СОЦІАЛЬНА ІНФОРМАТИКА

УДК 316.774: 316.776.22
DOI https://doi.org/10.32782/2710-4656/2023.2.2/29

Зінченко О. З.
Державний університет телекомунікацій

Яременко С. А.
Державний університет телекомунікацій

ТЕХНОЛОГІЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УПРАВЛІННІ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНОЮ ДІЯЛЬНІСТЮ В ОРГАНІЗАЦІЯХ

З появою інформаційних технологій та їх поширенням у всіх сферах життя зросла і потреба в забезпеченні інформаційної безпеки. Організації, які займаються інформаційно-комунікаційною діяльністю, є особливо вразливими до кібератак та інших загроз інформаційної безпеки. Витік конфіденційних даних, кібератаки та інші види кіберзлочинності можуть призвести до таких серйозних наслідків, як фінансові втрати, загроза безпеці, втрата репутації та інші. Тому в управлінні інформаційно-комунікаційною діяльністю в організаціях технології інформаційної безпеки є ключовими.

У дослідженні проаналізовано стратегії захисту даних у компаніях і наявні рамки інформаційної безпеки. Його ціль полягає у визначенні ефективності заходів безпеки, гарантуванні стратегічної боротьби з загрозами та захисті організаційних даних. Дослідження включає аналіз параметрів, які впливають на життєздатність інфраструктури інформаційної безпеки, а також використовує досвід компаній, що стикалися з витоками даних. Основна мета дослідження — проаналізувати стан інформаційної безпеки в компаніях і запропонувати рекомендації для поліпшення захисту даних.

У статті розглядаються конкретні заходи, які необхідно вживати для ліквідації загроз безпеці «інформаційного поля» організацій.

Висновки статті підкреслюють необхідність створення ефективної системи захисту інформації, зосередження на попередженні та реагуванні на інциденти, забезпечення безпеки та довіри взаємозв'язків зі споживачами та клієнтами, а також оновлення та вдосконалення політики безпеки. Зазначено, що безпека інформаційного поля є постійним процесом, який вимагає систематичного оновлення та навчання персоналу з питань кібербезпеки.

Ця стаття може бути корисною для організацій, які бажають забезпечити ефективний захист своєї інформації та протидіяти загрозам безпеки «інформаційного поля».

Ключові слова: *інформаційна безпека, загрози безпеці, інформаційне поле, оперативне реагування, система захисту, попередження і реагування, політика безпеки, навчання персоналу, кібербезпека.*

Постановка проблеми. Порушення безпеки інформації відбувається періодично. Колись управління інформаційною безпекою вважалося технічною проблемою, з якою доводилося мати справу ІТ-відділу. Поняття управління безпекою повинно бути зрозумілим усім співробітникам, не тільки ІТ-фахівцям. Кожен працівник повинен бути свідомим своєї ролі у забезпеченні безпеки інформації та вміти вживати необхідні заходи для запобігання загрозам і атакам. Керівники організацій, орієнтуючись на стратегічні цілі та бізнес-потреби організації, повинні бути активно залучені до процесу управління безпекою.

Аналіз ситуації показує, що захист інформації має два аспекти: широкий, який стосується захисту будь-яких відомостей незалежно від форми їх подання, і вузький – пов'язаний з захистом інформації в комп'ютерних системах [8].

Аналіз останніх досліджень і публікацій. Проблему технологій інформаційної безпеки

в управлінні інформаційно-комунікаційною діяльністю в організаціях вивчали в основному в рамках досліджень і публікацій з технічних наук Бабак В. П., Богуш В. М. [3], Грайворонський М. В. [4], Ільїн М. І. [6], Новіков О. М. [4], Швець М. Я., Якобчук Д. І. [6]. та інші. Необхідність досліджень технологій інформаційної безпеки в контексті комунікаційної діяльності в організаціях обумовлена збільшенням кількості комунікаційних каналів, загрозами соціального інжинірингу, необхідністю забезпечення конфіденційності та цілісності інформації, а також запобіганням інформаційним витокам.

