантовано не стануть відомими для всіх, окрім вас.

Одна з особливостей побудови та функціонування ЛОМ полягає в тому, що для того, щоб кожен з елементів мережі мав доступ до мережі Інтернет, локальна мережа повинна бути сполучена з мережею Інтернет елементом, який буде мати дві адреси, зовнішню та внутрішню. За допомогою зовнішньої адреси, локальна мережа поєднується з мережею Інтернет, а за допомогою внутрішньої адреси, користувачі з мережі Інтернет можуть мати доступ до локальної мережі. Даний елемент називається Proxy-сервер.

Proxy-сервер (від англ. Proxy - «представник, уповноважений») - служба (комплекс програм) в комп'ютерних мережах, що дозволяє клієнтам виконувати непрямі запити до інших мережних служб. Спочатку клієнт підключається до проксі-сервера і запитує який-небудь ресурс (наприклад, e-mail), розташований на іншому сервері. Потім проксі-сервер або підключається до зазначеного сервером та отримує інформацію у нього, або повертає ресурс з власного кешу (у випадках, якщо проксі має свій кеш) [1].

Системи захисту в розподілених системах можна поділити на дві незалежні частини. По-перше, це зв'язок між користувачами чи процесами на віддалених машинах. Спосіб гарантування надійності в такому випадку – захищений канал. По-друге, це авторизація, що гарантує надання доступу до ресурсів розподіленої системи тільки тим процесам, що мають на це право.

Захист інформації передбачає уникнення перехвату, переривань, модифікації та підробок. Перехват – можливість неавторизованому суб'єкту отримати доступ к службам чи даним. Переривання – ситуація, в якій служби та дані можуть стати недоступними чи непридатними для використання. Модифікації – зміна даних в системі неавторизованими суб'єктами. При підробці створюються додаткові дані неможливі в нормальній системі.

Правила захисту реалізуються в механізмах захисту і визначають вид допустимих та недопустимих дій для системи (користувачів, служб, даних, машин та інше). До механізмів захисту відносять:

1. Шифрування – трансформація даних в стан, що не може бути зрозумілим стороннім. Це засіб реалізації конфіденційності.

2. Аутентифікація - це процес перевірки та підтвердження ідентичності суб'єкта чи

об'єкта. В контексті інформаційної безпеки під процесом аутинтифікації розуміємо – єдиний метод, що використовується для управління доступом до облікового запису користувача та його особистим даним. Передбачається, що користувачем в інформаційній системі повинні бути пред'явлені особисті дійсні ідентифікаційні дані, що супроводжуються мінімально одним аутентифікуючим фактором для підтвердження дійсності.

3. Авторизація – надання аутентифікованому користувачу прав згідно з його рівнем доступу.

4. Аудит – контроль дій користувача.

Proxy, з точки зору захисту ЛОМ, являє собою маркер, який дозволяє оперувати з правами та привілеями їх власника, який надає маркер. Повинна бути можливість впевнитись, що proxy був наданий суб'єктом який він називає. Це проблема аутентифікації. Насправді суб’єкт з атрибутами прав доступу, що потребує спочатку аутентифікацію для себе, може надати маркер іншому суб’єкту просто передаючи ці атрибути доступу [2].

Для виходу за межі ЛОМ, користувач повинен мати права на виконання певного комплексу дій а також він повинен бути відомий за межами ЛОМ. Сервер, що надає таку можливість, має назву сервер авторизації. Він, отримуючи запит від авторизованого користувача, забезпечує його можливістю діяти від імені сервера для підтвердження прав на об’єкт. Обмеження визначаються даними бази серверу.

Для того, щоб користувач ЛОМ мав можливість працювати за її межами без виникнення конфліктних ситуацій з дублюванням «сірих» IP-адрес, Proxy-сервер використовує технологію трансляції адрес NAT.

Серед найбільш популярних Proxy-серверів авторизації є HTTP-proxy. Додаток створено спеціально для роботи через браузери та інші затребувані широкою користувальницькою аудиторією програми, що працюють на протоколі HTTP.

Для забезпечення захищеності Proxy-з’єднань можна використовувати додаткове програмне забезпечення, зокрема Програмний комплекс proxy захисту з’єднань «AI IIT», яка призначена для операційних систем типу Microsoft Windows.

Дане програмне забезпечення виконує наступні функції:

– автентифікацію proxy захисту на шлюзі захисту при підключенні до сервера;

– встановлення захищеного TCP-з’єднання proxy з шлюзом захисту в разі успішної автентифікації;

– встановлення відкритого TCP-з’єднання клієнтів з proxy захисту;

– прийом даних TCP-з’єднання від клієнтів та передачі їх на шлюз захисту;

– зашифрування даних TCP-з’єднання від клієнтів та передачі їх на шлюз захисту;

– розшифрування даних TCP-з’єднання від шлюзу захисту та передачі їх клієнтам;

– приймання та передачу управляючої (технологічної) інформації (моніторинг захисту тощо);

– прийом та введення в дію ключових даних.

Отже, Proxy-сервера, в залежності від виду, реалізують потреби у захисті, забезпечуючи такі функції: анонімність користувача у мережі та організація захищеного каналу зв’язку, попереджуючи фальсифікацію повідомлень. Для забезпечення максимального захисту створюють ланцюгову ієрархію серверів з використання VPN, SOCKS та Proxy технологій.

Література

1. https://uk.wikipedia.org/wikiПроксі сервер;
2. B. Cliford Neuman. Proxy-based authorization and accounting for distributed systems. Technical Report 91-02-01, Department of Computer Science and Engineering, University of Washington, March 1991.

ОБРОБЛЕННЯ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ІНФОСИСТЕМИ АРХІТЕКТУРНОГО БЮРО «ПРОЕКЦІЯ»

Орест Дупелич, Тарас Стецяк, Петро Гаранюк, Володимир Ромака
Національний університет «Львівська політехніка», м.Львів

Проведено аналіз та оброблення ризиків інформаційної безпеки комп'ютерної системи архітектурного бюро "Проекція". Описано бізнес-процес роботи архітектурного бюро "Проекція" та ідентифіковано його інформаційні активи. Ідентифіковано джерела загроз та уразливості інформаційній безпеці бюро. Обчислено значення ймовірності реалізації загроз, збитку та ризику інформаційної безпеки активам бюро. Проведено ранжування значень ризику інформаційної безпеки, встановлено значення прийнятного ризику.

Ключові слова: управління інформаційною безпекою, ідентифікація, безпека

An analysis and treatment of risks of information security of the computer system of architectural bureau "Proektsia" are conducted. The business process of work of architectural bureau "Proektsia" is described and identified it's information assets. The sources of threats and vulnerability to information security of bureau are identified. The value of probability of realization of threats, loss and risk of informative safety to the assets of bureau is calculated. A ranking of values of risk of informative safety is conducted, it is set value acceptable.

Key-words: management of information security, identification, security

Твір архітектури (ескізи, креслення, моделі, плани і т.д.) – є особливим об'єктом авторського права і підлягає правовій охороні у відповідності до Закону України "Про авторське право та суміжні права".

Запровадження інформаційних технологій при виготовленні, зберіганні та передаванні творів архітектури пов'язано з появою ризиків інформаційної безпеки. Основу ризику утворюють уразливості інформаційних систем, які джерела загроз використовують для реалізації загрози. *Оцінювання ризиків* дозволяє встановити значення ризику [1], а метою *оброблення ризиків* є, зокрема, зменшення їхніх значень до прийнятного рівня [2] (рис. 1).

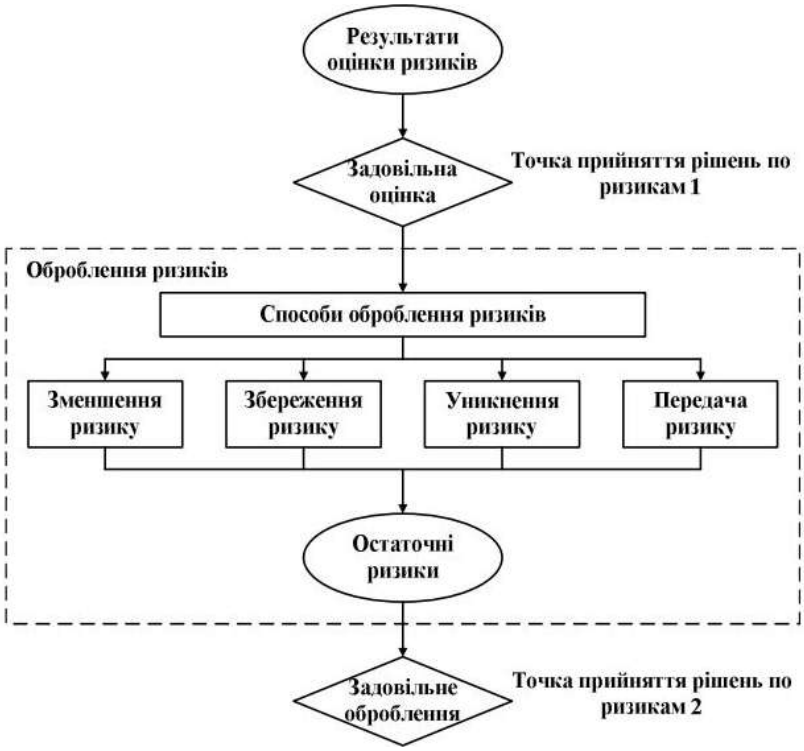


Рис. 1. Схема плану оброблення ризиків

Метою роботи є підвищення захищеності інформаційної системи архітектурного бюро "Проекція" шляхом оброблення ризиків інформаційної безпеки. На основі аналізу бізнес-процесів ідентифіковано інформаційні активи, джерела загроз та уразливості, а за допомогою розроблених методик якісного оцінювання значення ймовірності реалізації загроз та збитку

обчислено значення ризику інформаційної безпеки активам і здійснено ранжування значень ризику.

На рис. 2. показано фрагмент процедури оброблення ризиків інформаційної безпеки загроз цілісності інформаційних активів архітектурного бюро “Проекція”, а також обчислені значення збитку, ймовірності реалізації загрози та прийнятного ризику. Зазначимо, що значення прийнятного ризику для загроз цілісності, доступності та конфіденційності інформаційних активів бюро проводилося з урахуванням можливих фінансових втрат підприємства.

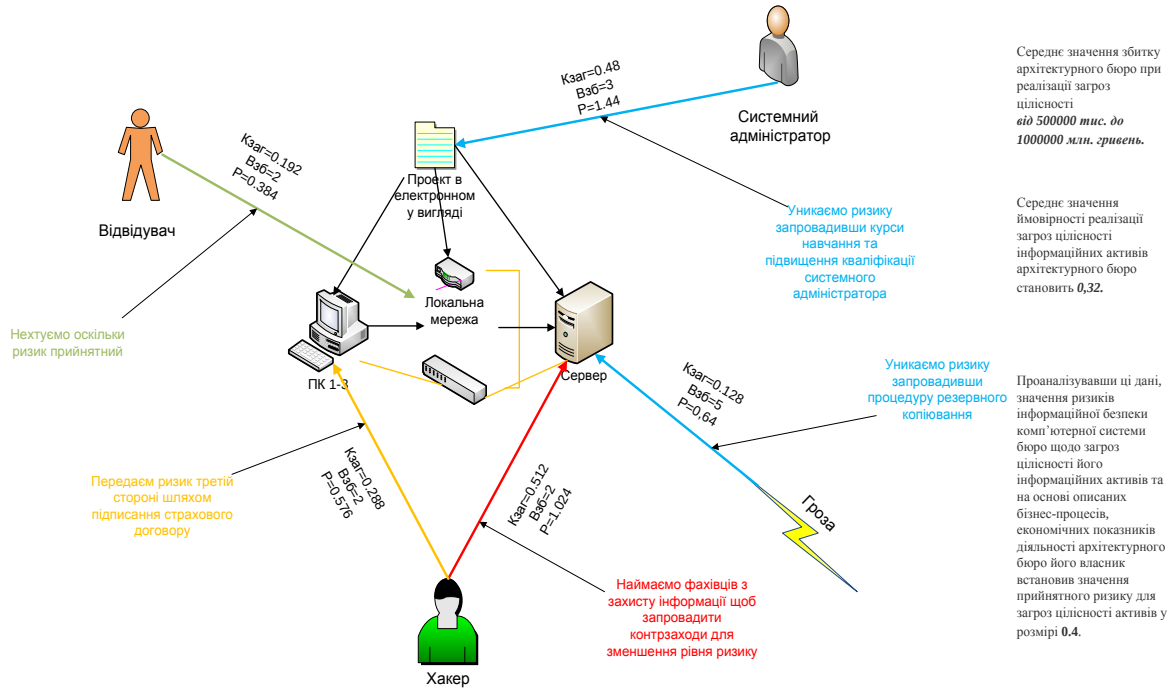


Рис. 2. Логічна схема оброблення ризиків інформаційної безпеки *загроз цілісності* інформаційних активів архітектурного бюро “Проекція”

Таким чином, у результаті аналізу ризиків інформаційної безпеки комп’ютерної системи архітектурного бюро “Проекція” ідентифіковано типові загрози інформаційним активам, зокрема, загрози хакера щодо порушення цілісності, доступності, конфіденційності проекту в електронному вигляді та програмного забезпечення сервера, комп’ютерів та маршрутизатора бюро.

Даний аналіз дозволив провести оброблення ризиків та сформулювати відповідні рекомендації щодо підвищення рівня інформаційної безпеки комп’ютерної системи архітектурного бюро “Проекція”.

Література

1. Ромака В.А., Лагун А.Е., Гарасим Ю.Р., Рак Т.Є., Самотий В.В., Рибій М.М. Аудит інформаційної безпеки: підручник. – Львів: СПОЛОМ, 2015. – 363 с.

2. Ромака В.А, Корж Р.О. , Гарасим Ю.Р. Менеджмент у сфері захисту інформації. – ЗУКЦ : Львів, 2013. – 462 с.

ДОСЛІДЖЕННЯ ПРОФІЛЮ ЗАГРОЗ ІНФОРМАЦІЙНІЙ СИСТЕМІ РАДІОСТУДІЇ

Ірина Калмикова, Тарас Стецяк, Володимир Ромака
Національний університет «Львівська політехніка», м.Львів

Побудований профіль загроз, який описує статичні характеристики загроз інформаційним активам радіостудії. Ідентифіковано загрозу, джерело загрози, спосіб реалізації загрози, вразливості та наслідки від загрози. Проаналізований бізнес-процес організації, встановлено бізнес-вимоги та вимоги безпеки інформаційних активів. Проведено обчислення імовірності реалізації загроз інформаційним активам, значення збитку та ризику за допомогою запропонованих методик, що дозолило виявити найбільш вразливі інформаційні активи.

Ключові слова: управління інформаційною безпекою, ідентифікація, безпека

The construction of the threat's profile is realized, which describes static characteristics of threats to informational assets of the radio station. The threat, source of threat, blind spots and consequences from the threat are identified. Business process of the organization and the role of informational assets in it are analyzed. Calculations of the probability of realization of the threats to informational assets, damage's value and risk are realized with the help of proposed methods, that allows to discover the most defenseless informational assets.

Key-words: management of information security, identification, security

На даний час відбувається широке застосування інформаційних технологій в усіх сферах життєдіяльності людини. З іншого боку, порушення стану інформаційної безпеки у системах телекомунікацій супроводжується зростанням ризику зазнати матеріальних, фінансових, моральних, репутаційних і т.д. збитків. Одним із способів такого порушення є кібернапад на інформаційні системи, зокрема, веб-сайт радіостудії. Враховуючи соціальну важливість неперервної та адекватної роботи веб-сайтів радіостудії, а також недостатню вивченість даної проблеми, ***метою роботи*** є виявлення найбільш вразливих інформаційних активів шляхом побудови профілю загроз інформаційній системі. Для досягнення мети було вирішено наступні ***завдання***:

– проведено аналіз бізнес-процесів радіостудії та ідентифіковано інформаційні активи, ідентифіковано загрози, джерела загроз та описано механізми реалізації нападу;

– на основі розроблених методик експертного оцінювання імовірності реалізації загроз інформаційним активам та збитку від їхньої реалізації проведено розрахунок значення ризику.

При нападі хакер шукає або створює уразливості веб-сайтів, до яких відносять SQL-ін'єкції, XSS та ін'єкції коду. Так, при SQL-ін'єкції змінюється логіка до запиту бази даних. У свою чергу, при XSS-ін'єкції, а нині розрізняють три основні моделі ін'єкції: XSS DOM, класичний XSS та збережений XSS, реалізується можливість впливу на віддаленого користувача через незахищений сайт.

Ін'єкція коду – це виконання стороннього коду на боці сервера через використання помилок серверних сценаріїв. Ін'єкція коду використовується для включення коду в комп'ютерну програму, щоб змінити її виконання. Ін'єкція коду відбувається тоді, коли програма надсилає дані без перевірки. Така загроза може призвести до пошкодження даних і навіть до їх втрати. Для виявлення уразливостей включення, зловмисники використовують спеціальні сканери.

Для побудови профілю загроз інформаційної системи радіостудії проведено аналіз бізнес-процесу організації, який дозволив ідентифікувати всі інформаційні активи та визначити їхню роль у забезпеченні неперервності бізнес-процесу радіостудії. До найбільш важливих інформаційних активів відносяться: аудіофайли, фотофайли та сайт радіостудії. На рис.1 показано зв'язок (інформаційні потоки) між інформаційними активами радіостудії. З рис. 1 видно, що життєвий цикл інформаційних активів проходить через всі підрозділи радіостудії, тому під час побудови профілю загроз необхідно врахувати можливі загрози від усіх організаційних підрозділів.

На основі відомої методики експертного оцінювання імовірності реалізації загроз інформаційним активам [1] та розробленої нами методики оцінювання значень збитку ($\boldsymbol{B_{зб}}$) від їхньої реалізації обчислено значення ризиків інформаційної безпеки (***P***) радіостудії, зокрема, досліджено властивості інформаційних активів, такі як цілісність, доступність та конфіденційність. У табл. 1 наведено фрагмент аналізу стосовно порушення цілісності одного активу.

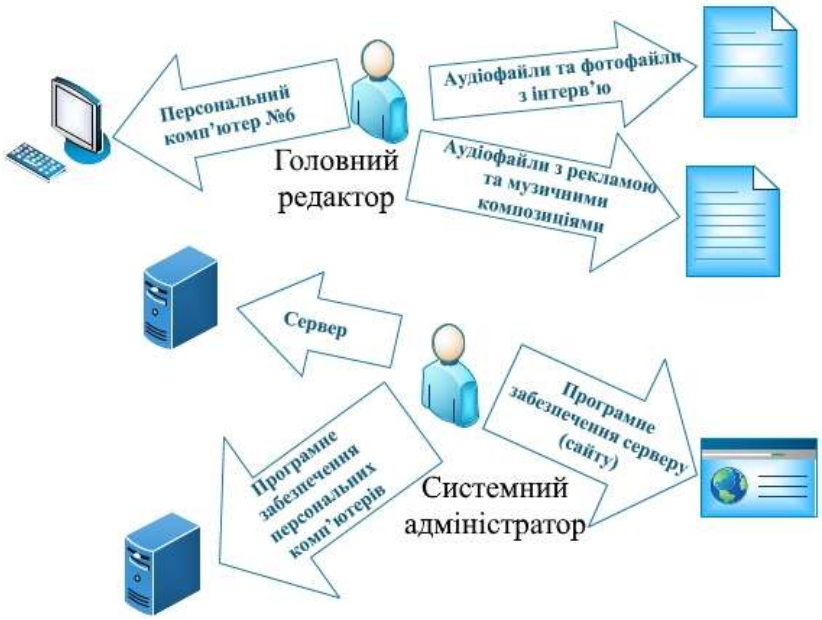


Рис. 1. Схема інформаційних потоків між інформаційними активами радіостудії

Критеріями порівняння (показниками) обрано: *можливість виникнення джерела* $(K_1)_i$, *готовність джерела* $(K_2)_i$ та *фатальність* $(K_3)_i$, значення яких оцінюється експертно-аналітичним методом за п'ятибальною шкалою. Загальний коефіцієнт $(K_{заг.})_i$ для окремого джерела можна визначити як відношення добутку наведених вище показників до максимального значення 125: $(K_{заг.})_i=((K_1)_i \times (K_2)_i \times (K_3)_i)/125$ [1].

Таблиця 1

Дослідження порушення цілісності інформаційних активів радіостудії

Назва активу	**Джерело загрози**	**Механізм реалізації нападу**	$(K_1)_i$	$(K_2)_i$	$(K_3)_i$	$(K_{заг.})_i$	$B_{зб}$	P
Аудіо файли та фото файли	Хакер	Видалення або модифікація фотофайлів або аудіофайлів.	4	5	5	0,8	4	3,2

Таким чином, у результаті аналізу ризиків інформаційної безпеки радіостудії ідентифіковано типові загрози, зокрема, видалення або модифікація аудіофайлів та фотофайлів, впровадження шкідливого коду в тіло сайту та зараження програмного забезпечення персональних комп'ютерів працівників вірусами та шкідливими програмами. Даний аналіз дозволив побудувати профіль загроз радіостудії. Проведене дослідження виявило вуразливості, зокрема, відсутність правил розмежування доступу, ідентифікації та аутентифікації працівників, відсутність правил регулярного оновлення антивірусних баз та сканування системи на наявність шкідливих програм.

