НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»
ФАКУЛЬТЕТ КІБЕРБЕЗПЕКИ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Кафедра кібербезпеки

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ СИСТЕМАХ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ»

Виконав: здобувач 4 курсу
Рівень бакалавр
Галузь знань 12 «Інформаційні технології»,
спеціальність 125 «Кібербезпека»
Третьяк Максим Владиславович

Керівник: к.т.н., доцент
Кухаренко Сергій Вікторович

Рецензент: к. фіз.-мат.наук, доцент
Чепурна Олена Євгенівна

Одеса – 2024

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»

Факультет **кібербезпеки та інформаційних технологій**

Кафедра **кібербезпеки**

Галузь знань: **12 Інформаційні технології**

Спеціальність: **125 Кібербезпека**

Назва освітньої програми: **Кібербезпека**

ЗАТВЕРДЖУЮ
Завідувач кафедри кібербезпеки
професор С.А. Горбаченко
_____ «____ »_____ 20__ року

З А В Д А Н Н Я
на кваліфікаційну (бакалаврську) роботу
здобувачу Третьяк Максиму Владиславовичу

1. Тема роботи: «Забезпечення захисту інформації в банківській сфері»
Керівник роботи: к.т.н, доцент Кухаренко Сергій Вікторович
затверджені наказом НУ ОЮА від «02» квітня 2024 року № 809-06
2. Строк подання здобувачем роботи «20» травня 2024 рік
3. Дата видачі завдання «15» вересня 2023 рік

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів бакалаврської роботи	Строк виконання етапів роботи	Примітка

Здобувач _____
(підпис) (прізвище та ініціали)

Керівник роботи _____
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Кваліфікаційна робота на тему «Методи захисту інформації в комп'ютерних системах від несанкціонованого доступу» на здобуття першого (бакалаврського) рівня вищої освіти за спеціальністю 125 Кібербезпека, освітньою програмою: Кібербезпека, містить 14 літературних джерел за переліком посилань. Робота виконана на 42 сторінках загального тексту та 36 сторінках основного тексту.

Метою роботи є дослідження та оцінка методів захисту від несанкціоного доступу до інформації. Увага приділяється аналізу апаратних методів захисту, політикам доступу та методам криптографічного захисту даних.

У рамках дослідження були систематизовані основні категорії загроз і розроблені методи їх нейтралізації. Була розроблена модель оцінки ризиків та система моніторингу вразливостей, що дозволяє оперативно реагувати на можливі кіберзагрози.

Результати роботи можуть бути використані будь якими комп'ютерними системами для удосконалення своїх систем інформаційної безпеки, підвищення рівня захисту клієнтських даних та фінансових активів. Рекомендації, розроблені в цій роботі, сприятимуть формуванню ефективних стратегій інформаційної безпеки.

Подальші дослідження в цій області можуть бути спрямовані на розробку автоматизованих систем раннього виявлення інцидентів безпеки, вивчення міжнародного досвіду в галузі кібербезпеки комп'ютерних систем та адаптацію найкращих практик з міжнародних стандартів безпеки до умов України. Це допоможе створити більш ефективні стратегії та механізми захисту інформації, що відповідатимуть сучасним викликам кіберпростору.

БЕЗПЕКА, АНАЛІЗ, СИСТЕМА, ІНФОРМАЦІЯ, ВИТОК, ЗАХИСТ.

ABSTRACT

Qualification work on the topic «Methods of protecting information in computer systems from unauthorized access» for the first (bachelor's) level of higher education in the specialty 125 Cybersecurity, educational program: Cybersecurity, contains 14 literature sources according to the list of references. The work is executed on 42 pages of the general text and 36 pages of the main text.

The purpose of the work is to study and evaluate methods of protection against unauthorized access to information. Attention is paid to the analysis of hardware protection methods, access policies and cryptographic data protection methods.

The study systematized the main categories of threats and developed methods to neutralize them. A risk assessment model and a vulnerability monitoring system have been developed that allows for a rapid response to possible cyber threats.

The results of the work can be used by any computer system to improve their information security systems, increase the level of protection of client data and financial assets. The recommendations developed in this paper will contribute to the formation of effective information security strategies.

Further research in this area could be aimed at developing automated systems for early detection of security incidents, studying international experience in the field of cybersecurity of computer systems, and adapting best practices from international security standards to the conditions of Ukraine. This will help create more effective strategies and mechanisms for protecting information that will meet the current challenges of cyberspace.

SECURITY, ANALYSIS, SYSTEM, INFORMATION, BREACH, PROTECTION.

ЗМІСТ

ВСТУП

Сьогодні, завдяки поширенню Інтернету, де інформація стала одним з найцінніших ресурсів, актуальним є питання конфіденційності та доступу до персональних даних користувачів.

В епоху цифрової інформації, коли дані передаються через глобальні мережі, ключовим завданням є захист приватності, цілісності та доступу до інформації. Численні кіберзагрози щоденно посилюються, а методи кібератак стають складнішими та більш винахідливими. Важливість вивчення та вдосконалення новітніх методів захисту мережевих даних стає дедалі очевиднішою.

Тенденції незаконного збору, зберігання та обробки особистих даних через підключені до Інтернету комунікаційні пристрої викликають зростаюче занепокоєння не тільки серед правозахисних організацій, але й у широких мас користувачів. Це створює необхідність для детального аналізу правил, що регулюють використання біометричних даних з комунікаційних пристроїв, особливо з веб-браузерів. Результати такого аналізу можуть значно покращити захист приватності та анонімності користувачів, знижуючи вплив монополій на ринку цифрового профілювання на їхні життєві рішення та вибір. Тому ця проблема та обрана тема роботи є надзвичайно актуальною.

Метою кваліфікаційної роботи є проведення аналізу та дослідження методів захисту інформації від несанкціоного доступу до неї.

Об’єкт дослідження – захист інформації від несанкціоного доступу в комп’ютерній мережі.

Предмет дослідження – методи захисту інформації.

Враховуючи розвиток різних систем для взлому, персональний розвиток хакерів у кіберпросторі та їх вплив на розвиток галузі забезпечення безпеки для інформації практична цінність роботи полягає в розробці рішення для покращення та посилення дійсних методів захисту інформації від несанкціонованого доступу до неї. Ці пропозиції можуть бути використані для створення більш надійних

систем захисту інформації, що дасть можливість суттєво зменшити ризики для загроз, які пов’язані з несанкціонованим доступом в комп’ютерних системах.

1 ТЕОРЕТИЧНІ ОСНОВИ ЗАХИСТУ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ СИСТЕМАХ

1.1 Правові основи захисту, основні поняття і визначення

Правові основи захисту даних базуються на правових актах, що утверджують права і свободи людини та якими встановлено відповідальність за злочини в галузі інформаційної безпеки. В Україні прийнято низку законів, постанов та нормативніх документів щодо забезпечення інформаційної безпеки: Закони України «Про інформацію», «Про захист інформації в інформаційно-комунікаційних системах», «Про державну таємницю», «Про захист персональних даних», «Про авторське право та суміжні права», Положення про технічний захист інформації в Україні, НД ТЗІ 1.1-003-99 «Термінологія у галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу», НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу», НД ТЗІ 2.5-005-99 «Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу», ТР ЕОТ-95, ДСТУ тощо.

Крім того існує низка законів згідно яких передбачена адміністратавна (Кодекс України про адміністративний правопорушення (КУпАП)) та кримінальна (Кримінальний кодекс України Розділ XVI. Злочини у сфері використання ЕОМ (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку) відповідальність за невиконання вимог захисту інформації

Інформаційна безпека – «розділ інформатики, що вивчає закономірності забезпечення захисту інформаційних ресурсів фізичних осіб, підприємств, організацій, державних установ тощо від втрати, порушення функціонування, пошкодження, спотворення, несанкціонованого копіювання та використання» [14].

Питання інформаційної безпеки загалом можна розділити на дві категорії: захист інформації (запобігання загроз інформації); захист від інформації (запобігання інформаційних загроз). Іншими словами, інформаційна безпека має

два аспекти: технічний та гуманітарний, кожен з яких має зовнішні та внутрішні елементи.

