ІНФОРМАЦІЙНА БЕЗПЕКА ТА ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Збірник тез доповідей V Міжнародної науково-практичної конференції ІБІТ 2024

27 листопада 2024 року

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

ІНФОРМАЦІЙНА БЕЗПЕКА ТА ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ІБІТ 2024

Збірник доповідей
V Міжнародної науково-практичної конференції

27 листопада 2024 року

Львів – 2024

ББК 32.81+78.362

*Інформаційна безпека та інформаційні технології: з*бірник доповідей V Міжнародної науково-практичної конференції, ІБІТ 2024, м. Львів, 27 листопада 2024 року. Львів, ЛДУ БЖД, 2024, 661 с.

Ольга МЕНЬШИКОВА – к.ф.-м.н., доцент, заступник начальника факультету цивільного захисту Львівського державного університету безпеки життєдіяльності з навчально-наукової роботи;

Андрій ІВАНУСА – к.т.н., доцент, доцент кафедри управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності;

Валентина ЯЩУК – к.е.н., доцент, доцент кафедри управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності;

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

Валерія БАЛАЦЬКА – викладач кафедри управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності;

Ігор МАЛЕЦЬ – к.т.н., доцент, доцент кафедри інформаційних технологій та систем електронних комунікацій Львівського державного університету безпеки життєдіяльності;

Назарій БУРАК – к.т.н., доцент, доцент кафедри інформаційних технологій та систем електронних комунікацій Львівського державного університету безпеки життєдіяльності;

Ольга СМОТР – к.т.н., доцент, доцент кафедри інформаційних технологій та систем електронних комунікацій Львівського державного університету безпеки життєдіяльності;

Юрій БОРЗОВ – к.т.н., доцент, доцент кафедри інформаційних технологій та систем електронних комунікацій Львівського державного університету безпеки життєдіяльності;

Роман ГОЛОВАТИЙ – к.т.н., старший викладач кафедри інформаційних технологій та систем електронних комунікацій Львівського державного університету безпеки життєдіяльності;

Олександр ХЛЕВНОЙ – к.т.н., старший викладач кафедри інформаційних технологій та систем електронних комунікацій Львівського державного університету безпеки життєдіяльності.

З М І С Т

СЕКЦІЯ 1

ІНФОРМАЦІЙНА БЕЗПЕКА ДЕРЖАВИ В УМОВАХ ВОЄННОГО СТАНУ

НАПРЯМ 1. УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ В УМОВАХ ВІЙНИ

що спрямована на захист стратегічних даних і запобігання їх несанкціонованому розголошенню. Використання комплексних організаційних, технічних і програмних заходів дозволяє значно зменшити ризики витоку інформації. Особлива увага приділяється захисту від акустичних, електромагнітних, оптичних і інших технічних загроз. Ефективна реалізація цих заходів потребує постійного моніторингу сучасних загроз, вдосконалення засобів захисту, навчання персоналу та інтеграції різних рівнів інформаційної безпеки, включаючи кіберзахист. Системний підхід до побудови багаторівневого бар'єра проти витоків забезпечує не лише збереження конфіденційності, але й підвищує ефективність оперативно-службової діяльності МВС, що має безпосередній вплив на національну безпеку держави.

Інформаційні джерела

1. Рибальский О.В Смаглюк В.М Хахановський В.Г. Основи інформаційної безпеки : підручник. Київ, 2011. 245 с.

2. Львівський державний університет внутрішніх справ. Інформаційна безпека у телекомунікаційній мережі НПУ: кейс заняття. Львів, 2022. 19 с.

УДК 004.056

ТЕХНІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ В ОРГАНАХ ТА ПІДРОЗДІЛАХ ДСНС УКРАЇНИ

Володимир ПИЛИПЕНКО
Олександр ТИМЧИШИН
Назарій ФЕДЕЦЬ

Кафедра інформаційних технологій та систем електронних комунікацій, Львівський державний університет безпеки життєдіяльності, м. Львів, Україна.