Література

1. Ромака В.А., Корж Р. О., Гарасим Ю.Р. Менеджмент у сфері захисту інформації, Львів, Видавництво Львівської політехніки, 2013, 462 с.

НСД ТА ЗАСОБИ ЙОГО ЗАПОБІГАННЯ

Петро-Павло Козяк, Марія Мандрона
Львівський державний університет безпеки життєдіяльності, м. Львів

Розглянуто статистику випадків несанкціонованого доступу у світі за 2016 рік. Проаналізовано методи нападу та сценарії дій зловмисників. Описано сучасні методи захисту від несанкціонованого доступу.

Ключові слова: несанкціонований доступ, програмні засоби захисту.

In the paper, we considered statistics of cases of unauthorized access in the world since 2016 year. The methods of the attack and the scenarios of the actions of the intruders are analyzed. The modern methods of protection against unauthorized access are described.

Key words: unauthorized access, software protection.

Високий рівень автоматизації створює ризик зниження безпеки, починаючи від особистої, так і до зниження безпеки самої держави. Доступність і широке поширення інформаційних технологій електронно-обчислювальних машин робить їх надзвичайно вразливими по відношенню до деструктивних впливів.

Відповідно до статистичних даних, у 2016 році по всьому світі було оприлюднено, в засобах масової інформації та в інших джерелах 1556 випадків витоку інформації з обмеженим доступом, що на 3.4% перевищує число, яке було зареєстровано в 2015 році.

Зовнішні атаки стали причиною 38% випадків витоку інформації, це на 6% більше ніж у 2015 році [1].

Саме тому, актуальним є аналіз засобів захисту від несанкціонованого доступу. Найбільше різноманіття мають програмні засоби захисту. До них відносяться програми для ідентифікації користувачів, контролю доступу, шифрування інформації, видалення залишкової (робочої) інформації, тобто тимчасових файлів, тестового контролю системи захисту та інші [1-3]. Перевагами програмних засобів захисту вважають їх надійність, простота установки, гнучкість, універсальність у використанні, здатність до модифікації і розвитку. До недоліків відносять обмежену функціональність мережі, висока чутливість до випадкових або навмисних змін, використання частини ресурсів файл-сервера і робочих станцій, можлива залежність від типів персональних комп'ютерів та їх технічних характеристик та апаратних засобів.

Аналізуючи літературні джерела, можна побачити, що методи нападу є численні і давно не обмежується прямими хакерськими атаками та застосуванням шкідливого програмного забезпечення. Для проникнення зазвичай використовують соціальну інженерію та інсайдерів. Проте, бувають випадки простої крадіжки матеріальних носіїв.

На рис. 1 наведено класифікацію методів реалізації несанкціонованого доступу до інформації.

Рис. 1. Класифікація методів реалізації НСД

При здійсненні несанкціонованого доступу, зловмисник переслідує три мети [2]:

- одержати необхідну інформацію для конкурентної боротьби;
- мати можливість вносити зміни в інформаційні потоки конкурента у відповідності зі своїми інтересами;
- завдати шкоди конкурентові шляхом знищення матеріалу інформаційних цінностей.

До найбільш відомих поширених сценаріїв НСД належать [3]: перегляд інформації, копіювання програм та даних, читання даних з лінії зв'язку, зміна потоку повідомлень, закладки, зміна алгоритмів програм, зміна апаратної частини автоматизованої системи, зміна режиму обслуговування або умов експлуатації, перерва функціонування автоматизованої системи або її компонентів, перерва потоку повідомлень, перерва компонент програмного забезпечення, перерва процесу функціонування або його складових, фізичне руйнування апаратних засобів мережі, підробка, додавання фальшивих процесів і підміна справжніх процесів фальшивими, додавання фальшивих апаратних засобів, імітація роботи апаратно-програмних компонент мережі з боку суб'єктів загрози

Програмні засоби захисту інформації від НСД містять програми для ідентифікації користувачів, контролю доступу, шифрування інформації, видалення залишкової (робочої) інформації типу тимчасових файлів, тестового контролю системи захисту та ін. [2, 3].

Системи захисту комп'ютера від вторгнення є різноманітними і класифікуються за такими групами рис. 2.

Рис. 2. Класифікація засобів захисту від НСД

Сучасні програмні засоби захисту даних, що функціонують у складі програмного забезпечення є такі: антивірусні програми, криптографічні засоби, VPN засоби, проксі-сервера, операційні системи, електронні ключі.

Література

1. Аналитический центр InfoWatch. Глобальное исследование утечек конфиденциальной информации в 2016 году [Електронний ресурс] – Режим доступу: https://www.infowatch.ru/report2016.

2. Методи та види несанкціонованого доступу. [Електронний ресурс] – Режим доступу: http://studopedia.ru/2_105290_metodi-ta-vidi-nsd.html.

3. Методи та види НСД . [Електронний ресурс] – Режим доступу: https://studopedia.ru/2_105290_metodi-ta-vidi-nsd.html

КІБЕРСКВОТИНГ –- ДОМЕННЕ РЕЙДЕРСТВО

Юлія Кордунова, Наталія Кухарська
Львівський державний університет безпеки життєдіяльності, м. Львів

У статті розглянуто явище кіберсквотингу, його види та особливості, а також способи вирішення доменних спорів.

Ключові слова: кіберсквотинг, домен, доменне ім’я.

The article deals with the phenomenon of cybersquatting, its types and peculiarities, and also ways how to resolve domain disputes.

Key words: cybersquatting, domain, domain name.

Розвиток Інтернет-технологій призвів до появи нового виду злочинності – кіберсквотингу. Термін «кіберсквотинг» походить від англійського слова «squatting», що означає самовільне захоплення землі.

Під кіберсквотингом розуміють незаконну діяльність, яка полягає у реєстрації доменних імен з метою їх подальшого продажу за значно вищою ціною або з метою отримати прибуток від паразитування на гудвілі чи торговельній марці, що є власністю іншої особи чи організації. Таке собі своєрідне доменне рейдерство. Вперше це явище було зафіксовано в США на початку 90-х років XX століття, коли ще реєстрація доменних імен проводилась безкоштовно. Перші кіберсквотери реєстрували короткі та звучні доменні імена, передбачаючи появу шаленого попиту на них.

Як показує статистика в наш час існує близько трьохсот мільйонів зареєстрованих доменних імен. Проте не всі вони використовуються за своїм призначенням. На них або розміщені дані власника, за якими можна зв’язатися з метою їх покупки, або розміщена реклама. Таких доменів є приблизно 45%. Їх власниками є кіберсквотери, які переслідують ціль заробити на них.

Слід зауважити, кіберсквотерів насправді цікавлять не всі підряд доменні імена. Існують певні критерії, за якими вони здійснюється підбір доменних імен, перспективних з їх точки зору. Залежно від критеріїв і тактики, яку використовує кіберсквотер, сферу діяльності під назвою кіберсквотинг можна поділити на кілька видів.

- Продаж коротких доменних імен. Велику популярність серед хапперів мають доменні імена, які мають невелику кількість символів. Два, три, чотири символи в доменному імені є дуже доречні. Велику роль у визначенні ціни, за якою можна перепродати домен, відіграє його лексичне значення. Такі доменні імена як eda.com, yes.com, kino.com. користуються високою популярністю серед користувачів мережі.
- Брендовий кіберсквотинг – реєстрація і продаж доменних імен, що містять точні або схожі назви компаній, торгових марок, Інтернет-магазинів. Наприклад це такі сайти, як: microcoft.com, coca-cola.ua, mts.ru. Цей вид кіберсквотингу називають «чорним» бізнесом, так як порушуються авторські права компаній. Такі спекуляції з доменними іменами мають високу ймовірність завершитися в суді. Правда, законні власники товарних знаків часто воліють не судитися, а викупляти захоплені домени.
- Іменний кіберсквотинг. Цей вид діяльності пов’язаний з реєстрацією доменних імен, в яких використовуються імена та прізвища світових знаменитостей. Такий вид кіберсквотингу використовується для реклами і є законним видом бізнесу, адже не викликає прецеденту порушення прав. Заробіток на ньому може бути навіть дуже непоганим, якщо взяти до уваги той факт, що відвідуваність таких доменів – кілька десятків тисяч відвідувачів на добу.
- Галузевий кіберсквотинг. Це реєстрація і продаж доменних імен, що позначають або співзвучні з послугами, предметами, товарами. Це, наприклад, сайти seo.com, doctor.ru, foto.de та інші. Галузевий один з найпопулярніших видів кіберсквотинга. Такі доменні імена легко сприймаються і на слух, і візуально, швидко запам'ятовуються, а це позитивно впливає на їх ранжування у пошукових системах. При цьому відсутня можливість втратити такий домен через порушення чиїх-небудь прав.

- Географічний кіберсквотинг. Цей вид кіберсквотингу полягає у реєстрації доменних імен, в яких використовуються назви географічних об'єктів: континентів, країн, міст, регіонів і т. д. Велику затребуваність мають домени з назвами популярних туристичних напрямків. Наприклад, egypt.ru або tailand.ru будуть приносити своїм власникам хороший цільовий трафік у пошукових системах.
- Тайпсквотинг. Тут мається на увазі реєстрація доменів дуже схожих з оригіналом, в яких використовується «право на помилку». Багато користувачів, набираючи адресу, допускаються друкарських помилок, через що можуть потрапити на зовсім інший Інтернет-ресурс. Наприклад: замість www.google.com користувачі можуть написати wwwgoogle.com або www.guogle.com та інші. У таких випадках за умови, що такі помилки трапляються часто, кіберсквотер може заробити непогані гроші на рекламі.
- Захисний кіберсквотинг. Цей вид кіберсквотингу не переслідує комерційні цілі. Навіть з назви зрозуміло, що він використовується для захисту від кіберсквотерів. Щоб убезпечити себе від неприємних наслідків кіберсквотингу, власники популярних брендів та й просто завбачливі власники доменів реєструють ідентичні доменні імена у всіх популярних доменних зонах, так само реєструють схожі доменні імена та імена з різними типовими описками. Потім вони просто перенаправляють з них відвідувачів на свій основний домен, де розташований сайт. Наприклад, торгівельна марка, що має у власності site.ru може зареєструвати імена site1.ru, site-msk.ru, anti-site.ru.
- Біт-сквотинг. Це реєстрація і продаж доменних імен, запис яких у двійковій системі числення на один біт відрізняється від оригінального імені (наприклад: символ r і 2 у двійковій системі мають вигляд 1110010 і 0110010). Цим користуються кіберсквотери, розраховуючи на помилки модулів оперативної пам’яті DNS-серверів.

Для України кіберсквотинг достатньо новий вид правопорушень. Судових справ щодо захисту доменних імен в Україні порівняно мало, доменні спори лише починають розглядатись судами. І це не говорить про досконалість законодавчої бази нашої країни, а скоріше є свідченням слабкого розуміння важливості Інтернету українським бізнесом. На жаль, національна правова база України не має спеціалізованих актів, що можуть регулювати цю сферу відносин. На сьогоднішній день, джерелами норм, якими керуються при вирішенні доменних спорів, є Цивільний кодекс України, а саме книга 4, Закон України «Про охорону прав на знаки для товарів і послуг», Закон України «Про телекомунікації».

До речі, в Європі, на відміну від України, нарівні з судами досить поширеним є вирішення спорів навколо доменних імен в позасудовому порядку, зокрема, способами альтернативного врегулювання спорів. Наприклад, спори вирішуються в порядку процедури UDRP – єдиної політики вирішення спорів щодо доменних імен, затвердженої ICANN (організація, яка на міжнародному рівні вирішує питання функціонування мережі Інтернет, в тому числі стосовно доменів).

Спори за зазначеною процедурою можуть розглядатися п’ятьма акредитованими організаціями (Approved Dispute Resolution Service Providers), серед яких: Азіатський центр з вирішення доменних спорів; Національний арбітражний форум; Центр BOIB з арбітражу та посередництва; Чеський арбітражний суд; Арабський центр з вирішення спорів.

Розгляд спорів за процедурою UDRP часто є більш простим, передбачуваним і дешевим способом захисту прав у порівнянні зі зверненням до національних судів.

Заради справедливості слід зауважити: цю систему вже запропоновано впровадити в Україні. Зокрема, компанія «Хостмастер» – представник адміністратора домену .UA – порушувала питання про використання цього альтернативного способу вирішення доменних спорів. Однак, ініціатива поки що залишилася на рівні заяв.

У підсумку – від кіберсквотингу виграють одиниці, а програємо всі ми.

Література

1. Киберсквотинг и киберсквотеры. [Электронный ресурс] // Режим доступа : http://www.internet-technologies.ru/articles/article_833.html.

2. Види кіберсквотингу. [Електронний ресурс] // Режим доступу : http://creativesite.org/news/2009-12-21-431.

НЕОБХІДНІСТЬ ТА ПЕРСПЕКТИВИ ЗАПРОВАДЖЕННЯ БІОМЕТРИЧНОГО БАНКОМАТУ В УКРАЇНІ

Вікторія Король, Олександр Белей
Львівський навчально-науковий інститут ДВНЗ «Університет банківської справи», м.Львів

У даній доповіді розглядаються причини, передумови та можливості запровадження в Україні біометричного банкомату. Наведені різні види біометричної ідентифікації користувача та їх основні переваги.

Ключові слова: шахрайство, біометричний банкомат, біометрична ідентифікація.

This report discusses the reasons, preconditions and possibilities of introducing a biometric ATM in Ukraine. The various types of biometric identification of the user and their main advantages.

Key words: fraud, biometric ATM, biometric identification.

Актуальність даної теми зумовлена тим, що за останні роки разом із активним зростанням частини населення України, яка користується пластиковими картками та банкоматами, зростає і кількість випадків незаконного заволодіння грошима з карткового рахунку.

Явище шахрайства в електронно-фінансовій сфері стає все більш поширеним. Злочинці вигадують нові способи крадіжок: копіюють магнітну смугу за допомогою підставних пристроїв зчитування, які зберігають дані з картки та ПІН-код; викрадають картки та ПІН-коди; встановлюють поруч з банкоматами мініатюрні камери; виготовляють фальшиві банкомати тощо. Тому, часто через неуважність та порушення правил безпеки при роботі з банкоматом люди стають жертвами таких шахрайських дій.

Враховуючи те, що рівень безпеки клієнтських даних є не надто високим, досить важливою та актуальною є проблема вибору ефективного методу та засобу автентифікації. Стрімкий розвиток інноваційних технологій, поява нових глибоких комп'ютерних знань, сприяє тому, що біометричні технології стають все більш популярні у сфері захисту грошових операцій. Цей унікальний засіб ідентифікації вражає своєю сучасністю та спектром можливостей здійснення розпізнавання особи.

Запровадження біометричного банкомату дійсно могло б стати досить хорошим способом вирішення даної проблеми, оскільки він має більш надійну систему захисту від несанкціонованого доступу до банківського рахунку клієнта, аніж звичайний банкомат.

Ідея створення біометричного банкомату з'явилась в Японії, після того, як у зв'язку із стихійними лихами у жовтні 2011 року багато людей втратило свої документи та банківські карточки, а отже змогу скористатись своїми коштами. Сьогодні ж біометричні банкомати використовують жителі Сполучених Штатів Америки, Бразилії, Польщі, Туреччини, Нігерії та інших країн.

У сучасному світі серед різноманітних способів захисту інформації неабияке місце займає ідентифікація особистості. І хоча в Україні дані технології на сьогодні в банківській сфері практично не використовуються, за кордоном вони стають все більш популярними, розвиваються та еволюціонують.

Сьогодні використовують вже більше десяти біометричних ознак, а саме автентифікація людини: за формою та термограмою обличчя; за відбитками пальців; за відбитком долоні; за розміщенням вен на лицьовій стороні долоні; за райдужною оболонкою та сітківкою ока; за голосом; за почерком; за формою вуха та інші.

Для того, щоб клієнт міг здійснювати банківські операції за допомогою біометричного банкомату, йому необхідно надати банку свої біометричні дані, які будуть внесені в спеціальну базу даних або записані на чіп карточки. Ці унікальні дані людини або повністю замінюють введення ПІН-коду або ж доповнюють його. На самих банкоматах мають знаходитись сенсорні пристрої, що зчитуватимуть інформацію та порівнюватимуть її з наявною в базі даних.

Існують певні скептичні думки, щодо надійності біометричної ідентифікації, і їх також варто враховувати, оскільки недоліки можливі в будь-якій системі. Дійсно, ймовірність підробки біометричних даних, хоч і невелика, та все ж є. Тому розробники даної технології

запровадили таку функцію, як запам'ятовування не лише даних клієнта банку, а й того, хто намагається видати себе за іншу особу. Банкомат фіксує біометричні дані шахрая, який намагається не санкціоновано отримати доступ до чужих даних. Згодом це може допомогти у пошуку злодія.

В Україні досвід роботи з біометричними даними розпочався ще у 2016 році, коли було видано Закон України «Про Єдиний державний демографічний реєстр» та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус», який передбачав запровадження оформлення і видачі паспорта громадянина України, що містить безконтактний електронний носій із біометричними даними власника документу. У відділеннях міграційної служби були встановлено спеціальне обладнання для зняття біометричних даних, яке дозволяло фіксувати зображення людини, отримувати відбитки пальців та електронний підпис.

Даний спосіб роботи з банкоматом є більш безпечним, надійним та зручним В Україні уже є основа для роботи з біометричними даними людини, тому запровадження біометричного банкомату – це ще один крок до розвитку новітніх технологій в нашій країні, покращення роботи та банківської системи, що в добу інформаційного суспільства є досить важливо.

Звісно, поруч із багатьма перевагами біометричного банкомату є і певні недоліки, які власне можуть завадити його впровадженню на території України. Зокрема, устаткування, яке дозволяє проводити біометричну ідентифікацію особи, є надто дорогим. Потрібно вкласти чимало коштів, аби забезпечити таку новітню технологію у всіх містах України, а також знайти спеціалістів, які змогли б розробити необхідні програми та прилади. Саме тому можуть виникнути проблеми з пошуком джерел фінансування. Враховуючи цей фактор, можна передбачити, що і ціна використання такої послуги буде досить високою.

Ще однією перепоною стане те, що велика частина українського суспільства є необізнаною у сфері сучасних технологій. Тому потрібні будуть додаткові зусилля, аби забезпечити людей необхідними знаннями щодо роботи та використання біометричного банкомату.

Також, деякі специфічні захворювання можуть стати на заваді до використання біометричної ідентифікації. Наприклад, були зафіксовані випадки, коли через катаракту кристалика ока унеможливлювалась ідентифікація за райдужною оболонкою та сітківкою ока.

Можна багато дискутувати про переваги та недоліки впровадження біометричного банкомату в Україні, та все ж я вважаю, що таке нововведення змогло б допомогти у боротьбі з шахрайством, адже підробити природні характеристики людини є досить складно.

Оскільки в Україні за останні роки покращується становище у галузі інноваційних технологій, то запровадження біометричного банкомату могло б створити нові напрями роботи по розробці технічного та програмного забезпечення, яке б обслуговувало такий банкомат. В Україні є досить багато талановитих, креативних та розумних людей, чий потенціал можна використати у впровадженні біометричної ідентифікації в банківській системі.

Отже, розвиваючи можливості керування фінансами та розширюючи коло своїх послуг, банки мають не забувати про ще одне досить важливе на сьогоднішній день завдання: удосконалення способів захисту даних своїх клієнтів від шахраїв, оскільки проблема безпеки даних досить гостро постає перед людством. Банки є зацікавлені у покращенні своєї політики захисту, адже якість, надійність та безпечність послуг – визначальні фактори формування їхнього іміджу, репутації та довіри своїх клієнтів.

Література

1. Біометрія як універсальний спосіб ідентифікації людини [Електронний ресурс]. – Режим доступу: http://bablyukh.clan.su/publ/1-1-0-4.

2. Біометрична ідентифікація [Електронний ресурс]. – Режим доступу до ресурсу: https://sites.google.com/site/identifikaciataautentifikacia/ponatta-pro-identifikaciu/biometricna-identifikacia.

3. Державна Міграційна Служба України. Біометричні документи в Україні [Електронний ресурс]. – Режим доступу до ресурсу: https://dmsu.gov.ua/faq/biometrichni-dokumenti-v-ukrajni.html.

ПРИХОВУВАННЯ ЦИФРОВИХ ВОДЯНИХ ЗНАКІВ В ЧАСТОТНІЙ ОБЛАСТІ ЗОБРАЖЕНЬ НА ОСНОВІ ВЕЙВЛЕТ-ПЕРЕТВОРЕННЯ

Юрій Кошеленко, Андрій Лагун
Львівський державний університет безпеки життєдіяльності, м. Львів

Проведено дослідження методів приховування інформації в частотній області з використанням вейвлет-перетворення і наведено рекомендації по застосуванню різних вейвлет-базисів для збільшення якості приховування, а також використанню порогу чутливості при вбудовуванні цифрових водяних знаків в нерухоме зображення у вигляді jpeg-файлу.

Ключові слова: стеганографія, контейнер, зображення, стего, вейвлет перетворення, пікове відношення сигнал-шум, середньоквадратичне відхилення, поріг чутливості.

Were researched the methods of hiding information in frequency domain with usage of wavelet transform. Also was recommended how using different wavelet-based for increasing quality of hiding and using threshold of sensitivity for digital watermarking embeding in static image (jpg- file)

Keywords: steganography, container, image, stego, wavelet transform, peak signal to noise ratio, mean square deviation, threshold of sensitivity.