Інформаційна безпека базується на таких принципах: доступність, конфіденційність, цілісність.

Основні загрози інформаційні безпеці:

– знищення та спотворення даних;
– отримання доступу до конфіденційних даних;
– пошкодження пристроїв інформаційної системи;
– отримання прав на виконання певних дій;
– отримання доступу до виконання фінансових операцій;
– отримання повного доступу до керування інформаційною системою.

Загрози безпеці інформаційної системи (ІС) класифікують за такими принципами:

– За обсягом завданих збітків (нешкідливі, шкідливі, дуже шкідливі);
– За метою (зловмисні, випадкові);
– За місцем виникнення (зовнішні; внутрішні);
– За походженням (природні; техногенні; антропогенні).

Етичні й правові основи інформаційної безпеки.

Засоби і методи підтримки інформаційної безпеки мають різне призначення:

– програмні засоби – захист від вірусів, ідентифікація користувачів тощо;
– технічні засоби – захист від несанкціонованого доступу, від пошкодження ІС тощо;
– адміністративні методи – регламентація порядку взаємодії користувачів із інформаційною системою;
– морально-етичні засоби – норми поведінки осіб в інформаційному просторі;
– правові методи – правила користування інформацією та відповідальність за їхнє порушення [7].

Кодекс етики визначає, що користувачі комп'ютерів не повинні використовувати комп'ютерне обладнання та програмне забезпечення для завдання шкоди іншим або для порушення авторських прав.

Організаційні положення щодо захисту даних:

– захист від втрати даних унаслідок стихійних явищ, збоїв у роботи електромереж, некомпететності працввників тощо;

– захист від умисного пошкодження комп'ютерного та мережевого обладнання, викрадення даних безпосередньо з пристроїв;

– захист від викрадення даних.

Авторське право.

Інтелектуальна власність – «це власність на результати інтелектуальної або творчої діяльності».

Об'єктами інтелектуальної власності є програмні продукти, бази даних, твори літератури, науки, мистецтва тощо.

Авторське право – це сукупність установлених і гарантованих державою прав автора щодо створення або використання об'єктів творчої діяльності.

Нормативно-правові акти, що пов'язані з захистом інтелектуальної власності це: Закон України «Про авторське право і суміжні права» та Цивільний кодекс України.

Знак охорони авторського права – знак © (перша літера англ. слова Copyright), що закріплює найменування власників авторського права та рік першої публікації твору.

Плагіат (лат. plagium – викрадення) – «привласнення авторства на чужий твір науки, літератури, мистецтва або на чуже відкриття, винахід, а також використання в своїх працях чужого твору без посилання на автора».

Використовуючи матеріали з Інтернету (копіюючи їх на носій інформації, вставляючи в презентацію або текстовий документ), необхідно дотримуватися певних правил, щоб не порушити законодавство про захист авторських прав. Тоб-то це значить що необхідно:

– «Запитувати дозвіл на використання матеріалів у автора. Це можна зробити, надіславши листа автору, якщо його ім’я або контактні дані вказано на сайті.

– Використовуючи матеріали, отримані з Інтернету, обов’язково вказувати адресу сайту, звідки вони були скопійовані.

– Не розповсюджувати чужі твори без дозволу автора.

Брандмауер – це «технічний пристрій (маршрутизатор, роутер тощо) або програмний засіб для контролю даних, що надходять до комп’ютера через мережу»[7].

1.2 Класифікація методів захисту інформації

Кожен вид захисту інформації забезпечує окремі аспекти безпеки:

– Технічний – забезпечує обмеження доступу до носія повідомлення апаратно-технічними засобами (антивіруси, фаєрволи, маршрутизатори, токіни, смарткарти тощо):

1) попередження витоку по технічним каналам;
2) запобігання блокуванню;

– Інженерний – запобігає руйнуванню носія внаслідок навмисних дій або природного впливу інженерно-технічними засобами (сюди відносять обмежувальні конструкції, охоронно-пожежна сигналізація).

– Криптографічний – попереджує доступ за допомогою математичних перетворень повідомлення (ІП):

1) попередження несанкціонованої модифікації;
2) попередження НС розголошення.

– Організаційний – попередження доступу на об’єкт інформаційної діяльності сторонніх осіб за допомогою організаційних заходів (правила розмежування доступу).

Технічний захист інформації з обмеженим доступом в комп’ютерних системах і засобах обчислювальної техніки, призначених для формування,

пересилання, приймання, перетворення, відображення та зберігання інформації, забезпечується «комплексом інженерних, організаційних, програмних і технічних заходів на всіх етапах їх створення й експлуатації» [9].

Закон України визначає інженерний захист інформації як «складову технічного захисту інформації. Але засоби і методи інженерного та технічного ЗІ дуже різняться хоча і мають спільну мету використання. Для прикладу: засоби обмеження доступу на територію і програмні засоби забезпечення автетифікації згідно із законодавчим визначенням складають одну категорію» [11].

Криптографічний метод захисту, безумовно, самий надійний метод захисту, так як охороняється безпосередньо сама інформація, а не доступ до неї (наприклад, зашифрований файл не можна прочитати навіть у випадку крадіжки носія). Даний метод захисту реалізується у вигляді програм або пакетів програм.

Перед сучасними криптографічними системами захисту інформації ставлять наступні вимоги:

– зашифроване повідомлення повинне піддаватися читанню тільки при наявності ключа;

– число операцій, необхідних для визначення використаного ключа шифрування по фрагменту шифрованого повідомлення і відповідного йому відкритого тексту, повинне бути не менше загального числа можливих ключів;

– число операцій, необхідних для розшифровування інформації шляхом перебору ключів, повинно мати чітку нижню оцінку і виходити за межі можливостей сучасних комп’ютерів (з урахуванням можливості використання мережевих обчислень);

– знання алгоритму шифрування не повинне впливати на надійність захисту;

– незначна зміна ключа повинна приводити до істотної зміни виду зашифрованого повідомлення навіть при використанні того самого ключа;

– структурні елементи алгоритму шифрування повинні бути незмінними;

– додаткові біти, що вводяться в повідомлення в процесі шифрування, повинні бути цілком і надійно сховані в шифрованому тексті;

– довжина шифрованого тексту повинна бути рівна довжині вихідного тексту;

– не повинно бути простих (які легко встановлюються) залежностей між ключами, що послідовно використовуються в процесі шифрування;

– будь-який ключ з безлічі можливих повинен забезпечувати надійний захист інформації;

– алгоритм повинен допускати як програмну, так і апаратну реалізацію, при цьому зміна довжини ключа не повинна призводити до якісного погіршення алгоритму шифрування [1].

Криптографічний алгоритм називається алгоритмом шифрування і представлений деякими математичними функціями, які використовуються для шифрування та дешифрування. Точніше, є дві такі функції: одна для шифрування та одна для дешифрування.

Розрізняється шифрування двох типів:

– симетричне (із секретним ключем);

– несиметричне (з відкритим ключем).

При симетричному шифруванні створюється ключ, файл разом з цим ключем пропускається через програму шифрування та отриманий результат пересилається адресатові, а сам ключ передається адресатові окремо, використовуючи інший (захищений або дуже надійний) канал зв’язку.

Несиметричне шифрування складніше, але і надійніше. Для його реалізації потрібні два взаємозалежних ключі: відкритий і закритий.

Одержувач повідомляє всім бажаючий свій відкритий ключ, що дозволяє шифрувати для нього повідомлення. Закритий ключ відомий тільки одержувачеві повідомлення. Коли комусь потрібно послати зашифрованет повідомлення, він виконує шифрування, використовуючи відкритий ключ одержувача. Одержавши повідомлення, останній дешифрує його за допомогою свого закритого ключа. За підвищену надійність несиметричного шифрування приходиться платити: оскільки обчислення в цьому випадку складніше, то процедура дешифрування займає більше часу [8].

Контроль цілісності при криптографічному контролі забезпечується за допомогою хеш-функції та електронного цифрового підпису.

Хеш-функція – «це складне перетворення даних (одностороння функція), яке зазвичай реалізується за допомогою симетричного шифрування з ланцюжком блоків. Зашифрований результат останнього блоку, який безпосередньо залежить від усіх попередніх блоків і є результатом хеш-функції» [3].

