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

Кафедра кібербезпеки

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«ІНСТРУМЕНТИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ТА АНОНІМІЗАЦІЇ КОРИСТУВАЧІВ У ЦИФРОВОМУ ПРОСТОРІ»

Виконав: здобувач 4 курсу
Рівень бакалавр
Галузь знань 12 «Інформаційні технології»,
Спеціальність 125 «Кібербезпека»
Якимов Віталій Олександрович

Керівник: к.т.н., доцент
Ахмаметьєва Ганна Валеріївна

Рецензент : д.т.н., професор
Казакова Надія Феліксівна

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 Якимову Віталію Олександровичу

1.Тема роботи: «Інструменти забезпечення безпеки та анонімізації користувачів у цифровому просторі»

Керівник роботи: к.т.н., доцент Ахмаметьєва Ганна Валеріївна
затверджена наказом НУ ОЮА № 809-06 від «02» квітня 2024 року

2. Строк подання здобувачем роботи «20» травня 2024 року

3. Дата видачі завдання«15» вересня 2023 року

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 «Інструменти забезпечення безпеки та анонімізації користувачів в цифровому просторі» на здобуття першого (бакалаврського) рівня вищої освіти за спеціальністю 125 Кібербезпека, освітньою програмою: Кібербезпека, містить 9 рисунків, 1 таблицю та 9 літературних джерел за переліком посилань. Робота виконана на 44 сторінки загального тексту і 35 сторінок основного тексту.

Метою роботи є дослідження та аналіз інструментів забезпечення безпеки та анонімізації користувачів у цифровому просторі. У рамках дослідження розглянуто такі методи, як використання мережі Tor, VPN-сервісів та проксі-серверів. Розроблено алгоритми оцінки ефективності та безпеки кожного з методів для різних сценаріїв використання, а також їх вплив на конфіденційність та швидкість доступу до інтернет-ресурсів.

Результати роботи можуть бути використані для підвищення рівня захисту приватних даних користувачів в інтернеті, а також для вдосконалення існуючих інструментів анонімізації. Зокрема, рекомендації щодо вибору оптимального інструменту залежно від конкретних потреб і загроз, дозволять користувачам краще захистити свою інформацію від зловмисників.

Можливими напрямками подальших досліджень є інтеграція розглянутих методів з іншими технологіями кібербезпеки, такими як системи виявлення та запобігання вторгнень (IDS/IPS), а також розробка нових алгоритмів, що забезпечують підвищену стійкість до сучасних кіберзагроз.

ЗАГРОЗИ, БЕЗПЕКА, АНОНІМІЗАЦІЯ, ПЕРСОНАЛЬНІ ДАНІ, ШИФРУВАННЯ, ІНТЕРНЕТ МЕРЕЖА

ABSTRACT

Qualification work on the topic ‘Tools for ensuring the security and anonymisation of users in the digital space’ for the first (bachelor's) level of higher education in the speciality 125 Cybersecurity, educational programme: Cybersecurity, contains 9 figures, 1 table and 9 references. The work consists of 44 pages of general text and 35 pages of the main text.

The purpose of the work is to study and analyse tools for ensuring the security and anonymisation of users in the digital space. The study considers such methods as the use of the Tor network, VPN services and proxy servers. Algorithms have been developed to assess the effectiveness and security of each method for different scenarios of use, as well as their impact on privacy and speed of access to Internet resources.

The results of the work can be used to increase the level of protection of users' private data on the Internet, as well as to improve existing anonymisation tools. In particular, recommendations on how to choose the best tool depending on specific needs and threats will allow users to better protect their information from intruders.

Possible areas for further research include the integration of the methods discussed with other cybersecurity technologies, such as intrusion detection and prevention systems (IDS/IPS), as well as the development of new algorithms that provide increased resistance to modern cyber threats.

THREATHS, SECURITY, ANONYMIZATION, PERSONAL DATA, ENCRYPTION, INTERNET

ЗМІСТ

ВСТУП

В сучасному цифровому світі питання забезпечення безпеки та анонімізації користувачів набули надзвичайної важливості. З розвитком інформаційних технологій та інтернету з'явилися нові загрози, що ставлять під загрозу конфіденційність і безпеку даних користувачів. Кіберзлочинці використовують різноманітні методи для незаконного доступу до приватної інформації, що створює необхідність у постійному вдосконаленні засобів захисту, тому важливо розуміти та використовувати сучасні інструменти безпеки та анонімізації, щоб ефективно протистояти цим загрозам.

Одним з ключових аспектів цифрової безпеки є анонімізація користувачів. Це означає приховування їхніх дій та ідентичності в інтернеті, що дозволяє уникати відстеження та зберігати приватність. В контексті цієї роботи основну увагу приділено трьом основним методам забезпечення анонімності: використанню мережі Tor, VPN-сервісів та проксі-серверів.

Метою цієї роботи є дослідження та порівняння ефективності зазначених інструментів для забезпечення безпеки та анонімізації користувачів у цифровому просторі. У ході дослідження буде розглянуто алгоритми оцінки ефективності та безпеки кожного з методів, а також їх вплив на конфіденційність та швидкість доступу до інтернет-ресурсів. Особливу увагу буде приділено аналізу ризиків і вразливостей, пов'язаних з використанням кожного з інструментів.

Забезпечення безпеки та анонімізації в цифровому просторі є надзвичайно важливим завданням для захисту приватності користувачів та запобігання несанкціонованому доступу до їхніх даних. Використання таких інструментів, як Tor, VPN та проксі-сервери, дозволяє значно підвищити рівень захисту в інтернеті. Однак, кожен з методів має свої переваги та недоліки, які слід враховувати при виборі найбільш підходящого рішення для конкретних потреб користувачів.

У подальших розділах цієї роботи буде детально розглянуто кожен з методів, а також запропоновано рекомендації щодо їх ефективного використання для забезпечення максимальної безпеки та анонімності в цифровому середовищі.

Діяльність з захисту персональних даних на території України регулюється Законом України "Про захист персональних даних", Конституцією України, іншими законами та нормативно-правовими актами, а також міжнародними договорами та стандартами.

Метою цієї роботи є розробка рекомендацій з підвищення рівня безпеки користувачів при використанні цифрового простору.

У роботі були поставлені наступні задачі:

-проаналізувати стан безпеки в цифровому просторі;

-проаналізувати технології та методи захисту;

-оцінити ефективність існуючих практик та політик безпеки;

-на основі загального регламенту про захист даних розробити рекомендації щодо підвищення рівня безпеки персональних даних.

Об’єктом досліджень є користувачі, інформаційні ресурси та програмне забезпечення.

Практична цінність роботи полягає у впровадженні рекомендацій для підвищення рівня інформаційної безпеки користувачів які зберігають, оброблюють та передають дані через мережу інтернет.

1 ТЕОРЕТИЧНИЙ АНАЛІЗ ЦИФРОВОЇ БЕЗПЕКИ ТА АНОНІМІЗАЦІЇ

1.1 Поняття цифрової безпеки та анонімності

Наприкінці 20 – на початку 21 століття, в умовах становлення та розвитку інформаційної цивілізації, інформаційно-цифрова безпека стала однією з найважливіших складових системи національної безпеки будь-якої країни, оскільки інформаційно-комунікаційні технології почали суттєво впливати на національну безпеку. Це стосується не лише соціальної економіки, політики та права, соціальної культури та інших сфер суспільного життя, а й національної безпеки. Інформаційно-комунікаційні технології тісно пов’язані з формуванням будь-якої національної інформаційної політики та захистом життєво важливих інтересів суспільства у сфері інформаційної безпеки. Після того як військова політика та інформаційна політика багатьох країн сформували тісний взаємозв'язок на різних рівнях (структурної функції, мети та семантики), з'явився новий напрям політики - військова інформація.

2014 рік став роком величезних змін у європейському просторі. Політична нестабільність в Україні та збройна агресія з боку Росії призвели до кардинальних змін геополітичній ситуації не лише в Європі, а й у всьому світі. Існуюча система безпеки, яка гарантувала відносну стабільність континенту, була повністю зруйнована. Нові геополітичні умови посилили старі конфлікти та спричинили за собою створення нових, серйозно вплинувши на реалізацію питань забезпечення кібербезпеки у багатьох сучасних країнах.

Отже, в сучасному світі інформаційно-комунікаційні технології стали не тільки впливовим політичним інструментом, але й потужним інструментом ведення гібридної війни. Зокрема, в умовах російсько-українського збройного конфлікту, який триває вже десятий рік, інформаційна безпека стає все більш істотним чинником забезпечення національної безпеки України.

Відомо, що цифрова безпека включає комплекс заходів, спрямованих на захист інформації, комп'ютерних систем і користувачів від кіберзагроз, з метою уникнення таких проблем :

а) неповнота, затримка або недостовірність використовуваної інформації;

б) негативні інформаційні впливи та шкідливі наслідки застосування інформаційних технологій;

в) несанкціоноване поширення й використання інформації;

г) порушення цілісності, конфіденційності та доступності інформації. [1, с. 297]

Фокусується на захисті цифрових технологій, систем і інфраструктури, охоплює заходи безпеки, спрямовані на захист від кіберзагроз, таких як хакерство, віруси, кібератаки, зловживання даними, тощо, займається захистом комп'ютерних мереж, електронних пристроїв, програмного забезпечення та даних, що зберігаються та передаються в цифровій формі. В той час як інформаційна безпека охоплює захист інформації, незалежно від форми або медіа, в якому вона знаходиться (цифрова, паперова, усна тощо), включає політики, процедури і технічні заходи для забезпечення конфіденційності, цілісності, доступності та надійності інформації, та займається не тільки технічними аспектами, але й охоплює людей, процеси, стандарти та культуру організації.[2]

Відомо також, що дослідники виокремлюють два види інформаційної безпеки: інформаційно-технічну (кібербезпеку) та інформаційно-психологічну. Однак, сьогодні увага здебільшого зосереджена на технічних і технологічних аспектах інформаційної безпеки, тоді як соціогуманітарний вимір, тобто інформаційно-технологічна безпека українського суспільства, залишається поза увагою. Це є негативною тенденцією, оскільки об’єктом інформаційно-психологічного впливу є ментальність, свідомість і поведінка населення та військовослужбовців, а також системи формування громадської думки і прийняття суспільно важливих рішень. Сутність інформаційно-психологічної безпеки полягає в захищеності від заподіяння шкоди як національних інформаційних ресурсів, так і психічного здоров’я людини й суспільства.[1, с. 297]

Інтернет – цифровий портал, який використовується щодня для безлічі завдань , таких як спілкування з друзями, отримання інформації, роботи або шопінгу. Він є невід’ємною частиною нашого повсякдення, надаючи безмежні

можливості, але й маючи безліч загроз, які можуть ставити під загрозу конфіденційність та безпеку. Ці загрози змушують дізнатися про те, що таке цифрова безпека та кібергігієна.