Розвиток засобів цифрової обчислювальної техніки сприяв розвитку комп'ютерної стеганографії, яка ґрунтується на вбудовуванні секретного повідомлення в цифрові дані, що, як правило, мають аналогову природу (аудіозаписи, зображення, відео). Для цього використовується стеганографічна система, основним призначенням якої є передавання з основною інформацією додаткової, котру не можна видалити без значного погіршення якості основного повідомлення.

Повідомлення вбудовується в контейнер за допомогою ключа стегокодером, формуючи стегоконтейнер. Стегоконтейнер на приймальній стороні поступає на стегодетектор, який здійснює видобування прихованого повідомлення. Часто як контейнер використовуються нерухомі цифрові зображення, а для захисту інтелектуальної власності використовують цифрові водяні знаки (ЦВЗ).

Провівши попередній аналіз існуючих методів приховування інформації в нерухомих зображеннях, можна зробити висновок про те, що найбільш оптимальними для практичних реалізацій є методи приховування інформації в часовій (просторовій) та частотній областях нерухомого зображення.

Найпоширенішим методом приховування інформації в часовій (просторовій) області є метод заміни найменшого значущого біта (LSB), що полягає в заміні надлишкової, малозначимої частини зображення бітами секретного повідомлення.

Найбільш ефективні стеганографічні методи, що працюють в частотній області, використовують вейвлет-перетворення й дискретне косинусне перетворення.

Дискретне косинусне перетворення поділяє зображення на спектральні ділянки різного значення стосовно візуальної якості зображення. Застосування методів такого типу для вбудовування водяних знаків в зображення показує хорошу стійкість до масштабування, JPEG компресії, згладжування спотворень, обрізки, сканування і т.д.

Рис. 1. 4-рівневе DWT

Вейвлет-перетворення (DWT) дозволяє зосередити низькочастотні деталі сигналу в частотній області, а високочастотні – в часовій. Дискретне вейвлет-перетворення дозволяє розкласти зображення в підзображення, що містяться в різних просторових та частотних областях, після чого результуюче зображення аналізується в одній низькочастотній (LL) і трьох високочастотних (LH, HL, HH) областях. Приклад чотирирівневої декомпозиції зображення з використанням вейвлет-перетворення наведено на рис. 1.

Якість приховування ЦВЗ в зображенні визначається за допомогою пікового відношення сигнал/шум (PSNR):

$$PSNR = 10\log_{10}\frac{Max^2}{MSE} \quad (1)$$

$$MSE = \frac{1}{mn}\sum_{x=1}^{m}\sum_{y=1}^{n}\left(St_{xy} - I_{xy}\right)^2, \quad (2)$$

де *Max* – максимальне значення піксела зображення, *MSE* – середньоквадратичне відхилення, *x* і *y* – координати піксела, *m* і *n* – розміри зображення, St_{xy} – створене стегозображення і I_{xy} – початкове зображення.

Вейвлет-перетворення дозволяє розкласти двохвимірне зображення на апроксимуючі та деталізуючі коефіцієнти, отримавши перший рівень розкладу.

а) б) в) г)

Рис. 2. Початкове зображення (а), ЦВЗ (б), стего без порогу чутливості (в), стего з порогом чутливості 0,1 (г)

В свою чергу, апроксимуючі коефіцієнти першого рівня можна розкласти на апроксимуючі та деталізуючі коефіцієнти другого рівня і так далі. Основна інформація про спектр зображення міститься в апроксимуючих коефіцієнтах. Таким чином, з'являється можливість приховування ЦВЗ в деталізуючих коефіцієнтах. Проведемо дослідження такого способу приховування ЦВЗ.

Як контейнер використаємо зображення tree.jpg розміром 1800x1800 пікселів (рис. 2а), а ЦВЗ у вигляді QR- коду – рис. 2б. Також використаємо для розкладу вейвлет-перетворення Добеші D8.

На початковому етапі контейнер розкладається на RGB складові, після чого вибирають складову кольору, по якій буде відбуватися розклад. Потім до зображення застосовується функція Matlab dwt2 аж до 5 рівня розкладу, кожен раз використовуючи апроксимуючі коефіцієнти попереднього рівня як зображення.

Спочатку вбудовуємо ЦВЗ в R-складову палітри зображення без врахування порогу чутливості. Вбудовування відбувається в апроксимуючі і деталізуючі коефіцієнти 5-го рівня розкладу. Результуюче стегозображення наведено на рис. 2в. Як бачимо, при вбудовуванні ЦВЗ поширився по всьому стегозображенню і може спостерігатися неозброєним оком.

Тому під час приховування було введено поріг чутливості (JND), який становить 0,1. Одержане стегозображення наведено на рис. 2г. При порозі чутливості 0,1 вбудований ЦВЗ взагалі не помітний. Про якість приховування свідчать коефіцієнти PSNR і MSE, значення яких наведено в таблиці 1.

Наступним етапом проведення досліджень є встановлення можливості приховування ЦВЗ в деталізуючих коефіцієнтах. Розмір розкладеного ЦВЗ (перший рівень розкладу) має бути таким, щоб ЦВЗ повністю помістився в деталізуючий або апроксимуючий коефіцієнт. Було проведено дослідження можливостей вбудовування ЦВЗ в горизонтальні (cH4), діагональні (cD4) і апроксимуючі (cA4) коефіцієнти без врахування порогу чутливості. Для всіх чотирьох випадків було обчислено значення коефіцієнтів якості стегозображення, які зведено в таблицю 2.

Таблиця 1. Коефіцієнти якості стегозображення

№ з/п	JND	PSNR	MSE
1	1	75.6065	0.0018
2	0.5	81.6271	4.5E-4
3	0.1	95.6065	1.8E-5

Таблиця 2. Коефіцієнти якості стегозображення для різних типів вейвлет коефіцієнтів

№ з/п	Тип вейвлет-коефіцієнтів розкладу	PSNR	MSE
1	Деталізуючі горизонтальні	75.8441	0.0017
2	Деталізуючі вертикальні	75.8308	0.0017
3	Деталізуючі діагональні	75.1354	0.002
4	Апроксимуючі	76.5639	0.0014

Проаналізувавши рис. 1 і таблиці, можна зробити висновок, що немає істотного значення, в які з коефіцієнтів вейвлет-розкладу зображення-контейнера вбудовувати ЦВЗ, оскільки і для апроксимуючих, і для вертикальних, і для горизонтальних, і для діагональних деталізуючих коефіцієнтів відбувається помітне спотворення стегозображення. Цього можна уникнути, якщо при вбудовуванні використати поріг чутливості, який дорівнює 0,1. В цьому випадку значення PSNR перевищують 90, що вказує на якість стегозображення.

Література

1. Конахович Г. Ф. Компьютерная стеганография. Теория и практика / Г. Ф. Конахович, А. Ю. Пузыренко. – К. : МК-Пресс, 2006. – 288 с.

2. Малла С. Вейвлеты в обработке сигналов / С. Малла. – М. : Мир, 2005. – 671 с.

3. Wolgang R. B. Perceptual Watermarking for Digital Images and Video / R. B. Wolgang, C. I. Podilchuk, E. J. Delp // Proceeding IEEE, Special Issue on Identification and Protection of Multimedia Information. – 1999. – Vol. 87, No 7. – P. 1088 – 1126.

РОЗРОБКА МОБІЛЬНОГО КРОСПЛАТФОРМНОГО ДОДАТКУ ДЛЯ ВІДПРАЦЮВАННЯ ПРАКТИЧНИХ НАВИКІВ З ПРОГРАМУВАННЯ (В НАВЧАЛЬНИХ ЦІЛЯХ)

Михайло Кунинець, Віталій Дзень, Олександр Придатко
Львівський державний університет безпеки життєдіяльності, м.Львів

Запропоновано ідею створення кросплатформного додатку для відпрацювання практичних навиків з програмування мовами Java, C# та C++. Принцип застосунку розробленого додатку полягає в аналізі та структурзації готового коду програми, який попередньо рандомізовано окремими частинами та представлено користувачеві у спотвореному вигляді.

Ключові слова: програмування, практичні навики, мобільність.

Created a cross-platform program for working on practical programming skills in Java, C # and C ++. The principle of the program is to analyze and structure the finished code of the program, which is pre-shared and incorrectly presented to the user.

Key words: programming, practical skills, mobility.

Застосування сучасних прогресивних технологій для підготовки майбутніх фахівців IT-індустрії є невід'ємною складовою цього процесу. Мова йтиме про підготовку майбутніх розробників програмного забезпечення. Очевидно, що для активізації роботи студента, як на занятті так і під час індивідуального навчання, слід використовувати методи засновані на вирішенні прикладних практичних завдань за допомогою конкретної мови та відповідного середовища розробки. Проте, нажаль, в сучасних реаліях не завжди можливе застосування інтегрованого середовища розробки (IDE). Сучасні «реалії» – це висока активність та мобільність студента, який в потоці вирішення власних справ та задоволення інтересів не завжди залишає достатньо часу для індивідуального навчання. А якщо задатись питанням: «Скільки часу студент проводить в соціальних мережах, чатах, іграх?». Однозначної відповіді немає, проте наближена – багато! Все це стає можливим з допомогою мобільних гаджетів. Відповідно змістовним зауваженням буде те, що мобільні пристрої вже давно необхідно активно застосовувати в цілях навчання. Сучасні технології дистанційного навчання вже наділені можливістю здобуття якісних теоретичних знань за допомогою мобільних додатків, використовуючи віртуальні навчальні середовища [1]. А як бути з практичною частиною? На даному етапі формування проблематики, ми повертаємось до складності використання інтегрованого середовища розробки на мобільних пристроях. Зважаючи на це та беручи за основу ідею творців підручника [2] виникає ідея створення кросплатформного додатку, використання якого дозволятиме відпрацьовувати практичні навики з програмування без прив'язки до IDE.

Ідея використання додатку полягає в аналізі деструктурованого коду програми та його подальшої структуризації для одержання відповідного вигляду. Деструктуризація полягає у випадковому поділі коду на окремі частини та хаотичному розміщенні частин між собою. Коротко про додаток. Вхід у додаток передбачено із обов'язковою реєстрацією, що необхідно для ідентифікації навчальних досягнень студента. Адміністративний доступ передбачено для керування роботою додатку. Основна задача викладача як адміністратора полягає у завантаженні готового коду програми та вибору методу його рандомізації. Залежно від тематики завдання адміністратор розміщує відповідних код програми у додатку. Розміщення відбувається шляхом завантажування попередньо підготовленого файлу з програмним кодом. На даному етапі створення програми передбачено завантаження файлів із розширенням *.java, *.cs, *.cpp, для розробників мовами Java, C# та C++ відповідно. Що стосується інших мов програмування, то код програми в додаток можна імпортувати з файлу розширення *.txt. Після завантаження коду програми адміністратор вибирає спосіб випадкового поділу та представлення окремих частин коду для користувача. Важливо згадати, що на цьому етапі обирається лише спосіб рандомізації коду, а сам процес відбувається під час завантаження додатку користувачем.

Вхід та ідентифікація користувача відбувається в декілька етапів (рис. 1). Далі користувач обирає відповідну тему та отримує індивідуальне завдання на виконання. Після

виконання одержаного завдання відбувається його перевірка з відповідним занесенням результатів до бази даних. Також передбачена можливість збереження результатів, без можливості їх редагування, на мобільний пристрій з метою подальшого завантаження у будь-яке віртуальне навчальне середовище для звітності.

З метою кращої уяви про додаток, принцип його роботи представлено у вигляді алгоритму, взятого за основу з результатів попередніх досліджень [3].

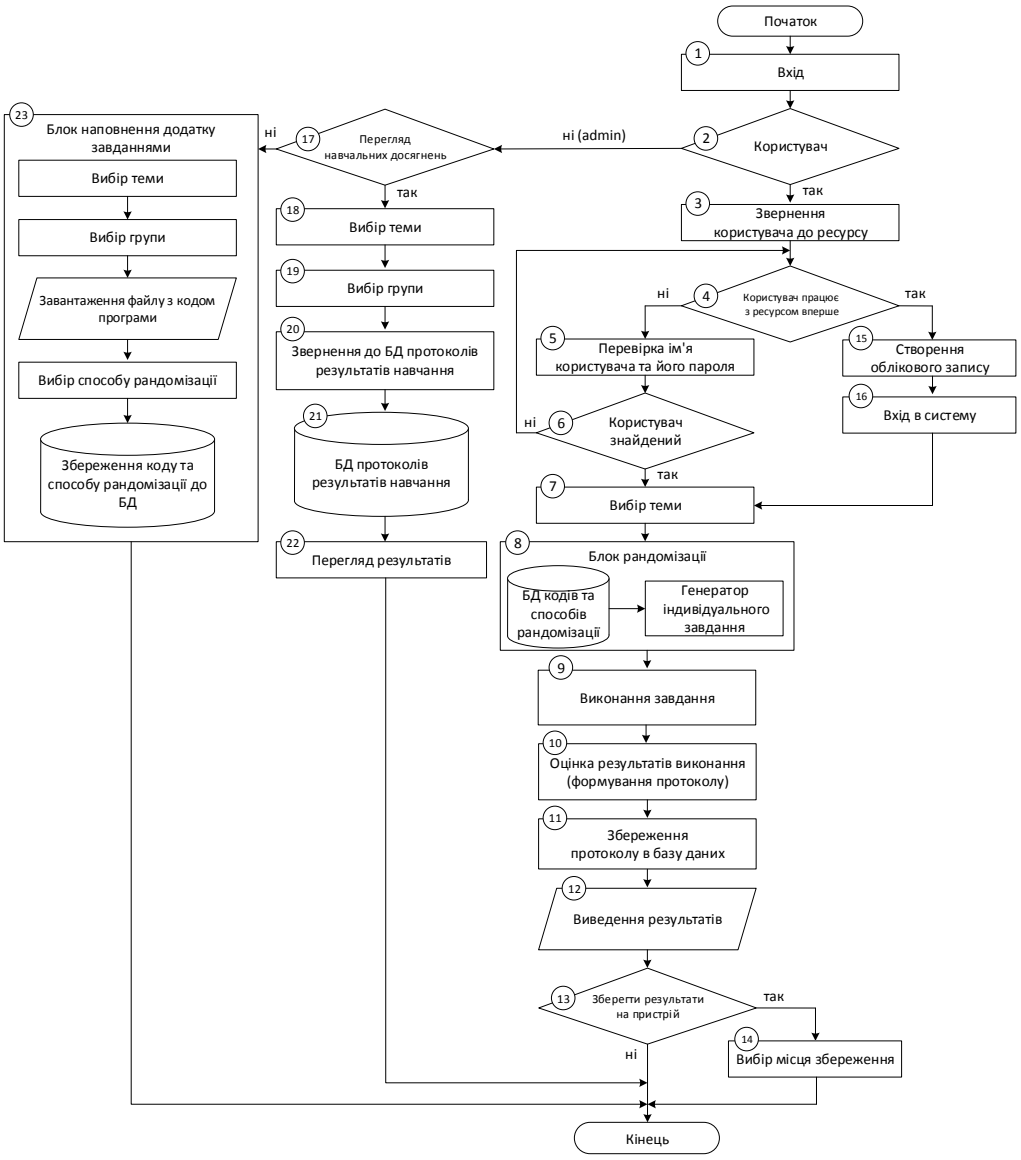


Рис. 1. Алгоритм принципу роботи додатку

В роботі реалізовано задум створення мобільного кросплатформного додатку, який дозволятиме відпрацьовувати практичні навики з програмування без прив’язки до IDE та підвищує успішність підготовки майбутніх розробників.

Література

1. Полотай О.І. Напрями вдосконалення управління проектами запровадження дистанційного навчання у вищому навчальному закладі / О.І. Полотай // Управління розвитком складних систем: Зб.наук.пр. К.: КНУБА, 2013. - № 13. – С.40-44.

2. Head First Java (изучаем Java) : пер. с англ. / Kathy Sierra, Bert Bates. – Москва : «Эксмо», 2012. – 718 с.

3. Придатко О. В. Інтеграція 3D-інтерактивних технологій навчання в освітні проекти безпеко-орієнтованих спеціальностей / О. В. Придатко, А. Г. Ренкас, Н. Є. Бурак, М. В. Лемішко // Вісник ЛДУБЖД: Зб. наук. праць. Львів: ЛДУ БЖД, 2017. – №15. – С.46-54.

МОДЕЛЬ РОЗКРИТТЯ КРИПТОСИСТЕМИ РАБІНА НА БАЗІ ГЕНЕТИЧНОГО АЛГОРИТМУ

Богдан Куровець, Наталія Кухарська, Ростислав Гриник
(Львівський державний університет безпеки життєдіяльності, м. Львів

The paper considers the principles of the asymmetric cryptosystem of Rabin, analyzes the methods of disclosure of ciphers constructed on the basis of the complexity of the decomposition of a large number on simple factors.
Rabin cryptosystem, cryptography, Genetic Algorithm, information security system, security system, information resources.

Шифрування інформації в даний час стало чи не основним методом її захисту. Доступність обчислювальної техніки та стрімкий прогрес у її розвитку привели до вдосконалення давно відомих криптографічних систем захисту інформації і застосуванню їх в масовому масштабі. Однак у цього прогресу є й інша сторона: великі можливості обчислювальних пристроїв сьогодні успішно застосовуються не тільки для шифрування, але і для розкриття тих криптосистем, які ще вчора, здавалося б, гарантували надійний захист інформації.

Алгоритм Рабіна - це асиметрична криптосистема яка використовує відкритий ключ *(n)* для шифрування повідомлення і закритий ключ *(q,n)* для розшифрування криптограми. Безпека даної криптосистеми визначається складністю пошуку квадратних коренів по модулю складного числа [1]. Генерування ключів відбувається наступним чином:

- Вибираються пара великих простих чисел *(p,q)* таких, щоб при діленні на 4 вони давали остачу 3.
- Обчислюється модуль $n=p*q$, який і є відкритим ключем

Крипостійкість алгоритму Рабіна визначається трудомісткістю факторизації великих чисел, тобто для розкриття криптограми необхідно відкритого ключа *(n)* отримати два простих числа *(p,q)*, тобто задача криптоаналізу зводить до розкладання на множники великого числах [2].

Перед побудовою інтелектуальної системи для вирішення задачі факторизації необхідно вирішити декілька задач, таких як:

- спосіб представлення хромосоми;
- побудова цільової функції;
- формування початкової популяції;
- вибір (комбінування) генетичних операторів, таких як: вибір батьківських хромосом, схрещення, мутації та селекція.

Структура хромосом являє собою бітову стрічку, котра зберігає інформацію про простий множник, а другий множник знаходиться з $n = p \times q$.

Побудова цільової функції. Декодування хромосоми дає значення першого потенційно простого множника *p*, для якого є лише один однозначний співмножник:

$$q = \frac{n}{p}$$

Далі, до отриманого результату застосовуємо імовірнісний тест Міллера-Рабіна з метою отримання інформації про ймовірність простоти числа *q*. Таким чином, значення цільової функції (ЦФ) визначається добутком ймовірностей двох співмножників:

$$P = P(q) \times P(p)$$

Формування початкової популяції. Просте число генерується випадковим вибором значення бітів. Останній біт завжди встановлюється рівним одиниці. Потім обчислюється середня відстань між простими числами – *r*, після чого в діапазоні $[G-r;G+r]$ здійснюється пошук найімовірнішого простого числа.

Вибір батьківських хромосом. Експериментальні дослідження показали, що найбільш ефективним є випадковий вибір [1]. Це обумовлено специфікою завдання. Оскільки ймовірність того, що $P(q)=0$ досить висока відповідно і ймовірність того, що цільова функція в цілому для багатьох хромосом в популяції буде дорівнювати нулю, висока, то елітний вибір і «колесо рулетки» будуть призводити до локалізації простору пошуку, а генетичний алгоритм увійде в стан стагнації.

Оператором схрещення *був обаний кросинговер* — це комбінування хромосом шляхом замін значень генів і утворення нових хромосом на їх місцях.

Оператор мутації. Після процесу рекомбінації відбувається процес мутації. Даний оператор необхідний для «вибивання» популяції з локального екстремуму і перешкоджає передчасній збіжності. Це досягається за рахунок того, що змінюється випадково обраний ген в хромосомі

Селекція полягає в тому, що батьками можуть стати тільки ті особини, значення пристосованості яких не менше порогової величини, наприклад, середнього значення пристосованості по популяції.

Криптосистема Рабіна являється одним з стійких алгоритмів шифрування інформації з відкритим ключем. Безпека алгоритму Рабіна обумовлюється складністю факторизації цілих чисел. Для розкриття цієї криптосистеми необхідно вирішити задачу розкладання модуля n на два простих числа p і q. Цю задачу можна вирышити з допомогою генетичного алгоритму, для цього необхідно підібрати спосіб представлення ключа та оптимальну фітнес-функцію.

Література

1. Шнайер Б., Прикладная криптография. 2-е издание. Протоколы, алгоритмы и исходные тексты на языке С. – Пер. с англ.: М.: Издательство ТРИУМФ, 2002. 816 с.

2. David Michael Chan, Automatic Generation of Prime Factorization Algorithms Using Genetic Programming, Stanford Bookstore, 2002.