Аудит – «це оперативний аналіз накопиченої інформації в режимі реального часу або за будь який період часу. Активний аудит або оперативний аудит це аудит з автоматичним реагуванням на виявлені позаштатних ситуації» [3].

При протоколюванні події рекомендується записувати, принаймні, наступну інформацію:

– дата й час події;
– унікальний ідентифікатор користувача – ініціатора дії;
– тип події;
– результат дії (успіх або невдача);
– джерело запиту (наприклад, ім’я термінала);
– імена порушених об’єктів (наприклад, відкритих або видалених файлів);
– опис змін, внесених у бази даних захисту (наприклад, нова мітка безпеки об’єкта).

Елемент правового захисту інформації передбачає:

– статут компанії, організаційні документи, контракти з працівниками та посадові інструкції повинні містити положення та зобов'язання щодо захисту конфіденційної інформації компанії та її партнерів, а механізми юридичної відповідальності за розголошення конфіденційної інформації повинні бути встановлені та доведені до відома всіх працівників компанії. Правові елементи системи захисту можуть також включати забезпечення захисту цінної інформації від різних ризиків. Організаційні елементи захисту інформації включають управління та обмеження, які заохочують працівників дотримуватися правил захисту конфіденційної інформації, такі як:

– підготовка та організація роботи служби безпеки підприємства, забезпечення її організаційно-методичними документами з питань організації та методики захисту інформації;

– організувати та регулярно оновлювати реєстр (перелік) захищеної конфіденційної інформації, а також підготувати та оновлювати реєстр конфіденційних документів компанії;

– організувати систему обмеження доступу працівників до конфіденційної інформації (систему класифікації);

– організувати методи захисту та управління конфіденційними діловими документами;

– побудова традиційного або нематеріального безпечного робочого процесу;

– створювати технології для документування цінної інформації та підготовки, дизайну, виробництва та публікації конфіденційних документів;

– побудувати технічну систему для управління та зберігання конфіденційних документів;

– документів;

– організація архівування конфіденційних документів;

– організація захисту цінної інформації компанії від несанкціонованих дій працівників;

– процедури та правила поводження працівників з конфіденційними документами та інформацією, а також контроль за виконанням цих процедур та правил усіма працівниками;

– підбір, навчання та підготовка працівників, які працюють з конфіденційною інформацією;

– процедури захисту інформації під час проведення нарад, обговорень конфіденційних питань, прийому відвідувачів, реклами, виставок та інших заходів;

– організація аналітичної роботи з виявлення загроз для цінної інформації компанії та каналів витоку інформації;

– обладнання і атестацію приміщень і робочих зон, виділених для здійснення конфіденційної діяльності, ліцензування технічних систем і засобів захисту інформації та охорони;

– підготовка та погодження приміщень і робочих зон для проведення конфіденційної діяльності та погодження систем і технічних засобів захисту та охорони інформації;

– організація пропускного режиму на територію, в приміщення, будівлі та філії компанії, ідентифікація осіб та вантажів;

– організація системи охорони території, приміщень, будівель, обладнання, транспортних засобів та осіб компанії;

– організація технічних засобів захисту та організаційні аспекти охоронної діяльності;

– організації, пов’язані з адмініструванням системи безпеки організації. Елемент організаційної безпеки є ядром системи, що пов'язує всі інші елементи. Одним з ключових аспектів розробки організаційного підходу до інформаційної безпеки є створення системи авторизації (обмеження) та доступу співробітників до конфіденційної інформації, документів і баз даних. Важливо визначити це чітко і однозначно:

– хто, до якої інформації, кому, коли, як довго і в який спосіб має доступ. Система авторизації повинна виконувати наступні завдання:

– Забезпечувати працівників усіма документами та інформацією, необхідними для виконання їхньої роботи;

– обмеження кола осіб, які допускаються до конфіденційних документів;

– виключення несанкціонованого доступу до документа Ієрархічна послідовність доступу реалізується за принципом «чим вища цінність конфіденційної інформації, тим менше співробітників може знати про неї». Відповідно до цієї послідовності визначається необхідний ступінь посилення заходів безпеки та структура меж (рівнів) захисту інформації. Доступ співробітника до конфіденційної інформації, який здійснюється відповідно до системи авторизації, називається санкціонованим. Дозвіл (авторизація) на доступ до цієї

інформації завжди суворо персоніфікований і видається керівником у письмовій формі:

– з наказом про надання службового або особистого доступу до інформаційної системи, рішенням щодо документа, переліком дозволів у документі або титульним аркушем з рецензією на документ. Організаційні заходи безпеки закріплені в нормативних та методичних документах. Тут зазвичай використовується одна назва для обох вищезгаданих елементів системи захисту: організаційний та правовий захист інформації. До елементів технічного захисту належать:

– засоби захисту технічних каналів від витоку інформації від роботи комп'ютерів, засобів зв’язку, ксероксів, принтерів, факсимільних апаратів та інших пристроїв і обладнання;

– засоби захисту будівель від візуальних та аудіальних засобів технічної розвідки;

– засоби захисту будівель і приміщень від проникнення сторонніх осіб (засоби спостереження, сигналізації та оповіщення, інформаційно-ідентифікаційні пристрої та технічні об’єкти);

– засоби протипожежного захисту;

– засоби виявлення технічних та інформаційних пристроїв (підслуховуючі та передавальні пристрої, аудіо- та телезаписуючі пристрої тощо). Програмне забезпечення та захист інформації повинні включати:

– організація використовує особисті паролі та інші прості методи безпеки, встановлені працівниками для доступа до електронних файлів;

– організація використовує спеціальні методи та продукти захисту програмного забезпечення;

– рганізація використовує методи шифрування для захисту інформації на комп'ютерах і в мережах, а також для шифрування (скремблювання) тексту при передачі традиційними каналами зв'язку, факсом і поштою.

– На практиці можна реалізувати лише частину кожного елементу захисту. Наприклад, організаційний захист може регулювати лише те, як співробітники

працюють з конфіденційними документами та отримують до них доступ. Шляхи та засоби, що використовуються для захисту інформації в системі безпеки, повинні регулярно коригуватися, щоб запобігти розголошенню інформації хакерами. Система інформаційної безпеки організації завжди повинна бути суворо конфіденційною [8].

– Фахівці, які розробили систему, ніколи не повинні бути її користувачами. Таким чином, система захисту конфіденційної інформації, що використовується компанією, являє собою індивідуалізований набір необхідних елементів захисту, кожен з яких окремо вирішує свої специфічні для даної компанії завдання і має конкретне наповнення щодо цих завдань;

– разом ці елементи утворюють багатогранний захист секретів компанії і забезпечують відносну гарантію безпеки підприємницької діяльності компанії [5].

2 МЕТОДИ ЗАХИСТУ ВІД НЕСАНЦІОНОВАНОГО ДОСТУПУ

2.1 Аутентифікація, авторизація та ідентифікація

Для пояснення контролю доступу в кібербезпеці існує три концепції: ідентифікація, аутентифікація та авторизація. Хоча ці терміни тісно пов’язані між собою, вони мають відмінності, які необхідно роз’яснити, щоб добре зрозуміти правильну термінологію.

Перш ніж пояснювати, що таке ідентифікація, аутентифікація та авторизація, спочатку слід визначити дві інші фундаментальні термінології контролю доступу, тобто суб’єкт і об’єкт.

Суб’єкт – це активна сутність, яка має доступ до об’єкта. У прикладі доступу користувача до файлу суб’єктом є користувач. Однак суб’єкт не обов’язково має бути живою сутністю, він також може бути програмою або процесом, який отримує доступ до об’єкта.

Об’єкт – це пасивний компонент, до якого суб’єкт має доступ. Файли, принтери, комп’ютери, бази даних є прикладами об’єктів у механізмі контролю доступу.