Питання анонімності користувача в цифровому просторі стає все більш актуальним. З одного боку прагнення до свободи слова та самовираження без контролю чи цензури, з іншого – ризики відстеження цифрових слідів та крадіжки персональних даних. Отже, анонімність – це стан, коли особистість та його дії в Інтернеті неможливо ідентифікувати. На жаль повної анонімності в Інтернеті досягти неможливо, можливо тільки мінімізувати ризики відстеження, шляхом виконання сукупності методів захисту приватності користувача.

Протилежне поняття анонімізації є деанонімізація (жарг. деанон; також доксинг) – порушення анонімності, що полягає в публікації персональних даних (справжніх ПІБ, місця проживання або роботи та ін.) учасника Інтернету, зокрема : вікіпроектів, блогів, форумів і т.д. Під деанонімізацією може також розуміти зіставлення кількох акаунтів однієї людини на одному або кількох інтернет-сайтах. Для деанонімізації користувача практично завжди достатньо відкритої інформації та відкритих способів її обробки, в першу чергу правильних пошукових запитів. Математично деанонімізація описується виявлення нових областей перетину множин, що відображають сліди користувача в мережі. В даний час користувач у місцях комунікації в Інтернеті має право розпоряджатися своєю анонімністю (у разі України, країн Євросоюзу, США тощо).

Анонімність користувачів в цифровому просторі є важливою з кількох причин:

– Захист конфіденційності: анонімізація допомагає захистити особисту інформацію користувачів, таку як ім'я, адреса, номер телефону та фінансова інформація, від несанкціонованого доступу та використання.

– Свобода слова: Анонімність дозволяє користувачам вільно висловлювати свої думки та ідеї в Інтернеті, не боячись цензури або переслідування.

1.2 Ризики та загрози для користувачів

Найголовнішим і найкритичнішим викликом є стрімкий розвиток технологій. Зростання обчислювальних потужностей та обсягів оброблюваних даних, а також розширення спектру завдань, що вирішуються інформаційними системами, ускладнюють ретельний і детальний аналіз потенційних вразливостей, ускладнюючи усунення умов для їх експлуатації. Після того, як користувачі опановують нову технологію і розробляють заходи безпеки для її захисту, ця технологія часто застаріває і на зміну їй приходять новіші інновації. Ці нові технології також вимагають специфічних знань і навичок, увічнюючи безперервний цикл адаптації у сфері цифрової безпеки.

Розглянемо причини появи уразливостей у комп’ютерній технології обробки інформації. Зазначимо, що вразливість (англ. system vulnerability) — нездатність системи протистояти реалізації загрози або сукупності загроз. Тобто це певні дефекти комп'ютерної системи, що дозволяють навмисно порушити її цілісність і спричини некоректну роботу. Уразливісті можуть виникнути через програмні помилки, недоілки в системі, ненадійні паролі, віруси та інші шкідливі програми, сценарії та впровадження SQL. Деякі уразливості відомі лише теоретично, а інші активно використовуються та експлуатуються.[3]

Цей цикл зміни технологій створює загрози можуть включати в себе аспекти, пов’язані з кібербезпекою, конфіденційністю даних, безпекою мережі чи приватністю користувачів :

– Віруси та шкідливе програмне забезпечення : можуть призвести до втрати даних, шкоди для системи або навіть крадіжки конфіденційної інформації.

– Інтернет-шахрайство: атаки, які спрямовані на використання соціальної інженерії з метою заволодіння конфіденційною інформацією, такою як паролі або фінансові дані.

– DDoS-атаки: атаки на інфраструктуру мережі з метою заборонити користувачам доступ до послуг або ресурсів.

– Витік даних: отримання доступу до особистої інформації користувачів

через веб-сайти, соціальні мережі або компрометовані облікові записи.

– Крадіжка ідентичності : зловмисник може використовувати викрадену інформацію для підробки облікових записів або здійснення шахрайства від імені потерпілого.

– Незахищеність бездротових мереж : недоцільно захищені бездротові мережі можуть використовуватися для перехоплення чутливої інформації.

Для забезпечення безпеки важливо розуміти ці загрози та приймати відповідні заходи для їх запобігання.

2 ТЕХНОЛОГІЇ ТА ІНСТРУМЕНТИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ

2.1 Шифрування і захист даних

Механізми захисту представляють собою різноманітні інструменти та методи, спрямовані на забезпечення конфіденційності, цілісності та доступності інформації, а також на запобігання несанкціонованому доступу та зловживанню. Ключовими аспектами що відіграють критичну роль є криптографічний захист, контроль доступу та механізми аутентифікації.

Шифрування – перетворення даних у шифрований формат, щоб лише авторизовані користувачі мали доступ до інформації. Процес шифрування став можливим завдяки комбінації ключів шифрування та математичних алгоритмів. Розглядатимемо два основних типи шифрування – симетричне та асиметричне, серед них виділимо часто використовувані алгоритми шифрування.

2.1.1 Симетричне шифрування

У симетричному шифруванні, як випливає з назви, для шифрування і розшифрування даних використовується один криптографічний ключ, схема зображена на рисунку 2.1.

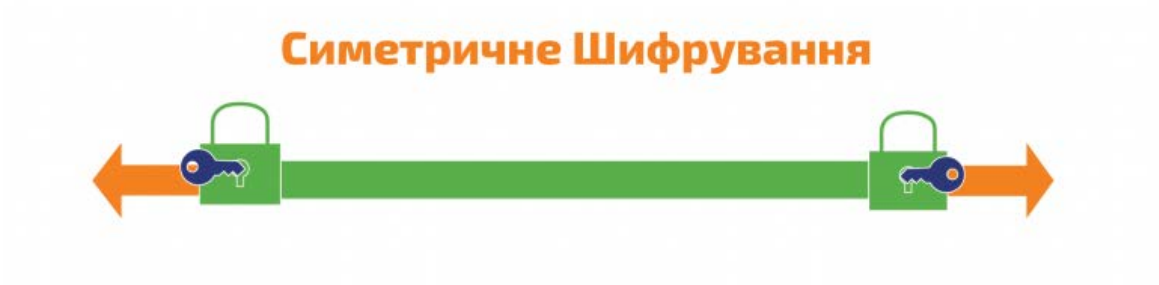

Рисунок 2.1 – Схема симетричного шифрування

Використання одного ключа для обох процесів робить процедуру простою. Найвизначнішою особливістю симетричного шифрування є простота процесу, оскільки один ключ використовується як для шифрування, так і для дешифрування.

Коли необхідно зашифрувати великий обсяг даних, симетричне шифрування виявляється чудовим варіантом. Тому алгоритми симетричного шифрування:

– Набагато швидші за свої асиметричні аналоги;
– Вимагають менше обчислювальної потужності;
– Не знижують швидкість інтернету.

Існують сотні симетричних алгоритмів. Найбільш поширені з них – AES, RC4, DES, 3DES, RC5, RC6 тощо. Розглянемо декілька :

1. Симетричний алгоритм 3DES

3DES також відомий як TDEA (Triple Data Encryption Algorithm). Це оновлена версія алгоритму DES розроблена для усунення його недоліків і введений в експлуатацію в кінці 1990-х років. Оновлений алгоритм застосовував цикли DES 3 рази до кожного блоку даних, що значно підвищує його стійкість до зламів, завдяки цьому знайшов використання в платіжних системах та інших технологіях фінансової галузі. Також став частиною протоколів TLS, SSH, IPsec і OpenVPN.

Усі алгоритми шифрування з часом втрачають надійність, і 3DES не виняток. Уразливість Sweet32 була виявлена Картікеяном Бхаварганом і Гаетаном Леурентом. Відкриття змусило індустрію безпеки розглянути питання щодо старіння алгоритму, про що Національний інститут стандартів і технологій США (англ. National Institute of Standards and Technology, NIST) офіційно оголосив у нормативному проекті, опублікованому в 2019 році.

Відповідно до проекту, після 2023 року використання 3DES було припинено у всіх нових програмах. Варто також відзначити, що TLS 1.3, новітній стандарт для протоколів SSL / TLS, також припинив використання 3DES.

2. Алгоритм симетричного шифрування AES

AES (Advanced Encryption System), також відомий як Rijndael, є одним з найпоширеніших алгоритмів шифрування. Він був розроблений як альтернатива DES і затвердженний NIST в 2001 році, ставши новим стандартом шифрування. AES – це сімейство блокових шифрів з різною довжиною ключів і розмірами блоків.

Методи шифрування AES включають підстановки і перестановки. Спочатку

дані розбиваються на блоки, після чого шифруюця з використанням ключа. Процес шифрування складається з різних етапів, таких як зсуви рядків, змішування стовпців і додавання ключів. Залежно від довжини ключа виконується 10, 12 або 14 раундів таких трансформацій. Варто зазначити, що останній раунд відрізняється від попередніх і не включає етап змішування.

Перевага використання алгоритму шифрування AES :

AES відзначається високою безпекою, швидкістю та гнучкістю. Він значно швидший за DES. Головною перевагою AES є варіанти довжиною ключів – чим довший ключ, тим складніше його зламати.

На сьогоднішній день AES є найпопулярнішим алгоритмом шифрування і використовується в багатьох додатках, зокрема:

- Бездротова безпека;
- Безпека процесорів і шифрування файлів;
- Протокол SSL / TLS (забезпечення безпеки вебсайтів);
- Безпека Wi-Fi;
- Шифрування мобільних додатків;
- VPN (Virtual Private Network).

2.1.2 Асиметричне шифрування

Для асиметричного шифрування використовується пара ключів для шифрування і дешифрування даних, які математично пов’язані між собою, схема зображена на рисунку 2.2. Один із цих ключів називається відкритим ключем, а інший закритим ».

