5. Таран Т. С. Педагогічна інклюзія : основи професійної підготовки. *Педагогічна думка,* 2021. № 2. С. 52–58.

БЕЗПЕКА В ІНФОРМАЦІЙНОМУ ПРОСТОРІ

Хома Надія Григорівна
кандидат фізико-математичних наук, доцент кафедри економічної кібернетики та інформатики, Західноукраїнський національний університет,
nadiia.khoma3@gmail.com
Цинайко Василь Петрович
здобувач першого рівня вищої освіти спеціальності Комп'ютерні науки, Західноукраїнський національний університет,
vasyl.tsynaiko@gmail.com

В сучасному світі інформаційні системи та мережі стали невід'ємною частиною усіх сфер людської діяльності, забезпечуючи обробку, зберігання та передачу даних. Однак разом із зростанням залежності від цифрових технологій збільшується й кількість загроз, які ставлять під сумнів безпеку інформації. Атаки на інформаційні системи, такі як DoS, SQL Injection і Phishing, є найбільш поширеними методами порушення їхньої цілісності, доступності та конфіденційності.

Для забезпечення захисту інформаційних ресурсів використовуються різноманітні технології та інструменти, серед яких важливе місце займають брандмауери, антивірусні програми та системи виявлення вторгнень. Не менш значущим є впровадження сучасних протоколів безпеки, таких як SSL/TLS, IPsec і VPN, що забезпечують безпечну передачу даних у мережах.

Окремої уваги потребує захист хмарних сервісів і віртуальних інфраструктур, які набувають популярності завдяки своїй гнучкості та ефективності, але водночас стають привабливою ціллю для зловмисників.

Дослідження питань безпеки інформаційних систем та мереж є ключовим для мінімізації ризиків втрати даних та збереження їхньої конфіденційності в умовах постійно зростаючих кіберзагроз. Розглянуто сучасні технології захисту інформації у мережах та хмарних інфраструктурах.

Захист від атак на інформаційні системи є одним із ключових завдань інформаційної безпеки. Для ефективного протистояння загрозам необхідно розуміти їхню природу, механізми реалізації та можливі наслідки. Серед найбільш поширених видів атак можна виділити DoS-атаки, SQL Injection та Phishing.

DoS (Denial of Service) атаки спрямовані на виведення з ладу системи або мережі шляхом перевантаження її ресурсів. Зловмисники створюють величезну кількість запитів, які система не може обробити, що призводить до зупинки її роботи або значного зниження продуктивності. Основна мета таких атак – зробити сервіс недоступним для користувачів, що може мати катастрофічні наслідки для бізнесу, залежного від безперебійного функціонування своїх інформаційних ресурсів.

SQL Injection є однією з найпоширеніших атак на веб-додатки. Цей вид атаки використовує вразливості у введенні даних користувачами для виконання шкідливих SQL-запитів до бази даних. Наприклад, зловмисники можуть отримати доступ до конфіденційної інформації, видалити дані або змінити їх. Вразливість виникає через відсутність належної валідації та очищення введених даних, що дозволяє виконувати довільні команди в базі даних від імені додатку.

Phishing – це техніка соціальної інженерії, яка спрямована на обман користувачів для отримання конфіденційної інформації, такої як паролі, дані банківських карток або особиста інформація. Найчастіше фішингові атаки реалізуються через електронну пошту або підроблені веб-сайти, які імітують легітимні сервіси. Користувач, довірившись підробленому ресурсу, вводить свої дані, які автоматично передаються зловмисникам.

Для ефективного захисту від цих атак необхідно впроваджувати комплексні заходи, включаючи використання технологій моніторингу трафіку, систем виявлення вторгнень, регулярне оновлення програмного забезпечення, налаштування правил фільтрації даних і навчання користувачів основам кібербезпеки. Розуміння природи цих загроз дозволяє зменшити ймовірність їх успішної реалізації та забезпечити надійний захист інформаційних систем.

Для забезпечення надійного захисту інформаційних систем і мереж використовуються різноманітні технологічні рішення, які допомагають виявляти, запобігати та нейтралізувати загрози. Одними з найважливіших інструментів є брандмауери [1], антивірусні програми та системи виявлення вторгнень.

Комбінація брандмауерів, антивірусних програм та систем виявлення вторгнень дозволяє створити багаторівневий захист, який ефективно протистоїть більшості сучасних загроз. Їх спільне використання забезпечує як запобігання атакам, так і оперативне реагування на інциденти, мінімізуючи ризики втрати даних або компрометації системи.

Протоколи безпеки в мережах є важливими компонентами захисту даних під час їхньої передачі. Вони забезпечують шифрування, автентифікацію та цілісність інформації, що дозволяє запобігти несанкціонованому доступу або перехопленню. До найбільш поширених протоколів безпеки належать SSL/TLS, IPsec та VPN, кожен із яких виконує специфічні функції у захисті мережевих з'єднань.

Використання SSL/TLS, IPsec та VPN [2] забезпечує комплексний підхід до захисту даних у мережах, мінімізуючи ризики перехоплення інформації та несанкціонованого доступу. Ці протоколи дозволяють створювати безпечні з'єднання, необхідні для сучасного цифрового світу.

Захист хмарних сервісів і віртуальних інфраструктур є одним із ключових завдань сучасної кібербезпеки [3]. З ростом популярності хмарних обчислень та віртуалізації організації отримали доступ до потужних і гнучких рішень для зберігання, обробки та обміну даними. Однак ці технології також відкривають нові можливості для кібератак, що вимагає особливої уваги до захисту даних і сервісів.

Однією з головних загроз у хмарних середовищах є ризик несанкціонованого доступу до даних через недостатню сегментацію або

неправильну конфігурацію. Захист таких сервісів починається з належного управління доступом. Це включає впровадження багатофакторної автентифікації, контроль привілеїв користувачів та регулярний аудит прав доступу.