Ідентифікація – «це процедура розпізнавання суб’єкта». Цього можна досягти за допомогою ідентифікатора користувача (наприклад, логін), ідентифікатора процесу тощо. Дуже важливо, щоб заявлені облікові дані були унікальними, щоб можна було розрізняти різні суб’єкти в системі. Тобто у системі не може бути зареєстровано два однакових ідентифікатора, два одинакових номери телефону, дві однакові електронні пошти і так далі. Наприклад, при спробі зареєструватись, користувач вводить свої дані в поле логіну, а система підсвічує поле з повідомленням «Такий користувач вже зареєстрований у системі». Це приклад ідентифікації.

Після того, як суб’єкт ідентифікує себе, його потрібно аутентифікувати, тобто суб’єкт має довести, що він той, ким себе видає. Цей доказ ідентичності досягається шляхом надання облікових даних механізму контролю доступу. Далі перевіряється дійсність наданих облікових даних перед тим, як затвердити запит на

аутентифікацію. Іншими словами, аутентифікація визначає, що суб’єкт як володіє, так і контролює надані облікові дані (аутентифікатори). Деякими прикладами облікових даних, які можна використовувати для підтвердження особи, є паролі, PIN-коди, цифрові підписи, біометричні дані тощо.

Облікові дані, які використовуються для аутентифікації, можна розділити на декілька різних груп, які також називають факторами аутентифікації:

Щось, що ви знаєте (фактор знання), як-от пароль, персональний ідентифікаційний номер (PIN-код) або парольна фраза. Однак, такий тип є слабозахищеним. Зловмисники знаходять способи дізнатись пароль, а також відповіді на контрольні запитання можуть бути відомі широкому загалу.

Те, що у вас є (фактор володіння), наприклад смарт-карта, карта пам’яті, смартфор, токен. Цей спосіб є більш захищеним, проте його вартість є високою.

Щось, що ви є (біометрія) (фактор властивості), як-от відбиток пальця, топологія долоні, геометрія руки, сканування райдужної оболонки/сітківки або розпізнавання фази. Цей фактор є досить перспективним, але також дороговартісним, оскільки біометрична система має бути вискочутливою.

Щось, що ви робите (поведінкова біометрія) (фактор властивості), наприклад шаблон набору тексту (динаміка натискання клавіш), шаблон підпису (динаміка підпису) або шаблон голосу.

Якщо система аутентифікації вимагає принаймні два види облікових даних, які належать до різних категорій аутентифікації, це називається багатофакторною аутентифікацією (multi-factor authentication, MFA). Наприклад, використання паролю (щось, що ви знаєте) і відбитка пальця (те, що ви є) для аутентифікації вважається багатофакторною аутентифікацією, тоді як використання паролю та PIN-коду – ні (оскільки і паролі, і PIN-коди належать до однакового фактору аутентифікації).

Як приклад:

– Користувач знаходиться на формі авторизації в систему.
– Користувач вводить своє ім’я та пароль (фактор знання).

– Коли система розпізнає користувача, йому буде запропоновано розпочати другий етап процесу входу в обліковий запис. На цьому етапі потрібно підтвердити наявність речі, наприклад посвідчення особи або смартфон, тобто підтвердити фактор володіння. Зазвичай використовується одноразовий код доступу, який надсилається на відповідний номер телефону, що далі використовується для підтвердження особи.

– Нарешті, користувач вводить код доступу, і після того, як сайт аутентифікує його, йому буде надано доступ.

Що таке авторизація?

Після аутентифікації система дізнається, хто є суб’єктом, який хоче отримати доступ до об’єкта.

Далі авторизація визначає рівень доступу суб’єкта до об’єкта. Іншими словами, авторизація перевіряє наявність прав для взаємодії з об’єктом.

Наприклад, у багаторівневій системі безпеки, де об’єкти позначені різними мітками класифікації (такими як «Цілком таємно», «Секретно», «З обмеженим доступом», «Несекретно»), факт аутентифікації суб’єкта не обов’язково означає, що він може мати повний доступ до будь-якого об’єкта (або повні привілеї над об’єктом). У такій системі суб’єктам надається доступ відповідно до їхніх рівнів доступу. Іншим прикладом є привілеї читання, запису та виконання, призначені суб’єктам керування файловою системою в операційних системах.

Наприклад, ви зайшли в систему як звичайний користувач, але система могла авторизувати вас як адміністратора. У даному випадку система надала право, наприклад, на редагування чи видалення інформації.

Це дуже важливо з погляду безпеки – наскільки система правильно поводиться на етапі ідентифікації, потім на етапі аутентифікації та в результаті авторизації.

Тестувальник перевіряє, чи все відбувається згідно з вимогами, чи немає помилок, тому що баги на етапах ідентифікації/аутентифікації/авторизації можуть бути критичними.

Підсумовуючи, що таке ідентифікація, аутентифікація та авторизація: ідентифікація відбувається, коли суб’єкт заявляє про свою особу, аутентифікація відбувається, коли цей суб’єкт додатково надає облікові дані, а через авторизацію керуються рівні доступу та привілеї суб’єкта.

2.2 Криптографічні методи захисту

Криптографічні методи захисту інформації – це «спеціальні методи шифрування, скремблювання або перетворення інформації таким чином, що її зміст стає недоступним без підготовки ключа шифрування та перешифрування» [10].

Криптографічний метод захисту є найнадійнішим, оскільки він захищає саму інформацію, а не доступ до неї (наприклад, зашифрований файл неможливо прочитати, навіть якщо носій інформації викрадено). Цей метод захисту реалізується у вигляді програм або програмних пакетів.

Сучасні системи захисту зашифрованих повідомлень мають наступні вимоги:

– зашифровані повідомлення можуть бути прочитані лише за наявності ключа;

– кількість операцій, необхідних для визначення ключа шифрування з частини зашифрованого повідомлення та відповідного відкритого тексту, має бути не меншою за загальну кількість можливих ключів;

– кількість операцій, необхідних для визначення ключа шифрування з частини зашифрованого повідомлення та відповідного відкритого тексту, має бути не меншою за загальну кількість можливих ключів шифрування. Кількість операцій, необхідних для отримання ключа шифрування та розшифрування повідомлення, має бути чітко визначеним мінімумом і (з урахуванням можливості використання сіткових обчислень) не повинна перевищувати можливостей сучасних комп'ютерів;

– знання алгоритму шифрування не повинно впливати на надійність захисту;

– навіть якщо використовується один і той самий ключ, невелика зміна ключа може суттєво змінити тип зашифрованого повідомлення;

– структурні елементи алгоритму шифрування не повинні змінюватися;

– будь-які додаткові біти, вставлені в повідомлення під час шифрування, повинні бути повністю приховані в зашифрованому тексті;

– довжина зашифрованого тексту повинна дорівнювати довжині відкритого тексту;

– між ключами, що використовуються в процесі шифрування, не повинно бути простих (легко розпізнаваних) залежностей;

– кожен ключ у наборі ключів повинен забезпечувати надійний захист повідомлення;

– якість алгоритму шифрування не повинна погіршуватися при зміні довжини ключів.

Алгоритми шифрування називаються криптографічними алгоритмами і представляють собою математичні функції, які використовуються для шифрування і розшифрування. Точніше, існує дві такі функції, одна для шифрування, а інша для розшифрування.

Основні криптографічні методи захисту включають:

– Симетричне шифрування: повідомлення шифруються і розшифровуються за допомогою одного ключа. Приклади: AES, DES і 3DES.

– Асиметричне шифрування: використовує пару ключів – відкритий для шифрування і закритий для дешифрування. Приклади: RSA, DSA, ECC.

– Гібридне шифрування: поєднує переваги симетричного та асиметричного шифрування для зменшення обчислювальних витрат і забезпечення високого рівня безпеки.

Криптографічні системи повинні бути стійкими до різних типів атак, включаючи грубу силу, криптоаналіз і атаки побічних каналів. Для підтримки високого рівня безпеки важливо регулярно оновлювати алгоритми шифрування та використовувати найновіші стандарти шифрування. Використання методів шифрування забезпечує високий рівень захисту конфіденційної інформації.

