ISU
INTERNATIONAL SCIENTIFIC UNITY

L INTERNATIONAL SCIENTIFIC AND PRACTICAL CONFERENCE «Innovative Education: Problems and Prospects of Scientific Research»

December 4-6, 2024
Stuttgart, Germany

ISBN 978-617-8427-40-5

DOI 10.70286/ISU-04.12.2024

INTERNATIONAL SCIENTIFIC UNITY

L INTERNATIONAL SCIENTIFIC AND PRACTICAL CONFERENCE
«Innovative Education: Problems and Prospects of Scientific Research»

Collection of abstracts

December 4-6, 2024
Stuttgart, Germany

– апаратні та програмні рішення, що використовуються для зберігання, пошуку, обміну та аналізу медичної інформації, медичних даних та знань для безперешкодної комунікації та прийняття рішень;

– програмне забезпечення для охорони здоров'я, що використовується для управління щоденними клінічними операціями та адміністративними завданнями, підвищення ефективності, зменшення витрат і помилок;

– дистанційні/віртуальні рішення для моніторингу здоров'я та консультування, медичні мобільні додатки, онлайн-медичні картки, носимі пристрої та інструменти самоконтролю для полегшення персоналізованого догляду.

В цілому, за сучасних умов використання інформаційних технологій стає особливо важливим у різних сферах життя людини. Це не лише дозвілля та повсякдення, але й здійснення багатьох важливих процесів, які загалом забезпечують існування людства. У майбутньому роль таких технологій буде лише зростати.

Список використаних джерел

1. Information technology (IT). URL: https://www.techtarget.com/ searchdatacenter/ definition/IT
2. Використання сучасних комп'ютерних технологій у процесі підготовки майбутніх фахівців з фізичної культури та спорту. URL: https://www.researchgate.net/publication/370419828_Vikoristanna_sucasnih_komp%27uternih_tehnologij_u_procesi_pidgotovki_majbutnih_fahivciv_z_fizicnoi_kulturi_ta_sportu
3. Інформаційні технології у сучасному житті людини: плюси і мінуси / Пікалова В.В., Деркач Т.М.// Міжнародний центр наукових досліджень. – Вінниця: ТОВ «УКРЛОГОС Груп, 2024. – С.200-201.

КІБЕРПРОСТОР: АНАЛІЗ ЗАГРОЗ ТА МЕТОДИ ЗАХИСТУ

Деркач Тетяна
к.т.н., доцент
Лавренко Микола
здобувач вищої освіти
Національний університет «Полтавська політехніка імені Юрія Кондратюка», Україна

У сучасну епоху цифрових технологій та глобальної мережі Інтернет питання кібербезпеки стає дедалі більш актуальним та важливим. Зростання обсягу оброблюваної інформації, розвиток Інтернету речей (IoT), впровадження штучного інтелекту та інших інноваційних технологій значно підвищили ефективність та зручність життя, але водночас створили нові виклики та загрози. Кіберзлочинність, зловмисні атаки на інформаційні системи, витоки

конфіденційних даних та інші форми кіберзагроз можуть мати серйозні наслідки як для окремих користувачів, так і для організацій та державних структур.

Кіберпростір – це цифровий простір, де здійснюється передача, обробка, зберігання та обмін інформацією через комп'ютерні мережі. Він є важливим елементом сучасного світу, але водночас стає об'єктом численних загроз.

Сучасний кіберпростір характеризується стрімким розвитком технологій, що супроводжується зростанням складності та кількості кіберзагроз. Загрози набувають нових форм, що вимагає підвищеної уваги до безпеки.

Аналіз загроз у кіберпросторі – це процес оцінки потенційних та існуючих ризиків для інформаційної безпеки з метою попередження атак, мінімізації шкоди та розробки ефективних механізмів захисту.

Етапи аналізу кіберзагроз.

