Добровольський Д. В., магістрант,
Державний університет «Житомирська політехніка»

АТАКИ НА ІНФОРМАЦІЙНУ СИСТЕМУ, ЇХ НАСЛІДКИ ТА МЕТОДИ ПРОТИДІЇ

В умовах швидкого розвитку технологій та зростання впровадження цифрових рішень, інформаційні системи стають ключовим елементом функціонування різних галузей. Однак разом із цим ростом збільшується й кількість загроз та атак, якими ці системи стають схильними.

Сучасні атаки на інформаційну систему не обмежуються вже класичними методами, а використовують передові технології та винахідливі підходи. Враховуючи поширення хмарних технологій та велику кількість підключених пристроїв, підвищується поверхня для потенційних атак.

Однією з передумов розвитку атак є швидке збільшення кількості підключених пристроїв, які часто виявляються вразливими до новітніх методів атак, таких як використання вразливостей програмного забезпечення та соціально-інженерні атаки. Зростаюча залежність від інтернет-підключення та обміну даними у реальному часі також створює нові виклики у забезпеченні безпеки.

Отже, розгляд сучасних атак на інформаційну систему важливий не лише для реакції на поточні загрози, але й для передбачення та запобігання майбутнім ризикам, що дозволяє розробляти та впроваджувати ефективні стратегії захисту.

Однією з основних загроз є атаки на рівень додатків, які можуть використовувати вразливості програмного забезпечення для отримання несанкціонованого доступу та викрадення конфіденційної інформації. Для уникнення таких атак важливо регулярно оновлювати програмне забезпечення та використовувати системи виявлення вразливостей.

Іншою серйозною загрозою є атаки з використанням вірусів, троянських програм та шкідливих кодів, які можуть пошкодити або вкрасти дані. Для захисту від таких атак важливо використовувати антивірусне програмне забезпечення та здійснювати регулярне сканування системи на предмет виявлення загроз.

Також серйозною загрозою є атаки на рівень мережі, такі як атаки на протоколи маршрутизації або атаки з переповненням буфера. Для захисту від таких атак важливо використовувати системи виявлення та захисту від вторгнень (IDS/IPS) та ефективно налаштовувати файерволи та інші захисні механізми.

Сучасні атаки на інформаційну систему можуть мати значущі та руйнівні наслідки для різних сфер діяльності, включаючи втрату конфіденційної інформації, порушення приватності та надійності, а також фінансові втрати та пошкодження репутації.

Отже, для ефективного захисту інформаційної системи важливо регулярно оновлювати програмне забезпечення, використовувати захисні механізми та системи виявлення вразливостей, а також надавати відповідне навчання персоналу з питань кібербезпеки. Тільки такий комплексний підхід може забезпечити надійний рівень захисту інформаційної системи в умовах сучасних технологій.

Список використаних джерел

1. A survey on cloud computing security: Issues, threats, andsolutions [Електронний ресурс] / S.Singh. – 2016. – Режим доступу до ресурсу: https://www.sciencedirect.com/science/article/abs/pii/S1084804516301990
2. Top 20 Most Common Types Of Cyber Attacks | Fortinet. [Електронний ресурс] / Fortinet. – 2021. – Режим доступу до ресурсу: https://www.fortinet.com/resources/cyberglossary/types-of-cyber-attacks
3. Active and Passive attacks in Information Security – Geeksfor Geeks. [Електронний ресурс] / GeeksforGeeks. – 2020. – Режим доступу до ресурсу: https://www.geeksforgeeks.org/active-and-passive-attacks-in-information-security/