2.3 Фізичний захист

Фізичні (технічні) засоби захисту інформації - це різноманітні механічні, електричні та електромеханічні пристрої, конструкції та матеріали, призначені для захисту від несанкціонованого доступу та крадіжки інформації, а також для запобігання втрати інформації внаслідок збоїв компонентів інформаційної системи, стихійних лих, вандалізму та диверсій. До цієї групи належить обладнання для захисту кабельних систем, обладнання для захисту систем електроживлення, обладнання для зберігання та копіювання інформації, а також обладнання для запобігання витоку інформації з різних фізичних зон. Механізми захисту можуть бути реалізовані як окремі компоненти інформаційної системи або розподілені на інші компоненти системи. Метою вивчення дисципліни «Фізичні основи захисту інформації» є надання теоретичних знань про фізичні принципи побудови технічних засобів захисту інформації, особливості передачі сигналів по різних каналах зв’язку, методи та принципи побудови технічних засобів захисту інформації, особливості їх застосування та застосування технічних засобів захисту інформації в різних каналах зв’язку. Сформувати практичні навички встановлення несанкціонованого доступу до каналів зв’язку різними способами.

Мета фізичного захисту – це гарантування безперешкодної роботи підприємств за будь-яких обставин з урахуванням усіх застосовних до них особливих вимог та ризиків. Кожне підприємство, зокрема навчальний заклад, несе відповідальність за його фізичний захист.

Система фізичного захисту інформаційних ресурсів охоплює різні сфери, зокрема: контроль доступу; відеоспостереження та інші засоби технічного нагляду та охорони; а також системи запобігання пожежам та зменшення збитків від псування обладнання систем водовідведення та водопостачання, пошкодження електричних мереж та систем кондиціонування повітря, крадіжок зі зломом тощо. Мінімальні вимоги до усіх заходів та систем, призначених для підвищення рівня безпеки підприємства визначають з урахуванням різноманітних вимог до безпеки, що стосуються певної території, будівлі, окремого об’єкту чи групи об’єктів.

Заходи щодо охорони території, новозбудованих та реконструйованих будівель мають бути впроваджені та покращені відповідно до категорії захисту, які можна застосувати одночасно з проведенням робіт з будівництва чи реконструкції. Як правило, за управління та заходи безпеки об’єкту несе відповідальність компанія з управління нерухомістю чи власник будівлі. Однак, керівництво підприємства, що несе відповідальність за усі рішення відносно безпеки має найкраще розуміння потреб безпеки різноманітного функціоналу та рішень щодо інформаційних технологій, які вони використовують. Потреби розвитку охорони території підприємства враховуються в процесі щорічного планування. Всі особи, які виконують монтажні та ремонтні роботи на території підприємства повинні мати чинну ліцензію співробітника служби безпеки.

Охорона підприємства, закладу освіти.

Відкриті майданчики:

Під час організації руху на відкритих майданчиках, необхідно відокремити рух службового транспорту та вантажного транспорту від стоянки для відвідувачів. Якщо стороннім особам заборонено вхід на територію, поставте огорожу довкола неї. Таким чином можна позначити зони, доступні для сторонніх осіб, а також направити їх до пунктів обслуговування за правильним маршрутом з відповідним типом воріт.

Пункти обслуговування:

Будь-які загальні пункти обслуговування, фойє для відвідувачів, пункти прийому товарів та інші подібні зони призначені для сторонніх осіб, мають бути легкодоступні.

Опис функціоналу дверей:

Електронні замки та автоматизовані дверні системи.

Системи контролю доступу:

Основне призначення системи контролю доступу – гарантувати безпеку різних об’єктів, захищати власність в їхніх межах та запобігати несанкціонованому доступу завдяки наявності працівника, який має доступ до цих об’єктів чи власності. Контроль доступу та запобігання несанкціонованому доступу

стосуються як сторонніх осіб, так і персоналу відповідного підприємства. Доступ персоналу контролюється за допомогою відомчого режиму доступу та обмежень робочого часу. Жодна стороння особа не може мати доступу до об’єктів призначених виключно для персонала підприємства, закладу освіти. Наприклад, працівник має доступ до складських приміщень та виробничих потужностей впродовж робочого дня, але в позаробочий час матиме доступ лише до складських приміщень.

Управління ключами:

Фізичні ключі можна замінити електронними ідентифікаторами. Таким чином, більшості користувачів системи взагалі не будуть потрібні фізичні ключі.

Ідентифікація персоналу:

Необхідно обмежити доступ сторонніх осіб до службових об’єктів. Усі особи, які потрапляють до охоронної зони, мають ідентифікувати себе починаючи з базового рівня безпеки.

Мережева безпека має бути ретельно розроблена за допомогою контрольного переліку структури мережі, оскільки це забезпечує захист всіх наявних активів. Усі мережі мають бути класифіковані за призначенням та логічно розділені на підмережі, зокрема, на внутрішні, адміністративні (управління/контроль), ресурсні, тестові та клієнтські мережі. Відповідно до призначення мережі, окремо визначається її база користувачів і конкретні вимоги до того, як її потрібно захищати та відокремлювати. Різні мережі та їхні частини мають бути відокремлені одна від одної логічно або фізично. У контрольному переліку структури мережі можна побачити різні вимоги до структури мережі, а також чи є вони обов’язковими на базовому або вищому рівнях [4].

Системи контролю доступу.

Функціональна будова системи контролю доступу складається з трьох головних сфер:

– безпека;
– управління;
– інший функціонал.

– Найвідповіднішу систему для кожного об’єкта та для досягнення окремої цілі можна створити за допомогою поєднання наведених аспектів. Безпека складається з наступних елементів:

– управління доступом;
– контроль обладнання;
– спостереження за дверима;
– контроль пристроїв сигналізації;
– візуалізація відеоспостереження;
– об’єднання усіх елементів.

Контроль доступу охоплює визначення усіх зон доступу та прав персонального доступу, а також контроль доступу до різних зон, приміщень та ліфтів. Крім цього, контроль доступу може охоплювати журнали подій, відвідування та входи в систему, контроль часу, пов’язаний із замиканням дверей або доступом в приміщення, а також ідентифікацію транспортних засобів.

Контроль обладнання охоплює ручний, автоматичний та таймерний режими ввімкнення сигналізації, протипожежних дверей, моторизованих замків та камер відеоспостереження.

Контроль дверей охоплює моніторинг приладів, пов’язаних з об’єктом, моніторинг дверей та відповідає за відображення стану цих дверей (зачинені\ відчинені).

Основні складові (елементи) контролю пристроїв сигналізації: нічний та\або денний режими, адресні сповіщувачі, замкнуті цикли контролю струму, переадресація сигналізації, групи циклів, замкнутих шляхів, які поєднують певні дії між собою та цикли в самих групах.

Візуалізація відеоспостереження виконує функції загального інтерфейсу для вищезгаданого функціоналу, що надає можливість користувачам переглядати усі сигнали тривоги, контролювати необхідні пристрої, переглядати інструкції з експлуатації для різних ситуацій, вивчати плани поверхів будівлі та залишати коментарі, повідомлення щодо окремих випадків за необхідності.

Об’єднання допомагає користувачам централізовано керувати різними системами безпеки, як, наприклад, сигналізацією, пожежними сповіщувачами та камерами відеоспостереження через єдиний інтерфейс [6].

3 АНАЛІЗ ІСНУЮЧИХ ПРОГРАМНИХ І АПАРАТНИХ РІШЕНЬ

3.1 Виявлення і аналіз поточних проблем в області захисту інформації

ІТ-компанії, стартапи та підприємства найрізноманітніших галузей піддаються кібератакам щодня. Тільки у 2023 році кількість кібератак зросла на 62% порівняно з 2022 роком. За даними статистики, аналітики та прогнозів, наданими різними компаніями з кібербезпеки:

– атаки програм-вимагачів відбуваються кожні 10 секунд;

– жертвами програм-вимагачів у 2023 році стали понад 70% компаній;

– 71% випадків атак на організації пов’язані зі шпигунством і крадіжкою даних;

– 80% усіх порушень безпеки належать до організованої злочинності;

– до 2026 року збитки від кіберзлочинності на глобальному ринку перевищать 20 трильйонів доларів на рік.

