MODERN RESEARCH IN SCIENCE AND EDUCATION

Proceedings of II International Scientific and Practical Conference

Chicago, USA

12-14 October 2023

Chicago, USA

2023

UDC 001.1

The 2nd International scientific and practical conference "Modern research in science and education" (October 12-14, 2023) BoScience Publisher, Chicago, USA. 2023. 498 p.

ISBN 978-1-73981-123-5

The recommended citation for this publication is:

Ivanov I. Analysis of the phaunistic composition of Ukraine // Modern research in science and education. Proceedings of the 2nd International scientific and practical conference. BoScience Publisher. Chicago, USA. 2023. Pp. 21-27. URL: https://sci-conf.com.ua/ii-mizhnarodna-naukovo-praktichna-konferentsiya-modern-research-in-science-and-education-12-14-10-2023-chikago-ssha-arhiv/.

Editor
Komarytskyy M.L.
Ph.D. in Economics, Associate Professor

Collection of scientific articles published is the scientific and practical publication, which contains scientific articles of students, graduate students, Candidates and Doctors of Sciences, research workers and practitioners from Europe, Ukraine and from neighbouring countries and beyond. The articles contain the study, reflecting the processes and changes in the structure of modern science. The collection of scientific articles is for students, postgraduate students, doctoral candidates, teachers, researchers, practitioners and people interested in the trends of modern science development.

e-mail: chicago@sci-conf.com.ua

homepage: *https://sci-conf.com.ua*

TECHNICAL SCIENCES

PHYSICAL AND MATHEMATICAL SCIENCES

GEOGRAPHICAL SCIENCES

УДК 004.056.5:004.03:61

ПРОБЛЕМИ ЗАХИСТУ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ СИСТЕМАХ ТА ЗАСОБИ І МЕТОДИ ЇХ ВИРІШЕННЯ

Нагорний Олександр Володимирович,
студент ФІТ, ДТЕУ
Жирова Тетяна Олександрівна,
к. пед. н., доцент, ДТЕУ
Нагорний Володимир Володимирович,
к. фарм. н., доцент, ЗДМФУ

Анотація: Широке використання комп'ютерних технологій в автоматизованих системах обробки інформації та управління призвело до загострення проблем захисту інформаційних ресурсів, каналів передачі даних та інформації, що циркулює в комп'ютерних системах, від несанкціонованого доступу.

Ключові слова: захист інформації, кібербезпека, комп'ютерні системи, антивірусне програмне забезпечення, фаєрвол, багатофакторна аутентифікація, криптографія.

Інформація має вирішальне значення в сучасному світі і відіграє різні важливі ролі у всіх сферах життя, включаючи технології, економіку, політику, медицину, соціальні відносини та багато інших аспектів. Ось кілька ключових ролей інформації в сучасному суспільстві:

1) Комунікація і обмін інформацією: Інформація служить основним засобом комунікації між людьми, компаніями, урядами та різними організаціями. Вона дозволяє нам спілкуватися, обмінюватися ідеями, повідомляти важливі події і вести бізнес.

2) Прийняття рішень: Інформація надає підстави для прийняття рішень в усіх сферах діяльності, включаючи бізнес, політику, науку і особисте життя. Вона допомагає аналізувати ситуації, передбачати наслідки і визначати

найкращі стратегії.

3) Технологічний прогрес: Інформація є основою для розвитку технологій. Вона стимулює наукові дослідження, інновації і винаходи, що покращують якість життя та сприяють економічному зростанню.

Захист інформації в комп'ютерних системах має низку специфічних особливостей, пов'язаних з тим, що інформація не є жорстко пов'язаною з носієм, може легко і швидко копіюватися і передаватися по каналах зв'язку.

Порушення інформаційної безпеки може мати серйозні наслідки, які варіюються від фінансових втрат до загрози національній безпеці. Ось деякі з потенційних наслідків порушення інформаційної безпеки:

1) Фінансові втрати: Кібератаки можуть призвести до значних фінансових втрат для компаній та організацій. Це включає в себе витрати на відновлення інфраструктури, компенсацію за шкоду, а також втрату прибутку внаслідок недоступності системи.