РОЗРОБКА 3-D ІНТЕРАКТИВНИХ ТЕХНОЛОГІЙ ДЛЯ ПІДГОТОВКИ ФАХІВЦІВ БЕЗПЕКО-ОРІЄНТОВАНИХ СПЕЦІАЛЬНОСТЕЙ

Михайло Лемішко, Олександр Придатко
Львівський державний університет безпеки життєдіяльності, м. Львів

Описано особливості застосування розроблених 3D-інтерактивних технологій навчання в процесі індивідуальної підготовки із можливістю віддаленого доступу. Зазначено основні досягнення в області розроблення освітніх 3D-інтерактивних технологій для навчання студентів безпеко-орієнтованих спеціальностей в Львівському державному університеті безпеки життєдіяльності. Окреслено основні перспективи та проблеми подальшого розвитку зазначеного напряму.

Ключові слова: 3D-інтерактивні технології, навчання, безпеко-орієнтовані спеціальності.

This paper describes the application features 3D-interactive learning technologies in the preparation of rescuers. Outlines the advances in the development of 3D-interactive educational training for students safety-oriented specialties in Lviv State University of Life Safety. The main prospects and problems of further development of this direction are outlined.

Keywords: 3D-interactive technologies, training, safety-oriented specialties

Враховуючи досвід передових вчених, які займаються питаннями інтеграції в освітнє середовище інноваційних технологій навчання [1, 2], встановлено, що одним з найбільш ефективних методів активізації пізнавальної діяльності студентів є навчання засноване на всебічному використанні методів інтерактивності.

Розпочати слід з досвіду створення та інтеграції в освітнє середовище 3D-інтерактивних технологій. У Львівському державному університеті безпеки життєдіяльності, розроблення 3D-технологій навчання зосереджено у двох напрямах. Перший напрям охоплює 3D-моделювання технічних об’єктів з метою детального вивчення їх конструкції та принципу роботи. Другий напрямок зосереджено на створенні 3D-віртуального комплексу вивчення дисциплін пожежно-профілактичного циклу.

Розроблення 3D моделей технічних об’єктів націлено на висвітлення особливостей будови протипожежного устаткування показуючи прилад з різних ракурсів. З цією метою обрано пакет програмного забезпечення Google Sketch Up. Використання цього пакету дає можливість огляду створеного об’єкта в різних ракурсах, в тому числі у збільшеному вигляді без погіршення якості зображення. Самостійний вибір ракурсу для огляду устаткування дає безсумнівну перевагу над звичайний плакатом, схемою, слайдом тощо. Крім того, з допомогою таких моделей з’являється можливість огляду як загальної конструкції протипожежного устаткування, так і будови його окремих елементів в розрізі у будь-якій площині. Трансформований 3D-плакат також піддається зміні масштабу та ракурсу огляду.

Додатковою перевагою застосування 3D-плакатів є можливість почергового огляду окремих елементів модельовано об’єкту. З цією метою пакет Google Sketch Up містить функцію «шари». Для цього при створенні плакату потрібно розміщувати окремі елементи об’єкту в окремих шарах, що надаватиме можливість їх почергового або одночасного виводу на екран.

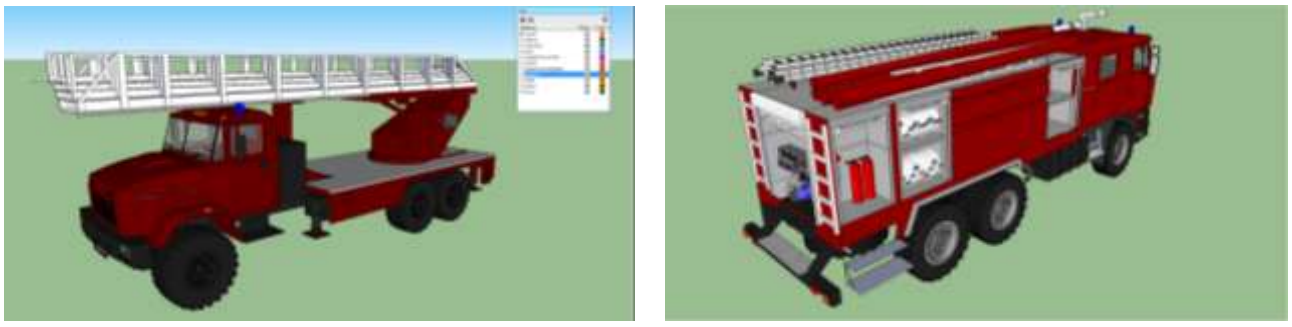


Рис.1. Загальний вигляд 3D-моделей протипожежних автомобілів

Рис. 2. Динамічний огляд 3D-моделей (у тому числі в розрізі)

За умови завантаження 3D-плакатів у віртуальне навчальне середовище, їх використання можливе під час індивідуальної підготовки в домашніх умовах. Це надаватиме можливість закріплювати отримані теоретичні знання під час самостійної роботи, а також ефективно засвоювати новий матеріал у випадку дистанційної форми навчання.

Щодо 3D-віртуального комплексу вивчення дисциплін пожежно-профілактичного циклу, то його створення також націлено на підвищення якості викладання нового теоретичного матеріалу. Застосування комплексу можливе для ознайомлення з особливостями об'ємно-планувальних рішень та проведення віртуальних перевірок протипожежного стану модельованих об'єктів. Реалізація в освітньому середовищі подібного комплексу дозволятиме візуалізувати теоретичний матеріал, інформативність якого полягає лише у висвітлення основних положень нормативних документів. Застосування комплексу надаватиме можливість наочно демонструвати можливі порушення норм та правил пожежної безпеки, що значно активізуватиме роботу та сприйняття студента на занятті.

Під час роботи з моделлю конкретного приміщення можливо вибирати будь-який кут огляду, переміщуватись об'єктом, виконувати заміри, оглядати його елементи, збільшувати зображення без погіршення якості тощо. Власне за рахунок цих можливостей відтворюється задум віртуальної присутності на об'єкті.

В результаті виконання роботи отримано такі висновки:

1. Шляхом комп'ютерного моделювання технічних об'єктів одержано принципово нову технологію навчання у форматі 3D плакатів, яка надає можливість вивчати детальну конструкцію протипожежного устаткування як під час аудиторних занять, індивідуальної підготовки, так і у випадку дистанційної форми навчання.

2. Шляхом комп'ютерного моделювання будівель різнопланового призначення та створення програмної оболонки випадкового генерування індивідуальних завдань одержано 3D віртуальний комплекс вивчення дисциплін пожежно-профілактичного циклу, який надає можливість ознайомлюватись з особливостями об'ємно-планувальних рішень та проводити віртуальні перевірки стану протипожежної безпеки із складанням відповідних документів без необхідності виходу на реальні об'єкти.

Література

1. Козяр М. М. Інтерактивні методики навчання у ВНЗ / М. М. Козяр // Проблеми та перспективи формування національної гуманітарно-технічної еліти : зб. наук. праць. – Харків : НТУ «ХПІ», 2015. - №42(46). – С. 285-292.

2. Гуревич Р. С. Інформаційно-комунікаційні технології в професійній освіті майбутніх фахівців : монографія / Р. С. Гуревич, М. Ю. Кадемія, М. М. Козяр. – Львів : ЛДУБЖД, 2012. – 380 с.

3. Придатко О. В. Інтеграція 3D-інтерактивних технологій навчання в освітні проекти безпеко-орієнтованих спеціальностей / О. В. Придатко, А. Г. Ренкас, Н. Є. Бурак, М. В. Лемішко // Вісник ЛДУБЖД: Зб. наук. праць. Львів: ЛДУ БЖД, 2017. – №15. – С.46-54.

4. Дерев'янчук А. Й. Доцільність використання 3D графіки під час підготовки військових спеціалістів / А. Й. Дерев'янчук, Д. Р. Москаленко // Сучасні інформаційні технології у сфері безпеки та оборони : зб. наук. пр. – К. : Національний університет оборони України імені Івана Черняховського, 2014 – № 2. – С. 119–124.

5. Гумен О. М. Графічні інформаційні технології у підготовці фахівців технологічних спеціальностей / О. М. Гумен, С. Є. Лясковська, Є. В. Мартин // Теорія і методика електронного навчання : зб. нак. пр. – Кривий Ріг : Криворізький національний університет, 2013 – Вип. IV. – С. 65-68.

БЕЗПЕКА ВЕБ-РЕСУРСІВ У КОМП'ЮТЕРНИХ МЕРЕЖАХ

Володимир Лисак, Олександр Белей
Львівський навчально-науковий інститут ДВНЗ «Університет банківської справи», м. Львів

У даній доповіді висвітлюється значимість захисту веб-ресурсів від несанкціонованого проникнення. Також описуються найпопулярніші атаки на веб-сайти та рівні захисту мережі.

Ключові слова: інформаційна безпека, веб-сайт, атака, ієрархія захисту.

This report highlights the importance of protecting web resources from unauthorized intrusion. It also describes the most common attacks on websites and network security levels.

Key words: informational security, website, attack, protection hierarchy.

На сьогоднішній день, людство створює і розвиває технології, які змінюють наше життя. Зокрема, при появі веб-технологій, перевернулись людські уявлення про роботу з інформацією, яка є доступною користувачам інтернету. Із розвитком комерційної і підприємницької діяльності збільшилося число спроб несанкціонованого доступу до конфіденційної інформації, а проблеми захисту інформації виявилися в центрі уваги вчених і спеціалістів. Одним із найважливіших напрямків інформаційної безпеки являється захист веб-ресурсів. Кожного року кількість веб-ресурсів збільшується, так само як кількість конфіденційної інформації, яка збирається на серверах. Частина Інтернету, що є його безпосереднім обличчям, і яка стосується практично кожного користувача – це веб-сайти. Актуальність проблеми безпеки такого виду ресурсів зростає з кожним днем, а більшість вразливостей, що існують на даний момент в цій сфері, пов'язані з помилками і недоліками, допущеними на етапі розробки сайту.

У сучасному світі хакерство є зростаючою загрозою для кожного, починаючи від приватної особи і закінчуючи державною або комерційною установою. Хакери можуть у будь-який момент серйозно вплинути на розвиток подій, незалежно від того, чи це крадіжка приватних даних, контроль над приватним комп'ютером або атака веб-сайту. Щодо останнього, то кожен сайт може послужити для них певним інструментом, наприклад як місце зберігання конфіденційних даних або, принаймні, надати корисні ресурси для надсилання спаму або нападу на інші цілі. Існує цілий ряд інструментів і методів, які використовують для нападів сьогодні. Серед них можна виділити:

1) **Ін'єкції SQL (SQLI).** Багато серверів, які зберігають критичні дані для веб-сайтів і служб, використовують SQL для управління даними у своїх базах даних. Атака SQL інєкції спрямована саме на цей тип сервера, використовуючи шкідливий код, для того, щоб сервер міг розкривати інформацію, яку він, як правило, тримав під захистом. Це особливо небезпечно, якщо сервер зберігає приватну інформацію клієнта з веб-сайту, наприклад номери кредитних карток, імена користувачів і паролі (облікові дані) або іншу особисту інформацію, яка є привабливою та прибутковою ціллю для атакуючого.

2) **Cross-Site Scripting (XSS).** Подібно до атаки на ін'єкцію SQL, ця атака також включає введення шкідливого коду на веб-сайт, але в цьому випадку сама веб-сторінка не зазнає нападу. Навпаки, шкідливий код, який вводить зловмисник, запускається тільки в браузері користувача, коли він відвідує сайт, і цей код діє безпосередньо на відвідувача, а не на веб-сайт. Атаки XSS можуть значно пошкодити репутацію веб-сайту, ставлячи інформацію про користувачів під загрозу без будь-яких вказівок про те, що щось зловмисне навіть сталося.

3) **DDOS.** Якщо ви наводнюєте веб-сайт із більшим обсягом трафіку, ніж було створено для обробки, ви будете перевантажувати сервер веб-сайту, і буде майже неможливим надання його вмісту відвідувачам, які намагаються отримати доступ до нього. Найпоширенішим прикладом атаки DDoS може бути надсилання «тонн» URL-запитів на веб-сайт або веб-сторінку за дуже короткий проміжок часу. Це спричиняє вузькі місця на стороні сервера, оскільки процесор просто вичерпує свої ресурси.

4) **Brutal force.** Метод атаки грубої сили це, по суті, спроби «використати» всі можливі комбінації імені користувача та пароля на веб-сайті. Атаки «брутальної сили» шукають

слабкі паролі для використання та надання хакерам доступу до обраного сайту. Для використання такої форми входу, одразу налаштовуються спеціалізовані скрипти, які постійно намагаються використовувати різні комбінації імені користувача та пароля, доки не буде знайдено відповідність, а атакуючий не отримає доступ.

5) **Symlinking.** Символьне посилання, в основному, є спеціальним файлом, який "вказує" на міцний зв'язок на встановленій файловій системі. Напад на символьні зв'язки виникає, коли хакер розміщує символьне посилання таким чином, що користувач або програма, що має доступ до кінцевої точки, вважає, що отримує доступ до потрібного файлу, коли це насправді не так. Якщо файл кінцевої точки є вихідним, наслідком атаки символьного посилання є те, що його можна змінити у передбачуваному місці. Зміни до файлу кінцевої точки можуть включати додавання, перезапис, пошкодження або навіть зміну дозволів.

Веб-сайти представляють собою потужний інструмент, що дозволяє комерційним, урядовим і громадським організаціям, а також громадянам обмінюватися інформацією та вести справи в мережі Інтернет. З цієї ж причини вони і стають ціллю зловмисників. Як відомо, загроз занадто багато, і треба щось закласти в основу ієрархії захисту. Якщо більшість інцидентів викликають лише роздратування чи незручність, це не означає, що хакер не зможе заподіяти серйозного збитку. Тому кожна організація повинна вжити заходів щодо забезпечення безпеки своїх ресурсів, оцінивши при цьому рівень ризиків і матеріальних витрат. Захист мережі можна розділити на шість рівнів складності:

1) **Встановлення firewall.** Програми firewall контролюють і фільтрують доступ до сервера. Установка міжмережевого екрану між корпоративною (внутрішньою) мережею і веб-серверами загального доступу дозволяє запобігти проникненню в мережу організації: якщо зловмисник проникає на зовнішній веб-сервер, то потрапити в корпоративну мережу організації через firewall йому буде важко.

2) **Видалення зайвих додатків.** Все привілейоване програмне забезпечення, яке є не обов’язковим для веб-сервера, повинне бути вилучене. Під привілейованим в даному випадку розуміється програмним забезпеченням, що працює з мережевими пакетами або запускається з правами адміністратора. Деякі операційні системи запускають привілейовані програми за замовчуванням, а адміністратори часто просто не знають про їх існування. Між тим, кожна така програма може бути використана хакером для атаки на веб-сервер.

3) **Модернізація програмного забезпечення.** Це один з найбільш простих, але, разом з тим, найбільш ефективних способів зменшення ризиків. Проблеми безпеки веб-сайтів найчастіше виникають зі сторони веб серверів, на яких вони працюють. Всі наявні веб-сервери повинні постійно (іноді щодня) перевірятися на предмет оновлення встановленого програмного забезпечення. Ця вимога викликана тим, що будь-яке програмне забезпечення, встановлене на веб-сервері, може бути використане хакером для проникнення в систему.

4) **Використання маршрутизаторів із фільтрацією пакетів.** Маршрутизатори встановлюють для того, щоб відокремити веб-сервери від іншої частини мережі. Цей крок допоможе запобігти багатьом атакам і хакеру залишиться ще менше можливостей для проникнення в мережу.

5) **Системи виявлення вторгнень (IDS).** Системи виявлення вторгнень, що розміщуються на серверах, краще справляються із завданням визначення стану мережі, ніж мережеві IDS. Володіючи всіма можливостями мережевих IDS, у багатьох випадках серверні IDS краще виявляють спроби порушення захисту, так як володіють більш високим рівнем доступу до веб-сервера.

6) **Використання тільки довірених операційних систем і додатків, які працюють під їхнім управлінням.** Функціонуючі програми та операційні системи повинні бути або максимально адаптовані, або розроблені спеціально для специфічних потреб компанії. Це найдорожчий, але водночас і найефективніший спосіб захисту.

Література

1. Захист веб-додатків [Електронний ресурс]. – Режим доступу до ресурсу: http://www.ereading.club/bookreader.php/1012355/DJ-Andrey-sXe_-_Zaschita_veb-prilozheniy.html.

2. Методи проникнення в корпоративні мережі [Електронний ресурс]. – Режим доступу до ресурсу: https://www.kitgsm.com.ua/stati/bezpeka/metodi-proniknennya-v-korporativni-merezhi.html

3. WhiteHat Website Security Statistics Report [Електронний ресурс]. – Режим доступу до ресурсу: http://www.whitehatsec.com/home/resource/stats.html

ДЕЯКІ АСПЕКТИ ІНТЕГРАЦІЇ WEB-СЕРЕДОВИЩА ТА СИСТЕМИ УПРАВЛІННЯ БАЗОЮ ДАНИХ

Андрій Микитин
Івано-Франківський національний технічний університет нафти і газу, м. Івано-Франківськ

Проаналізовано трирівневу архітектуру засобів інтеграції WEB-середовища та системи управління базою даних.

Ключові слова: WEB-середовище, система управління базою даних (СУБД), засоби інтеграції, трирівнева архітектура

The three-level architecture of WEB-environment integration tools and database management systems was analyzed.

Keywords: WEB-environment, database management system (DBMS), integration tools, three-level architecture.

Комплексний підхід до створення автоматизованих систем (АС) обробки інформації, як WEB-сторінки, охоплює: якісний аналіз даних у предметній сфері, концептуальне моделювання бази даних [1]; обгрунтування критеріїв вибору бази даних, системи управління базою даних, мови програмування; програмне забезпечення (ПЗ); захист інформації в АС. Етап розроблення ПЗ передбачає інтеграцію СУБД у WEB-середовище, застосування архітектури засобів інтеграції. У контексті розроблення ПЗ розглянемо основні компоненти WEB-середовища і трирівневу архітектуру засобів інтеграції WEB та СУБД.

WEB-середовище складається з мережі комп'ютерів, які можуть діяти або як сервери, що надають інформацію, або як клієнти (браузери), що реалізують запит інформації. Основна частина інформації в Web-середовищі зберігається в документах, створених на мові HTML. За допомогою протоколу HTPP відбувається обмін інформацією між WEB-сервером і браузером. Схема взаємодії основних компонентів WEB-середовища представлена на рис. 1.

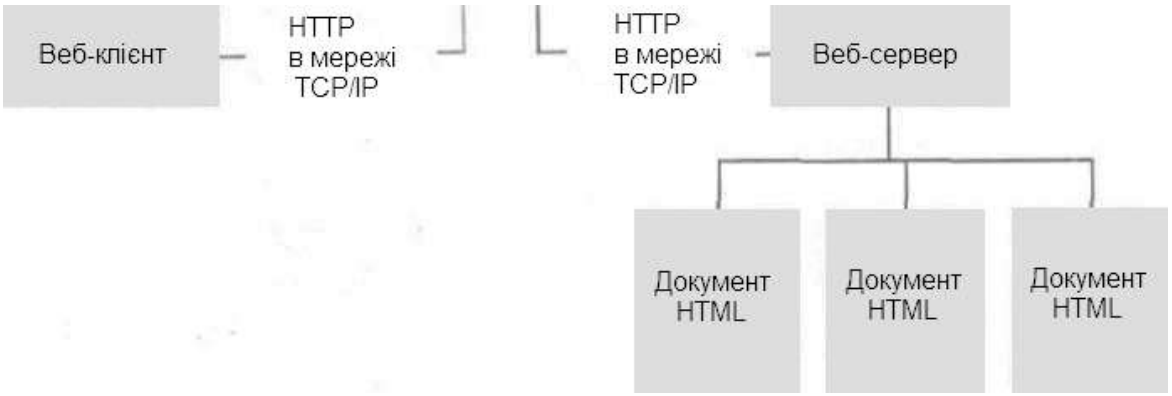


Рис. 1. Основні компоненти WEB-середовища

Протокол HTTP діє за принципом запит-відповідь, тому будь-яка транзакція HTTP складається з етапів: підключення – клієнт встановлює з'єднання з WEB-сервером; запит – клієнт надсилає Web-серверу повідомлення із запитом; відповідь – WEB-сервер надсилає клієнтові відповідь; закриття – з'єднання з Web-сервером закривається. WEB-середовище**,** як платформа**,** використовується з метою надання користувачам інтерфейсу для роботи з однією/ декількома БД. Вимоги щодо інтеграції у WEB-середовище: можливість захищеного доступу до корпоративних даних; спосіб підключення, що не залежить від даних і розробника ПЗ, що забезпечує необхідний вибір СУБД; можливість взаємодії з БД, незалежно від типу використовуваних браузера, Web-сервера; відкритість архітектури, що дозволяє взаємодіяти з різними системами і технологіями; підтримка транзакцій, які охоплюють декілька запитів http; підтримка аутентифікації на рівні сеансу і додатку.