Основною і найбільш очевидною перевагою цього типу шифрування є підвищена безпека, яку він пропонує. У цьому підході відкритий ключ, доступний кожному, використовується для шифрування даних, тоді як закритий ключ, який повинен зберігатися в безпеці, використовується для розшифрування даних. Цей механізм захищає дані від атак типу «людина посередині» (Man in the middle). Для веб-серверів та серверів електронної пошти, які з'єднуються з численними

клієнтами, потрібно керувати та захищати лише один ключ. Значною перевагою є те, що криптографія з відкритим ключем дозволяє створювати зашифроване з'єднання без необхідності попереднього обміну ключами в автономному режимі.

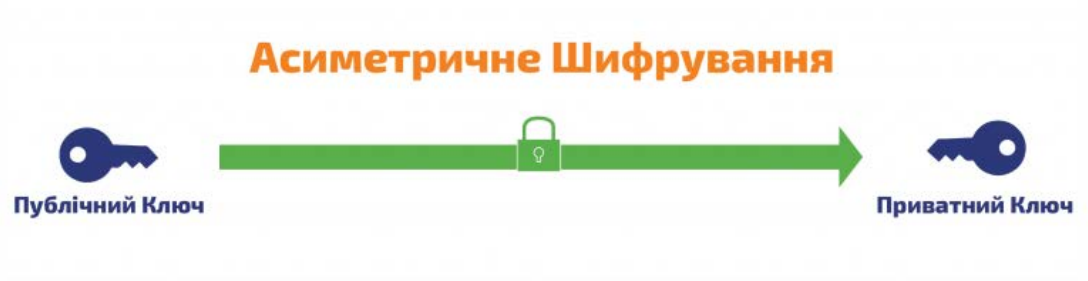

Рисунок 2.2 – Схема асиметричного шифрування

Ще однією важливою особливістю асиметричного шифрування є автентифікація. Оскільки дані, зашифровані відкритим ключем, можуть бути розшифровані лише за допомогою відповідного закритого ключа, це гарантує, що тільки передбачуваний одержувач може отримати доступ до даних і розшифрувати їх. Це гарантує, що комунікація або обмін інформацією відбувається з законною особою або організацією.

Алгоритм асиметричного шифрування RSA був винайдений у 1977 році трьома вченими з Массачусетського технологічного інституту Рон Ривест, Аді Шамір і Леонард Адлеман (Ron Rivest, Adi Shamir, Leonard Adleman звідси «RSA»). Сьогодні цей алгоритм є найпоширенішим. Його сила полягає в методі «простої факторизації». По суті, вибираються два різних випадкових простих числа певного розміру і перемножуються, щоб сформувати велике складне число. Завдання полягає в тому, щоб вирахувати вихідні числі з цього складеного числа, що майже неможливо

У 2010 році група добровольців провела дослідження і їм знадобилося більше 1500 років обчислювального часу (розподіленого по сотням комп'ютерів), щоб зламати 768-бітний ключ RSA, що набагато нижче стандартного 2048-бітного, який використовується сьогодні.

Одна з основних переваг RSA полягає у його гнучкості, що дозволяє

використовувати ключі різної довжини: 768-бітні, 1024-бітні, 2048-бітні, 4096-бітні та інші. Завдяки можливості налаштовувати довжину ключів, RSA забезпечує відповідний рівень безпеки залежно від потреб користувача.

RSA базується на фундаментальних математичних принципах, що спрощує його впровадження в інфраструктуру відкритих ключів (PKI). Простота реалізації, висока адаптивність і надійність зробили RSA найбільш популярним алгоритмом асиметричного шифрування для широкого спектру застосувань, таких як сертифікати SSL/TLS, криптовалюти і шифрування електронної пошти.

Переваги симетричного і асиметричного шифрування зібрані в таблицю 2.1:

Таблиця 2.1 – Переваги симетричного і асиметричного шифрування

Симетричне шифрування	Асиметричне шифрування
шифрування/дешифрування виконується одним ключем	шифрування/дешифрування виконується різними ключами
простий процес шифрування	складний процес шифрування
шифрування великих об’ємів тексту	забезпечення автентифікації.
швидкий процес при малої потужності	потребує більше часу та потужності
для шифрування даних використовується менша довжина ключа (128-256 біт).	використовуються довші ключі шифрування (1024-4096 біт).

Симетричне та асиметричне шифрування мають свої переваги залежно від контексту використання. Симетричне шифрування використовує один ключ для шифрування та дешифрування, що робить процес простим і швидким, особливо для великих обсягів даних. Воно потребує менше обчислювальних ресурсів і використовує коротші ключі (128-256 біт).

Асиметричне шифрування використовує різні ключі для шифрування і дешифрування, що підвищує безпеку. Воно забезпечує автентифікацію і є важливим для перевірки джерела інформації. Хоча цей метод вимагає більше часу та ресурсів і використовує довші ключі (1024-4096 біт), він надає додаткові

переваги безпеки.

Вибір між цими методами залежить від потреби у швидкості, ресурсах і рівні безпеки.[4]

2.2 Системи ідентифікації та автентифікації

Ідентифікація є частиною будь-якої системи безпеки для контролю доступу до ресурсів та захисту конфіденційної інформації від несанкціонованого доступу. Процес визначення особистості або об’єкта в системі є ключовим елементом для забезпечення захищеного доступу, але не менш важливим є перевірка належності ідентифікатора об’єкту – автентифікація.

Автентифікація – процес підтвердження належності ідентифікатора суб’єкту на основі секретного елемента (автентифікатора), яким володіє суб’єкт і інформаційна система. Замість того, щоб зберігати сам секретний елемент, інформаційна система зберігає певні дані про нього, які вона використовує для перевірки ідентифікатора суб'єкта. Спочатку система запитує у користувача ім'я користувача та пароль. У ролі ідентифікатора виступає введене ім'я користувача, а в ролі аутентифікатора - пароль. Зазвичай операційна система зберігає хеш пароля, а не сам пароль, що підвищує безпеку, ускладнюючи відновлення оригінального пароля.

Методи автентифікації умовно розділяють на :

Однофакторна автентифікація (Single-Factor Authentication, SFA) – найбільш поширений базовий метод, при якому перевіряється лише один фактор. Користувач вводить унікальний пароль або PIN-код для доступу, недоліком якого є крадіжка або злам паролю.

Двофакторна автентифікація (Two-Factor Authentication, 2FA) вимагає два різні фактори для перевірки користувача. Фактори поділяються на три категорії : логічні, ідентифікаційні та біометричні.

а) Логічні (те, що ви знаєте) : користувач вводить пароль або секретну фразу відому лише йому.

b) Ідентифікаційні (те, що у вас є) : фізичні пристрої, призначені для носіння автентифікаційних даних в різних формах читання, такі як токени, смарт-карти, магнітні-карти, тарт-карти, штрих кодові карти.

c) Біометричні (те, ким ви є) ключовою інформаціює є унікальні дані людини, такі як : відбитки пальців (сканування відбитка для підтвердження), райдужна оболонки ока (сканування райдужки для автентифікації), розпізнавання обличчя (популярна технологія FaceId), голос (використання голосових команд).

Приклади двофакторної автентифікації :

a) Логічний + Ідентифікаційний : введення пароля і одноразового коду;

b) Логічний + Біометричний: використання пароля і сканування відбитка пальця.

c) Ідентифікаційний + Біометричний : використання смарт-карти і сканування райдужної оболонки ока.

Недоліками логічних методів є те , що паролі можуть бути вкрадені або вгадані, ідентифікаційних методів те, що фізичні носії можуть бути загублені, викрадені або пошкодженні, а біометричних є те що в обслуговуванні вони дорожчі та складніші, також чутливі до змін фізичних параметрів користувача.

Багатофакторна автентифікація (Multi-Factor Authentication, MFA) – цей метод включає використання більше ніж двох факторів підтвердження об’єкта системи, що суттєво підвищує рівень безпеки порівняно з однофакторною та двофакторною автентифікацією.

Кожен клас методів має свої переваги і недоліки. Майже всі методи автентифікації страждають на один недолік - вони, насправді, автентифікують не конкретного суб’єкта, а лише фіксують той факт, що автентифікатор суб’єкта відповідає його ідентифікатору. Тобто всі відомі методи не захищені від компрометації автентифікатора.

2.3 Захист мережі та програмного забезпечення

Захист мережі та програмного забезпечення є критично важливим для запобігання кіберзагрозам, які можуть призвести до втрати даних, фінансових збитків та порушення приватності. Надійний захист забезпечує безперебійну роботу систем, захищає конфіденційну інформацію та безпеку користувачів цифрових послуг.

2.3.1 Мережевий фаєрвол

Одним із найважливіших елементів інфраструктури для захисту мережі є мережевий фаєрвол, також відомий як брандмауер — це пристрій безпеки мережі, призначений для моніторингу, фільтрації та контролю вхідного та вихідного мережевого трафіку на основі заздалегідь визначених правил безпеки. Основне призначення брандмауера – встановити бар’єр між довіреною внутрішньою мережею та ненадійними зовнішніми мережами. Брандмауери бувають як апаратного, так і програмного забезпечення перевіряючи пакети даних визначаючи дозволяти чи блокувати їх на основі набору правил, окремо можна налаштувати ці правила, щоб дозволяти або забороняти трафік на основі різних критеріїв, таких як IP-адреси джерела та призначення, номери портів і тип протоколу.

Традиційно брандмауери регулюють трафік, утворюючи безпечний периметр навколо мережі або комп’ютера. Це запобігає доступу будь-кого до мережевих ресурсів, якщо вони не авторизовані на це. Без цього захисту практично будь-хто міг увійти і робити, що йому заманеться. Сучасний ландшафт кібербезпеки вимагає багаторівневого підходу. Хоча брандмауери залишаються надійним захистом мережі, просунуті загрози вимагають додаткових заходів безпеки. Розвиток хмарних обчислень і гібридних робочих середовищ ще більше підкреслює потребу в комплексних рішеннях безпеки.

На щастя, передові технології брандмауера з послугами на основі штучного інтелекту прискорюють безпеку мережі. Поєднуючи сильні сторони традиційних

інструментів з інноваційними можливостями нових рішень, постачальники сучасних брандмауерів допомагають захищатися навіть від найскладніших стратегій атак.