Abstract. *Technical protection of information in the units of the State Emergency Service of Ukraine is an important component of ensuring the reliability of processing and protecting critical systems from cyber threats. The main principles, protection methods and recommendations for improving cybersecurity in the bodies and units of the State Emergency Service of Ukraine are considered. Ensuring information security is the key to effective activity in emergency conditions. Investigation of cases of violations of norms and requirements on information security issues that pose a threat to the confidentiality, integrity and availability of information.*

Keywords*: technical protection, SES of Ukraine, information security, cyber threats. однією з найважливіших сфер, а особливо в державному секторі.*

Анотація. *Технічний захист інформації у підрозділах ДСНС України є важливою складовою забезпечення надійності обробки та захист критично важливих си-*

стем від кіберзагроз. Розглянуто основні принципи, методи захисту та рекомендації щодо вдосконалення кібербезпеки в органах та підрозділах ДСНС України. Забезпечення інформаційної безпеки є запорукою ефективної діяльності в надзвичайних умовах. Розслідування випадків порушення норм та вимог з питань ТЗІ, що створюють загрозу конфіденційності, цілісності та доступності інформації.

***Ключові слова**: технічний захист, ДСНС України, інформаційна безпека, кіберзагрози.*

У сучасних світових реаліях та з початком повномасштабної війни на території України, забезпечення кібербезпеки державного сектору стало одним з пріорітетним завданням, яке постало перед державою і зокрема перед Державною службою України з надзвичайних ситуацій (далі – ДСНС України). Для забезпечення кібербезпеки в інформаційних системах ДСНС України, визначають основні цілі та ризики, щоб встановити пріоритет їх значущості щодо зниження ризиків та зуміти реалізувати механізми управління ними на всіх критичних об'єктах інформаційної інфраструктури. Оскільки, інформації обробляється дуже багато, пов'язаної з управлінням наявних сил та засобів, які ліквідовують наслідки надзвичайних ситуацій, залучені до евакуації населення, а також зберігають конфіденційну інформацію співробітників та громадян. Якщо цю інформацію не захистити як слід це призведе до витоку персональних даних та інформації з обмеженим доступом, а використання її в корисливих цілях зловмисників буде загрожувати безпеці як працівників ДСНС України, так і державі в цілому. В умовах війни це дуже гостре питання, адже ворог здійснює сотні масованих кібератак кожного дня на ресурси ДСНС України.

Отож головні загрози захисту інформації:

– захист від кіберзлочинності;

– кібератаки на системи управління;

– захист від несанкціонованого доступу до інформації;

– забезпечення надійного функціоналу систем в умовах війни.

Основні кіберзагрози, які фіксують в інформаційних системах ДСНС України відбуваються за допомогою шкідливого програмного забезпечення, а саме :

– класичні комп'ютерні віруси ("троянський кінь", мережеві черв'яки);

– спеціальними засобами (експлойти, генератори ключів).

Тож розглянемо системи, які борються з кібератаками. Одною з якої є система контролю та управління доступу (СКУД), яка являє собою поєднання технічних та програмних засобів. Вона забезпечує доступ до об'єктів, інформацію про події та ідентифікацію суб'єкта. Також є системи моніторингу кіберзагроз. Апаратні та програмні мережеві екрани (фаєрволи), які запобігають несанкціонованому доступу до мережі ДСНС України.

Державні платформи кіберзахисту така як національна платформа "Державний центр кіберзахисту Держспецзв'язку" допомагає відстежувати

та реагувати на загрози в державних органах та критично важливих структурах не виняток й внутрішні інформаційні системи ДСНС України, які використовує для обміну даними про виникнення надзвичайних ситуацій. Протидія кіберзагрозам в ДСНС України включає регулярне оновлення антивірусних баз, виконання перевірок щодо відповідності нормативним вимогам з кібербезпеки. Окрім того, важливо здійснювати контроль за функціонуванням служб захисту інформації та кібербезпеки в інформаційно-телекомунікаційних системах, що знаходяться на об’єктах органів та підрозділів ДСНС України. Важливим аспектом є регулярне оновлення антивірусного програмного забезпечення (наприклад, антивірус Zillya!) для захищених комп'ютерів, що здійснюється кожного тижня, що є необхідною мірою для забезпечення захисту від кіберзагроз.