2) Втрата конфіденційності: Порушення інформаційної безпеки може призвести до розкриття конфіденційної інформації, такої як особисті дані користувачів, медичні записи або фінансові дані. Це може призвести до порушення приватності і спричинити серйозні проблеми для людей та організацій.

3) Втрата робочого часу і продуктивності: Внаслідок кібератак може втратитися робочий час і продуктивність, оскільки організації вимушені вирішувати проблеми з відновленням систем та даних.

4) Збитки репутації: Компанії і організації можуть стати об'єктом публічного обурення та втрати довіри клієнтів через порушення інформаційної безпеки. Репутаційні збитки можуть бути важкі для відновлення.

Економічні аспекти захисту інформації:

1) Фінансові витрати: Захист інформації вимагає фінансових витрат на розробку, впровадження та підтримку технологій і заходів з кібербезпеки. Компанії повинні бути готові інвестувати у кібербезпеку, оскільки недостатні заходи можуть призвести до фінансових втрат через кібератаки.

2) Збитки від втрати продуктивності: Кібератаки і порушення інформаційної безпеки можуть спричинити втрати робочого часу і продуктивності працівників, оскільки вони повинні вирішувати проблеми, пов’язані з відновленням роботи систем та даних.

3) Втрати на ринку: Компанії, які не можуть забезпечити адекватний рівень захисту інформації, можуть втратити довіру клієнтів і ринкову конкурентоспроможність.

Правові аспекти захисту інформації:

1) Закони і регулювання: Багато країн впроваджують закони та регулювання щодо захисту інформації, які вимагають від організацій дотримуватися стандартів кібербезпеки та повідомляти про порушення безпеки. Недотримання таких вимог може призвести до адміністративних або юридичних санкцій.

2) Кримінальна відповідальність: Великі кібератаки можуть мати кримінальну сторону, і злочинці можуть бути притягнуті до відповідальності. Багато країн мають закони, які передбачають кримінальну відповідальність за кіберзлочини.

3) Цивільна відповідальність: Компанії можуть бути позовами за недостатні заходи з кібербезпеки, якщо їхні дії (або недії) спричинили фінансову шкоду або втрату даних клієнтів.

Захист інформації вимагає врахування як економічних, так і правових аспектів, і організації повинні дотримуватися відповідних законів та стандартів для забезпечення ефективної інформаційної безпеки.

Розглянемо засоби захисту інформації.

Антивірусне програмне забезпечення (антивіруси) є ключовим елементом захисту комп’ютерних систем від вірусів, шкідливих програм і кіберзагроз загалом. Ось деякі основні аспекти антивірусного програмного забезпечення:

- Виявлення і вилучення загроз: Основна функція антивірусного програмного забезпечення - це виявлення та вилучення вірусів та інших шкідливих програм з комп’ютера. Вони аналізують файли і активності на

комп’ютері, шукаючи підозрілі дії і підписи вірусів, і видаляють або ізолюють знайдені загрози.

- Оновлення вірусних баз даних: Антивіруси регулярно оновлюють свої вірусні бази даних, щоб впізнавати нові віруси та шкідливі програми. Це важливо, оскільки кіберзлочинці постійно створюють нові загрози.

- Захист в реальному часі: Багато сучасних антивірусів працюють в режимі реального часу, що означає, що вони постійно моніторять активність комп’ютера і намагаються блокувати загрози до їх виконання.

Фаєрвол (Firewall) та інші мережеві заходи безпеки грають важливу роль в захисті комп’ютерних мереж та систем від кіберзагроз. Розрізняють внутрішній та зовнішній фаєрвол: внутрішній - захищає мережу від внутрішніх загроз, тоді як зовнішній фаєрвол контролює доступ з зовнішнього Інтернету до внутрішньої мережі. Фаєрволи використовують правила доступу для керування тим, які типи трафіку дозволені або блоковані. Правила можуть бути засновані на IP-адресах, портах, протоколах тощо. Сучасні фаєрволи використовують методи Stateful Inspection, які відстежують стан та контекст пакетів даних, що проходять через них, що дозволяє забезпечити більшу безпеку.