Може працювати на різних рівнях мережі, включаючи мережевий , прикладний та рівень з'єднання захищаючи від шкідливого трафіку. Стратегічно розташовані в центрі обробки даних, що дозволяє стежити за всіма спробами перетнути цю межу. Ця видимість також дозволяє мережевому брандмауеру детально перевіряти та автентифікувати пакети даних у реальному часі. Це передбачає перевірку пакета даних на відповідність заздалегідь визначеним критеріям, щоб визначити, чи становить він загрозу. Якщо він не відповідає критеріям, брандмауер блокує його вхід або вихід з мережі.

Брандмауери регулюють як вхідний, так і вихідний трафік, захищаючи мережу від

– Зовнішніх загроз , такі як віруси, бекдори, фішингові електронні листи та атаки на відмову в обслуговуванні (DoS). Брандмауери фільтрують вхідні потоки трафіку, запобігаючи несанкціонованому доступу до конфіденційних даних і перешкоджаючи потенційному зараженню шкідливим програмним забезпеченням.

– Внутрішніх загроз, брандмауер може застосовувати правила та політики для обмеження певних типів вихідного трафіку, що допомагає виявити підозрілу активність і зменшити викрадання даних.

Класифікують мережеві екрани в залежності відстеження поточного з'єднання :

а) «безстаний» (stateless), захищає мережу, аналізуючи трафік у протоколі транспортного рівня — місці, де пристрої спілкуються один з одним. Замість того, щоб зберігати інформацію про стан мережевого з'єднання, він перевіряє трафік на основі пакетів. Потім він вирішує заблокувати або дозволити трафік на основі даних, розташованих у «заголовку пакета». Це може включати IP-адреси джерела та призначення, номери портів, протоколи та іншу інформацію, цей процес називається фільтрацією пакетів. Незважаючи на швидкість і недорогість, stateless брандмауери мають свої вразливості. Важливо те, що вони не бачать послідовності

пакетів. Це означає, що вони не можуть виявити нелегітимні пакети, які можуть містити вектори атаки або не мати відповідного запиту. Крім того, вони мають уявлення лише про заголовок пакета, а не про його фактичний вміст. Це унеможливлює виявлення зловмисного програмного забезпечення, прихованого в корисному навантаженні пакета.

b) «зі станом» (stateful) відстежують останній або безпосередній стан активних підключень. Моніторинг стану та контексту мережевих комунікацій може допомогти виявити загрози на основі більш глибокої інформації. Наприклад, блокують або дозволяють трафік, аналізуючи, звідки він надходить, куди прямує та вміст його пакетів даних. Крім того, вони оцінюють поведінку пакетів даних і мережевих з'єднань, каталогізують шаблони та використовують цю інформацію для покращення майбутнього виявлення загроз. Цей підхід забезпечує більший захист порівняно з фільтрацією пакетів, але значно погіршує продуктивність мережі, оскільки виконує більш глибокий аналіз.[5]

Мережеві фаєрволи, хоча і ефективні у контролі та фільтрації трафіку, можуть бути обмежені в здатності виявляти складні кіберзагрози. Системи виявлення та запобігання вторгнень забезпечують додаткові можливості для виявлення і реагування на потенційні загрози в режимі реального часу.

2.3.2 IDS/IPS системи

Системи виявлення та запобігання вторгнень (IDS/IPS) відіграють ключову роль у сучасній кібербезпеці, забезпечуючи активний моніторинг і захист мережі від зловмисних атак. IDS (Intrusion Detection Systems) фіксують і повідомляють про потенційні загрози, що дозволяє швидко реагувати на порушення безпеки. IPS (Intrusion Prevention Systems), окрім виявлення загроз, автоматично блокують або пом'якшують атаки в режимі реального часу, запобігаючи шкоді. Використання IDS/IPS забезпечує багаторівневий захист, підвищуючи стійкість до кіберзагроз і зменшуючи ризик несанкціонованого доступу та витоку даних.

2.3.2.1 Система виявлення вторгнень (IDS)

Система виявлення вторгнень (IDS) — це пасивна система безпеки, яка відстежує мережевий трафік або системну діяльність для виявлення потенційних інцидентів безпеки, порушень політики або ненормальної поведінки. IDS аналізує мережеві пакети, журнали або системні події, щоб виявити відомі моделі атак, вразливості або відхилення від встановлених базових показників.

Класифікація IDS

а) Мережевий IDS (NIDS):

1) Захоплення пакетів: NIDS відстежує мережевий трафік, захоплюючи та аналізуючи пакети, коли вони проходять через мережевий інтерфейс. Він перевіряє трафік на мережевому рівні і вище.
2) Виявлення на основі сигнатур: це найпоширеніший метод, який використовується NIDS. Він порівнює мережевий трафік із базою даних відомих моделей атак або сигнатур. Коли він виявляє збіг, він генерує сповіщення.
3) Виявлення на основі аномалій: деякі NIDS використовують методи виявлення аномалій на додаток до виявлення на основі сигнатур. Вони встановлюють базову лінію нормальної поведінки мережі, а потім позначають будь-які відхилення від цієї базової лінії як потенційні вторгнення. Виявлення аномалій може допомогти виявити раніше невідомі загрози.
4) Виявлення на основі евристики: цей метод використовує правила та евристики для виявлення підозрілих моделей поведінки мережі. Він більш гнучкий, ніж виявлення на основі сигнатур, але може генерувати більше помилкових спрацьовувань.
5) Попередження та звітування: коли NIDS виявляє підозрілу або зловмисну активність, він створює сповіщення для адміністраторів мережі. Ці сповіщення можуть містити інформацію про виявлену загрозу, її серйозність і рекомендації щодо усунення.

b) Системи виявлення вторгнень на основі хоста (HIDS):

1) Моніторинг на основі агентів: HIDS встановлюється на окремих хостах (серверах або кінцевих точках) і відстежує системну діяльність на цих хостах.
2) Моніторинг цілісності файлів: HIDS перевіряє цілісність системних і конфігураційних файлів. Будь-які неавторизовані зміни або модифікації викликають сповіщення.
3) Аналіз системних журналів: HIDS аналізує системні журнали, шукаючи шаблони або події, які вказують на несанкціонований доступ або незвичайну активність на хості.
4) Аналіз поведінки: Подібно до виявлення аномалій у NIDS, HIDS може відстежувати поведінку процесів і програм на хості для виявлення відхилень від очікуваної поведінки.
5) Попередження та звітування: так само, як NIDS, HIDS створює сповіщення адміністратору, коли виявляє підозрілу активність на хості.

Адміністратори повинні визначити, які дії чи поведінка вважаються підозрілими або зловмисними, і відповідно налаштувати систему сповіщень. IDS часто використовуються з системами запобігання вторгненням (IPS), які не тільки виявляють, але й можуть виконувати автоматизовані дії для блокування або пом’якшення виявлених загроз.

2.3.2.2 Система запобігання вторгень (IPS)

Системи запобігання вторгнень відстежують мережевий трафік у реальному часі, аналізуючи пакети даних і порівнюють їх із відомими моделями атак або сигнатурами. Як зазвичай працює IPS:

Моніторинг трафіку: IPS постійно відстежує вхідний і вихідний мережевий трафік, перевіряючи пакети даних, коли вони проходять мережею.

Перевірка пакетів: виконує глибоку перевірку пакетів, яка передбачає перевірку вмісту кожного пакета даних, включаючи заголовок і корисне

навантаження. Ця ретельна перевірка дозволяє IPS аналізувати поведінку та характеристики трафіку.

Виявлення на основі сигнатур: одним із основних методів, які використовує IPS, є виявлення на основі сигнатур. Він порівнює характеристики пакетів даних із базою даних відомих сигнатур атак, пов’язаних зі зловмисним програмним забезпеченням, вірусами чи іншими шкідливими діями. Якщо збіг знайдено, IPS може заблокувати або зареєструвати шкідливий трафік.

Виявлення на основі аномалій: деякі IPS використовують виявлення на основі аномалій. Вони встановлюють базову лінію поведінки мережі, яка вважається нормальною. Якщо IPS виявить трафік, який суттєво відхиляється від цього базового рівня, він може позначити його як підозрілий. Цей підхід корисний для виявлення раніше невідомих атак або атак нульового дня.

Блокування трафіку: коли IPS визначає потенційно зловмисний трафік на основі свого аналізу, він може вживати різних дій для захисту мережі. Ці дії можуть включати блокування зловмисного трафіку, скидання пакетів або перенаправлення трафіку в зону карантину для подальшого аналізу.

Попередження та звітування: IPS зазвичай створює сповіщення, щоб сповістити мережевих адміністраторів про виявлені загрози або підозрілу діяльність. Ці сповіщення надають інформацію про природу загрози, джерело та призначення трафіку, а також дії, вжиті IPS. Потім мережеві адміністратори можуть досліджувати сповіщення та реагувати на них.

Індивідуалізація та налаштування: системи IPS можна налаштувати та налаштувати відповідно до потреб організації. Це може включати створення власних підписів, налаштування рівнів чутливості та налаштування відповідних дій.

Інтеграція з іншими інструментами безпеки: IPS часто працює в поєднанні з іншими технологіями безпеки, щоб забезпечити багатошаровий захист безпеки.

Постійні оновлення: для ефективного захисту від нових і нових загроз необхідно регулярно оновлювати бази даних IPS із сигнатурами атак і моделями виявлення аномалій. Ці оновлення гарантують, що IPS може розпізнавати останні

загрози.

Порівнюючи IDS і IPS, можна відмітити, що IPS є активним засобом кібербезпеки, тоді як IDS є пасивним засобом безпеки. IDS головним чином зосереджується на виявленні та попередженні, тоді як IPS йде далі, активно запобігаючи або пом’якшуючи загрози. IPS та IDS — це системи безпеки, які використовуються для захисту комп’ютерних мереж від різних загроз, але вони служать різним цілям і працюють дещо по-різному. Основна мета IPS — активно блокувати або запобігати зловмисним діям і мережевим вторгненням у режимі реального часу. Він відстежує мережевий трафік на наявність підозрілої або несанкціонованої активності та негайно блокує або запобігає їй, наприклад, скидання пакетів, закриття з’єднань або переналаштування мережевих правил. З іншого боку, IDS призначений для виявлення підозрілої або потенційно шкідливої активності в мережі та попередження про неї, але не вживає жодних активних заходів для запобігання або блокування виявленої активності. Він надає сповіщення або журнали, які аналізуються співробітниками служби безпеки, які потім вживають відповідних заходів на основі сповіщень.