Трирівнева архітектура засобів інтеграції Web і СУБД (рис. 2) характеризується трьома рівнями ПЗ, кожен з яких може функціонувати на різних платформах: рівень користувальницького інтерфейсу, який розташовується на комп'ютері кінцевого користувача (клієнт); рівень реалізації прикладних алгоритмів і засобів обробки даних. Цей проміжний рівень розташовується на сервері, який часто називається сервером додатків; СУБД, в якій зберігаються дані, необхідні для

функціонування проміжного рівня. Цей рівень може бути реалізований на окремому сервері, який називається сервером бази даних. Клієнт відповідає тільки за користувальницький інтерфейс і, можливо, виконує деяку дуже просту обробку даних, наприклад перевірку введеної інформації, тому клієнтська частина додатку може бути побудована з використанням так званого «тонкого» клієнта. Основні прикладні алгоритми реалізовані на окремому рівні, на сервері додатків, який фізично пов'язаний з клієнтом і сервером БД за допомогою локальної/ розподіленої обчислювальної мережі. При цьому передбачається, що один сервер додатків може обслуговувати безліч клієнтів.

Трирівнева архітектура має переваги перед одно- і дворівневою моделями, серед яких: "тонкий" клієнт, для якого потрібне недороге апаратне забезпечення; централізація супроводу додатків завдяки передачі засобів реалізації прикладних алгоритмів, застосовуваних численними кінцевими користувачами, на єдиний сервер додатків; додаткова модульність, яка спрощує модифікацію або заміну ПЗ кожного рівня без надання впливу на решту рівнів; відділення основних засобів реалізації прикладних алгоритмів від функцій БД спрощує задачу рівномірного розподілу навантаження.

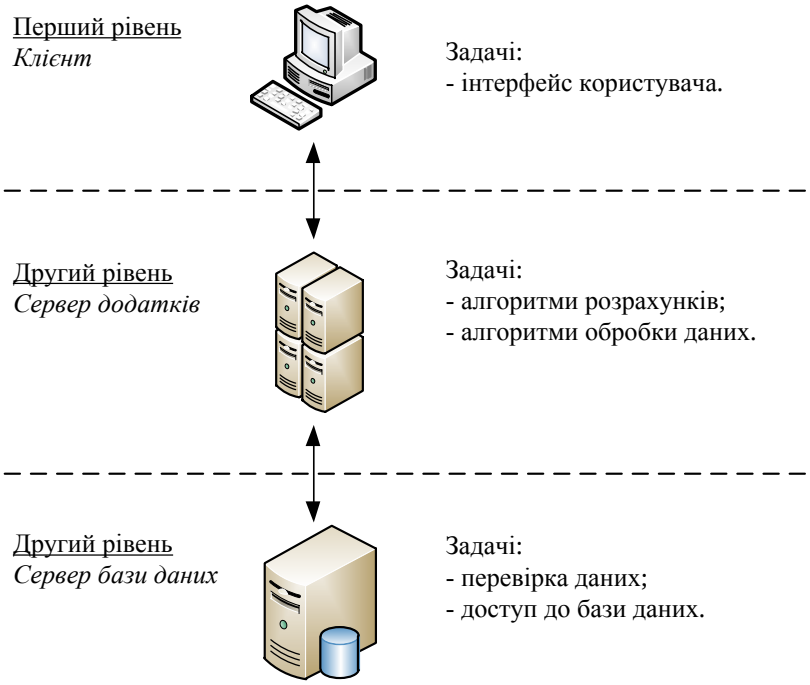


Рис. 2. Трирівнева архітектура

Трирівнева архітектура засобів інтеграції є ефективною, оскільки: природно вписується в WEB-середовище, де браузер виконує функції «тонкого» клієнта, а WEB-сервер – сервера додатків.; може бути розширена до багаторівневої архітектури з додатковими рівнями, які дозволяють підвищити гнучкість і масштабованість створюваних додатків. Інтерфейс АС може бути реалізований мовою програмування PHP, як однієї з широко застосовуваних мов сценаріїв з відкритим вихідним кодом, оператори якої можуть вбудовуватися в код HTML. Вона підтримується багатьма Web-серверами, включаючи HTTP-сервер Apache та Internet Information Server. Загальне функціонування АС, як WEB-сторінки, може дійснюватися на основі технології Apache-MySQL-PHP.

Література

1.Коннолли Т., Бегг К., Страчан А. Базы данных: проектирование, реализация, сопровождение. Теория и практика, 2-е изд.: Пер. с англ.: Уч. Пос. - М.; СПб.: Издательский дом «Вильямс», 2000. – 1120с.

ЗАБЕЗПЕЧЕННЯ ПЕРЕДАЧІ ДАНИХ В БПЛА

Костянтин Мирончук, Олег Вацлавик
Львівський державний університет безпеки життєдіяльності, м. Львів

Наукові відкриття і технологічний розвиток займають вагоме місце в історичному розвитку усіх прогресуючих країн. У зв'язку із ситуацією, яка склалася у нашій країні, ми потребуємо кардинальних рішень і нових ідей для збереження географічної цілісності України. Важливим чинником можуть стати нові розробки безпілотних літальних апаратів, дронів.

Ключові слова: дрон, атака, зв'язок.

Scientific discoveries and technological development occupy an important place in the historical development of all progressive countries. Due to the situation prevailing in our country, we need radical solutions and new ideas for preserving the geographical integrity of Ukraine. An important factor may be the development of unmanned aerial vehicles, drones.

Key words: drone, attack, connection.

Дрони виконують різноманітті завдання, вони вже давно підкорили військову сферу. Так, за думками фахівців, до 2020 року третина військових літаків в розвинених державах стануть "безлюдні"- зменшиться використання кількості людських ресурсів, адже ніякий комп'ютер не зрівняється з людиною в прийнятті рішень в нестандартних ситуаціях.

Одним з перспективних напрямків в області інтелектуальних технологій управління та обробки інформації є розробка безпілотних літальних апаратів (БПЛА). Надійна і безпечна інформаційна взаємодія за допомогою каналу передачі даних між об'єктом і наземною станцією управління являється обов'язковою частиною функціонування комплексу, що включає БПЛА і наземну інфраструктуру управління БПЛА і обмін даними з ним здійснюється по бездротових каналах, в тому числі через Інтернет, що вимагає особливих заходів щодо захисту інформації.

Особливості сучасних бездротових технологій зв'язку вимагають в певних ситуаціях посилення існуючих стандартних засобів захисту даних. Основними вимогами, які пред'являються до сучасних систем шифрування, є вимоги надійності, швидкості, простоти реалізації і використання. З урахуванням специфіки каналу передачі даних БПЛА - НСУ потрібні швидкі і не потребуючі значної обчислювальної потужності і великого обсягу пам'яті. Для забезпечення надійності каналів передачі даних доцільно використовувати комплексний підхід, що включає програмні, апаратні та змішані кошти захисту.

Основною проблемою, розвитку та прогресу БПЛА, є забезпечення передачі даних по каналах зв'язку між "безпілотником" і будь-яким пунктом управління. Для розв'язання цієї проблеми потрібно збільшити пропускну здатність і завадостійкість каналів передачі інформації, а також зосередити на борту БПЛА пристрої, що працюють в сонному режимі без необхідності постійного обміну інформацією. Наступною проблемою є вразливість самих каналів передачі даних. Ця проблема розв'язується за рахунок закриття ліній зв'язку, застосування автономних БПЛА, використання супутникових ретрансляторів і т.п. Ще одна організаційна і технічна проблема полягає в необхідності сумісного застосування угруповання БПЛА в єдиних бойових порядках, а також сумісно з пілотованими літальними апаратами.

Література

1. Куряча О. «Роботы на поле боя. Солдаты завтрашнего дня» // Robotics.1. - URL: http://robotics.com.ua/shows/series_robots_and_humans/572-robots_on_the_battlefield_soldiers_of_tomorrow

2. Корсунский А.С., Маттис А.В., Масленникова Т.Н. «О некоторых аспектах защиты информации в беспилотных и роботизированных средствах военного назначения» // Морские информационно-управляющие системы. − 2012. − No 1. − С. 16−23

ЗАГРОЗИ ТА НЕБЕЗПЕКИ У ВИКОРИСТАННІ ІНТЕРНЕТ-БАНКІНГУ

Ольга Новосядла, Олександр Белей
Львівський навчально-науковий інститут ДВНЗ «Університет банківської справи», м.Львів

У даній роботі досліджено сутність та сучасний стан розвитку інтернет-банкінгу, зокрема розглянуто питання безпеки користування його послугами. Досліджено питання загроз та небезпек у використанні інтернет-банкінгу, а також дано головні поради щодо безпечного користування платіжними інтернет серверами.

Ключові слова: загрози, інтернет-банкінг, фішинг, безпека, вішинг, PIN-код, пароль, сервер.

In this work the essence and the current state of development of Internet banking are investigated, in particular the questions of safety of its services are considered. The issue of threats and risks of using Internet banking has been explored, and the main advice for safe use of payment Internet servers are given.

Keywords: threats, internet-banking, fishing, security, vishing, PIN-code, passwords, server.

В сучасному світі, де інтернет став невід'ємною частиною нашого життя і банківська сфера теж стрімко розвивається, з'явилось таке поняття як internet-banking, яке характеризує себе як систему управління банківськими рахунками. Актуальність дослідження теми інтернет-банкінгу обумовлена збільшенням кількості банків, які пропонують таку послугу. А також збільшується кількість людей, які починають активно користуватися наданими їм можливостями.

Вперше, банк, що обслуговує клієнтів через Інтернет, з'явився в 1995 році. Ним був Security First Network Bank. В Україні першим, хто започаткував обслуговування клієнтів через інтернет у 1999 році став ПриватБанк. Успіх технології спонукав банк розробити систему Приват24. Вже за кілька років потому її користувачі змогли отримувати електронні виписки, перевіряти баланс банківського рахунку, переказувати кошти між рахунками та поповнювати мобільний телефон. З розвитком цієї технології все більше і більше людей починало користуватися нею.

Сьогодні, кількість клієнтів інтернет-банкінгу в Європі й США вже перевищила за 120 млн. людей, а європейський оборот інтернет-банкінгу перевищує 5 млрд. євро. За останні 5 років ПриватБанк збільшив кількість своїх клієнтів на 300 тис. осіб за допомогою технологій інтернет-банкінгу.

Втім, разом з банківськими клієнтами користуватися сервісами банків стали й шахраї. Вони застосовують схему викрадень чужих грошей в інтернеті, теж не встаючи з дивану. Постає питання безпеки інтернет-банкінгу та надійності його використання. Кількість випадків крадіжки коштів через Інтернет тільки за минулий рік зросло більш ніж у два рази, незважаючи на те, що на ринок виходять все нові засоби захисту. Чи може людина бути впевненою, що завтра вона не стане черговою жертвою, і з її рахунку не зникнуть усі гроші? Звісно, засоби захисту інформаційних технологій розвиваються так само стрімко як і нововведення. Однак, не можна виділити єдиного способу чи технології, що надавали б 100% гарантії безпеки від зловмисників.

Жоден з нас не хоче стати жертвою шахраїв, кожен прагне захистити свої кошти та бути впевненим у надійності того чи іншого сервера при його використанні. Для того, щоб бути готовим до можливої небезпеки при користуванні інтернет-банкінгом, потрібно підвищувати свою обізнаність у цій сфері. Сьогодні, у відділах банків працівники пропонують клієнтам буклети із правилами, на офіційних сайтах можна знайти детальні інструкції щодо правильного користування інтернет-серверами, створюються різноманітні рекламні ролики, в яких даються певні рекомендації до застосування захисних заходів.

Перед тим як розглядати засоби захисту, слід визначити з яких сторін існує можливість небезпеки і яких загроз варто побоюватись. При створені систем інтернет-банкінгу, традиційно виділяють загрози порушення конфіденційності та цілісності електронних платежів, проте після введення електронного підпису і застосування засобів шифрування вони були вирішені. Часто виникає проблема захисту від несанкціонованих платежів, що може здійснюватися через заражений комп'ютер: в результаті вірусної атаки зловмисника,

що намагається «вкрасти» пароль, чи визначає його після того як користувач самостійно вводить дані на підробленому сайті. Отож, користувачеві слід уважно стежити за наявністю сертифіката безпеки, тобто перевіряти канал по якому проходить зв'язок з банком. Безпосередньо, в банку для забезпечення захисту транзакції часто використовують прилади, програмним забезпеченням яких неможливо маніпулювати, наприклад SafeTouch.

Додатковий захист інтернет-банкінгу забезпечує строге регламентування числа операцій. Наприклад, банк повинен автоматично скидати з'єднання, якщо користувач певний час не проводив жодних операцій – таким чином нікому не вдасться скористатися відкритим вікном браузера чи додатком у смартфоні за відсутності власника.

Війна за безпеку користувача - це перш за все інформаційна війна. Більшість інтернет-банків володіє гідними заходами безпеки, проте вони можуть не спрацювати, якщо користувачу не правильно пояснити як ними користуватися та яких небезпек він повинен уникати.

Одним із найпопулярніших та найвідоміших способів інтернет шахрайства – є фішинг або «Банківська афера». Концепція цього методу полягає у тому, що шахрай будь-яким можливим способом намагається витягнути з власника картки інформацію. Це може бути підроблений лист, наприклад, від банку або платіжної системи, клієнтом якої є власник, із проханням так чи інакше повідомити інформацію, за допомогою якої зловмисник може отримати доступ до коштів – запит PIN-коду, логіна, пароля тощо.

Ще один відомий спосіб шахрайства – є вішинг. Для даного типу шахрайства використовується технологія передачі мовного сигналу через мережі Інтернет Voip (Voice over IP). Скажімо, на ваш телефон надходить дзвінок від представника банку або автоматичного інформатора про те, що ваш рахунок був заблокований, і вам необхідно перевести телефон у тоновий набір і ввести PIN-код доступу до картки. В даному випадку, не слід одразу реагувати на даний дзвінок та вводити PIN-код. Переконайтесь, що дана ситуація дійсно існує, зателефонувавши до банку. Як правило, вішери здійснюють не один дзвінок, а декілька. У першій розмові вони витягають конфіденційну інформацію, потім відволікають, заспокоюють пильність користувача повторним дзвінком, повідомляючи, що проблема розв'язалася, тим самим виграючи час, щоб потерпілий не зателефонував у банк і не заблокував картку. Цей вид шахрайства більше націлений на Європу та Сполучені штати, де телефон широко використовується для рекламних повідомлень, дзвінків співробітників банків та інших компаній.

Кожній людині, що користується інтернет-банкінгом слід дотримуватись кількох порад, з якими вона може почувати себе та свої кошти у безпеці: не передавати стороннім інформацію про себе та свою платіжну картку, не вводити паролі та PIN-коди на підозрілих сайтах та регулярно перевіряти стан свого рахунку.

Отож, тема загроз та небезпек у використанні інтернет-банкінгу є дуже важливою. Виникає потреба у постійному її дослідженні, аналізуванні та вивчені. Оскільки ми все частіше починаємо користуватися цією системою, тим частіше виникає питання захисту від шахрайства у цій сфері. Як банки, так і люди, у цьому серйозному питанні, є зацікавленими сторонами. З кожним роком росте кількість розрахунків, що здійснюється через мережу інтернет, банки, в свою чергу, докладають чимало зусиль, аби зробити цей процес якомога безпечнішим та надійнішим, а також максимально інформують людей про різноманітні методи захисту розрахунків.

Література

1. ИТ в банках и страховых компаниях [Електронний ресурс] // CNA. – 2012. – Режим доступу до ресурсу: http://www.cnews.ru/reviews/free/banks2012/index.shtml

2. Інтернет-шахрайство з платіжними картками та методи захисту від нього [Електронний ресурс] // інформаційно-аналітичний портал 0Українського агентства фінансового розвитку – Режим доступу до ресурсу: http://www.ufin.com.ua/analit_mat/poradnyk/094.html

3. Як користуватися інтернет-банкінгом.. [Електронний ресурс]. – 2016. – Режим доступу до ресурсу: https://vn.20minut.ua/infographics/yak-koristuvatisya-internet-bankingom-schob-shahrayi-ne-distalis-do-va-10563744.html

ЗАХИСТ ІНФОРМАЦІЇ ЯК ОДИН З КЛЮЧОВИХ ІНСТРУМЕНТІВ У ДОСЯГНЕННІ БЕЗПЕКИ ЖИТТЄДІЯЛЬНОСТІ

Софія Огурчак, Тарас-Михайло Фірман
Львівський національний університет імені Івана Франка, м.Львів

Задоволення потреб в інформації призводить до інформованості особистості, суспільства та держави та оволодіння відомостями про процеси та явища ,що відбуваються у світі. Інформаційна безпека має велике значення для забезпечення життєво важливих інтересів будь-якої держави, зокрема охорони безпеки довкілля.

Ключові слова: захист інформації, загрози, інформаційна безпека, система захисту інформації.

Satisfying the information needs leads to awareness of the individual, society and the state and to capture information about the processes and phenomena occurring in the world. Information security is essential for the vital interests of any state, in particular environmental protection.

Key words: information protection, threats, information security, information security system.

Створення розвиненого і захищеного середовища є неодмінною умовою розвитку суспільства та держави, в основі якого повинні бути найновіші автоматизовані технічні засоби.

Останнім часом в Україні відбуваються якісні зміни у процесах управління на всіх рівнях, які зумовлені інтенсивним упровадженням новітніх інформаційних технологій. Однак швидке вдосконалення інформатизації зумовило крім безперечних переваг, появу низки стратегічних проблем. Посилюється небезпека несанкціонованого втручання в роботу комп'ютерних, інформаційних і телекомунікаційних систем. Збій в системі, викликаний цим, може призвести до численних аварій, катастроф, стихійних лих, порушень в технологічних процесах компаній та підприємств.

Рівень актуальності проблеми захисту інформації від різних загроз, можна побачити на прикладі даних, опублікованих Computer Security Institute (Сан-Франциско, штат Каліфорнія, США), згідно з якими порушення захисту комп'ютерних систем відбувається з таких причин:несанкціонований доступ — 2 %, укорінення вірусів — 3 %; технічні відмови апаратури мережі — 20 %; цілеспрямовані дії персоналу — 20 %; помилки персоналу (недостатній рівень кваліфікації) — 55% [5].

Таким чином, однією з потенційних загроз для інформації в інформаційних системах слід вважати цілеспрямовані або випадкові деструктивні дії персоналу (людський фактор), оскільки ,на мою думку,вони становлять 75 % усіх випадків. Це у свою чергу може призвести до фатальних наслідків,що порушать безпеку праці та мирне життя мільйонів людей.

Інформаційну безпеку можна поділити на такі поняття щодо забезпечення стану захищеності:

– особистості, суспільства, держави від впливу неякісної інформації;

– інформації та інформаційних ресурсів від несанкціонованого впливу сторонніх осіб;

– інформаційних прав і свобод людини і громадянина.

Інформаційна безпека – це одна із сторін розгляду інформаційних відносин у межах інформаційного законодавства з позицій захисту життєво важливих інтересів особистості, суспільства, держави та акцентування уваги на загрозах цим інтересам і на механізмах усунення або запобігання таким загрозам правовими методами [7].

Інформаційна зброя – сукупність спеціально організованої інформації та інформаційних технологій, яка дозволяє цілеспрямовано змінювати (знищувати, спотворювати), копіювати, блокувати інформацію, долати системи захисту, обмежувати допуск законних користувачів, здійснювати дезінформацію, порушувати функціонування носіїв інформації, дезорганізовувати роботу технічних засобів комп’ютерних систем та інформаційно-обчислювальних мереж, що застосовується в ході інформаційної війни (боротьби) для досягнення поставлених цілей [3].

Загроза несанкціонованого доступу — це подія, що кваліфікується як факт спроби порушника вчинити несанкціоновані дії стосовно будь-якої частини інформації в інформаційній системі [4].

Вимоги національних стандартів і нормативних документів з питань технічного захисту інформації в Україні, а також досвід розвитку міжнародних стандартів безпеки досліджено у працях О.М. Юрченка, В.В. Домарева, М.С. Вертузаєва.

Основні загрози інформаційній безпеці – сукупність умов і факторів, що створюють небезпеку життєво важливим інтересам особистості, суспільства і держави в інформаційній сфері [4].

Система захисту інформації є інструментом адміністраторів інформаційної безпеки, які виконують функції із забезпечення захисту інформаційної системи і контролю її захищеності.

Система захисту інформації повинна виконувати такі функції:

– реєстрація і облік користувачів, носіїв інформації, інформаційних масивів;

– забезпечення цілісності системного та прикладного програмного забезпечення та інформації яка оброблюється;

– захист комерційної таємниці, включаючи використання сертифікованих засобів криптографічного захисту;

– створення захищеного електронного документообігу з використанням сертифікованих засобів криптографічні перетворення і електронного цифрового підпису;

– централізоване управління системою захисту інформації;

– управління доступом;

– забезпечення ефективного антивірусного захисту, тощо[4].

Захист на технологічному рівні (програмний продукт і технічні засоби обробки інформації) повинен бути автономним, але забезпечувати реалізацію єдиної політики безпеки і будуватись на основі використання сукупності вбудованих систем захисту операційної системи і систем управління базами даних та знань.

На локальному рівні організується розподілення інформаційних ресурсів на сегменти за рівнями конфіденційності по територіальному і функціональному принципах, а також виділяється в окремий сегмент засоби обробки конфіденційної інформації. Підвищенню рівня захищеності сприяє обмеження і мінімізація кількості точок входу/виходу (точок взаємодії) між сегментами, створення надійної оболонки по периметру сегментів і інформаційної системи в цілому, організація захищеного обміну інформацією між сегментами.

На мережевому рівні організується захищений інформаційний обмін даними між автоматизованими робочими місцями.

Усі загрози безпеки, спрямовані проти програмних і технічних засобів інформаційної системи, впливають на безпеку інформаційних ресурсів і призводять до порушення основних властивостей інформації, яка зберігається і обробляється в системі.