Правові основи технічного захисту інформації в ДСНС України

Технічний захист інформації в Україні коригується Положенням про технічний захист інформації, затвердженим Указом Президента України від 27 вересня 1999 року № 1229. У цьому Положенні виявити основи, принципи та порядок захисту інформації, яка підлягає захисту відповідно до законодавства, в установах та організаціях, що належать до сфери ДСНС України. Важливою складовою є організація відповідальних структур для виконання вимог технічного захисту та кібербезпеки. Організація технічного захисту інформації та відповідальність за його стан в апараті ДСНС України та Установах полягає на керівників. До об’єктів технічного захисту належить інформація, вимога щодо захисту якої встановлена законом. До об’єктів захисту ІТС, крім того, відноситься програмне забезпечення, що призначене для обробки цієї інформації. Організаційна структура та завдання комісії з технічного захисту інформації. Комісія з питань технічного захисту інформації в ДСНС України призначається наказом керівника організації. Очільником комісії є заступник керівника установи, а його заступником – керівник підрозділу зв'язку та інформатизації. Це забезпечує ефективне управління та координацію дій, спрямованих на технічний захист інформації. Оскільки захист інформації є пріоритетним завданням, головним завданням комісії є розробка заходів для забезпечення безпеки інформації, що циркулює в системах установи.

Основні завдання і функції у сфері технічного захисту інформації.

Захист інформації: Основним завданням є організація захисту інформаційних ресурсів і забезпечення технічної безпеки на всіх рівнях управління. Це включає як захист від зовнішніх кіберзагроз, так і внутрішній захист від витоків конфіденційної інформації.

Контроль за виконанням вимог технічного захисту інформації та кібербезпеки є важливою частиною роботи підрозділів служб захисту інформації. Проводяться перевірки, що включають перевірку стану виконання вимог

законодавства з питань захисту інформації та кібербезпеки, а також перевірки на наявні кібер загрози на робочих машинах

Забезпечення захисту інформації та оновлення токенів

Щорічно здійснюється оновлення токенів доступу до інформаційних систем, що є частиною заходів з технічного захисту. Це забезпечує безпеку та правильне функціонування систем доступу до інформації, що є критично важливою для захисту державних ресурсів.

Запити до Держспецзв'язку та взаємодія з іншими органами

Для забезпечення належного рівня кібербезпеки та захисту інформації в установах ДСНС кожного року надаються запити до Держспецзв'язку щодо розташування іноземних представництв поблизу установ Головних управлінь ДСНС України. Це дозволяє вчасно виявляти потенційні загрози та вжити необхідних заходів для забезпечення безпеки. Розслідування порушень та заходи для попередження. Участь в розслідуванні порушень вимог щодо технічного захисту інформації та кібербезпеки. В разі виявлення порушень вживаються заходи для усунення ризиків та запобігання подібним ситуаціям у майбутньому.

У сучасних умовах забезпечення інформаційної безпеки є не лише технічним завданням, але й складовою стратегічного управління, що дозволяє ДСНС України ефективно функціонувати в надзвичайних умовах і гарантувати захист громадян та держави. Для надійного захисту інформаційних ресурсів потрібний належний контроль, що включає регулярне оновлення систем захисту інформації. Наприклад, системи моніторингу, які використовують штучний інтелект, який останнім часом сильно розвинувся, яким можна аналізувати загрози різних типів. Постійне вдосконалення нормативно-правових актів. Співпраця з партнерами інших країн для обміну досвідом, інформацією та залучання технічної допомоги та фахівців в галузі забезпечення кібербезпеки. Також важливе проведення регулярних навчань серед працівників щодо правильного використання інформаційних систем та сервісів в умовах воєнного стану Проводити різні контрольовані атаки на інформаційні системи, щоб бачити де є вразливості та вдосконалювати системи захисту.

Інформаційні джерела

1. Стратегія кібербезпеки України – [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/447/2021#Text

2. Стандарти ISO/IEC управління інформаційною безпекою. [Електронний ресурс] – Режим доступу до ресурсу: https://studfile.net/preview/5367198/page:3/

3. Державний центр кіберзахисту Державної служби спеціального зв'язку та захисту інформації України – [Електронний ресурс] – Режим доступу до ресурсу: https://scpc.gov.ua/uk.

4. Наказ ДСНС 01.10.2020 №533 "Положення з організації заходів забезпечення кібербезпеки ДСНС"