Блокування та запобігання проти спостереження та аналізу: IPS активно вживає заходів для запобігання або блокування зловмисної діяльності. Це може включати блокування мережевого трафіку, зміну правил брандмауера або скидання з’єднань для захисту мережі від загроз. Водночас IDS пасивно спостерігає та аналізує мережевий трафік, генеруючи сповіщення, коли виявляє підозрілу або потенційно шкідливу активність. Аналітики безпеки або адміністратори повинні переглянути ці сповіщення та прийняти рішення про відповідні дії.

Частота помилкових спрацьовувань: оскільки IPS активно блокує трафік на основі свого аналізу, вона може мати більшу ймовірність генерувати помилкові спрацьовування, потенційно блокуючи законний трафік у разі неправильного налаштування або якщо правила виявлення надто суворі. Навпаки, системи IDS, як правило, мають менше помилкових спрацьовувань, оскільки вони активно не блокують трафік. Однак вони можуть генерувати більше сповіщень, які повинні бути перевірені операторами.

Вплив на продуктивність мережі: природа активного блокування IPS може мати прямий вплив на продуктивність мережі та може викликати затримку, якщо вона обробляє великий обсяг трафіку або якщо її неправильно налаштовано для блокування законного трафіку. IDS, будучи пасивною системою моніторингу, має менший вплив на продуктивність мережі, оскільки не заважає мережевому трафіку.

IPS зазвичай розміщується поруч із мережевим трафіком, тобто весь трафік проходить через нього, дозволяючи йому активно блокувати загрози. Це вважається шлюзом безпеки, однак IDS можна розгортати різними способами, включаючи вбудований (подібний до IPS), позасмуговий (де він відстежує копію мережевого трафіку) або як IDS на основі хоста на окремих пристроях.

Мережеві фаєрволи, хоча і ефективні у контролі та фільтрації трафіку, можуть бути обмежені в здатності виявляти складні кіберзагрози. Системи виявлення та запобігання вторгнень забезпечують додаткові можливості для виявлення і реагування на потенційні загрози в режимі реального часу. Однак для комплексного захисту мережі та програмного забезпечення важливо також використовувати антивірусне програмне забезпечення. Антивірусні програми відіграють ключову роль у виявленні та видаленні шкідливих програм, таких як віруси, трояни, шпигунське програмне забезпечення та інші види зловмисного коду, що можуть проникнути в систему. Вони працюють разом із IDS/IPS та фаєрволами, забезпечуючи багаторівневий підхід до кібербезпеки.

2.3.3 Антивірусне програмне забезпечення

Антивірусне програмне забезпечення призначене для запобігання, сканування, виявлення та видалення вірусів. Після встановлення більшість антивірусного програмного забезпечення працює у фоновому режимі, щоб забезпечити захист від вірусів у реальному часі. Антивірусна програма, яка зазвичай встановлюється на комп’ютер як профілактичний засіб кібербезпеки, може допомогти запобігти широкому спектру кіберзагроз, таких як клавіатурні шпигуни, зловмисники браузера, троянські програми, хробаки, руткіти,

шпигунське програмне забезпечення, рекламне ПЗ, ботнети, спроби фішингу та атаки програм-вимагачів тощо.

Окрім описаних вище методів виявлення, типи сканувань, які пропонує антивірус, є рівним показником його успішності :

– Сканування за вимогою: сам термін «сканування за вимогою» означає, що ця функція або запускається, коли користувач хоче просканувати свій комп'ютер, підозрюючи будь-яку ненормальну поведінку, або користувач планує її запуск у визначений час.

– Захист у режимі реального часу: Майже всі сучасні антивірусні програми пропонують цей тип автоматичного захисту, який працює у фоновому режимі, таким чином збільшуючи шанси зловити зловмисне програмне забезпечення до того, як воно завдасть шкоди. Таким чином, ці типи сканування також відомі як «фонові охоронці». Він відстежує будь-яку підозрілу активність системи в режимі реального часу, поки дані завантажуються в активну пам'ять. Наприклад, коли вставляється USB-накопичувач або виконується завантажений файл.

– Інтелектуальне сканування: під час інтелектуального сканування антивірус сканує лише вибрані файли, які мають більшу ймовірність зараження. Цей тип сканування зменшує потребу в системних ресурсах, одночасно захищаючи від більш поширених типів вірусів, загроз і ризиків.

– Сканери шпигунського програмного забезпечення: сканують і видаляють шпигунське програмне забезпечення, тобто програмне забезпечення, яке, можливо, було встановлено на вашому комп'ютері без вашого відома для збору даних.

– Антивірус бази даних: використовує базу даних відомих небезпек для пошуку, ідентифікації та усунення загроз.

– Засоби видалення зловмисного програмного забезпечення: замість того, щоб запобігти проникненню зловмисного програмного забезпечення у вашу систему, вони призначені для видалення існуючого зловмисного програмного забезпечення.

– Антивірус електронної пошти: Антивірус електронної пошти в основному використовується для сканування та запобігання поширенню зловмисного програмного забезпечення електронною поштою.

– Евристичний антивірус: ідентифікує невиявлені віруси, перевіряючи код на наявність підозрілих ознак.

Антивірусне програмне забезпечення часто працює у фоновому режимі, скануючи комп'ютери, сервери та мобільні пристрої на наявність зловмисного програмного забезпечення та запобігаючи його розповсюдженню. Багато антивірусних програм містять функцію виявлення та запобігання загрозам у реальному часі для захисту від потенційних вразливостей. Сканує каталоги або окремі файли на предмет бібліотеки, яка містить зловмисні сигнатури, щоб визначити незвичайні шаблони, які вказують на наявність шкідливого програмного забезпечення. Дозволяє користувачам планувати сканування для автоматичного запуску. Користувачі можуть ініціювати нове сканування в будь-який момент. Видаляє будь-яке виявлене зловмисне програмне забезпечення або автоматично у фоновому режимі, або шляхом інформування користувачів про проблеми та запиту видалити файли. Щоб повністю сканувати комп'ютери, антивірусне програмне забезпечення має отримати привілейований доступ до всієї системи. Це робить антивірусне програмне забезпечення легкою мішенню для зловмисників, і останніми роками дослідники виявили віддалене виконання коду та інші серйозні недоліки в продуктах антивірусного програмного забезпечення.

Однією з таких антивірусних програм є продукт української компанії «Лабораторія Zillya», перша версія якого з'явилася у квітні 2009 року.

В жовтні 2013 р. анонсовано і звісно відбувся 13 листопада 2013 р. вихід Zillya! Антивірус для Бізнесу - який призначений для захисту мереж.

30 травня 2014 р. відбувся реліз, технічна підтримка завершена з 1 лютого 2017 р., а у 2021 року завершився випуск продукту — Zillya! Антивірус Безкоштовний.

15 березня 2016 р. відбувся реліз Zillya! Mobile Antivirus, який призначений для мобільних Android-пристроїв. 25 березня 2019 р. вийшла оновлена версія

Zillya! Internet Security for Android 2.0.

12 лютого 2020 р. стало відомо що Zillya!Total Security 3.0 отримав Gold сертифікацію OPSWAT.

Надає користувачеві захист від вірусів, троянських програм, шпигунських програм, руткітів, рекламних програм, а також невідомих загроз за допомогою проактивного захисту. Антивірус сертифіковано ДССЗЗІ, рівень захисту Г-2.

Ось деякі ключові характеристики та переваги антивірусу Zillya:

– Ефективний захист: Zillya використовує різноманітні методи виявлення та блокування шкідливих програм, включаючи сигнатурний аналіз, аналіз поведінки та хмарні технології, що дозволяє ефективно виявляти та блокувати навіть найновіші загрози.

– Швидка реакція: Zillya забезпечує швидку реакцію на нові загрози шляхом автоматичного оновлення бази даних вірусних сигнатур та технологій виявлення.

– Мінімальне вплив на продуктивність: Антивірус Zillya має оптимізовану архітектуру, яка мінімізує вплив на продуктивність комп'ютера під час сканування файлів та роботи в режимі реального часу.

– Додаткові функції: Крім базового захисту від вірусів, Zillya може також містити додаткові функції, такі як захист від шпигунського ПЗ, захист фінансових та банківських операцій в Інтернеті та інші.

– Користувацький інтерфейс: Програма має зручний та інтуїтивно зрозумілий інтерфейс, що дозволяє користувачам легко керувати параметрами захисту та переглядати статистику захоплення.

Підтримує всі версії операційні системи Windows, Android 4.2 та вище.[6]

3 ПРАКТИЧНІ АСПЕКТИ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ

3.1 Загальні рекомендації для забезпечення безпеки користувачів

Використання паролів та регулярна їх зміна. Пароль має складатися з комбінації різних символів, чисел і букв, щоб забезпечити надійність, актуальні сервіси з генерації паролів запропонують пароль різної довжини і складності. Для кожного акаунту пароль має бути унікальним, якщо зламають один акаунт, інші будуть в безпеці. Для зберігання паролів використовуйте спеціальні програми такі як LastPass або 1Password.

Встановлення антивірусного забезпечення та брендмауера. Захистить ваш пристрій від вірусів, шкідливих програм та інших кіберзагроз. Брендмауер допоможе захистити від несанкціонованого доступу з мережі Інтернет.

Регулярне оновлення програмного забезпечення.

Операційні системи постійно вдосконалюються, і з кожним оновленням усуваються нові вразливості. Хакери безперервно шукають слабкі місця в системі, які можуть використовуватися для несанкціонованого доступу або поширення шкідливого програмного забезпечення. Оновлення часто включають нові або покращені захисні механізми, такі як вдосконалені брендмауери, антивірусні програми та інші інструменти забезпечення безпеки, що підвищують здатність системи протистояти кіберзагрозам. Нові версії також включать оптимізації, які покращують загальну продуктивність та стабільність системи, знижуючи вразливість до збоїв, які можуть бути використані хакерами для здійснення атак. Це безкінечна гра у кішку - мишку, де розробники змагаються з кіберзлочинцями, щоб захистити своїх користувачів. Чим операційна система не оновлюється, тим більше «відкритих дір» залишаються доступними для кіберзлочинців.[7]

Звертай увагу до електронних листів або повідомлень в соціальних мережах з підозрілими посиланнями, в яких явно або побічно закликають ввести конфіденційні дані. Не слід завантажувати файли з невідомих джерел, яке б розширення вони не мали, файл може містити код шкідливого програмного

забезпечення. Скориставшись актуальними сервісами перевірки файлів або посилань, можна виявити підозрілу активність, для прикладу один з таких : https://freevpnplanet.com/ua/virus-scan/.