Як правило, загрози інформаційній безпеці розрізняються за способом їх реалізації. Дослідження і аналіз численних випадків впливів на інформацію і несанкціонованого доступу до неї показують, що їх можна розділити на випадкові і навмисні.

Навмисні загрози можуть бути реалізовані шляхом довготривалої масованої атаки несанкціонованими запитами або вірусами тощо. Наслідки такі: руйнування (втрата) інформації, модифікація (зміна інформації на помилкову, яка коректна за формою і змістом, але має інший сенс) і ознайомлення з нею сторонніх осіб. Попередження зазначених наслідків в інформаційній системі є основною метою створення системи безпеки інформації, розроблення та вдосконалення існуючих методів захисту інформації в інформаційно-комунікаційних системах та мережах.

Оцінка вразливості інформаційної системи і побудова моделі впливів припускають вивчення всіх варіантів реалізації перерахованих вище загроз і виявлення наслідків, до яких вони призводять.

Принцип розмежування інформаційних потоків може мати місце при записі секретної інформації на несекретні носії і в несекретні файли, її передачі програмам і процесам, які не призначені для обробки секретної інформації, а також при передачі секретної інформації по незахищених каналах зв'язку, необхідно здійснювати відповідне розмежування інформаційних потоків.

Принцип персональної відповідальності передбачає, що кожен користувач повинен нести персональну відповідальність за свою діяльність в системі, включаючи будь-які операції з конфіденційною інформацією і можливі порушення її захисту.

Принцип цілісності засобів захисту передбачає, що засоби захисту інформації в ІКСМ повинні чітко виконувати свої функції у відповідності з переліченими принципами і бути ізольованими від користувачів, а для свого супроводу повинні включати спеціальний захищений інтерфейс для засобів контролю, сигналізації про спроби порушення захисту інформації і впливу на процеси в системі.

Реалізація перелічених принципів здійснюється з допомогою так званого «монітору звернень», який контролює будь-які запити до даних чи програм з боку користувачів (чи їх програм) за установленими для них видами доступу до цих даних і програм. Найбільш розповсюджена модель отримала назву – багаторівнева модель захисту Белла Ла Падула. Основою цієї моделі є поняття рівня конфіденційності (форми допуску) і категорії (прикладної області) суб'єкта і об'єкта доступу. На основі присвоєних кожному суб'єкту і об'єкту доступу конкретних рівнів і категорій в моделі визначаються їх рівні безпеки, а потім встановлюється їх взаємодія [4] .

Розмежування доступу в ІКСМ полягає в розділенні інформації на частини і організації доступу до неї користувачів відповідно до їх функціональних обов'язків і повноважень. Завдання такого розмежування доступу до інформації: скорочення кількості користувачів, що не мають до неї відношення при виконанні своїх функцій, тобто захист інформації від порушника серед законних користувачів.

В результаті вище викладеного, можна зробити висновок: безпека в інформаційно-комунікаційних системах повинна підтримуватися на належному рівні,регламентуватися відповідними законами та бути під пильним наглядом відповідних владних структур,оскільки нехтування нею може призвести до небачаних досі наслідків,що порушать функціонування виробничих процесів і ,звісно ж, мирне життя мільйонів людей по усьому світу .

Література

1. Закон України «Про інформацію» від 02.10.1992 № 2657-XII

2. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 05.07.1994 № 80/94-ВР

3. Гончарова Л.Л. Возненко А. Д. «Основи захисту інформації в телекомунікаційних та комп'ютерних мережах» [Електронний ресурс].- Режим доступу :

http://lib.detut.edu.ua/files/Nauk_trud_vukladahiv/Fakultet%20Infrastruktur_ruxomuy_sklad%20"/Kafedra_tel_texn_avtomatuka/nauk_trud_voznenko.pdf

4.[Електронний ресурс].- Режим доступу :

http://pidruchniki.com/13670622/informatika/zahist_informatsiyi_informatsiynih_sistemah

5.[Електронний ресурс]. - Режим доступу: http://e-works.com.ua/work/2563_Zahist_informacii_ta_informacii-na_bezpeka.html

СЕЛФІМАНІЯ – НОВА ЗАГРОЗА КІБЕРПРОСТОРУ

Юлія Приходько, Олег Вацлавик
Львівський державний університет безпеки життєдіяльності, м. Львів

У статті обґрунтовано актуальність удосконалення використання біометричних даних для ідентифікації користувачів у різних сервісах і системах. Визначено найзручніші способи ідентифікації – селфі-авторизація. Встановлено, що дана ідентифікація безпечна, і головне, вигідніша для клієнта, але вимагає від банків і платіжних вендорів більшою мірою безпеки.

Ключові слова: селфі, банк, валідація, ідентифікація.

The article substantiates the relevance of improving the use of biometric data to identify users in various services and systems. Identified the most convenient ways of identification - selfi- authorization. It is established that such identification is safe, and most importantly, more profitable for the client, but requires banks and payment vendors more security.

Key words: selfi, bank, validation, identification.

Сьогодні банки та банківська сфера, шукають шляхи для захисту даних своїх клієнтів за допомогою впровадження сервісів. Розробники нешкідливого ПЗ обирають як класичні методики, так і досить своєрідні — авторизація за сприянням селфі.

Біометрична ідентифікація є модерним трендом на ринку платежів у всьому світі, оскільки завбачає посилену безпеку. Біометрична ідентифікація може розглядатися як «чиста» біометрична автентифікація, але її набагато складніше застосовувати через складність пошуку в біометричній базі даних: кожний з біометричних зразків повинен бути порівняння з кожним записом з бази даних. Платіж засвідчується або натисканням в смартфоні, або за допомогою селфі. У будь-якому інциденті та стороні банку має існувати сховище біометричних даних клієнтів. У момент прийняття платежу здійснюється контроль цих даних зі смартфона з банком біометричних даних. Дана ідентифікація безпечна, і головне, вигідніша для клієнта, ніж наявні зразки, але вимагає від банків і платіжних вендорів більшою мірою безпеки. Це пов'язано з тим, що річ йде вже про біометричну інформацію клієнта, яка у разі витоку даних може бути використана не тільки в меті фінансового шахрайства, а й не фінансовій меті до клієнта.

Так, наприклад, одна з найбільших фінансових компаній світу – Mastercard, запропонувала своїм клієнтам новий вид верифікації. За допомогою нової технології користувачі зможуть забути про паролі і здійснювати виключно біометричні платежі. Користувачу-клієнту треба встановити на смартфон, планшет або ПК спеціальний додаток-розширення Mastercard Selfi Pay та пройти перший рівень валідації – загрузити своє фото. Згодом виконуються алгоритми, за допомогою яких система обробляє отриману інформацію і відтворює рідкісний код. Фото можна зробити в меню оплати, потім інформація шифрується і передається в систему MasterCard, яка порівнює її з унікальним кодом клієнта, що був згенерований на першому рівні при підтвердженні платежу. Для мінімізації несанкціонованого доступу до рахунків клієнтів потрібно здійснити найпростіші маніпуляції обличчям – моргнути або посміхнутися одразу в самому додатку. Для нетрадиційних випадків у MasterCard є Masterpass - система дворазової авторизації, яка при спробі оплати зажадає від покупця ввести код, надсилається в SMS або записаний на скретч-карті. Система Masterpass як правило активується, якщо у системи виникають підозри в тому, що транзакція шахрайська. Також, деякі сайти викликають її примусово. Тепер же, любителі Селфі і всі інші зможуть замість введення пароля позувати перед камерою, трохи позалицятися до неї, або прикласти палець до сканера - якщо у них смартфон відповідного класу.

Платіжні системи та провайдери планують повне введення таких служб, а вихід на клієнтуру України може відбутися при існуванні задовільної кількості пристроїв, які підтримують такі техніки ідентифікації. До того ж, дуже важливою є наявність законодавчої бази, щоб біометрична ідентифікація була очевидним способом ідентифікації клієнта і могла бути використана в судовій практиці при виникненні сперечань.

Захист безпеки безготівкових виплат і зберігання персональних даних клієнтів є одним з основних задач. Упевненість користувачів у своїй грошовій безпеці при проведенні виплат безпосередньо впливає на вибір ними платіжного інструменту.

Для вирішення цього завдання використання біометричних даних для ідентифікації користувачів в різних сервісах і системах є світовим трендом. Технології біометричної ідентифікації в своїх сервісах вже вживають такі велетні, як Google Pay, Samsung Pay та інші. Компанія MasterCard, яка є одним зі світових лідерів платіжної індустрії, повністю дотримується цих тенденцій.

Під час селфі-авторизації система безпеки банку порівнює отримане зображення із фото клієнта в інформаційній базі банку. Система дозволяє чітко відокремлювати реальні фото клієнтів від підроблених зображень. Також у банку зазначають, що величезна популярність селфі серед користувачів дасть можливість не тільки проводити авторизацію клієнтів у зручному та приємному для них форматі, але й у майбутньому проводити конкурси селфі серед клієнтів Банку, звісно, за їх згоди.

Але чи буде подібна "Селфі процедура" більш популярна, ніж підтвердження операції за допомогою відбитка пальця, покаже час. А найголовніше, щоб швидкість створення подібних технологій аж ніяк не позначалася на питаннях безпеки. Адже не можна недооцінювати шахраїв, які з радістю почнуть експериментувати з фотографіями осіб, 3D печатками відбитків пальців і т.д.

Так, у 2018 році користувачі Mastercard в Україні можуть скористатись послугами Selfi Pay в одному з сервісів Приват24. Перевагою своєї нової технології в банку обґрунтували так: селфі зараз неймовірно популярні, а тому і клієнти зможуть здійснити авторизацію в приємному для них форматі, і можливість здійснення будь-яких шахрайських дій зведеться до нуля. Станом на сьогодні система верифікації Приватбанку вже використовує одну з трьох складових Selfi Pay – ідентифікація відбитку пальців.

Також, не потрібно забувати про те, що разом із простотою підтвердження фінансових операцій виникає загроза кіберпростору, тому що багато людей поширюють свої фото/відео у соціальних мережах, які злочинці можуть використати для складання математичних 3D-моделей та проходження верифікації, для отримання неправомірної вигоди. Тому потрібно звернути увагу на створення додаткових алгоритмів для покращення систем отримання, обробки та генерування інформації, та нових документів міжнародного права для регулювання відносин «користувач-компанія».

Література

1. Про захист персональних даних [Текст] : Закон України від 2 червня 2010 року № 2297-V. [Електронний ресурс]. - Режим доступу: http://www.president.gov.ua/documents/11965.html.
2. Про інформацію [Текст] : Закон України від 10.08.2012 року № 2657-XII [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/2657-12.
3. Про затвердження Типового порядку обробки персональних даних у базах персональних даних : Закон України від 30.12.2011 року №3659/5 . [Електронний ресурс]. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/z0001-12.
4. [Електронний ресурс]. – Режим доступу: http://stop-x-files-ua.org/pryvatbank-zapustyv-selfi-avtoryzatsiyu/
5. [Електронний ресурс]. – Режим доступу: http://channel4it.com/publications/Kogda-selfi-stanovitsya-poleznym-avtorizaciya-platezhey-avtoportretom-18615.html#

ДОСЛІДЖЕННЯ ХАРАКТЕРИСТИК ТА ПРИНЦИПІВ РОБОТИ ІНФОРМАЦІЙНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Кирило Ржавський, Євген Мартин
Львівський державний університет безпеки життєдіяльності, м.Львів

В роботі проведено аналі існуючого програмного забезпечення з метою створення анімації для попередньо розробленої моделі пожежного автомобіля, яка може бути використана при вивченні дисциплін пожежно-рятувального спрямування.

Ключові слова: Програмне забезпечення, аналіз

The analysis of the software was carried out in order to create animation for a pre-designed model of a fire truck. The model can be used in the study of disciplines of fire and rescue direction.

Keywords: software, analysis

В процесі навчання за напрямком пожежної безпеки від майбутнього фахівця вимагається досконале знання своєї галузі діяльності, зокрема, як працює те чи інше пожежно-рятувальне обладнання та техніка, у тому числі як влаштований пожежний автомобіль того чи іншого призначення. У зв'язку з недосконалістю та обмеженістю пожежно-навчальної бази, та, зважаючи на стрімкий розвиток комп'ютерних технологій, є доцільним використання спеціалізованого програмного забезпечення у навчальному процесі.

Враховуючи специфіку навчального процесу пожежних-рятувальників, слід розуміти потреби та принципи, які мусять задовольняти програмне забезпечення. Саме тому воно повинно відповідати наступним критеріям:

1. Простота використання:
- логічний та зрозумілий інтерфейс;
- доступність та точність інструкцій роботи з програмним забезпеченням.
2. Постійна підтримка та оновлюваність матеріальної бази:
- постійне оновлення матеріальної бази додаванням до неї інформації про нове пожежного обладнання;
- систематичне оновлення програмного забезпечення з додаванням до неї нового функціоналу та покращення роботи існуючого.
3. Доступність.
4. Надійність.
5. Мультиплатформеність.

Говорячи про мультиплатформеність, маємо на увазі, що навчальне програмне забезпечення повинно працювати незалежно від того, яке операційне програмне забезпечення використовується (Windows, Linux, MacOS, Android та інші), та на якій платформі воно встановлене (персональний комп’ютер, смартфон, планшет та інші). Відповідно до операційної системи та платформи дизайн програмного забезпечення має підлаштовуватись під користувача та розмір екрану, маючи гнучкий дизайн. Доступ до програмного забезпечення не має бути складним. Паролі для запуску та роботи з ним використовуватись не будуть, тобто доступ може отримати будь-який курсант чи рятувальник. Водночас софт має бути відлагодженим, щоб знизити можливість помилок у програмному коді, гальмування програмного забезпечення, самостійне вимкнення, а також воно має мати надійний захист від зовнішніх втручань у програмний код.

Програмне забезпечення повинне систематично оновлюватись, щоб покращити зручність для користувача та виправити можливі помилки в процесі роботі. Разом з цим розширення функціоналу та матеріальної бази може спростити навчальний процес та зробити його більш інтерактивним.

Інтерфейс повинен бути зрозумілим та легким у використанні, щоб користувач не витрачав велику кількість часу на освоєння принципів роботи програмного забезпечення, а також мав доступ до усіх програмних інструкцій та підказок.

Для розробки концепту програмного забезпечення використовуємо програмне забезпечення **Adobe Photoshop.** Наведений растровий редактор повністю задовольняє усім потребам для виконання поставленої задачі. Приклад концепту програмного забезпечення можна організувати на базі операційної системи **Android.**

Враховуючи розміри платформ, які працюють на базі системи **Android**, важливо не засмічувати екран непотрібними кнопками та функціями, саме тому для спрощення роботи меню буде випадним, та з'являтиметься при натисканні або відтягуванні стрілки у нижній частині екрана користувача.

Для повороту об'єкта використовується коло з стрілками під об'єктом, яке також при подвійному натисканні на ньому вмикає режим огляду, під час якого модель самостійно обертається навколо своєї осі. Також користувач може здійснювати поворот використовуючи сенсорні можливості пристрою.

Програмне забезпечення передбачає наступний функціонал:

- Можливість перегляд широкого списку пожежно-рятувального обладнання, устаткування та пожежно-рятувальної техніки.
- Можливість вмикати та вимикати показ окремих деталей моделі.
- Можливість отримати необхідну інформацію про обладнання у текстовій та, в наступних версіях, аудіо формі.
- Можливість зв'язку з групою підтримки програмного забезпечення.
- Можливість перемикання між кольоровим та чорно-білим варіантом моделей.
- Можливість вмикати та вимикати напівпрозорий режим перегляду об'єкта.

Програма передбачає використання в оффлайн режимі, тобто не потребує інтернет з'єднання для доступу в бібліотеку, але для зменшення ваги моделі для **Android** версій будуть спрощені, тобто для роботи можуть бути використані низько-полігональні та середньо-полігональні моделі. В результаті це також зменшить навантаження на пристрій.

Для розроблення програмного забезпечення нами переглянуто та досліджено кілька рушіїв, але вибір ми зупинили на ігровому рушії **Unity** від компанії Unity Technologies (рис.1).

Рис.1. Логотип рушія **Unity**

Unity — це багатоплатформовий інструмент для розроблення дво- та тривимірних додатків та ігор, що працює на операційних системах Windows, OS X. Створені за допомогою Unity застосування працюють під системами Windows, OS X, Android, Apple iOS, Linux, а також на гральних консолях Wii, Playstation 3 та XBox 360.

Враховуючи специфіку цього рушія, доступність його матеріальної бази та характеристики — це вибір однозначний.

Література

1. Михайленко В. Є. Інженерна та комп'ютерна графіка / В. Є. Михайленко, В.М. Найдиш, А. М. Підкоритов, І.А. Скидан. - К.: Видавничий дім «Слово», 2011. - 352с.

2. Ковальов С. М. Прикладна геометрія та інженерна графіка / С. М. Ковальов, М.С. Гумен, С. І. Пустюльга, В.Є. Михайленко, І. Н.Бурчак. – К. – Луцьк: ЛДТУ, 2006. – С. 177-205.

3. Гумен О. М. Графічні інформаційні технології у підготовці фахівців технологічних спеціальностей / О. М. Гумен, С. Є. Лясковська, Є. В. Мартин // Теорія і методика електронного навчання : зб. нак. пр. – Кривий Ріг : Криворізький національний університет, 2013 – Вип. IV. – С. 65-68.

4. Гумен О. М. Комп'ютерне моделювання технічних об'єктів / О. М. Гумен, С. Є. Лясковська, І. О. Малець. – Львів: НУ "Львівська політехніка", 2014. – 180 с.

ВПЛИВ НОВІТНІХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ НА НАВЧАЛЬНИЙ ПРОЦЕС У ВИЩІЙ ШКОЛІ В УКРАЇНІ

Дар'я Романчук, Валерія Мотуз
Навчально-науковий інститут історії і філософії
Черкаського національного університету імені Богдана Хмельницького, м.Черкаси

У науковій розвідці приділена увага проблемі розвитку навчального процесу у вищій школі в Україні в умовах соціальної інформатизації.

Ключові слова: вища школа, інформатизація освіти, технології навчання, інформаційні технології.

In scientific research attention is paid to the problem of development of educational process in high school in Ukraine in the conditions of social informatization.

Key words: higher school, informatization of education, teaching technology, information technologies.

Завдяки своїм можливостям впливати на світогляд особистості, сучасні інформаційні технології вважаються дієвим засобом модифікації психофізичного розвитку людини. Більш того, своєю присутністю в її повсякденному житті, вони спонукають науковців все частіше і частіше замислюватися над питанням про те, чи продовжує сучасне людство нести горду назву «Людина розумна» чи вже можна говорити про існування нового виду роду Homo – «Людина техногенна»?

Пряму відповідь на це питання, на нашу думку, спроможна дати сучасна освіта, зокрема, вища, яка, в Україні розвиваючись в інформаційному просторі, створює необхідні умови для реалізації особистісного виміру. Згадуючи про останній у контексті окресленої на початку проблеми, хотілося б звернути увагу на таку його особливість, як можливість інформаційного середовища освітньої установи впливати на формування ціннісностей і пріоритетів особистісного розвитку студентів під час навчання. Йдеться про направленість відповідної сукупності на забезпечення повноцінного самовизначення, розвиток внутрішньої відповідальності та суб'єктивної позиції, а також розширення сфери компетентностей та самореалізації [2, с. 114].

Сучасні інформаційні технології охоплюють велику кількість людей, в нашому випадку, студентську молодь. Одним із пріоритетних завдань вищої школи в Україні щодо гармонійного розвитку в інформаційному суспільстві вважається необхідність її перебування в авангарді останнього [1, с. 67]. Тож, в умовах інформаційної соціалізації вищі навчальні заклади України I–IV рівнів акредитації вибудовують свій освітньо-інформаційний простір у відповідності з новітніми тенденціями у плані соціокультурного і професійного розвитку особистості.

Формуванням відповідного простору у вищій школі в України не тільки посилює ефективність інформаційного забезпечення студентської самостійної діяльності, насамперед, у підготовці до практичних занять і науково-дослідній роботі, а й спрощує життя викладачам, які значну частину часу у своїй професійній діяльності приділяють саме передачі інформації. Для них ці технології стали незамінними професійними засобами, які допомагають їм перестати бути інформаторами і направити свої зусилля на виконання ними таких педагогічних функцій, як навчання та виховання студентів [4, с. 32].

Виходить, що головними трансформаціями, які переживає вища школа в України, пов'язаними з використанням у її навчальному процесі новітніх інформаційних технологій, є втрата викладацьким співтовариством монополії на знання та контролю над навчальною інформацією. У відповідних умовах виникає гостра потреба в модифікації освітньої парадигми, коли замість однонаправленої суб'єктно–об'єктної освіти починає домінувати відкрите розвиваюче суб'єктно–суб'єктне навчання, де студент і викладач виступають як активно змінюючи учасники освітнього процесу. Тобто, в новій парадигмі вже немає місця колишній інформаційній залежності студента від викладача [5, с. 3].

Інформатизацію освіти можна розглядати як певний виклик, точніше перевірку на педагогічну спроможність сучасної вищої школи України. Застосування у ній новітніх інформаційних технологій відкриває можливості для посилення особистісного підходу в

навчанні. Так, освітні можливості, що створені сучасними інформаційними технологіями, як і будь-які інші навчальні засоби, у повній мірі реалізовуються, якщо слугують інструментом розвитку освітніх комунікацій в особистісному вимірі практики підготовки у вищій школі України. Зокрема, педагогічно правильне використання новітніх інформаційних технологій сприяє подоланню недоліків у масово-репродуктивній системі підготовки [3, с. 16].