Мета даного дослідження полягає в аналізі технологій інформаційної безпеки та їх впливу на управління інформаційно-комунікаційною діяльністю в організаціях.

Основні завдання дослідження включають:

– вивчення сучасних технологій інформаційної безпеки, їх функціональних можливостей і принципів роботи;

– аналіз впливу технологій інформаційної безпеки на управління інформаційно-комунікаційною діяльністю в організаціях;

– розробка рекомендацій щодо ефективного використання технологій інформаційної безпеки в управлінні інформаційно-комунікаційною діяльністю організацій;

– оцінка потенційних ризиків та визначення стратегій забезпечення безпеки інформаційно-комунікаційних процесів.

Виклад основного матеріалу. Безпека інформаційного поля відіграє важливу роль у сучасному цифровому середовищі, де інформація стала одним з найцінніших активів організацій. Інформаційне поле охоплює всі аспекти, пов'язані зі зберіганням, обробкою, передачею та використанням інформації в організації. Основна мета безпеки інформаційного поля полягає в захисті конфіденційності, цілісності та доступності інформації. Конфіденційність забезпечує, щоб лише авторизовані особи мали доступ до конфіденційної інформації. Цілісність гарантує, що дані залишаються незмінними та недоступними для несанкціонованого впливу. Доступність забезпечує, що інформація доступна і використовується вчасно та відповідно до потреб організації.

Для ефективної ліквідації загроз безпеці «інформаційного поля» організацій необхідно вживати конкретні заходи, зокрема:

– створення досконалої інформаційно-аналітичної діяльності: організація повинна розвивати внутрішні інформаційні ресурси та експертні знання для аналізу загроз та виявлення неправдивої інформації; це включає постійний моніторинг соціальних мереж, медіа та інших джерел інформації, а також використання спеціалізованих інструментів аналітики даних;

– оперативне реагування на випадки поширення неправдивої інформації про організацію: організація повинна мати встановлені процедури та комунікаційні канали для швидкого виявлення та втручання у випадках дезінформації або поширення неправдивої інформації; експерти зі зв'язків з громадськістю та комунікаційні спеціалісти повинні бути готові швидко реагувати та надавати точну інформацію для запобігання поширенню негативного впливу;

– скоординоване і централізоване поширення рекламної, маркетингової та іншої інформації, що підвищує імідж і сприйняття організації клієнтами: організація повинна ретельно планувати та виконувати стратегії зв'язків з громадськістю, маркетингу та реклами, спрямовані на зміцнення іміджу та сприятливого сприйняття організації [9].

Кіберзлочинці постійно шукають способи використати ці ризики для власної користі й завдати шкоди індивідуальним користувачам, підприємствам і суспільству в цілому. З розвитком інформаційних технологій та зростанням використання комп'ютерів й Інтернету з'явилися нові загрози та ризики, пов'язані з безпекою інформації, наприклад:

– соціально-інженерні атаки, які базуються на маніпулюванні людьми з метою отримання конфіденційної інформації;

– крадіжка та вилучення даних, які можуть бути використані для вчинення таких кримінальних дій, як шахрайство, вимагання викупу, крадіжки особистої інформації;

– відмова в обслуговуванні через недоступність сервісів, пов'язаних з мережею, або затримки в їх роботі;

– несанкціонований доступ до пристроїв, що приєднуються до мережі, таких як маршрутизатори та комутатори;

– використання недостатньо захищених паролів, які можуть бути легко підібрані або скомпрометовані;

– виток конфіденційної інформації через недостатній рівень захисту даних, такий як незашифроване зберігання або передача даних;

– використання ненадійних програм та програмного забезпечення, які можуть містити вразливості та використовуватися для атак на систему;

– фішинг та фармінг: атаки для викрадення логінів та паролів шляхом маскування у підроблених електронних листах та веб-сторінках;