Приділяти увагу кібербезпеці для компаній будь-яких видів у 2024 році дуже важливо, оскільки, як мінімум:

– Витік даних загрожує репутаційними ризиками. Вебсайти, CRM-системи, поштові сервіси та інші подібні системи зберігають важливу інформацію про клієнтів, яка привертає увагу зловмисників: особисті дані, телефони, адреси, електронні гаманці, кредитні картки. Якщо шахраї отримають до неї доступ, бізнесу загрожують неприємності: від компрометацій облікових записів і численних скарг користувачів до крадіжок активів і судових позовів. Не менш серйозні проблеми виникають у бізнесі під час зупинки бізнес-процесів через програми-здирники, DDoS-атаки та пошкодження даних унаслідок несанкціонованого доступу.

– Кіберзлочинці перешкоджають розвитку компаній, атакуючи IoT. За допомогою нових технологій багато підприємств, зокрема, у сфері “розумних будинків”, промисловості, енергетики, комунальних сервісів, сільського господарства тощо, можуть заощаджувати на робочій силі та підвищувати продуктивність завдяки автоматизації та оптимальному розподілу ресурсів. Збої в

налагодженій роботі пристроїв, підключених до IoT, можуть призвести до непоправних наслідків для довкілля, здоров'я і життя людей. Залишається високим ризик криптоджекінгу – атак на пристрої в спробах несанкціонованого використання для видобутку криптовалюти. Цілями стають усі види гаджетів, сервери, камери відеоспостереження, принтери та навіть побутові прилади на кшталт холодильників і пилососів, під'єднаних до Інтернету.

– Кібератаки погіршують позиції сайтів у пошуковій видачі. Якщо сайт регулярно піддається DDoS-атакам або, що ще гірше, заражений вірусами, можна забути про SEO-просування і регулярний безкоштовний трафік. Навіть запуск реклами буде проблематичним, якщо веб-сайт не пройде модерацію на відповідних майданчиках. Бізнес, який більшу частину клієнтів отримує з мережі Інтернет, у таких умовах просто не виживе.

Важливість програмно-апаратних рішень для кібербезпеки

З кожним роком актуальність ефективного управління інформаційною безпекою компаній стає дедалі нагальнішою. Термінове втручання є необхідністю, оскільки проблема не тільки не зникає, а й набуває дедалі критичнішого характеру. Ситуація продовжить погіршуватися через розвиток нейромереж – так званого "штучного інтелекту" (ШІ), який у руках зловмисників перетворюється на страшну зброю.

ШІ посилює навички Інтернет-шахраїв, даючи змогу створювати:

– більш витончені атаки та ефективні дипфейки;
– унікальні шкідливі програми, що ефективно маскуються від виявлення;
– разюче переконливі листи для фішингових атак тощо.

Крім того, через потужні можливості штучного інтелекту поріг входження в кіберзлочинність різко знижується. З урахуванням локальних криз, коли багато людей залишаються без роботи та засобів для існування, це забезпечує постійне поповнення у лавах кіберзлочинців.

Водночас середній і малий бізнеси стикаються з такими проблемами, як:

– бюджетні та часові рамки;
– відсутність можливості у керівників вникати в технічні тонкощі;
– гостра нестача кваліфікованих фахівців з інформаційної безпеки (ІБ).

3.2 Перегляд сучасних програмних і апаратних рішень

Організувати програмний захист від комп’ютерних вірусів можна такими способами:

– Розмежування доступу до інформації та зберігання її на додаткових серверах, у хмарних сховищах, щоб у випадку пошкодження мати змогу швидко відновити її;

– апаратні пристрої антивірусного захисту – набувають популярності останнім часом;

– антивірусні програми – найрозповсюдженіший засіб протидії кібератакам.

Своєю чергою антивірусні програми розподіляються на кілька видів за різними функціями:

– програми-детектори;

– програми-лікарі;

– програми-ревізори;

– програми-фільтри;

– програми-вакцини.

Переваги та недоліки

Антивірусні програми-детектори

Програми-детектори (утиліти) призначені для виявлення загроз безпеці інформації – таких як віруси, шпигунське програмне забезпечення, троянські програми, мережеві хробаки та інші види шкідливого коду. Вони сканують файли та диски, використовуючи бази даних відомих вразливостей і шаблони зловмисних програм. У разі виявлення шкідливого коду, утиліта сповіщає користувача. Або може прийняти заходи для блокування, карантинування чи видалення шкідливої програми.

Недоліки програм-детекторів. Можливості цих програм обмежені інформацією, що міститься у їхніх базах даних, і вони не можуть забезпечити 100 % захисту від усіх видів загроз, особливо нових. Блокуючи роботу шкідливих

програм, вони можуть видалити й потрібні користувачу файли. Також детектори не призначені для запобігання проникнення загроз в комп’ютери.

Антивірусні програми-лікарі.

Програми-лікарі призначені для “лікування” файлів, дисків або програм, заражених вірусами. Тобто вони здатні відновити пошкоджені шкідливим кодом програми до первинного стану, не видаляючи сам файл-носій вірусу. У цьому їх перевага у порівнянні з утилітами – детекторами.

Недоліки програм-лікарів. Як і в попередньому випадку, антивірусні програми-лікарі базуються на виявленні відомих шаблонів шкідливого коду. Тож нові шкідливі програми, які не входять у їхні бази даних, можуть пройти непоміченими. Постійне оновлення програм може частково вирішувати це питання.

Антивірусні програми-ревізори.

Програми-ревізори працюють за принципом порівняння первинного стану системи з поточним. Таким чином вони швидко реагують на будь-які підозрілі зміни у файлах. На відміну від сканерів вони працюють в рази швидше та здатні виявляти нові віруси, які ще відсутні в будь-яких базах даних. Можуть відновлювати деякі пошкоджені файли до первинного стану коштом зберігання їхніх копій.

Недоліки ревізорів: На жаль ревізори не можуть на 100% захистити від всіх вірусів, а відкат системи до попереднього стану не завжди буде гарним рішенням для користувача. Тож зазвичай ревізори використовують в комплексі з іншими антивірусними програмами.

Програми-фільтри

Програми-фільтри дозволяють виявити шкідливі програми, створені для розмноження, які звертаються безпосередньо до оперативної пам’яті системи. Так само як ревізори, вони здатні виявляти ще невідомі віруси, яких немає в антивірусних базах.

Недоліки: віруси, які завантажуються користувачем разом з легітимними програмами або звертаються до постійної пам’яті фільтрами не виявляються.

Програми-вакцини.

Вакцини призначені для обробки файлів таким чином, що віруси, які потрапляють до системи вважають їх зараженими, хоча останні працюють коректно та без перешкод для роботи користувача.

Недоліки програм-вакцин: не призначені для виявлення вірусів та лікування файлів.

До апаратних пристроїв, що запобігають викраденню паролів та надійно захищають навіть від фішингу та фізичного доступу до пристроїв відносяться апаратні ключі безпеки, смарт-картки, токени та апаратні модулі (HSM).

Апаратні ключі безпеки або токени – це невеличкі пристрої, які діють по принципу ключа від квартири чи автомобіля. Тільки відмикають вони вхід до облікового запису операційної системи або до акаунтів, що зберігаються у веб-застосунках, і на відміну від звичайних ключів, їх неможливо підробити або скопіювати. Токени здатні зберігати ідентифікаційні дані, сертифікати, ключі шифрування та іншу конфіденційну інформацію. Вони зазвичай використовуються для автентифікації, підпису документів, забезпечення безпеки та доступу до різних ресурсів.

Смарт-картки – це зазвичай пластикові картки, які містять вбудовану мікросхему з обробником, пам’яттю та інтерфейсами зв’язку. Вони можуть використовуватись для зберігання інформації, включаючи особисті дані, фінансові дані, медичну інформацію та інше. Смарт-картки часто використовуються для автентифікації, безконтактних платежів, контролю доступу, електронного паспорта та інших сфер застосування.

Основна відмінність між токенами і смарт-картками полягає у їхній формі та функціональних можливостях, проте обидва типи пристроїв використовуються для зберігання і захисту конфіденційної інформації та забезпечення безпеки в різних сферах. Проте деякі ключі безпеки, а саме – YubiKey серії 5 та YubiKey FIPS мають режим смарт-карти (PIV та CCID) [1].