Проте, новітні інформаційні технології не вирішують всіх проблем в освітній сфері України. До того ж, їх впровадження у вищу школу не убезпечує останню від певних труднощів у даному процесі, Точніше, не призводить до автоматичних змін у методиці навчання, оскільки технократичне використання новітніх інформаційних технологій лише посилює недоліки у вищезгаданій системі підготовки [1, с. 98].

Варто розуміти, що загроза появи відповідної проблеми може з'явитися при домінуванні у викладацькій практиці пояснювально-ілюстративної методики навчання [4, с. 35]. Тож, якщо зазначений випадок стане дійсністю, то процес інформатизації навчання, скоріш за все, спрацює у зворотньому напрямку, коли викладач опинеться поза освітнім простором.

Крім того, при створені належних умов для реалізації особистісного виміру, з'являється можливість направити навчання з використанням новітніх інформаційних технологій, зокрема комп'ютера, у вищій школі в України на шлях всезагальної індивідуалізації [5, с. 7]. Мова йде про відмову від застосування колективної форми навчання (діалогічне спілкування і взаємодія), що вже само по собі створює загрозу для згортання соціальних контаків між студентами.

Ще однією не менш важливою складовою навчального процесу у вищій школі України є живе спілкування між викладачем і студентом, яке в умовах інформаційної соціалізації також зазнало кардинальних трансформацій. У певному сенсі таке спілкування є різновидом інформаційних технологій з тією лише різницею, що тут йдеться про міжособистісну взаємодію. Тобто, коли інформатизація освіти сприяє підвищенню рівня компетентності, підготовленості студентів до спілкування з викладачами як із рівним партнером, колегою і співучасником процесу їх власного професійного становлення [2, с. 149].

Досліджуючи проблему «Вплив новітніх інформаційних технологій на навчальний процес у вищій школі в Україні» автор наукової розвідки дійшов висновку, що не так вже просто вмонтовувати новітні інформаційні технології у звичний навчальний процес. Їх застосування в освітній сфері ще не є революцією в навчанні. Цей процес довготривалий, він вимагає зміни самої концепції навчання, де новітні інформаційні технології виступали б як новий засіб навчання, що сприяє формуванню наукового світогляду та цілісного мислення студентської молоді, а також орієнтує їх на пошук системних зв'язків і закономірностей.

Література

1. Вернидуб Р. Організація і управління навчальним процесом у вищому навчальному закладі: Навч. посіб. / Р. Вернидуб / Національний педагогічний ун-т ім. М. П. Драгоманова. – Київ : НПУ ім. М. П. Драгоманова, 2005. – 110 с.
2. Дубас О. Інформаційний розвиток сучасної України у світовому контексті: [моногр.] / О. Дубас. – Київ : Ґенеза, 2004. – 208 с.
3. Корольов Б., Тимошенко З. Вибір вищої школи України в дії / Б. Корольов, З. Тимошенко // Вища школа. – 2004. – № 5–6. – С. 14–21.
4. Козлакова Г. Інформатизація навчального процесу – передумова інтеграції європейського освітнього простору / Г. Козлакова // Вища школа. – 2006 – № 3–4. –С. 31–38.
5. Лізунов П., Білощицький А. Моделі та засоби формування комплексного інформаційно-освітнього середовища навчального закладу / П. Лізунов, А. Білощицький // Системи обробки інформації. – Харків : ХУ ПС, 2007. – Вип. 5(63). – С. 2–7.

КОМП'ЮТЕРНА ГРА. ІНСТРУМЕНТИ І МЕТОДОЛОГІЯ СТВОРЕННЯ КОМП'ЮТЕРНИХ ІГОР

Надія Тарапата, Марія Сємьонова, Ольга Смотр
Львівський державний університет безпеки життєдіяльності, м. Львів

Висвітлено процес створення комп'ютерних ігор. Розглянуто та проаналізовано існуючий на сьогодні інструментарій для розробки комп'ютерних ігор. Окреслено основні етапи створення комп'ютерних ігор.

Ключові слова: комп'ютерна гра, мови програмування, двигун гри, 3D моделі

The article is devoted to highlighting the process of computer games creation. The existing toolkit for the development of videogames is considered and analyzed. The basic stages of computer games creation are outlined.

Key words: computer game, programming languages, engine of game, 3D model

Комп'ютерні ігри протягом останніх десятиліть набули значної популярності як в дитячому й підлітковому середовищі, так і серед дорослих. Комп'ютерні ігри та пов'язані з ними продукти й заходи мають значний вплив на інші види розваг та приносять величезні прибутки. Світовий ринок комп'ютерні ігор зростає з кожним роком. У 2015 році він був оцінений у 74,2 млрд. доларів, а кількість гравців по всьому світу склала 1,8 млрд чоловік. Обсяг прибутків української відеоігрової індустрії у 2013 році став найбільшим за всю історію та становив понад 300 млн. доларів [1]. Деякі видання називають комп'ютерні ігри головним культурним експортом України на Захід. Ігрова індустрія потребує кадрів та ідей. Так, інвестиційний фонд «Vostok Ventures» готовий вкладати кошти (300 тис. доларів) в розробку потенційно якісної комп'ютерної гри [2]. І це притому, що гра може бути створена навіть на ранніх стадіях проекту. Робота над створенням та розробкою комп'ютерних ігор – це одна з затребуваних та перспективних галузей в IT сфері.

Перш ніж розглянути інструментарій та методологію створення комп'ютерних ігор, дамо визначення комп'ютерної (відео) гри. Існує ціла ієрархія комп'ютерних ігор, та й саме поняття комп'ютерної гри, з розвитком IT-технологій, значно трансформувалось. На сьогодні комп'ютерна гра – це гра, яка відбувається через керування візуальними образами на моніторі чи іншому дисплеї та може забезпечуватися як програмованим, так і не програмованим електронним пристроєм [1].

Розглянемо основні етапи створення комп'ютерної гри та інструментарій, що є наявним у гейм-разробників на даному етапі розвиту IT.

Створення комп'ютерної гри (перший етап) розпочинається з самої ідеї (концепції) гри та вибору її класу (браузерний, клієнтський, каузальний, консольний або он-лайн). Гра повинна бути цікавою і затребуваною для широкого кола аудиторії. Адже комп'ютерну гру можна представити як результат уміння людини "подивитися з боку" на те, що їй цікаво в житті, це добре відбивається в симпатії до певних видів ігор. Згідно з рейтингами аналітичного агентства NewZoo [3] найбільш популярними ігровими жанрами на сьогодні є: - Action; - Shooter; - Racing та - Life emulation.

Наступний етап – вибір мови програмування для написання коду гри. На сьогодні це: – C++; – Java; – Python; – Ruby; – Java Script тощо. На даному етапі усе залежить лише від професійного рівня розробників, їх вмінь, навичок та вподобань. Професіонали геймдеву стверджують, що розробка комп'ютерної гри вимагає C++. Вона багатоплатформова і швидка. На ній пишуть код для PC-games та Android. Однак вона є складною у вивченні. Потребує компіляції, має громіздкий синтаксис та архаїчні бібліотеки. На відміну C++, Python та Java Script мови з простим синтаксисом, масою бібліотек, з безкоштовною і відкритою реалізацією. Їх можуть засвоїти навіть діти. Вони мають інструменти, що дозволяють створювати прості анімації, власні відеоігри, ботів.

Наступний етап – вибір середовища розробки (двигуна гри). Двигун гри - це кодова база, набір засобів та інструментів розробки. Ось деякі з таких двигунів:

- *Unity 3D* (розроблені такі ігри, як: Assassin's Creed: Identity та Hearthstone: Heroes of Warcraft, Wasteland 2) – універсальний движок для створення 3D і 2D ігор. Серед

переваг: - низький поріг входження, - охоплює 24 платформи, включаючи Android і iOS, - безліч графічних редакторів, що дозволяє створювати елементи ігор без програмування;

- *Unreal Engine* (Tom Clancy's Splinter Cell: Blacklist, Batman: Arkham Asylum) – поріг входження вищий, ніж у Unity3D, розрахований на середній рівень геймдеву. Безкоштовний інструмент для створення та програмування гри, однак якщо ваш проект буде успішним і прибуток від його реалізації перевищить 3000 доларів, потрібно буде сплатити винагороду в розмірі 5% від прибутку;
- *Game Maker* - ігровий конструктор за принципом WYSIWYG інтерфейс drag-and-drop. Дозволяє створити 2D-гру для мобільних платформ Android, iOS, а також для Windows, Mac і Ubuntu. Має свою мову – GML. Серед переваг – те, що не вимагає спеціальної підготовки і знань програмування. Створити гру можна не написавши жодної стрічки коду. Серед недоліків – ціна конструктора (2499 євро - за щомісячне використання), ефективно працює лише з 2D-іграми або примітивною 3D-графікою.

Наступний етап – дизайн рівнів, вибір графіки та звукове оформлення. Графічний дизайн - це графічне мистецтво у поєднанні з продуктами розробки та розвитку новітніх технологій комп'ютерної графіки. До сучасних графічних редакторів можна віднести: Photoshop, Corel Painter, Illustrator, InDesign, CorelDraw, Dreamweaver, Flash Pro, After Effects. Реалістичність та деталізація графіки сучасних комп'ютерних ігор обмежена лише потужностями користувацьких комп'ютерів. Майже усі об'єкти, що ми бачимо у комп'ютерній грі — це 3D моделі. Приклади програм для моделювання: 3D Max, Blender 3D тощо.

Завершальним етапом створення комп'ютерної гри є її тестування.

Вся проведена робота збирається в єдине ціле у двигуні гри. Усі об'єкти розташовують на карті і змушують їх взаємодіяти між собою за допомогою програмного коду. При запуску комп'ютерної гри починає виконуватися програма — плеєр гри. Він виконує всі сценарії і є основним інструментом для взаємодії користувача з інтерфейсом.

Підводячи підсумки можна стверджувати:

1. Створення комп'ютерних ігор – це процес поєднання креативності та професіоналізму. Креативність ідеї, правильний вибір концепції гри та її дизайну настільки ж важливі, як програмна частина комп'ютерної гри.
2. У процесі створення комп'ютерних ігор умовно можна виділити такі основні віхи:
   - концепція;
   - програмування;
   - дизайн рівнів;
   - графіка;
   - звукове оформлення;
   - тестування.
3. Робота над створенням комп'ютерної гри – це командна робота (сценаристів, програмістів, художників, дизайнерів, аніматорів тощо).

Література

1. Вільна енциклопедії "Вікіпедіа" [Електронний ресурс]. – Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/%D0%92%D1%96%D0%B4%D0%B5%D0%BE%D0%B3%D1%80%D0%B0
2. Офіційний сайт інвестиційної компанії Компания "Vostok Ventures" [Електронний ресурс] – Режим доступу до ресурсу: http://vostokventures.com/
3. Офіційний сайт аналітичного агентства NewZoo https: [Електронний ресурс] – Режим доступу до ресурсу: //newzoo.com/insights/articles/newzoo-2017-report-insights-into-the-108-9-billion-global-games-market/

ЗАХИСТ КОНТЕНТУ ЕЛЕКТРОННОГО КУРСУ НАВЧАННЯ (НА ПРИКЛАДІ ВІРТУАЛЬНОГО УНІВЕРСИТЕТУ ЛДУ БЖД)

Анжела Стародуб, Орест Полотай
Львівський державний університет безпеки життєдіяльності, м.Львів

Показано основні види інформації, яка може бути розміщеною у електронному курсі Віртуального університету, що працює на основі модульної системи навчання Moodle. Розглянуто основні способи реалізації захисту електронного курсу. Описано основні типи ролей користувачів, які можуть бути присутніми у електронному курсі, та їхні права та рівні доступу до певних категорій ресурсів.

Ключові слова: електронний курс, захист інформації.

The main types of information, which can be placed in the virtual course of the Virtual University operating on the basis of the modular system of training Moodle, are shown. The main ways of implementing the protection of the electronic course are considered. The main types of user roles that can be present in the electronic course, and their rights and levels of access to certain categories of resources are described.

Keywords: electronic course, information protection.

Останніми роками все актуальнішою виступає проблема збереженості контенту електронного курсу, тобто інформації, яка служить допоміжною як для слухачів курсу (студентів) так і для тих, хто цю інформацію законно поширює (викладачів-тьюторів).

Надійність інформації в електронному курсі – це інтегральний показник, що характеризує якість інформації з точки зору:

– фізичної цілісності, тобто наявності або відсутності спотворень або знищення елементів цієї інформації;

– довіри до інформації, тобто наявності або відсутності в ній підміни (несанкціонованої модифікації інформації) її елементів при збереженні цілісності;

– безпеки інформації, тобто наявності або відсутності несанкціонованого отримання інформації особами, які не мають на це відповідних повноважень.

Уся інформація, яка розміщується в електронному курсі, умовно поділяється на два типи:

– інформація для студентів;

– інформація для викладачів.

До першого виду інформації відносяться різноманітні лекційні матеріали, завдання на самопідготовку, тестові завдання, інструкції до виконання завдань та інші додаткові матеріали, як допомагають слухачам електронного курсу по-перше успішно засвоювати матеріал курсу та по-друге ефективно використовувати контент курсу.

До другого виду інформації відноситься інформація про студентів, що навчаються на електронному курсі, їхня статистика відвідуваності курсу, результати навчання, тощо.

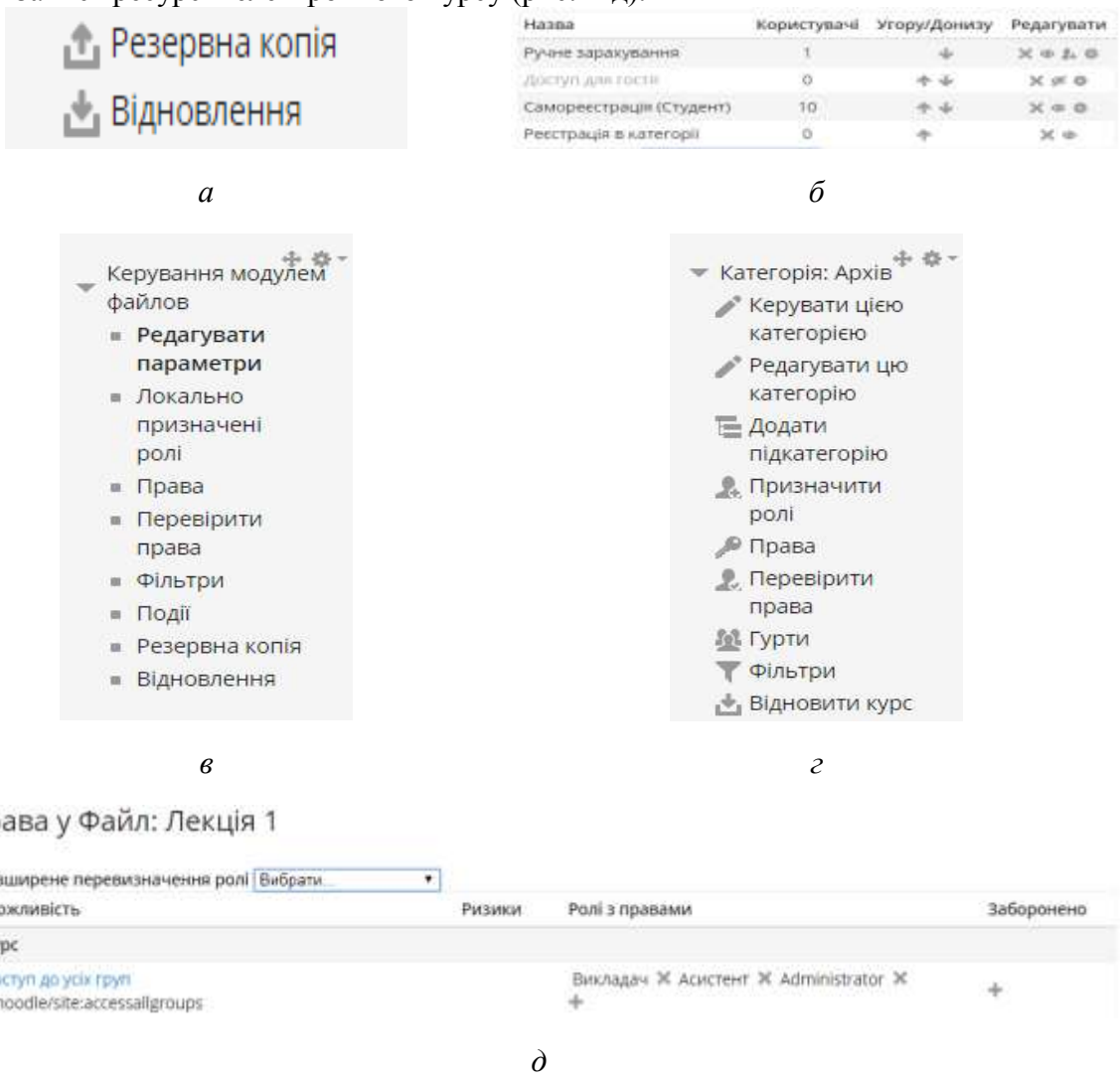
Обидва типи інформації, з точки зору захищеності є дуже важливими. Наприклад, як інформація першого типу буде спотворена, то студенти отримають порцію неправдивих знань, що рівнозначне їхній відсутності. Це призведе до нульового результату навчання студента в електронному курсі, тобто повної відсутності його компетенцій певної галузі. Також, в разі отримання несанкціонованого доступу до контенту електронного курсу, останній в свою чергу може бути банально знищений. Це призведе до зриву навчального процесу. Також варто розглядати питання авторських прав викладача на контент електронного курсу. Якщо ж буде модифікована інформація другого типу, то це призведе до неадекватного оцінювання результатів навчання слухачів електронного курсу.

Отже, існує потреба у захисті контенту електронного курсу. Розглянемо основні способи захисту контенту електронного курсу Віртуального університету ЛДУ БЖД. Це:

1. Резервна копія електронного курсу (рис. 1-а);
2. Способи зарахування на електронний курс (рис. 1-б);
3. Налаштування прав та заборон користувачів електронного курсу різних типів (рис. 1-в);

4. Налаштування прав та заборон користувачів в межах груп електронних курсів (рис. 1-г);

5. Захист ресурсів електронного курсу (рис. 1-д).



а *б*

в *г*

д

Рис. 1. Способи захисту електронного курсу

Найбільш простим та банальним способом забезпечення збереженості контенту першого типу є створення резервної копії електронного курсу з можливістю у подальшому його відновлення. Це дає гарантію відновлення електронного курсу і разі його втрати або пошкодження.

Спосіб налаштування на електронний курс вказує чи зможуть і як зможуть попасти в курс різні категорії користувачів. Тут розглядається самореєстрація з паролем, ручне зарахування викладачем студентів на курс, заборона доступу на курс користувачу типу «гість», тощо.

Налаштування прав та заборон користувачів дають змогу надати дозвіл чи заборонити здійснювати певну дію користувачу певної групи, серед яких: гість, студент, асистент, викладач, власник курсу, адміністратор. Таким чим налаштовується розподіл прав на виконання повний спектр дій серед користувачів. Дані права призначаються як в межах одного курсу так і в межах цілої категорії курсів.

Кожен ресурс електронного курсу також можна налаштувати з точки зору доступу до нього. Це може бути згадана вище політика прав груп користувачів (для ресурсів типу лекція), так і права на редагування ресурсу (тести).

Отже, правильне налаштування параметрів електронного курсу дасть змогу забезпечити цілісність, правдивість та захищеність контенту електронного курсу.

Література

1. Віртуальний університет Львівського державного університету безпеки життєдіяльності. [Електронний ресурс]. – Доступний з http://virt.ldubgd.edu.ua/

ОСОБЛИВОСТІ ДИТЯЧО-МОЛОДІЖНОГО КІБЕРЕКСТРЕМІЗМУ

Ірина Хомич, Наталія Кухарська
Львівський державний університет безпеки життєдіяльності, м. Львів

У статті розглянуто явище кіберекстремізму, виокремлено чинники, які йому сприяють, а також описано способи профілактики його розповсюдження серед дітей та молоді.

Ключові слова: кіберекстремізм, мережа Інтернет, діти, молодь.

The article deals with the phenomenon of cyber-terrorism, identifies the factors that contribute to it, and also describes ways of preventing its spread among children and youth.

Key words: cyber extremism, Internet network, children, youth.

Глобалізація інформаційних процесів, повсюдне проникнення інформаційних технологій, масовість використання мережевих сервісів і їх доступність все частіше призводять до того, що маловідомі для широких кіл негативні явища з реального життя перекочовують в Інтернет, привертаючи там увагу користувачів. У такий спосіб в кіберпростір проник екстремізм.

Екстремізм найпростіше визначити як схильність особи або групи осіб до крайніх поглядів або дій. Найчастіше цим словом позначають радикальні громадські рухи – терористичну діяльність, розпалювання соціальної, расової, національної чи релігійної ворожнечі і т.д.