Періодичне створення резервного копіювання даних з носія (жорсткого диска, дискета, тощо) надасть можливість виконати відновлення інформації при втраті оригіналу. Під втратою треба розуміти настання події, що призвела до зміни даних, після чого вони втратили цінність або були видалені з носія.

3.2 Анонімне використання Інтернету

Один із способів захисту своєї анонімності в інтернеті є використання браузера Tor. Tor (The Onion Router) – це мережа, яка забезпечує анонімність в Інтернеті, дозволяючи користувачам захищати свою особисту інформацію та приватність. Tor браузер – це спеціально налаштований веб-браузер, який використовує мережу Tor для шифрування та анонімізації інтернет трафіку. Основна його мета захистити конфіденційність користувачів та забезпечити доступ до інформації без стеження та цензури.

3.2.1 Tor для збереження анонімності

Одним із ключових принципів роботи є багатошарове шфирування, що часто називають onion routing (цибулева маршрутизація). Кожне з’єднання через проходить через кілька випадкових вузлів, при цьому дані шифруються на кожному етапі. Це створює кілька шарів шифрування, схожими за будовою на шари цибулі. Кожен вузол знає лише попередника та наступника ланцюжка, але не весь маршрут, що значно ускладнює відстеження оригінального джерела трафіку. Ще один важливий принцип – випадкове вибирання маршруту через мережу, трафік проходить через випадково вибрані вузли. Кожне з’єднання використовує різний маршрут, що робить відстеження трафіку ще складнішим. Вузли постійно змінюються, забезпечуючи динамічність мережі та захищаючи користувачів від

довготривалого моніторингу. Вихідний вузол є останнім через який трафік виходить у відкритий Інтернет і може бути перехопленим, тому важливо використовувати шифрування на рівні додатків (HTTPS) для захисту даних від вихідного вузла до кінцевого серверу.[10]

Використання браузера Tor :

1. Завантаження та інсталювання. Браузер можна безкоштовно завантажити з офіційного веб-сайту проєкту Tor ,зображений на рисунку 3.1. Доступний для різних операційних системи, включаючи Windows, macOS, Linux та Android.

Рисунок 3.1 – веб сайт проєкту Tor

2. Після простого встановлення браузера можна відразу почати його використовувати. При першому запуску браузера користувачеві пропонується підключитися до мережі Tor, зображено на малюнку 3.2 або налаштувати з’єднання вручну, якщо це необхідно.

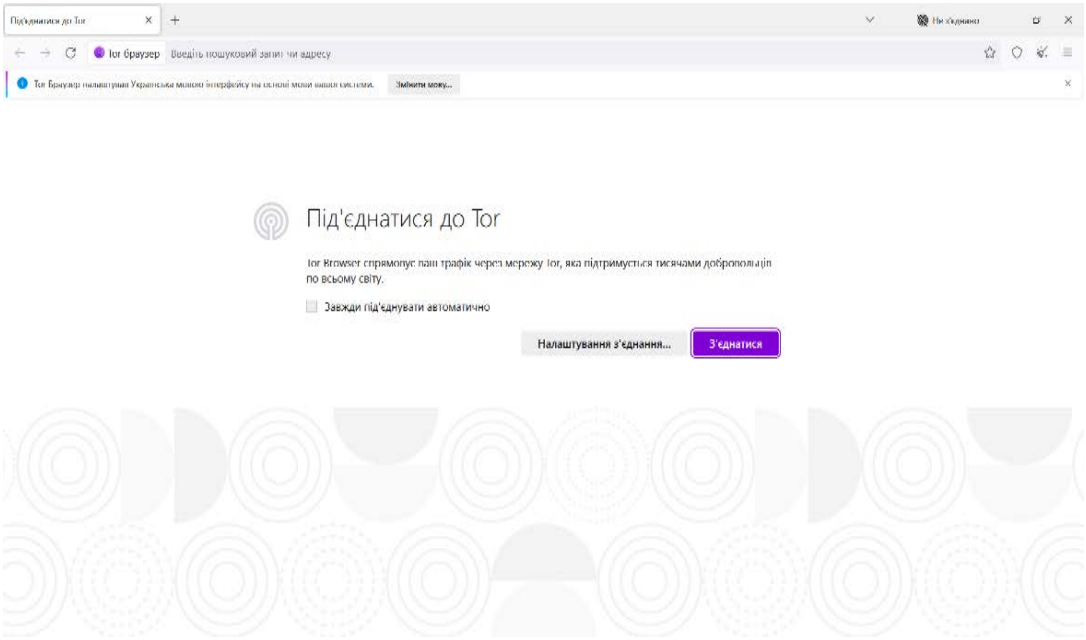

Рисунок 3.2 – З’єднання з мережею Tor

3. Після встановленого з’єднання ваш трафік буде спрямований через мережу Tor . Зображення готового до безпечного пошук браузера на рисунку 3.3.

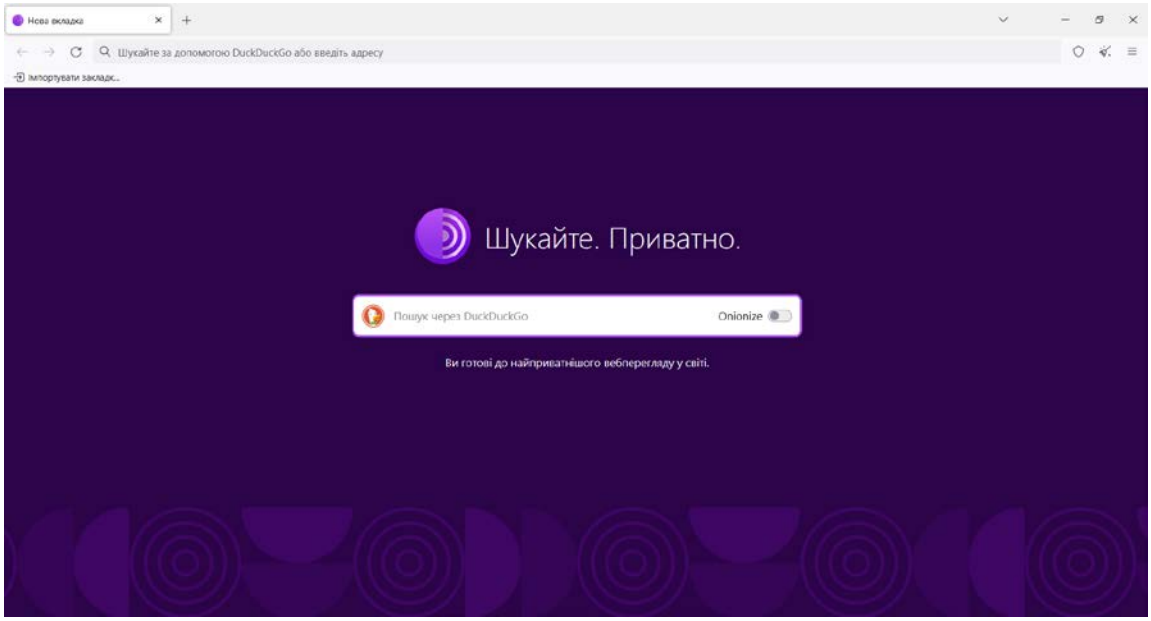

Рисунок 3.3 – Налаштований Tor-браузер

3.2.2 Віртуальні приватні мережі

Наступний метод захисту це віртуальні приватні мережі (VPN), технологія, що створює захищене з’єднання між пристроєм користувача та віддаленим сервером, через який здійснюється доступ до Інтернету. VPN дозволяє шифрувати трафік, приховувати реальну IP-адресу та забезпечувати конфіденційність користувачів, що особливо важливо у публічних мережах або при доступі до обмеженого контенту. Основний принцип роботи полягає в шифруванні трафіку, що проходить між користувачем та сервером. Коли користувач підключається до VPN, всі дані шифруються за допомогою різних алгоритмів шифрування (наприклад AES-256), що забезпечує захист від перехоплення та читання даних третіми сторонами, такими як хакери або Інтернет-провайдери. VPN використовує технологію тунелювання для створення захищеного з’єднання. Тунелювання — це процес інкапсуляції мережевих пакетів у нові пакети, що передаються через захищений тунель. Існує кілька протоколів тунелювання, таких як OpenVPN, L2TP/IPsec, PPTP та SSTP, кожен з яких має свої особливості та рівні безпеки.

VPN дозволяє користувачам обходити цензуру та геоблокування, встановлені урядами або сервісам. Підключаючись до VPN-сервера в іншій країні, користувач може отримати доступ до контенту, заблокованого у його регіоні. Це особливо корисно для доступу до потокових сервісів, соціальних мереж або новинних сайтів.[11]

Використання VPN :

1. Завантаження та інсталювання. Сервіси доступні у вигляді програмного забезпечення для різних операційних систем, включаючи Windows, macOS, Linux, Android та iOS. Користувачі можуть завантажити VPN-клієнт з офіційного сайту обраного провайдера, встановити його на свій пристрій та створити обліковий запис. Встановимо сервіс VPN компанії Proton AG з офіційного сайту, веб-сайт на рисунку 3.4 .