Апаратний криптографічний модуль – це пристрій, що призначений для захисту криптографічних ключів (PKI) та прискорення криптографічних операцій.

Він забезпечує автентичність цифрових підписів учасників мережі блокчейн та створює безпечне середовище для реалізації IT-рішень.

Криптографічні модулі існують у різних формфакторах:

– PCI Express плати, що вбудовуються;

– мережеві модулі.

3.3 Виявлення оптимальних інструментів захисту інформації від несанкціонованого доступу до неї

Чим можуть допомогти інструменти для виявлення вторгнень

Крім інноваційних рішень на основі ШІ, як і раніше, популярними є класичні технології та системи виявлення вторгнень (IDS), зокрема:

– Мережеві системи виявлення вторгнень (Network-based IDS, NIDS). Вони моніторять як вхідний, так і вихідний мережевий трафік у реальному часі й аналізують його на наявність аномалій або сигнатур атак. Ці системи визначають такі загрози, як DoS-атаки, сканування портів і навіть спроби проникнення в мережу [2].

– Хост-орієнтовані системи виявлення вторгнень (Host-based IDS, HIDS). Ці системи встановлені на окремих хостах (наприклад, серверах або робочих станціях) і моніторять їх, включно із системними журналами, файлами та ресурсами, для виявлення незвичайної або підозрілої активності.

– Системи, що аналізують поведінку в мережі (Behavior-based IDS). Вони вивчають зразки нормальної поведінки програм або користувачів, після чого визначають аномальні дії або зміни, які можуть вказувати на можливе вторгнення.

– Системи виявлення вторгнень із гібридним підходом. Деякі IDS комбінують елементи мережевого, хост-орієнтованого, поведінкового і нейромережевого підходів, щоб забезпечити повніше виявлення загроз.

Ці технології лежать в основі більш досконалих технологій виявлення інцидентів і загроз безпеки, таких як Network Behavior Anomaly Detection (NBAD), Endpoint Detection and Response (EDR) і Network Detection and Response (NDR).

Які проблеми вирішують системи управління мережевою безпекою (SIEM)

Обсяг цифрової інформації постійно зростає. Тому дуже важливо швидко аналізувати та зіставляти дані з різних джерел і між різними інформаційними системами. Системи SIEM були одним із першокласних систем безпеки, спрямованих на надання цієї можливості – збір і представлення даних про безпеку в одному зрозумілому інтерфейсі користувача. Це дає змогу аналітикам безпеки швидко відстежувати загрози та інциденти, і реагувати на них. Тому системи SIEM досі популярні й активно розвиваються [12].

Що саме можуть такі системи:

– аналізувати вразливості та ступінь захищеності організації;

– відстежувати події, інциденти, атаки, їхні наслідки та надавати зручну візуалізацію даних;

– моніторити спроби змін прав користувачів, активувати системи оповіщення в разі порушення доступу або інсайдерських витоків;

– використовувати для збору відомостей такі джерела, як файлові сервери, фаєрволи, антивірусні програми, а також звіряти та зіставляти дані з різних джерел;

– фільтрувати події з подальшим видаленням надлишкової або повторюваної інформації;

– довгостроково зберігати дані, зібрані в хронологічному порядку, для можливості подальшого розслідування інцидентів.

Системи SIEM настільки зручні, що з ними можуть ефективно працювати навіть фахівці-початківці. Тому ці сервіси не тільки продовжать брати участь у забезпеченні безпеки компаній, а й продовжуватимуть стрімко розвиватися. Зокрема, з використанням модулів ШІ, що підвищують ефективність аналізу великої кількості даних.

Як саме працюють сучасні антивіруси, звані платформами захисту кінцевих точок (EPP):

– Проводять сканування всіх файлів і програм, що знаходяться на пристрої.

– Блокують потенційні загрози та загрози, що активувалися.

– Інтегруються з фаєрволом, скануючи вхідний і вихідний мережевий трафік.

– Захищають від фішингу, блокуючи підроблені сайти, що збирають дані.

– Надають антиспам-захист, аналізуючи вхідний поштовий трафік.

– Беруть на себе функції батьківського контролю, блокуючи сайти для дорослих, що корисно на пристроях, якими користуються діти. Аналог батьківського контролю в організаціях можна налаштувати для блокування певних сайтів, щоб офісні співробітники не відволікалися під час роботи.

– Передові EPP також можуть мати додаткові корисні функції:

– Забезпечувати резервне копіювання даних. Важливий превентивний захід, у разі, якщо шахраям вдасться обійти всі системи захисту і знищити або зашифрувати цінні дані.

– Надавати віддалене управління з іншого пристрою. Це важливо для миттєвої реакції на інцидент у разі перебування адміністратора за межами офісу або, якщо, наприклад, вірус уже проник на комп’ютер і частково заблокував роботу програм.

– Вмикати захищену віртуальну клавіатуру. Таке рішення протидіє перехопленню кейлоггерами інформації, що вводиться з фізичної клавіатури.

Незважаючи на перераховані вище функції, все ж EPP мають недоліки:

– Обмеженість у виявленні загроз. Традиційні EPP-системи можуть бути неефективними проти нових загроз, які не відповідають відомим сигнатурам або поведінковим шаблонам.

– Складність управління EPP-системи може відчуватися у великих організаціях із безліччю кінцевих точок.

– Можливий перетин функцій. При використанні функцій EPP- і EDR-рішень, система може призвести до надмірності оброблюваної інформації та відповідно – до збільшення витрат.

– Недостатня адаптація до нових реалій. Деякі класичні EPP-рішення можуть мати складнощі під час адаптації до нових реалій, таких як розвиток мобільних платформ і пристроїв IoT.

Тому світові лідери в галузі інформаційної безпеки, такі як Palo Alto Networks, вважають, що системи захисту кінцевих точок уже застаріли. Хоча можливості EPP можуть бути розширені за рахунок нових інтеграцій.

Розвиток нових технологій в області захисту інформації в комп'ютерних системах від несанкціонованого доступу супроводжується низкою викликів, які необхідно враховувати для забезпечення ефективного захисту даних. Ось приклад деяких з цих викликів:

1. Зростання складності атак. Сучасні кіберзлочинці використовують все більш складні методи для отримання несанкціонованого доступу до інформації.

2. Постійна еволюція загроз. Загрози постійно змінюються та еволюціонують, що ускладнює процес їх виявлення та нейтралізації.

3. Інтеграція нових технологій, таких як Інтернет речей (IoT), хмарні обчислення та блокчейн, створює додаткові вразливості та виклики для захисту інформації.

4. Нестача кваліфікованих кадрів. Існує значний дефіцит кваліфікованих спеціалістів у сфері кібербезпеки, що ускладнює процес розробки та впровадження ефективних методів захисту.

5. Зміна нормативної бази. Зміни в законодавстві та нормативних актах, що стосуються захисту даних та конфіденційності, можуть створювати додаткові виклики для компаній.

6. Управління великими обсягами даних. Зростання обсягів даних, які необхідно захищати, ускладнює процес їх управління та моніторингу.

7. Кібербезпека в умовах гібридної роботи. Поширення гібридної моделі роботи, коли співробітники працюють як в офісі, так і віддалено, створює додаткові виклики для захисту інформації. Необхідно забезпечити безпечний доступ до корпоративних ресурсів з різних місць та пристроїв, що вимагає впровадження додаткових заходів безпеки. Ці виклики підкреслюють необхідність постійного розвитку та вдосконалення методів захисту інформації в комп'ютерних системах для ефективного протистояння новим загрозам та забезпечення надійного захисту даних [13].