За своїм механізмом, способам вчинення та приховування кіберекстремістська діяльність має певну специфіку, характеризуються високим рівнем латентності і низьким рівнем розкриття. Кіберпростір дає змогу отримати безпрецедентний ступінь свободи у виборі об’єктів екстремістських дій і культивування об’єктів ненависті. Екстремісти завдяки Інтернету можуть «керувати сприйняттям» – тобто показувати себе саме такими, якими хочуть здаватися, без фільтрів, що накладаються традиційними ЗМІ.

Розглянемо фактори, які сприяють тому, що будь-хто всупереч його волі може виявитися втягнутим в кіберекстремістську діяльність.

- Анонімність в мережі. Людиною опановує ілюзія захищеності: «ніхто мене не знає, отже, мене неможливо буде знайти і покарати».
- Груповий характер дій. Екстремісти в мережі Інтернет найчастіше діють групою, організованою або не дуже.
- «Жартівливий» характер дій. Цей фактор актуальний у випадку цькування: учасники часто думають, що вони просто жартують, не усвідомлюючи, що жертва може сприймати їх слова цілком серйозно.
- Бажання належати до будь-якої соціальної групи, причому абсолютно не має значення: буде ця група займатися чимось, умовно кажучи «хорошим» чи «поганим».
- Вміле експлуатування екстремістами можливостей Інтернету: легкий доступ; мізерні масштаби державного регулювання і цензури або повна їх відсутність; швидка передача інформації; потенційно великі масштаби аудиторії; мультимедійність середовища, що дає можливість комбінувати різні типи інформації: текстову, графічну, аудіовізуальну.
- Використання сучасних засобів масової комунікації широкими верствами населення, інформатизації суспільства.
- Активізація діяльності різних екстремістських організацій.

Стосовно підлітків можна виокремити ще декілька чинників, які роблять їх набагато уразливішими до спроб залучення до кіберекстремістської діяльності.

- Допитливість: ця риса властива всім підліткам. Вони активно пізнають світ, хочуть спробувати якомога більше різних речей, отримати якомога більше вражень від життя.

- Несформована система життєвих цінностей: підлітки перебувають в активній стадії формування моральних, етичних і духовних цінностей, їх погляд на світ дуже часто змінюється, на нього можна легко вплинути.
- Юнацький максималізм: поряд з тим, що система поглядів ще не сформована, як не дивно, має місце упередження, що «моя» думка або «наша» думка (якщо підліток відчуває свою приналежність до якоїсь групи), є єдино правильною.
- Слабка виховна діяльність у дитячо-молодіжному середовищі.
- Тривала криза інституту сім'ї, сімейного виховання як головних інститутів соціалізації молодого покоління.
- Падіння рівня життя населення.
- Зростання асоціальних проявів у дитячо-молодіжному середовищі (алкоголізм, наркоманія, протиправна поведінка).

До небажаної інформації екстремістського спрямування в мережі Інтернет, розрахованої на молодь, дітей, можна віднести [1]:

- шокуючі сцени вбивства тварин, людей;
- пропагування наркотичних засобів і їх переваг;
- пропагування соціальної, расової і релігійної нетерпимості;
- рецепти з виготовлення зброї і вибухових речовин
- пропагування депресивного способу життя і т. д.

Способи захисту від розповсюдження кіберекстремізму:

- Суспільний вплив: до цієї групи захисту належать закони, суспільна мораль, вплив на людину різних ЗМІ антиекстремістського спрямування.
- Особистий вплив: захист, розрахований на близьке коло спілкування людини – друзів, родичів. До цієї групи так само можна віднести вплив особи на саму себе: самоосвіта, самоконтроль.
- Програмно-технічні засоби захисту. Існує велика кількість програмно-технічних засобів для обмеження доступу підлітків до небажаної інформації: різні мережеві екрани, програми для контролю діяльності дітей в мережі, різні послуги типу «дитячий Інтернет» від провайдерів.

Незважаючи на численні спроби, вжиті на різних рівнях – від власників сайтів до урядів різних держав – поставити розповсюдження кіберекстремізму в Інтернеті під контроль, сьогодні ми не можна говорити про беззаперечний успіх. Знаходячи різноманітні лазівки в законах, на програмно-апаратному рівні, кіберекстремізм і далі продовжує поширюватися.

Найбільш ефективним способом профілактики дитячо-молодіжного кіберекстремізму, на нашу думку, є виховання – виховання культури міжнаціональних відносин, толерантності, розвиток соціальної компетентності, виховання поваги до честі та гідності кожної людини незалежно від її раси, віросповідання. У сучасних соціокультурних умовах українського суспільства саме виховання має стати орієнтиром у розробці повномасштабної наукової концепції профілактики розповсюдження кіберекстремізму в дитячо-молодіжному середовищі.

Література

1. Ошурков В.А. Механизмы защиты обучающихся от киберэкстремизма в условиях развития облачных образовательных сервисов ./ Ошурков В.А., Макашова В.Н., Цуприк Л.С. // Фундаментальные исследования. – 2014. – № 12–5. – С. 1089-1092.

ОСОБЛИВОСТІ ВИКОРИСТАННЯ ХМАРНИХ СЕРВЕРІВ ЗБЕРІГАННЯ ІНФОРМАЦІЇ

Павло Чмир, Назарій Бурак
Львівський державний університет безпеки життєдіяльності, м. Львів

Проведено аналіз сучасних технологій зберігання даних з використанням засобів «хмарних» віртуальних серверів. Визначено особливості хостингу серверів та процес забезпечення безпеки даних. Проведено дослідження можливості використання хмарних серверів у в органах і підрозділах служби цивільного захисту України.

Ключові слова: інформаційні технології, сервер, зберігання інформації, хмарні технології, система цивільного захисту.

In the article were analyzed modern technologies of data storage that used means of "cloud" virtual servers. The features of server hosting and data security process are determined. Were researched the possibility of using cloud servers in the departments of the Civil Protection Service of Ukraine.

Key words: information technology, server, storage of information, cloud technologies, civil defense system.

Розвиток науки та техніки, швидкі темпи інформатизації суспільства, інтегрованість інформаційних технологій у повсякденне життя призводять до накопичення значної кількості інформації, а це у свою чергу породжує потребу у збільшенні кількості пристроїв, де її можна зберегти та в подальшому використовувати.

Сучасний ринок пропонує великий асортимент зовнішніх магнітних дисків(HDD) з великою та швидких твердотілих накопичувачів (SSD) з незначною, у порівнянні з попередніми, ємністю. Дані пристрої задовільнять потреби середньостатичного користувача та невеликих компаній, де об’єми циркулюючої інформації незначні та не потребують довготермінового зберігання.

Однак, з часом виникає проблема, коли користувачу потрібно на певний термін зберегти великий об’єм даних. У такому разі придбання додаткових HDD чи декількох SSD є не ефективним рішенням з точки зору економіки. Розміщувати інформацію на особистих персональних комп’ютерах не завжди надійно і безпечно, оскільки ймовірність виходу із ладу одного HDD, на якому зберігається уся інформація, призведе до її втрати. Все частіше поява такої проблеми і призвела до появи новітнього методу зберігання інформації – використання хмарного віртуального сервера.

Такий продукт появився і в Україні досить недавно, однак вже поступово витісняє альтернативні рішення за рахунок своєї доступності та функціональними можливостями.

Хмарний сервер — це віддалений сервер, який може складатись з декількох окремих серверних частин та розміщуватись як в одному місці, такі розподіллено, об’єднуючись в одну велику базу. Такі сервери призначені для розміщення найважливішої інформації організації, завжди доступної з будь-якого пристрою у будь-який момент.

Інтеграція в хмарний сервер – це перенесення Вашої інформації, даних, програмного забезпечення тощо на хмарний хостинг(віддалений доступ), який забезпечує доступ до інформації в режимі on-line.

Яскравим прикладом застосування хмарного сервера є відома база даних «Google Диск», яка надає змогу зберігати, опрацьовувати та поширювати інформацію не використовуючи простір власного ПК, а користуючись віртуальною пам’яттю віддалених серверів.

У десятку найпопулярніших сьогодні таких хмарних сховищ даних відносять наступні: Dropbox, Google Drive, Mega, Box, Deggo, OneDrive, iCloud, pCloud, iDrive та SpiderOak.

Надійність використання такого методу зберігання інформації досягається за допомогою створення багаторівневої інфраструктури, яка захищає дані від несанкціонованого доступу на таких стадіях з’єднання з кінцевим користувачем: мережевий рівень, рівень додатків, рівень даних та фізичний рівень.

Такий підхід дозволяє надійно убезпечити інформацію використавши засоби управління обліковими записами користувачів, якісної та повної ізоляції даних, поділу сховища на сегменти, систем мережевого захисту, безпечних сучасних способів шифрування та можливості відновлення втраченої інформації з резервної копії.

Типова схема організації зберігання інформації на хмарних серверах подана на рис. 1.

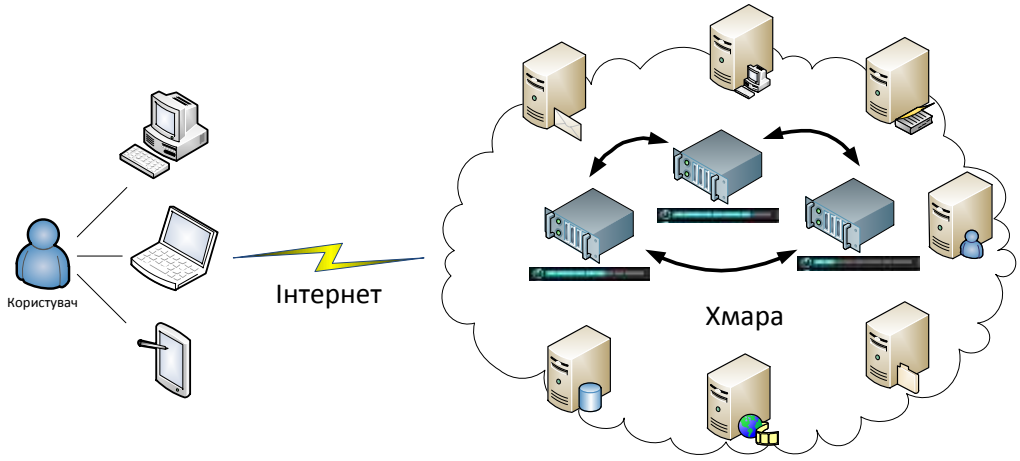


Рис. 1. Організаційна схема роботи хмарного сервера

Інформація, яка зберігається на хмарних серверах, автоматично та рівномірно розподіляється між усіма виділеними фізичними HDD, що дозволяє максимально ефективно використовувати пам'ять та підвищити швидкість доступу до неї. Такий принцип розподіленого зберігання забезпечує можливість оперативного масштабування серверної частини хмари, що значно спрощує процес розширення організації.

Перевагами такого типу організації зберігання інформації є мобільність у доступі до даних хмарного сервера – отримати необхідну інформацію можливо з будь-якої точки Землі за допомогою будь-якого пристрою підключеного до мережі Інтернет.

Створення віртуального хмарного сервера на базі спеціалізованих структурних підрозділах Державної служби України з надзвичайних ситуацій дасть змогу забезпечити швидкий та безпечний доступ підпорядкованим підрозділам до оперативної інформації, підвищить рівень ефективності та швидкодії її опрацювання.

Література

1. Волокита А., Мухін В., Стешин В. Специфіка інформаційних систем на основі технології cloud computing [Електронний ресурс]. – Режим доступу: http://archive.nbuv.gov.ua/portal/natural/vcndtu/2011_53/29.htm.

2. Жовтянський М. С. Моделювання проектного середовища впровадження «хмарних сервісів» у вищі навчальні заклади системи цивільного захисту / М. С. Жовтянський, Н. Є. Бурак // Управління проектами, програмами, портфелями : Тези доповідей І Міжнародної науково-практичної конференції : [у 2т.]. – Одеса, 2016. – Том 1. – С. 54–56.

3. Сабліна М. А. Можливості використання хмарних технологій в освітній та соціальній сферах / М. А. Сабліна // Освітологічний дискурс. - 2014. - № 3. - С. 191-200. - Режим доступу: http://nbuv.gov.ua/UJRN/osdys_2014_3_21.

4. Шевченко М. Хмарний сервіс зберігання даних / Шевченко М. // Збірник тез X Всеукраїнської студентської науково-технічної конференції „Природничі та гуманітарні науки. Актуальні питання", 25-26 квітня 2017 року. — Т. : ТНТУ, 2017. — Том 1. — С. 104–105. — (Секція: Інформаційні технології).

УЗАГАЛЬНЕНА КЛАСИФІКАЦІЯ ГЕНЕРАТОРІВ ПСЕВДОВИПАДКОВИХ ПОСЛІОВНОСТЕЙ

Володимир Шадий, Марія Мандрона
Львівський державний університет безпеки життєдіяльності, м.Львів

Запропоновано узагальнену класифікацію генераторів випадкових і псевдовипадкових послідовностей за способом їх реалізації.

Ключові слова: генератор випадкових чисел, генератор псевдовипадкових послідовностей, класифікація.

In this paper, we offered generalized classification of random and pseudorandom sequences for different way of contraction.

Key words: random number generator, pseudorandom sequence generator, classification.

Генератори випадкових і псевдовипадкових чисел (послідовностей) знайшли широке застосування у різних галузях науки і техніки, серед яких сфери захисту інформації, елементи побудови вимірювальних приладів, засоби імітаційного моделювання. Існування різних типів генераторів, постійно викликало труднощі для розуміння. Саме тому нами запропоновано класифікацію генераторів, яка дає змогу чітко зрозуміти відмінності між такими генераторами.

Для проведення узагальненої класифікації ми пропонуємо оперувати такими поняттями: генератори – усі типи випадкових і псевдовипадкових генераторів чисел та бітових послідовностей; генератори випадкових послідовностей (ГВП) – узагальнена назва для генераторів випадкових чисел (ГВЧ) і генераторів випадкових бітових послідовностей (ГВБП); генератори псевдовипадкових послідовностей (ГПВП) – узагальнена назва для генераторів псевдовипадкових чисел (ГПВЧ) і генераторів псевдовипадкових бітових послідовностей (ГПВБП).

На рис. 1. наведено запропоновану узагальнену класифікацію генераторів.

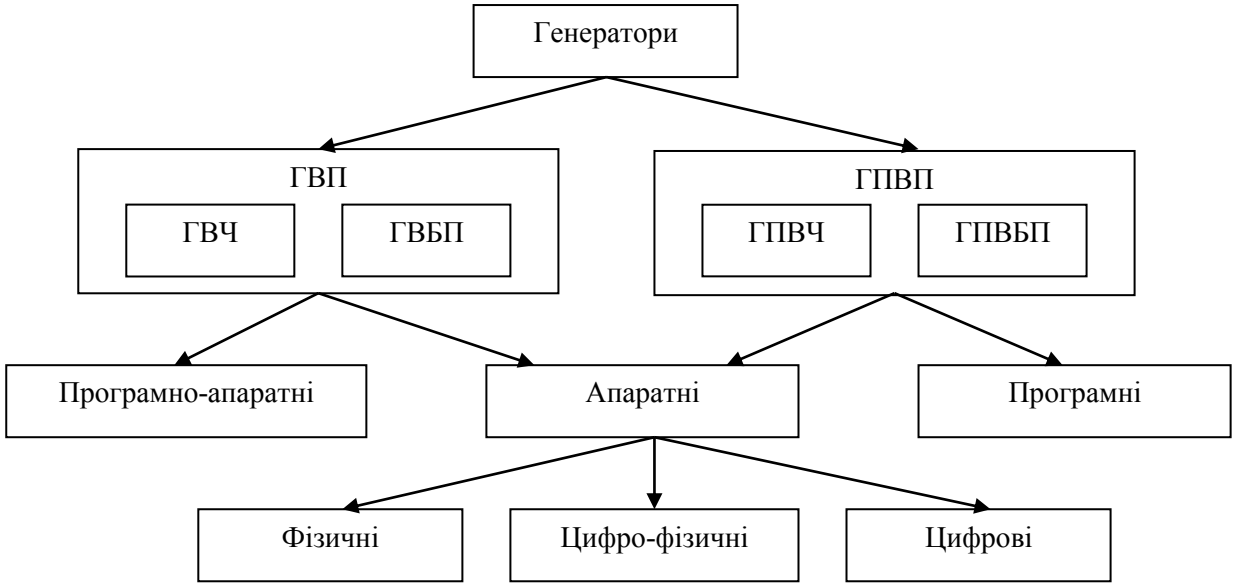


Рис. 1. Узагальнена класифікація генераторів

Поділ генераторів на випадкові і псевдовипадкові.

Принциповою відмінністю генераторів істинно випадкових послідовностей від генераторів, що формують псевдовипадкову послідовність є те, що псевдовипадкова послідовність може бути відновлена у просторі та часі без попереднього її запису при заданні тих самих початкових умов чи значень і, в більшості випадків, має період повторення. Істинна випадкова послідовність не має періоду повторення і може бути відновлена тільки, якщо її попередньо записати [1-3].

Поділ генераторів за способом реалізації.

Програмні генератори реалізуються з допомогою цифрової (мікропроцесорної) техніки і функціонують у відповідності до певних алгоритмів: рекурентних, криптографічних та інших. За своєю суттю вони є детермінованими і тому відносяться виключно до ГПВП.

Програмно-апаратні генератори відрізняються від програмних тим, що використовують додаткові

джерела ентропії. Ентропія є мірою невизначеності, яка пов'язана з випадковою величиною. Для програмно-апаратних ГВП ентропія джерела – це випадкові події в комп'ютерній системі, які можуть бути отримані за допомогою програмного забезпечення. До таких випадкових подій можуть відноситись: рух і клацання миші, натискання клавіш, системний годинник, вміст вхідних і вихідних буферів, шум звукової карти, значення лічильника тактів процесора. Програмно-апаратні генератори є недетермінованими і відносяться до ГВП.

Апаратні генератори можуть бути віднесені до трьох типів:

- фізичні;
- цифрові;
- цифро-фізичні.

Робота фізичних генераторів заснована на використанні надійних джерел ентропії, таких як тепловий шум в електронних і напівпровідникових приладах, фотоелектричний ефект, інші квантові явища. Ці процеси, абсолютно непередбачувані [1]. Генератори засновані на квантових процесах, зазвичай містять спеціальний підсилювач і перетворювач. Підсилювач підсилює слабкі сигнали, одержувані в результаті певних фізичних явищ, до прийнятних розмірів, які перетворюються далі до цифрового виду. Зрозуміло, що фізичні генератори відносяться до ГВП.

До цифрових можна віднести генератори, що реалізуються на елементній базі цифрової техніки – логічних елементах, тригерах, регістрах, лічильниках, суматорах, і т.д. Зокрема, такі генератори можуть бути створені на основі програмованих логічних інтегральних схем (ПЛІС). За своєю природою вони є детермінованими і, отже, відносяться до ГПВП.

Цифро-фізичні генератори відрізняються від цифрових наявністю в їх складі додаткового джерела (джерел) ентропії, яке може бути реалізоване на основі явищ, що є в основі роботи фізичних генераторів. Цифро-фізичні генератори можна віднести до ГВП.

Поділ генераторів за криптографічними властивостями.

Криптографічна стійкість – здатність криптографічного алгоритму протистояти криптоаналізу [2, 3]. Стійким вважається алгоритм, який для успішної атаки вимагає від противника недосяжних обчислювальних ресурсів, недосяжного обсягу перехоплених відкритих і зашифрованих повідомлень чи ж такого часу розкриття, що по його закінченню захищена інформація буде вже не актуальна, і т. д [2, 3].

Поняття криптостійкості, як правило, стосуються тільки ГПВП. Криптостійкими чи некриптостійкими можуть бути як програмні так і цифрові ГПВП в залежності від алгоритму їх роботи, діапазону значень їх змінних (для програмних) чи розрядів структурних елементів (для цифрових), множини початкових значень чи установок [1-3].

Статистично безпечними [3] вважаються генератори, вихідна послідовність яких проходить стандартизований набір статистичних тестів. Крипостійкість таких генераторів потребує додаткових досліджень.

Розроблено узагальнену класифікацію генераторів, яка на наш погляд, дає змогу чітко зрозуміти відмінності та особливості випадкових і псевдовипадкових генераторів.

Література

1. Иванов М.А. Криптографические методы защиты информации в компьютерных системах и сетях: учебное пособие / М.А. Иванов, И.В. Чугунков : под ред. М.А. Иванова. – М. : НИЯУ МИФИ, 2012. – 400 с.
2. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке СИ / Б. Шнайер. – М. : Изд-во «Триумф», 2002. – 797 с.
3. Горбенко І.Д. Прикладна криптологія: Теорія. Практика. Застосування: монографія / І.Д. Горбенко, Ю.І. Горбенко. Харків: Вид-во «Форт», 2012. – 608 с.

ПОКАЖЧИК АВТОРІВ

ТЕЗИ ДОПОВІДЕЙ

ІІ Міжвузівської науково-практичної конференції студентів і курсантів

ЗАХИСТ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ

24 листопада 2017 р.

Відповідальний за випуск – професор **Самотий В.В.**
Комп'ютерне макетування та верстка – **Паркасевич М.І.**

Друк ЛДУ БЖД
79000, Україна, м. Львів, вул.. Клепарівська, 35
Тел./факс: (032)233-32-40, 233-24-79
e-mail: mail@ubgd.lviv.ua, ndr@ubgd.lviv.ua

Підписано до друку 20.11.2017 р.
Формат 60Х85/16. Гарнітура TimesNewRoman.
Ум.друк.арк. 3,8. Наклад 50 прим.