Системи виявлення вторгнень (Network Intrusion Detection System (NIDS)) та системи запобігання вторгненням (Network Intrusion Prevention System (NIPS) аналізують мережевий трафік для виявлення незвичних або підозрілих активностей, які можуть бути ознакою кібератаки. Блокування вторгнень: NIPS може надавати можливість блокувати атаки в реальному часі, перешкоджаючи вторгненням до мережі.

Віртуальні приватні мережі (Virtual Private Networks - VPNs): VPN-підключення дозволяють шифрувати трафік та забезпечувати анонімність користувачів в Інтернеті, що робить їх корисними для захисту конфіденційної інформації.

Радикальне вирішення проблем захисту електронної інформації може бути отримано тільки на базі використання криптографічних методів, які дозволяють вирішувати найважливіші проблеми захищеної автоматизованої

обробки та передачі даних. При цьому сучасні швидкісні методи криптографічного перетворення дозволяють зберегти початкову продуктивність автоматизованих систем. Криптографічні перетворення даних є найбільш ефективним засобом забезпечення конфіденційності даних, їхньої цілісності і справжності. Тільки їх використання в сукупності з необхідними технічними та організаційними заходами можуть забезпечити захист від широкого спектру потенційних загроз.

Основні проблеми, що виникають з безпекою передачі інформації в комп'ютерних мережах, можна поділити на такі:

- Перехоплення інформації - цілісність інформації зберігається, але її конфіденційність порушена;

- Модифікація інформації - вихідне повідомлення змінюється або повністю підміняється іншим і надсилається адресату;

- Підміна авторства інформації. Дана проблема може мати серйозні наслідки. Наприклад, хтось може надіслати листа від чужого імені (цей вид обману прийнято називати спуфінгом) або Web-сервер може прикидатися електронним магазином, приймати замовлення, номери кредитних карт, але не висилати ніяких товарів.

Потреби сучасної практичної інформатики призвели до виникнення нетрадиційних завдань захисту електронної інформації, однією з яких є автентифікація електронної інформації в умовах, коли сторони що обмінюються інформацією не довіряють одна одній. Ця проблема пов'язана зі створенням систем електронного цифрового підпису. Технічною основою переходу в інформаційне суспільство є сучасні мікроелектронні технології, які забезпечують безперервне зростання якості засобів обчислювальної техніки і служать базою для збереження основних тенденцій її розвитку - мініатюризації, зниження електроспоживання, збільшення обсягу оперативної пам'яті і місткості вбудованих і змінних накопичувачів, зростання продуктивності і надійності, розширення сфер і масштабів застосування. Дані тенденції розвитку засобів обчислювальної техніки призвели до того, що на сучасному етапі захист

комп’ютерних систем від несанкціонованого доступу характеризується зростанням ролі програмних та криптографічних механізмів захисту в порівнянні з апаратними.

Цифровий підпис використовується для перевірки автентичності повідомлення та визначення, чи були змінені дані під час передачі. Він створюється за допомогою приватного ключа і перевіряється за допомогою відповідного публічного ключа.

Хеш-функції перетворюють вхідні дані в фіксований розмірний хеш-код, який можна використовувати для перевірки цілісності даних. MD5 і SHA-256 - це приклади хеш-функцій.

Засоби ідентифікації та аутентифікації використовуються для впізнавання та підтвердження ідентичності користувачів, що намагаються отримати доступ до комп’ютерних систем, мереж, додатків або ресурсів. Ці засоби грають критичну роль в забезпеченні безпеки і захисту інформації.

Логін - це ідентифікатор користувача, який зазвичай вводиться в текстовому форматі.

Пароль - це секретний код або фраза, яка пов’язана зі звільненим логіном. Паролі мають бути складними та унікальними для кожного облікового запису.

Біометричні методи:

Відбиток пальця використовує унікальні фізичні риси пальця для ідентифікації користувача.

Розпізнавання обличчя - цей метод використовує камери та програмне забезпечення для розпізнавання обличчя користувача.

Розпізнавання ірису очей вимагає сканування ірису, який також є унікальним для кожної особи.

Двофакторна і багатофакторна аутентифікація:

Двофакторна аутентифікація (2FA): Вимагає двох різних засобів аутентифікації, наприклад, пароля і одноразового коду, який надсилається на мобільний телефон.