1. Ідентифікація загроз: визначення потенційних кіберзагроз, таких як шкідливе програмне забезпечення, фішинг, DDoS-атаки, витік даних тощо.

Вивчення джерел загроз (хакери, інсайдери, конкурентні організації, державні структури, автоматизовані системи).

2. Класифікація загроз:

– зовнішні: атаки з боку зловмисників, які не мають доступу до внутрішньої системи.

– внутрішні: дії інсайдерів (навмисні або ненавмисні помилки співробітників).

– технічні: вразливості програмного забезпечення, обладнання або мереж.

3. Аналіз вразливостей: оцінка слабких місць в інформаційній системі, через які можуть реалізуватися загрози (незахищені порти, застаріле ПЗ, ненадійні паролі).

4. Оцінка ризиків: визначення ймовірності реалізації загроз та потенційних наслідків для організації. Розрахунок ризиків на основі ймовірності атаки, рівня вразливості та цінності активів.

5. Моніторинг кіберзагроз: постійне спостереження за активністю в мережі, використання систем виявлення та запобігання вторгненням (IDS/IPS).

Аналіз загроз у кіберпросторі є ключовим елементом забезпечення інформаційної безпеки. Він дозволяє виявити слабкі місця системи, оцінити потенційні ризики та розробити стратегії їхнього усунення. Постійний моніторинг і вдосконалення механізмів захисту є необхідними умовами для забезпечення безпечного функціонування організації в сучасному цифровому світі.

Ефективний захист від кіберзагроз вимагає комплексного підходу, що поєднує технічні засоби, організаційні заходи та освітні ініціативи. Основна мета – забезпечення конфіденційності, цілісності та доступності інформації.

На сучасному етапі у сфері кібербезпеки можна виділити основні методи захисту від кіберзагроз.

1. Технічні засоби захисту:

– Антивірусне програмне забезпечення.

– Брандмауери (файрволи).

– Шифрування даних.
– Системи виявлення та запобігання вторгненням (IDS/IPS).
– Многофакторна аутентифікація (MFA).
– Резервне копіювання даних.
– Оновлення програмного забезпечення.

2. Організаційні заходи:
– Розробка політик кібербезпеки.
– Контроль доступу.
– Розподіл зон безпеки.
– Моніторинг системи.
– План реагування на інциденти.

3. Навчання та обізнаність:
– Освіта співробітників.
– Тренінги з реагування на атаки.
– Політика складних паролів.

4. Інноваційні підходи:
– Використання штучного інтелекту.
– Блокчейн-технології.
– Карантин для невідомих файлів.
– Zero Trust Architecture (ZTA).

5. Зовнішній захист та кіберрозвідка:
– Постачальники кібербезпеки.
– Тестування на проникнення (Penetration Testing).
– Багатостороння співпраця.

Окрім цього, варто дотримуватися таких рекомендацій щодо підвищення захисту:

1. Створення багаторівневої системи безпеки. Встановлення фільтрів, антивірусів, брандмауерів. Використання шифрування для захисту даних.

2. Розробка політик кібербезпеки. Чітке регулювання доступу до даних, правила зберігання та передачі інформації.

3. Навчання персоналу. Освіта співробітників для підвищення обізнаності про загрози (особливо фішинг та соціальну інженерію).

4. Регулярний моніторинг і аудит. Перевірка стану систем безпеки, моніторинг журналів подій.

5. Застосування кіберрозвідки. Отримання оперативної інформації про нові загрози для вчасного реагування.

Захист від кіберзагроз потребує постійного вдосконалення технологій, управлінських підходів і підвищення кіберкультури. Лише комплексний підхід із залученням сучасних технологій і людського ресурсу забезпечить ефективний захист у сучасному цифровому світі.

Сучасний кіберпростір є полем для складних викликів, що вимагає постійної адаптації до нових загроз. Ефективний аналіз ризиків, підвищення культури кібербезпеки та використання передових технологій дозволять мінімізувати втрати та забезпечити безпеку в цифрову еру.