– соціальна інженерія: атаки, спрямовані на взаємодію з людиною з метою отримання конфіденційної інформації або виконання шкідливих дій, використовуючи маніпуляцію та обман;

– несанкціонований доступ до комп'ютерної інформації, під яким слід розуміти доступ до комп'ютерної інформації, здійснюваний із порушенням встановлених вітчизняним законодавством правил розмежування доступу [8];

– крадіжка облікових даних: викрадення логінів та паролів користувачів, що дозволяє зловмисникам отримувати доступ до чужих даних;

– небажане програмне забезпечення: віруси, черв'яки, троянські програми та інші види шкідливого програмного забезпечення, які можуть призвести до пошкодження або несанкціонованого доступу до системи або даних;

– Деніал-оф-сервіс (DoS) атаки: спроби перевантажити або паралізувати роботу комп'ютерних систем або сервісів шляхом надмірного завантаження їх ресурсів;

– атаки «людський фактор»: використання слабкостей або помилок людей, що працюють з комп'ютерною системою, для отримання незаконного доступу або поширення шкідливого програмного забезпечення;

– атаки на безпеку мережі: використання різних методів для зламу або порушення безпеки комп'ютерної мережі, зокрема перехоплення трафіку, впровадження шкідливого програмного забезпечення або зміна налаштувань мережевих пристроїв;

– злам паролів: спроби отримати доступ до системи або облікових записів шляхом відгадування або підбору паролів.

Інформаційна безпека організації залежить від заходів, що виконуються відповідно до вимог безпеки. Основними джерелами цих вимог є:

1) оцінка ризиків для організації, яка враховує бізнес-стратегію та цілі;

2) правові вимоги, які визначені законодавством, договорами та угодами з партнерами організації. [1];

3) розроблені організацією принципи, цілі та бізнес-вимоги для оброблення інформації, що підтримують її функціонування [7].

Можна виділити три аспекти уразливості комп'ютерної інформації: 1. Її фізичне знищення – наявність ризику фізичного пошкодження або втрати інформації. 2. Можливість несанкціонованої модифікації – можливість змінити інформацію неправомірно або недбало. 3. Небезпека несанкціонованого отримання інформації – ризик доступу до інформації особами, для яких вона не призначена, незалежно від намірів цих осіб [8].

Щодо України, то серйозна війна на нашому «кіберфронті почалася у 2014 році, коли Росія запустила масштабну DDoS-атаку на Дарницьку ТЕЦ. Згодом таких атак стало більше. Через три дні після лютневого вторгнення Росії кібератаки на державно-військовий сектор України зросли на 196 % порівняно з довоєнним періодом. У 2022 році урядова команда реагування на комп'ютерні надзвичайні події зареєструвала 2194 кібератаки, чверть з них на органи влади» [5] Для вирішення таких проблем встановлюють засоби захисту від DDoS-атак: системи виявлення та блокування підозрілого трафіку, покращують архітектуру мережі та оптимізації її продуктивності. В результаті розробки стратегії захисту інформації, яка включає плани дій у разі виникнення інцидентів безпеки, таких як кібератаки або витік даних, компанія зможе уникнути подібних атак у майбутньому.

Методи захисту інформації у комп'ютерній мережі можуть бути різними і зазвичай включають в себе такі технології: аутентифікація та авторизація користувачів, шифрування та дешифрування даних, захист від вірусів та інших шкідливих програм, фільтрація трафіку та захист від DDoS-атак, а також захист від внутрішніх загроз.

Аутентифікація та авторизація користувачів є одним із найважливіших методів захисту інформації. Вона включає перевірку правильності введення логіна та пароля, а також перевірку прав доступу користувача до різних ресурсів комп'ютерної мережі. Одна з великих компаній вирішила покращити безпеку своєї комп'ютерної мережі, ввівши двофакторну аутентифікацію для своїх користувачів. Це означає, що, крім пароля, користувач повинен ввести додатковий код, отриманий на мобільний пристрій або поштою. Це значно підвищило безпеку мережі та зменшило ризики несанкціонованого доступу.