Багатофакторна аутентифікація (MFA): Вимагає використання трьох або

більше засобів аутентифікації, таких як пароль, відбиток пальця та смарт-карту, для підвищення безпеки.

Важливим є створення плану захисту інформації.

Аналіз ризиків кібербезпеки - це процес визначення потенційних загроз і вразливостей в інформаційних системах та розроблення стратегій для їх запобігання та вирішення. Даний аналіз допомагає організаціям зрозуміти, які кіберризики можуть вплинути на їхню діяльність і як вони можуть зменшити ці ризики. Ось кроки, які включаються в процес аналізу ризиків кібербезпеки:

Ідентифікація активів: Визначення всіх інформаційних систем, даних, програмного забезпечення та обладнання, які використовуються в організації.

Ідентифікація загроз: Визначення потенційних загроз для інформаційних активів. Загрози можуть включати в себе кібератаки, внутрішні загрози, природні катастрофи, людські помилки і т. д.

Оцінка вразливостей: Визначення вразливостей, які можуть бути використані загрозами для атаки на інформаційні активи. Вразливості можуть бути пов’язані з програмним забезпеченням, конфігурацією, людським фактором тощо.

Оцінка ризику: Оцінка ймовірності та впливу потенційних загроз та вразливостей на організацію. Визначення, наскільки серйозним може бути вплив ризику на діяльність організації.

Реалізація та моніторинг заходів безпеки: Здійснення запланованих заходів безпеки, щоб запобігти або зменшити ризики.

Розробка та впровадження політик безпеки є важливими кроками для забезпечення захисту інформації та зменшення ризиків кібербезпеки в організації. Розробляючи політику безпеки інформації, спочатку визначають об’єкти, які треба захистити, і їх функції. Потім оцінюють ступінь інтересу потенційного супротивника до цих об’єктів, ймовірні види нападу і спричинений ними збиток. Нарешті, визначають вразливі для впливу області, в яких наявні засоби протидії не забезпечують достатнього захисту.

Автоматизований комплекс можна вважати захищеним, якщо всі операції

виконуються у відповідності з чітко визначеними правилами (рис. 1), що забезпечують безпосередній захист об’єктів, ресурсів і операцій.