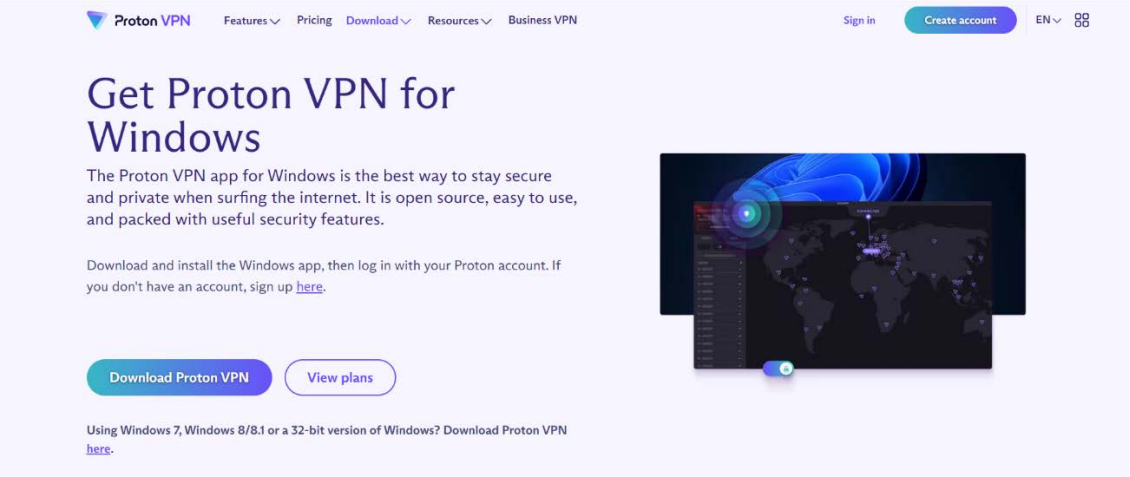

Рисунок 3.4 - Використання VPN

2. Після встановлення в систему потрібно створити обліковий запис користувача сервісу. В безкоштовному тарифі нам доступне 1 підключення VPN до 244 сервери в 5 країнах світу, платний тариф надає більше можливостей.

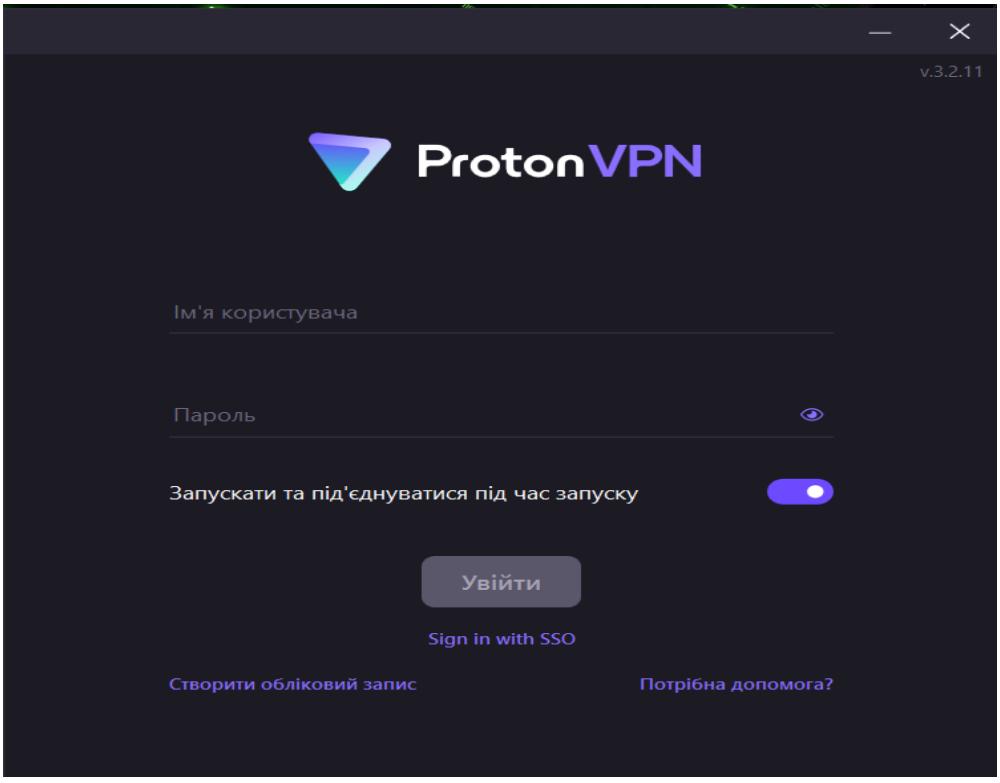

Рисунок 3.5 – Сторінка облікового запису VPN

3. Активувавши обліковий запис підключаємось до доступного віддаленого серверу і користуємось наданою конфіденційністю. Правильно

налаштований VPN на рисунку 3.6 .

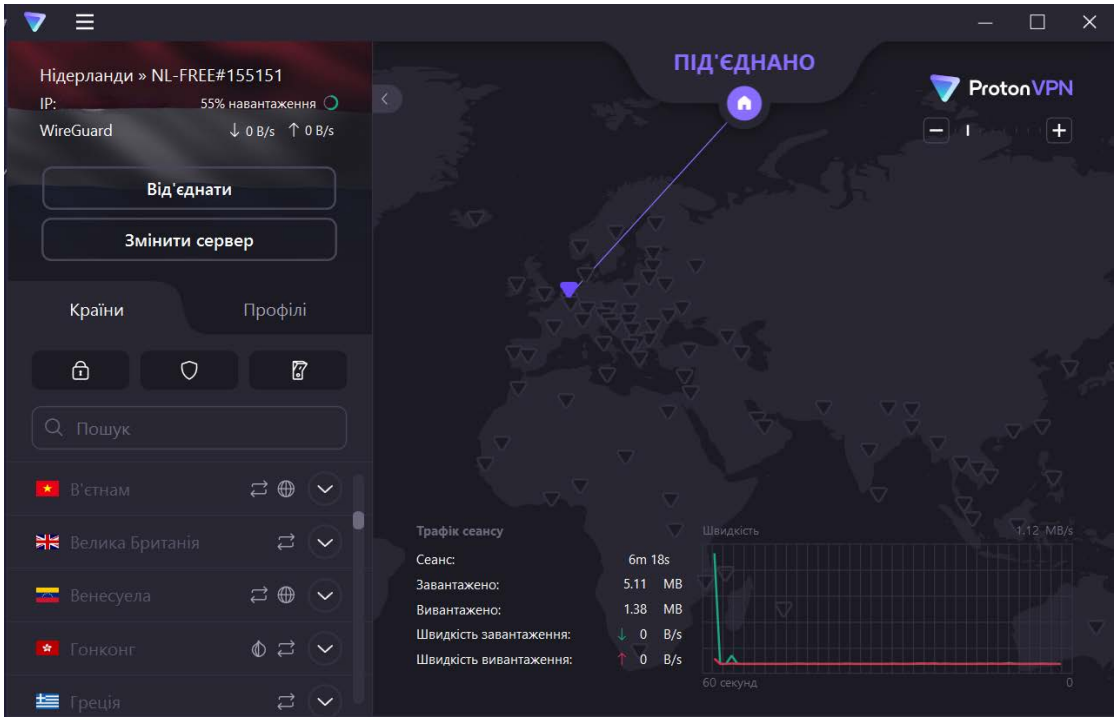

Рисунок 3.6 – Налаштований VPN

3.2.3 Проксі-сервер

Ще одним потужним інструментом є проксі-сервер — це проміжний сервер, який діє як посередник між клієнтським пристроєм і кінцевим ресурсом в Інтернеті. Він приймає запити від клієнта, передає їх до цільового сервера, отримує відповідь і відправляє її назад клієнту. Це дозволяє приховати реальну IP-адресу користувача, підвищити конфіденційність та забезпечити додатковий рівень безпеки. Один з головних принципів роботи проксі-сервера полягає в приховуванні реальної IP-адреси користувача. Коли користувач надсилає запит через проксі-сервер, цільовий сервер бачить IP-адресу проксі, а не реальну IP-адресу користувача. Це допомагає залишатися анонімним в Інтернеті та уникати стеження. Проксі-сервери часто використовують кешування для збереження копій веб-сторінок та інших ресурсів. Це дозволяє зменшити навантаження на мережу та прискорити доступ до популярних ресурсів. Коли користувач запитує вже кешований ресурс, проксі-сервер може надати його безпосередньо з кешу, не звертаючись до кінцевого

сервера. Проксі-сервери можуть забезпечувати додатковий рівень безпеки, захищаючи користувачів від шкідливих веб-сайтів і програм. Вони можуть сканувати трафік на наявність вірусів і шкідливого коду, забезпечуючи таким чином захист користувачів від потенційних загроз.

Використання проксі

1. Вибір типу проксі-сервера, існує кілька типів серверів кожен з яких має свої особливості та застосування :

- HTTP-проксі використовується для обробки HTTP-запитів, що дозволяє переглядати веб-сторінки анонімно.
- HTTPS-проксі: Підтримує шифрування за допомогою SSL/TLS, забезпечуючи безпеку під час роботи з веб-сайтами.
- SOCKS-проксі: Підтримує будь-які типи трафіку, включаючи HTTP, FTP, SMTP та інші протоколи, що робить його більш універсальним.

2. Знаходимо надійного постачальника послуг. При виборі враховуйте такі фактори : репутація та відгуки, швидкість, надійність і політику конфіденційності. Не рекомендується використовувати безкоштовні сервери через низький рівень безпеки, відсутність конфіденційності та нестабільного з’єднання.

3. Після вибору провайдера реєструємось на його веб-сайті та оплачуємо обраний тарифний план. Більшість пропонують різні варіанти оплати, включаючи кредитні картки, PayPal, криптовалюту тощо. Після успішної оплати ви отримаєте доступ до налаштувань проксі-сервера. Зазвичай це IP-адреса, порт, логін та пароль для авторизації.

4. . В операційній системі Windows 10, див.рисунок 3.7, це можна зробити в меню налаштування «Мережа й Інтернет».