Шифрування та дешифрування даних є методом захисту інформації, що використовується для захисту від несанкціонованого доступу до конфіденційної інформації шляхом зашифрування цих даних. Після отримання зашифрованих даних, їх можна дешифрувати за допомогою відповідного ключа.

Крім загроз з боку зловмисників та шкідливих програм, інформаційна безпека також може бути під загрозою з боку користувачів самої мережі.

Захист від внутрішніх загроз передбачає захист від зловживань та інцидентів, що виникають внаслідок недбалості або злочинних дій співробітників. Наприклад, неправильне використання паролів та обміну чутливою інформацією може призвести до витоку даних. Тому важливо проводити організаційні заходи, такі як політика безпеки, стандарти безпеки, навчання та свідоме ставлення до безпеки даних. Ці заходи допомагають забезпечити ефективний захист мережі, запобігають людським помилкам та знижують ризики використання слабких паролів й інших недостатньо надійних методів захисту.

Ефективним в цьому плані є встановлення правил і вимог до співробітників, які стосуються захисту конфіденційної інформації та використання ресурсів комп'ютерної мережі, тобто проведення політики безпеки. Політика інформаційної безпеки повинна описувати наступні етапи створення засобів захисту інформації:

– визначення інформаційних і технічних ресурсів, що підлягають захисту;

– виявлення повної кількості потенційно можливих загроз і каналів витоку інформації;

– проведення оцінки вразливості і ризиків інформації за наявної кількості загроз і каналів витоку;

– визначення вимог до системи захисту;

– здійснення вибору засобів захисту інформації та їх характеристик;

– впровадження та організація використання обраних заходів, способів та засобів захисту;

– здійснення контролю цілісності і керування системою захисту[9].

Також важливо проводити регулярні навчання для працівників з питань безпеки комп'ютерної мережі, щоб вони могли усвідомлювати потенційні загрози та приймати відповідні заходи для їх запобігання. Крім того, слід надавати інформацію про те, як діяти в разі виявлення підозрілої діяльності в мережі або втрати даних. Навчання користувачів з правил безпеки та обізнаності з ризиками може допомогти зменшити кількість ненавмисних загроз та помилок. Як правило, більшість вразливостей виникає через помилки та непоінформованість користувачів. Проведення тренінгів та навчання допомагає підвищити обізнаність користувачів та зменшити ймовірність виникнення загроз у мережі. Це включає навчання правилам використання паролів, небезпекам використання громадських Wi-Fi мереж, а також тому, як розпізнати фішингові атаки. Користувачі повинні бути свідомі того, що їхні дії можуть вплинути на безпеку всієї системи. Відповідальність за порушення законодавства про захист інформації в системах передбачена статтею 11. Чинного Закону України Про захист інформації в інформаційно-комунікаційних системах [2].

Захист від внутрішніх загроз є важливою складовою комплексної стратегії інформаційної безпеки. Інсайдери, тобто працівники компанії, можуть нанести значної шкоди безпеці комп'ютерної мережі, якщо не приймати відповідних заходів для їх виявлення та запобігання. Захист від витоку інформації базується на застосуванні методів шифрування, моніторингу мережевого трафіку та заборони використання зовнішніх пристроїв для збереження інформації.

Одним з найбільш ефективних методів захисту від внутрішніх загроз є встановлення системи контролю доступу. Це може бути реалізовано шляхом використання ідентифікаційних карток, паролів, біометричних даних тощо. Працівникам слід надавати лише необхідні повноваження для виконання їхніх обов'язків. Також, слід вести ретельний моніторинг активності працівників у комп'ютерній мережі. Це можна реалізувати за допомогою спеціальних програм, які записують всю активність користувачів, таку як перегляд веб-сторінок, використання електронної пошти тощо. Це допоможе виявити несанкціоновану поведінку користувачів, яка може бути зв'язана зі зловживанням повноваженнями або намаганням злому безпеки мережі.