Шифрування даних також відіграє вирішальну роль у захисті хмарних сервісів. Дані повинні бути зашифровані як під час передачі між клієнтом і сервером, так і при зберіганні. Сучасні хмарні провайдери пропонують інструменти для управління ключами шифрування, які дозволяють клієнтам зберігати контроль над своїми даними.

Захист віртуальних інфраструктур, що використовують хмарні середовища, вимагає впровадження міжмережевих екранів і систем виявлення вторгнень, які адаптовані до специфіки віртуальних середовищ. Наприклад, віртуальні брандмауери дозволяють контролювати трафік між віртуальними машинами, що мінімізує ризик поширення атак всередині інфраструктури.

Іншою важливою складовою є безпека API, які використовуються для інтеграції та управління хмарними ресурсами. Недоліки в конфігурації або вразливості в API можуть стати входом для зловмисників, тому їх захист вимагає регулярного тестування, обмеження доступу та використання методів автентифікації.

Крім того, важливим є планування та впровадження стратегії резервного копіювання та відновлення даних. Це дозволяє мінімізувати втрати у разі збоїв, атак або випадкових видалень даних.

Віртуальні середовища, як і хмарні сервіси, значною мірою залежать від спільної відповідальності між провайдером і клієнтом. Провайдери відповідають за захист інфраструктури, тоді як користувачі несуть відповідальність за налаштування доступу, шифрування та управління своїми ресурсами.

Захист хмарних сервісів і віртуальних інфраструктур є багатогранним завданням, яке вимагає постійного моніторингу, впровадження сучасних технологій безпеки та дотримання кращих практик кіберзахисту. Це дозволяє зберегти конфіденційність, цілісність і доступність даних у динамічному хмарному середовищі.

У сучасному світі інформаційна безпека є ключовим аспектом функціонування цифрових систем, без яких неможливо уявити життя суспільства, бізнесу та держави. Зростання кількості атак і розвиток кіберзагроз ставлять перед спеціалістами завдання розробки ефективних засобів захисту, здатних забезпечити конфіденційність, цілісність і доступність даних.

Розглянута класифікація атак, таких як DoS, SQL Injection і Phishing, показує важливість комплексного підходу до їх попередження, який включає як технічні, так і організаційні заходи. Брандмауери, антивірусні програми та системи виявлення вторгнень є основними інструментами захисту, що дозволяють створювати багаторівневу систему оборони від сучасних загроз.

Протоколи безпеки, такі як SSL/TLS, IPsec і VPN, відіграють важливу роль у забезпеченні безпечної передачі даних у мережах. Вони забезпечують захищеність комунікацій, зберігаючи конфіденційність інформації навіть у відкритих і публічних мережах.

Особливої уваги потребує захист хмарних сервісів і віртуальних інфраструктур, які стають дедалі популярнішими. Забезпечення належної сегментації, шифрування, контролю доступу, а також використання сучасних систем моніторингу дозволяє мінімізувати ризики, пов'язані з використанням цих технологій.

Отже, забезпечення інформаційної безпеки [4] є багатогранним завданням, що вимагає постійного розвитку технологій, адаптації до нових викликів і тісної співпраці між усіма учасниками процесу. Тільки завдяки впровадженню комплексних заходів можна ефективно протистояти кіберзагрозам та забезпечувати стабільність і безпеку інформаційних систем у динамічному цифровому середовищі.

Список використаних джерел

1. Найкращі протоколи VPN та відмінності між типами VPN. URL: https://nordvpn.com/uk/blog/protokoly/. (дата звернення 2.04.2025).

2. Роль брандмауера у забезпеченні особистої кібербезпеки – захист від загроз і зламів в мережі. URL: https://mediacom.com.ua/rol-brandmauera-v-osobistij-kiberbezpetsi. (дата звернення 2.04.2025).

3. Хмарна безпека. URL: https://nordvpn.com/uk/cybersecurity/cloud-security/. (дата звернення 2.04.2025).

МЕТОДИ І АЛГОРИТМИ АНАЛІЗУ КОРЕЛЯЦІЙ МІЖ ТЕКСТОВИМИ ДАНИМИ І ПОВЕДІНКОВИМИ ПОКАЗНИКАМИ КОРИСТУВАЧІВ

Ясінський Андрій Михайлович
здобувач другого (магістерського) рівня вищої освіти спеціальності Комп'ютерні науки,
Тернопільський національний педагогічний університет імені Володимира Гнатюка,
yasinskyj_am@fizmat.tnpu.edu.ua
Лень Андрій Володимирович
кандидат історичних наук, асистент кафедри інформатики та методики її навчання,
Тернопільський національний педагогічний університет імені Володимира Гнатюка,
lenandr@tnpu.edu.ua

У сучасному інформаційному середовищі значну роль відіграє аналіз великих обсягів даних, які активно генеруються користувачами у цифровому просторі. Текстові повідомлення, коментарі, пости та інші форми контенту, створені у межах соціальних мереж, інформаційних ресурсів і освітніх платформ, містять велику кількість прихованих закономірностей, які відображають поведінкові характеристики та інтереси користувачів. Тому актуальним є питання вивчення методів, які дозволяють встановити взаємозв'язки між текстовими даними та показниками взаємодії з контентом. Застосування відповідних методів аналізу відкриває можливості для глибшого розуміння цифрової поведінки, прогнозування тенденцій та формування ефективних стратегій залучення.

Одним із головних напрямів у цьому контексті є використання алгоритмічних методів аналізу текстових даних, які дозволяють не лише структурувати інформацію, а й виявити приховані закономірності у поведінці користувачів.