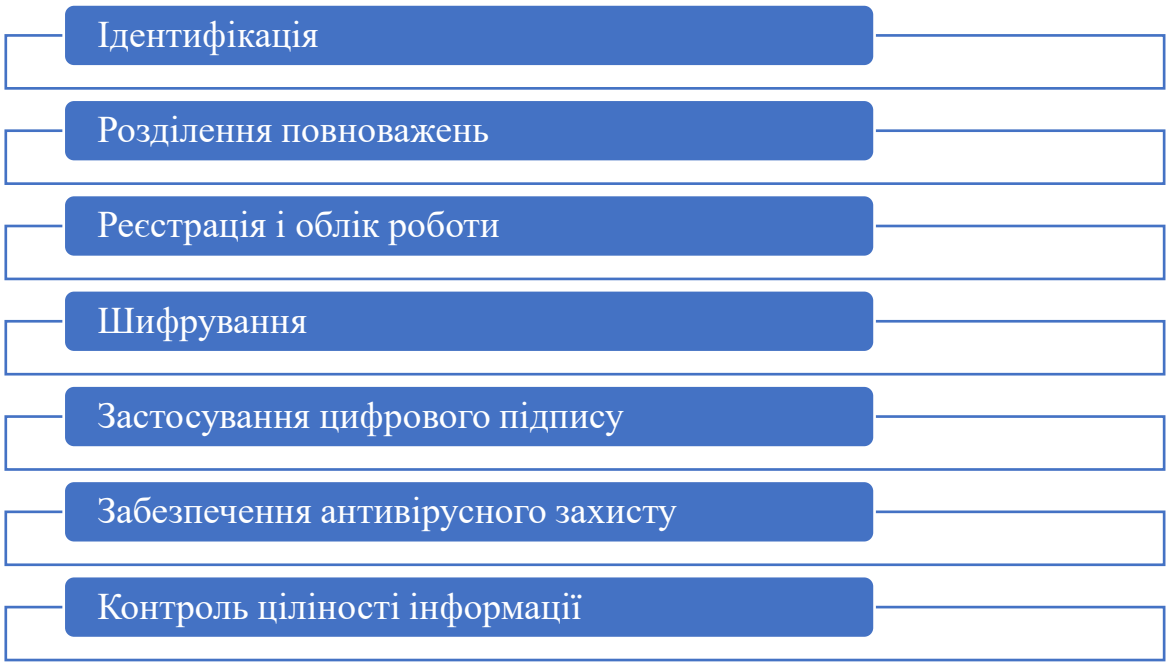

Рис. 1. Основні правила забезпечення політики безпеки інформації

Основу для формування вимог до захисту складає список загроз. Коли такі вимоги відомі, можуть бути визначені відповідні правила забезпечення захисту. Ці правила, в свою чергу, визначають необхідні функції і заходи захисту. Чим суворіші вимоги до захисту і більше відповідних правил, тим ефективніші його механізми і тим більш захищеним виявляється автоматизований комплекс.

Отже, захист інформації в комп’ютерній мережі ефективніший в тому випадку, коли проектування і реалізація системи захисту відбувається в три етапи:

– аналіз ризику;
– реалізація політики безпеки;
– підтримка політики безпеки.

На першому етапі аналізуються вразливі елементи комп’ютерної мережі, визначаються й оцінюються загрози і підбираються оптимальні засоби захисту.

Аналіз ризику закінчується прийняттям політики безпеки.

Політикою безпеки (Security Policy) називається комплекс взаємозалежних засобів, спрямованих на забезпечення високого рівня безпеки.

У теорії захисту інформації вважається, що ці засоби повинні бути спрямовані на досягнення наступних цілей:

– конфіденційність (засекречена інформація повинна бути доступна тільки тому, кому вона призначена);

– цілісність (інформація, на основі якої приймаються рішення, повинна бути достовірною і повною, а також захищена від можливих ненавмисного і злочинного перекручувань);

– готовність (інформація і відповідні автоматизовані служби повинні бути доступні та, у разі потреби, готові до обслуговування).

Другий етап – реалізація політики безпеки – починається з проведення розрахунку фінансових витрат і вибору відповідних засобів для виконання цих задач. При цьому, необхідно врахувати такі фактори як: безконфліктність роботи обраних засобів, репутація постачальників засобів захисту, можливість одержання повної інформації про механізми захисту і надані гарантії.

Третій, найбільш важливий, етап – підтримка політики безпеки. Заходи, проведені на даному етапі, вимагають постійного спостереження за вторгненнями у мережу зловмисників, виявлення «дір» у системі захисту об’єкта інформації, обліку випадків несанкціонованого доступу до конфіденційних даних.

При цьому основна відповідальність за підтримку політики безпеки мережі лежить на системному адміністраторі, що повинен оперативно реагувати на усі випадки злому конкретної системи захисту, аналізувати їх і використовувати необхідні апаратні і програмні засоби захисту з урахуванням максимальної економії фінансових засобів.

Безпека інформації є надзвичайно важливою в сучасному світі. Вона відіграє критичну роль у захисті даних, інформаційних ресурсів та приватності в умовах все більшого цифрового світу. Безпека інформації стає на перший план

в бізнесі, технологіях, урядових органах та для кожного користувача, оскільки загрози кібербезпеки стають більшими та різноманітнішими. Захист інформації від несанкціонованого доступу, кібератак і втрати стає нашим спільним завданням, і від нього залежить безпека наших даних, фінансова стабільність, репутація та функціонування суспільства в цілому. Тому безпека інформації має залишатися в центрі уваги для всіх, хто використовує інформаційні технології.

СПИСОК ЛІТЕРАТУРИ

1. Означення поняття криптографія [Електронний ресурс]. – Режим доступу: https://uk.wikipedia.org/wiki/

2. Про проблеми захисту інформації в комп`ютерних мережах [Електронний ресурс]. – Режим доступу: https://core.ac.uk/reader/84825465

3. Методи та засоби захисту комп’ютерної інформації. Інформація як об’єкт захисту [Електронний ресурс]. – Режим доступу: http://pmf.uad.lviv.ua/storage/uploads