Ось ще кілька прикладів реалізації політики безпеки на підприємствах:

– забезпечення фізичної безпеки: одним із важливих аспектів захисту інформації є забезпечення фізичної безпеки приміщення, в якому знаходяться сервери та інші пристрої з доступом до конфіденційної інформації; це може бути забезпечено за допомогою фізичних бар'єрів, системи контролю доступу, відеоспостереження тощо;

– школи безпеки для співробітників: підприємства можуть організовувати тренінги та навчання для своїх співробітників з питань безпеки інформації; це може включати навчання профілактики соціальної інженерії, захисту від шкідливих програм, критеріїв для створення паролів та багато іншого;

– резервне копіювання: підприємства можуть використовувати системи резервного копіювання для захисту від втрати даних у разі відмови обладнання, природної катастрофи, кібератаки або будь-якого іншого непередбачуваного випадку;

– моніторинг системи безпеки: підприємства можуть використовувати системи моніторингу

безпеки, які відслідковують та аналізують активність на комп'ютерних системах та мережах, що дозволяє оперативно реагувати на потенційні загрози та запобігати їхньому розвитку.

Загалом ефективний захист від внутрішніх загроз вимагає комплексного підходу та в достатньому рівні обізнаності користувачів щодо можливих ризиків та правил безпеки.

Висновки. Інформаційна безпека є надзвичайно важливою для будь-якої компанії, що працює з комп'ютерною мережею. Існують різноманітні методи захисту інформації, такі як шифрування, захист від вірусів та інших шкідливих програм, фільтрація трафіку та захист від DDoS-атак, захист від внутрішніх загроз. Для ефективного захисту інформації в комп'ютерній мережі необхідний комплексний підхід та використання різноманітних засобів захисту, таких як firewalls, антивіруси, IDS, IPS тощо. Компанії повинні регулярно оновлювати свої системи захисту та перевіряти їх на вразливості. Успішні кейси вирішення проблем інформаційної безпеки показують, що захист інформації в комп'ютерній мережі є можливим та ефективним завдяки використанню сучасних технологій та підходів.

Отже, політика безпеки на підприємстві включає в себе ряд заходів, що забезпечують захист інформації від зовнішніх та внутрішніх загроз. Ось декілька прикладів реалізації політики безпеки на підприємствах:

– встановлення фірмового програмного забезпечення на всі комп'ютери, що використовуються на підприємстві, включаючи антивірусні програми, програми для фільтрації трафіку, IDS та IPS системи;

– регулярне оновлення програмного забезпечення та оперативної системи на всіх комп'ютерах, що використовуються на підприємстві;

– встановлення прав доступу до інформації на рівні користувача та рольового доступу до файлів та папок;

– використання паролів та ключів доступу для захисту від несанкціонованого доступу до систем та програм;

– використання захищених каналів зв'язку для обміну конфіденційною інформацією;

– проведення регулярних аудитів та перевірок безпеки на підприємстві;

– забезпечення надійного зберігання даних та резервного копіювання інформації;

– навчання персоналу правилам безпеки та проведення регулярних тренінгів;

– встановлення фізичних заходів безпеки, таких як системи контролю доступу до приміщень та відеоспостереження;

– регулярна оцінка ризиків та впровадження нових методів захисту від нових загроз;

– створення політики безпеки: підприємства можуть створювати політику безпеки, яка визначає правила та процедури щодо захисту інформації.

Отже, забезпечення інформаційної безпеки є надзвичайно важливим завданням для будь-якої компанії, що працює з комп'ютерною мережею. Різноманітні методи та засоби захисту інформації можуть допомогти попередити багато типів загроз та зберегти конфіденційні дані та інформацію компанії в безпеці. Важливо використовувати всі доступні інструменти технологій інформаційної безпеки для захисту своєї інформації та зменшення ризиків від кібератак та витоків даних. Для ефективного захисту інформації організації повинні створити досконалу інформаційно-аналітичну діяльність, оперативно реагувати на поширення неправдивої інформації та скоординовано поширювати рекламну та маркетингову інформацію. Також важливим є налагодження інформаційної співпраці з органами державної влади і місцевого самоврядування в межах чинного законодавства.