Переглянувши усі складові компоненти захисту інформації від несанкціонованого доступу, можемо визначити що усі вони разом складають велику систему захисту яка має як свої переваги та недоліки. Судячи з цього можна виділити декілька з них які будуть найефективніше захищати будь яку інформацію у різноманітних системах. На прикладі банківської системи можна запровадити наступні методи захисту інформації від несанкіонованого доступу: у банківській системі важливо впровадити низку технічних заходів для захисту інформації від несанкціонованого доступу. Шифрування всіх конфіденційних даних клієнтів та транзакцій, як під час передачі, так і при зберіганні, є обов'язковим. Для цього слід використовувати протоколи TLS/SSL та алгоритми шифрування, такі як AES. Надійні алгоритми шифрування та регулярне оновлення ключів забезпечать захист даних навіть у разі втрати чи перехоплення. Використання багатофакторної аутентифікації значно підвищує безпеку доступу до банківських ресурсів. Крім пароля, важливо застосовувати додаткові методи аутентифікації, такі як SMS-коди або додатки для аутентифікації. Впровадження чіткої системи контролю доступу до інформаційних ресурсів допоможе обмежити доступ до даних тільки тим, кому це необхідно для виконання їхніх обов'язків. Регулярний перегляд та оновлення прав доступу є важливим кроком для підтримання безпеки. Системи моніторингу та логування повинні бути встановлені для виявлення будь-якої підозрілої активності. Це дозволить швидко реагувати на потенційні загрози та запобігти несанкціонованому доступу. Регулярне оновлення антивірусного програмного забезпечення на всіх комп'ютерах та пристроях є необхідним для захисту від вірусів та інших шкідливих програм. Важливо, щоб всі співробітники дотримувалися цього правила. Використання міжмережевих екранів та VPN для захисту мережевого трафіку та безпечного доступу до внутрішніх ресурсів ззовні є необхідним для забезпечення мережевої безпеки [13].

Наразі розберемо які можна вжити організаційні заходи: розробка та впровадження чітких політик інформаційної безпеки, які будуть зрозумілі та доступні для всіх співробітників, є основою організаційних заходів. Регулярні навчання та інструктажі допоможуть підвищити обізнаність щодо безпекових

заходів та забезпечать відповідальне ставлення до захисту інформації. Регулярні оцінки ризиків та вразливостей допоможуть виявляти потенційні загрози та розробляти ефективні заходи для їх усунення. Планування дій на випадок інцидентів забезпечить швидке та ефективне реагування на непередбачені ситуації. Проведення регулярних аудитів безпеки дозволить перевіряти відповідність політикам та виявляти вразливості. Залучення зовнішніх експертів для незалежних аудитів забезпечить об’єктивну оцінку безпеки та надасть рекомендації щодо її покращення. Регулярне оновлення програмного забезпечення та операційних систем допоможе усувати відомі вразливості. Автоматизація цього процесу зменшить ймовірність людських помилок та забезпечить своєчасне оновлення усіх систем.

Головні практичні рекомендації які рекомендуються к застосуванню для повсякденної роботи співробітників та користувачів це: регулярно проводити тренінги для співробітників щодо основ інформаційної безпеки. Це включає навчання розпізнаванню фішингових атак, використанню надійних паролів та загальним правилам безпеки в Інтернеті. Здійснення регулярного резервного копіювання важливих даних забезпечить можливість їх відновлення у разі втрати або пошкодження. Це стосується як даних клієнтів, так і адміністративних даних. Забезпечення безпеки всіх кінцевих точок, таких як комп’ютери та мобільні пристрої, шляхом встановлення антивірусного програмного забезпечення та використання засобів управління мобільними пристроями (MDM) є важливим для захисту інформації від загроз. Крім того, важливо постійно нагадувати співробітникам про важливість дотримання внутрішніх політик безпеки та регулярного оновлення знань у цій сфері.

ВИСНОВКИ

Проведене дослідження з теми «Методи захисту інформації в комп'ютерних системах від несанкціонованого доступу» дозволило всебічно розглянути актуальні питання та виклики, пов'язані із забезпеченням безпеки інформації у сучасному цифровому середовищі. Робота була структурована за кількома ключовими підтемами, які охоплюють як теоретичні аспекти, так і практичні рішення.

На основі проведеного дослідження можна зробити висновок, що захист інформації в комп'ютерних системах банківських установ від несанкціонованого доступу є надзвичайно важливим і багатогранним завданням. Це завдання потребує комплексного підходу, що включає технічні, адміністративні та організаційні заходи.

Технічні заходи відіграють ключову роль у забезпеченні захисту інформації. Вони включають впровадження багаторівневої аутентифікації, шифрування даних, використання міжмережевих екранів, систем виявлення вторгнень та інших засобів безпеки. Впровадження сучасних криптографічних методів дозволяє забезпечити конфіденційність та цілісність даних, а також захистити їх від перехоплення та модифікації під час передачі.

Адміністративні заходи включають розробку та впровадження політик безпеки, що регламентують порядок доступу до інформації та її використання. Це може включати регламентацію прав доступу користувачів, проведення регулярних перевірок безпеки, навчання та інструктажі персоналу щодо безпекових процедур і вимог.

Організаційні заходи спрямовані на формування культури безпеки в установі. Вони включають регулярні навчання персоналу, проведення тренувань з реагування на інциденти, моніторинг та аналіз поточних загроз і вразливостей, а також регулярні аудити систем безпеки. Залучення зовнішніх експертів для проведення незалежних аудитів дозволяє отримати об'єктивну оцінку стану безпеки і розробити рекомендації щодо її покращення.

Результати роботи можуть бути використані будь якими інформаційними системами для удосконалення свого захисту інформаційної безпеки, підвищення рівня захисту клієнтських даних та фінансових активів. Рекомендації, розроблені в цій роботі, сприятимуть формуванню ефективних стратегій інформаційної безпеки, адаптованих до специфіки банківської діяльності.

Таким чином, ефективний захист інформації в будь яких інформаційних системах потребує постійного оновлення та вдосконалення методів і засобів безпеки, дотримання нормативних вимог та стандартів, а також активного залучення персоналу до процесів забезпечення безпеки. Тільки комплексний підхід дозволить забезпечити надійний захист інформаційних ресурсів в умовах стрімкого розвитку технологій і зростання кіберзагроз.На основі проведеного дослідження можна зробити висновок, що захист інформації в комп’ютерних системах від несанкціонованого доступу є багатогранним завданням, яке вимагає комплексного підходу. Сучасні методи та засоби захисту повинні постійно оновлюватися та вдосконалюватися, щоб відповідати новим викликам та загрозам, які виникають в умовах стрімкого розвитку технологій. Важливо також приділяти увагу навчанню персоналу, дотриманню нормативних вимог та інтеграції новітніх технологій безпеки для забезпечення надійного захисту інформаційних ресурсів.

ПЕРЕЛІК ПОСИЛАНЬ

1. Захист інформації – огляд технічних засобів. URL: http://surl.li/tzbzs
2. Тенденції кіберпроблем і рішень від 10.04.2024 URL: http://surl.li/tzcbk
3. Програмно-апаратне забезпечення та захист мобільних пристроїв від 19.12.2022 URL: http://surl.li/tzlcn
4. Каганюк О.К., Чернящук Н.Л., Бурчак І.Н, [Електронний ресурс]: Науковий журнал «Комп'ютерно-інтегровані технології: освіта, наука, виробництво» Луцьк, 2022. Випуск № 47 Режим доступу : http://surl.li/tygos
5. Комплексний захист URL: http://surl.li/tzldu
6. Фізичні основи захисту інформації URL: http://surl.li/tygqd
7. Захист інформації в локальних мережах матеріал з вікіпедії – вільної енциклопедії. URL: http://surl.li/tygqx
8. Цінна інформація і конфіденційні документи: система захисту URL: http://surl.li/tzchz
9. Інженерний захист інформації матеріал з вікіпедії – вільної енциклопедії. URL: http://surl.li/tygtl
10. Криптографічні методи захисту інформації. Контроль цілісності програмних і інформаційних ресурсів. [Електронний ресурс]: Освітній журнал «На Урок». Режим доступу : http://surl.li/tzcce
11. Поняття інженерно-технічного захисту URL: https://studfile.net/preview/6012701/page:38/
12. Інженерний захист інформації матеріал з вікіпедії – вільної енциклопедії. URL : http://surl.li/tygyy
13. Поради для захисту даних від 20.12.2019 URL: http://surl.li/tzccr
14. Про інформацію: Закон України від 02.10.1992р. № 2657-XII. Дата оновлення 27.07.2023р. № 3005-IX. URL: https://zakon.rada.gov.ua/laws/show/2657-12