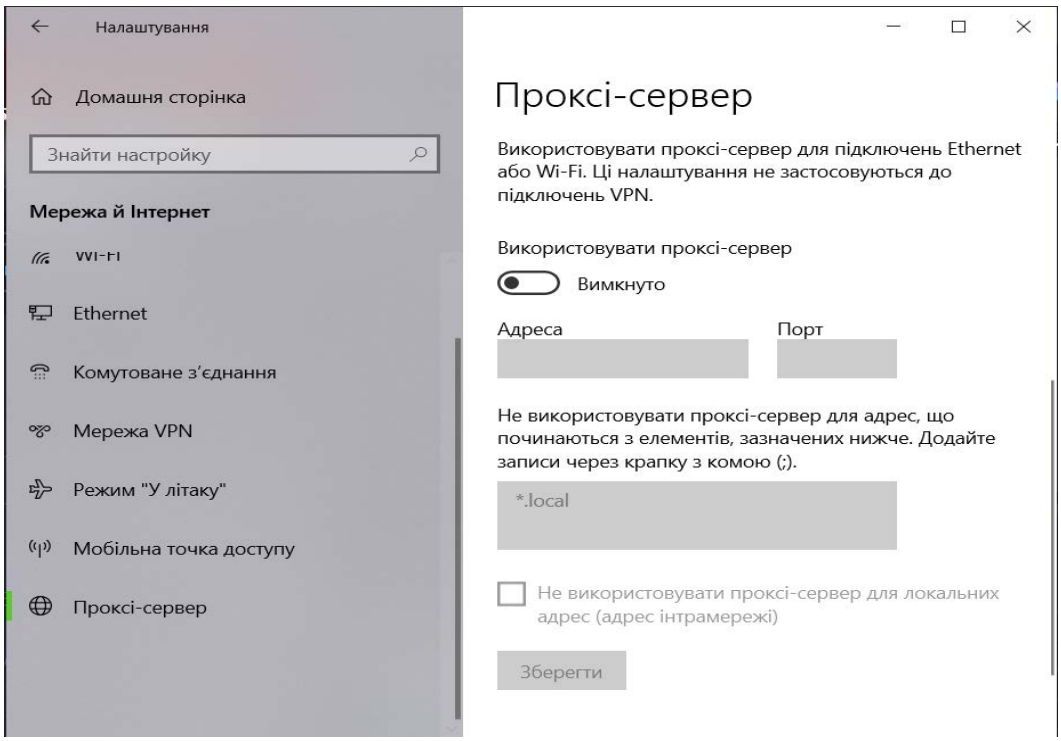

Рисунок 3.7 – Налаштування проксі-серверу

Користувач вказує IP-адресу та порт проксі-сервера, а також, за необхідності, вводить дані для авторизації Налаштування може відрізнятися залежно від операційної системи та веб-браузера.[12]

3.3 Міжнародні стандарти та норми кібербезпеки

Національний інститут стандартів і технологій (NIST) Cybersecurity Framework (CSF) - це добровільний фреймворк, розроблений для покращення кібербезпеки та управління ризиками в будь-якій організації. Він ґрунтується на існуючих стандартах і найкращих практиках, пропонуючи чітку структуру для оцінки, вдосконалення та підтримки кіберстійкості. Розробка NIST CSF розпочалася у 2013 році за наказом президента США "Покращення кібербезпеки критичної інфраструктури". Фреймворк був створений у співпраці з приватним сектором з метою надання організаціям орієнтирів для управління кіберризиками. Закон про посилення кібербезпеки (CEA) 2014 року ще більше закріпив роль NIST CSF як провідного фреймворку кібербезпеки.

NIST CSF складається з п'яти основних функцій:

– Визначте: Організація має чітке розуміння своїх активів, ризиків та середовища кібербезпеки.

– Захистіть: Впровадження відповідних заходів безпеки для захисту активів.

– Виявіть: Швидке виявлення кібератак та інших кіберінцидентів.

– Відповідайте: Ефективна реакція на кіберінциденти для мінімізації збитків.

– Відновіть: Відновлення систем та операцій після кіберінцидентів.

Кожна функція поділена на категорії та підкатегорії, які описують конкретні кроки та заходи для виконання. NIST CSF також надає інформаційні посилання, які зв'язують фреймворк з іншими стандартами та найкращими практиками.

NIST CSF пропонує ряд переваг для організацій:

– Гнучкість: Фреймворк можна адаптувати до потреб будь-якої організації, незалежно від її розміру, галузі або рівня зрілості кібербезпеки.

– Ефективність: NIST CSF пропонує чітку структуру для оцінки та вдосконалення кіберзахисту.

– Зрозумілість: Фреймворк ґрунтується на загальновизнаних стандартах і найкращих практиках, що робить його легким для розуміння та впровадження.

– Підтримка: NIST та інші організації надають ресурси та підтримку для допомоги організаціям у впровадженні та використанні NIST CSF.

NIST CSF може бути використаний організаціями для:

– Розробки та впровадження програми кібербезпеки.

– Оцінки та вдосконалення існуючих заходів кібербезпеки.

– Демонстрації відповідності нормативним вимогам та галузевим стандартам.

– Підвищення обізнаності та навчання співробітників з питань кібербезпеки.

– Покращення кіберстійкості та реагування на кіберінциденти.[8]

ISO 27001 є міжнародним стандартом управління інформаційною безпекою, який визначає вимоги до системи управління інформаційною безпекою (СУІБ). Цей стандарт розроблено Міжнародною організацією зі стандартизації (ISO) у співпраці з Міжнародною електротехнічною комісією (IEC). Основною метою ISO 27001 є допомога організаціям у забезпеченні конфіденційності, цілісності та доступності інформації за допомогою систематичного підходу до управління ризиками.

ISO 27001 базується на кількох ключових принципах, спрямованих на забезпечення ефективного управління інформаційною безпекою:

– Систематичний підхід: стандарт передбачає структурований та систематичний підхід до управління інформаційною безпекою, включаючи ідентифікацію, оцінку та управління ризиками.

– Безперервне покращення: ISO 27001 наголошує на важливості постійного вдосконалення системи управління інформаційною безпекою, включаючи регулярні аудити, оцінку ризиків та моніторинг заходів безпеки.

– Увімкнення всіх рівнів організації: успішне впровадження ISO 27001 потребує участі та підтримки всіх рівнів організації від керівництва до окремих співробітників.

– Орієнтація на ризики: основою ISO 27001 є управління ризиками, що включає виявлення потенційних загроз, оцінку їх впливу та впровадження відповідних заходів захисту.

Впровадження ISO 27001 допомагає організаціям підвищити рівень захисту інформації, що знижує ризик виникнення інцидентів безпеки та зменшує їх наслідки, відповідати вимогам законодавства та регуляторів захисту інформації, що особливо важливо для компаній, що працюють у регульованих галузях, таких як фінанси або охорона здоров'я. Сертифікація ISO 27001 свідчить про високий рівень безпеки організації, що підвищує довіру клієнтів та партнерів. Це може стати конкурентною перевагою та сприяти залученню нових клієнтів. ISO 27001 надає організаціям систематичний підхід до управління ризиками, що дозволяє своєчасно виявляти та знижувати загрози. Це сприяє стабільності та безперервності бізнесу.

Впровадження ISO 27001 допомагає покращити процеси в організації, що підвищує ефективність її роботи. Це включає впровадження кращих практик управління інформаційною безпекою та забезпечення чіткого розподілу відповідальності.

ISO 27001 є важливим інструментом для забезпечення інформаційної безпеки в організаціях. Він забезпечує систематичний підхід до управління ризиками, допомагає відповідати вимогам законодавства та регуляторів, підвищує довіру клієнтів та покращує ефективність процесів. Впровадження цього стандарту сприяє захисту конфіденційності, цілісності та доступності інформації, що є критично важливим для успішної діяльності будь-якої організації в сучасному цифровому світі.[9]

ВИСНОВКИ

Дослідження інструментів та методів забезпечення безпеки в сучасному цифровому просторі дало змогу зробити ряд висновків науково-теоретичного та прикладного характеру :

1. Забезпечення безпеки користувачів є надзвичайно важливим завданням, оскільки це є загроза конфіденційності та цілісності, а інколи доступності інформації.
2. Користувачі повинні використовувати доступні інструментів та методи, щоб захистити себе та свої дані.
3. Шифрування даних робить їх нечитабельним для будь-кого, хто не має ключа для розшифрування.
4. Контроль доступу обмежує дані лише для авторизованих користувачів.
5. Антивірусне програмне забезпечення, брендмауери та інші інструменти можуть допомогти захистити від несанкціонованого доступу та шкідливих програм.
6. Резервна копія даних допоможе відновити їх у разі втрати або пошкодження.
7. Анонімізація даних допомогає приховати особисту інформацію користувача простору.

Узагальнюючи, безпека користувачів є невід’ємною частиною цифрового простору. Впровадження стандартів безпеки, застосування захисних методів та засобів, а також постійний моніторинг та прогнозування загроз допомогають забезпечити надійний рівень захисту власника та інформації що обробляється.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. ІНФОРМАЦІЙНА БЕЗПЕКА УКРАЇНИ: СОЦІАЛЬНО-ФІЛОСОФСЬКІ АСПЕКТИ. *Філософські науки*. 2020. Т. 86, № 10. С. 297. URL: https://molodyivchenyi.ua/index.php/journal/article/view/319/308.
2. Піпченко, Н. (2015). Міжнародна інтернет-комунікація як інструмент зовнішньополітичної діяльності: автореф. дис. ... д-ра політ. наук : 23.00.04; Київ. нац. ун-т ім. Тараса Шевченка. Київ.
3. Вразливості інформаційних та комунікаційних систем – UA5.org. *UA5.org – Матеріали з інформаційних технологій*. URL: https://ua5.org/cve/2193-vrazlyvosti-informaczijnyh-ta-komunikaczijnyh-system.html.
4. Shalini Subramani, Selvi M, Kannan A & Santhosh Kumar Svn (2023) Review of Security Methods Based on Classical Cryptography and Quantum Cryptography, Cybernetics and Systems
5. What Is a Firewall? Definition and Types of Firewall | Fortinet. *Fortinet*. URL: https://www.fortinet.com/resources/cyberglossary/firewall .
6. How an Antivirus Works? - GeeksforGeeks. *GeeksforGeeks*. URL: https://www.geeksforgeeks.org/how-an-antivirus-works/ (date of access: 20.05.2024).
7. Чому варто оновлювати програмне забезпечення на пристроях Android?. *Imena.ua*. URL: https://www.imena.ua/blog/update-android/.
8. What is the NIST Cybersecurity Framework? | IBM. *IBM in Deutschland, Österreich und der Schweiz*. URL: https://www.ibm.com/topics/nist (date of access: 23.05.2024).
9. Стандарт ISO 27001. Система менеджменту інформаційної безпеки | TMS Academy. *TMS Academy*. URL: https://academy.tms.ua/uk/sertificat-ua/standart-iso-27001-systema-menedzhmentu-informatsijnoi-bezpeky/#h_4724832851159541610445 7.