Список літератури:

1. Закон України Про основні засади забезпечення кібербезпеки. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 10.05.2023).

2. Закон України Про захист інформації в інформаційно-комунікаційних системах від 5 липня 1994. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text (дата звернення 25.05.23).

3. Богуш В. М. Інформаційна безпека держави / В. М. Богуш, О. К. Юдін. К.: МК-Прес, 2005. 432 с.

4. Грайворонський, М. В. Безпека інформаційно-комунікаційних систем: *підручник* /М. В. Грайворонський, О. М. Новіков. Київ: Видавнича група BHV, 2009. 698 с URL: https://ela.kpi.ua/handle/123456789/44867 (дата звернення: 27.05.2023).

5. За рік РФ здійснила понад дві тисячі кібератак на держоргани України. *Держспецзв'язку. Суспільне. Новини.* URL: https://suspilne.media/360848-v-ukraini-zrostatime-kilkist-kiberatak-z-boku-rf-derzspeczvazku/ (дата звернення: 06.05.2023).

6. Ільїн М. І. Зворотна розробка та аналіз шкідливого програмного забезпечення. *Лабораторний практикум [Текст] : посіб. для здобувачів ступеня бакалавра за спец. 113 «Прикладна математика», 125 «Кібербезпека»* / М. І. Ільїн, Д. І. Якобчук ; [відп. ред. І. В. Стьопочкіна]; Нац. техн. ун-т України «Київ. політехн. ін-т ім. Ігоря Сікорського». Київ: КПІ ім. Ігоря Сікорського: Політехніка, 2020. 117 с.

7. Інформаційна безпека банківської установи. URL: http://obt.inf.ua/page10.html (дата звернення: 10.05.2023).

8. Інформаційно-комунікаційна безпека в суспільстві: витоки проблем. *URL:* https://lexinform.com.ua/dumka-eksperta/informatsijno-komunikatsijna-bezpeka-v-suspilstvi-vytoky-problem/ (дата звернення: 10.05.2023).

9. Системи забезпечення інформаційної безпеки (редакція від 17.08.2022). URL: https://valtek.com.ua/ua/system-integration/security-control-system/integrated-security-systems/information-security-system-review» (дата звернення: 10.05.2023).

Zinchenko O. Z., Yaremenko S. A. INFORMATION SECURITY TECHNOLOGIES IN INFORMATION AND COMMUNICATIONS MANAGEMENT IN ORGANIZATIONS

With the emergence and widespread adoption of information technologies in all spheres of life, the need for ensuring information security has grown. Organizations engaged in information and communication activities are particularly vulnerable to cyber attacks and other threats to information security. Data breaches, cyber attacks, and other forms of cybercrime can lead to serious consequences such as financial losses, reputation damage, and threats to security, among others. Therefore, in the management of information and communication activities in organizations, information security technologies are crucial.

This research analyzes data protection strategies in companies and existing frameworks of information security. Its goal is to determine the effectiveness of security measures and ensure strategic combat against threats and protection of organizational data. The study includes an analysis of parameters that impact the viability of information security infrastructure and utilizes the experiences of companies that have faced data breaches. The primary objective is to understand the state of information security in companies and provide recommendations for enhancing data protection.

The article discusses specific measures that need to be taken to eliminate threats to the security of organizations' «information field.» The conclusions of the article underscore the necessity of creating an effective information protection system, focusing on prevention and incident response, ensuring the security and trustworthiness of relationships with consumers and clients, as well as updating and improving security policies. It is noted that information field security is an ongoing process that requires systematic updates and staff training in cybersecurity.

This article can be beneficial for organizations seeking to ensure effective protection of their information and counteract threats to the «information field» security.

Key words: *information security, security threats, information field, incident response, security system, prevention and response, security policy, staff training, cybersecurity.*