Секція 1

АНАЛІЗ ХАКЕРСЬКИХ АТАК НА МІНІСТЕРСТВО ЗАКОРДОНИХ СПРАВ

Вірський Я. М.
Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ»
Науковий керівник: Тецький А. Г.

Актуальність. Атаки з боку зловмисників на державні установи, в тому числі на Міністерство закордонних справ (МЗС), є серйозною загрозою національній безпеці. Вони можуть призвести до витоку конфіденційної інформації, порушення роботи державних систем та навіть до дестабілізації ситуації в країні. Хакерські атаки на МЗС є все більш поширеними. У 2022 році було зафіксовано низку таких атак, зокрема на офіційні сайти МЗС США, Великобританії та України [1]. Атаки на МЗС можуть мати далекосяжні наслідки. Наприклад, виток конфіденційної інформації може призвести до витоку державної таємниці, а порушення роботи державних систем може призвести до перебоїв у дипломатичній діяльності [2].Тому дослідження хакерських атак на МЗС є важливим напрямком наукових досліджень. Воно дозволяє підвищити рівень розуміння цієї загрози та розробити ефективні методи її протидії. Тема є актуальною та перспективною для наукової конференції.

Метою даної роботи є дослідження принципів «безпечного» кодування. даної роботи є обговорення актуальних проблем безпеки, пов'язаних із кібератаками на Міністерство закордонних справ. Конференція дозволить обмінятися досвідом і знаннями в галузі кібербезпеки, сприяти розвитку наукових досліджень у цій галузі та розробці ефективних методів протидії кібератакам.

Покращити розуміння хакерських атак на МЗС. Це дозволить учасникам обговорити різні типи кібератак на МЗС, їхні мотиви та наслідки. Розробити ефективні методи протидії кібератакам на МЗС. Конференція дозволить обговорити актуальні дослідження та розробки в галузі кібербезпеки, спрямовані на підвищення рівня захисту МЗС від кібератак [3].

Основні положення. Безпечне Для своєчасної протидії загрозам використовуються антивірус та мережевий екран. Серед популярних та ефективним антивірусів є Microsoft Defender, це потужний автономний інструмент перевірки, який можна запустити із довіреного середовища без завантаження ОС. Також віддається перевага такому міжмережевий екран як FortiClient. Це програмний продукт, що забезпечує безпеку настільних комп'ютерів, ноутбуків та мобільних пристроїв. FortiClient включає антивірус, захист від шпигунського програмного забезпечення, персональний міжмережевий екран, фільтр для web-контенту і антиспам.

Форензіка є важливим інструментом для аналізу кібератак на МЗС. Вона дозволяє зібрати та зберегти докази, які можуть бути використані для ідентифікації хакерів, розуміння їхніх мотивів та запобігання майбутнім атакам [4].

Висновки. Швидкі зміни технологій та методів кібератак вимагають постійного моніторингу та адаптації заходів безпеки. Аналіз минулих атак може слугувати важливим інструментом для покращення існуючих стратегій та запобігання майбутнім загрозам. Хакерські атаки на МЗС можуть мати міжнародний характер, і співпраця на міжнародному рівні стає критично важливою для виявлення та припинення подібних загроз. Це стає серйозною загрозою для національної безпеки, оскільки це може призвести до втрати чутливої інформації, порушення дипломатичних відносин та інших наслідків, що можуть шкодити інтересам країни. Розробка та впровадження ефективних заходів протидії хакерським атакам є невід'ємною частиною стратегії національної безпеки. На основі аналізу можна розробити конкретні рекомендації для удосконалення захисту інформації та інфраструктури МЗС.

Список літератури

1. 2022 Ukraine cyberattacks. *Wikipedia*. URL – https://en.wikipedia.org/wiki/2022_Ukraine_cyberattacks (дата звернення: 14.10.2023);
2. Bad Magic's Extended Reign in Cyber Espionage Goes Back Over a Decade. *Hacker News*. URL – https://thehackernews.com/2023/05/bad-magics-extended-reign-in-cyber.html (дата звернення: 15.10.2023);
3. Кібербезпека: Все Що Необхідно Знати Кожному Користувачу Мережі Інтернет. *Ukraine lifehacker*. URL – https://www.ukraine-lifehacker.com/kiberbezpeka-vse-shcho-neobkhidno-znaty (дата звернення: 15.10.2023);
4. Carier B. File System Forensic Analysis. 2005. Page 511. URL – https://repo.zenksecurity.com/Forensic/File%20System%20Forensic%20Analysis.pdf (дата звернення: 16.10.2023).

Відомості про авторів

Вірський Ярослав Михайлович, студент кафедри комп’ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», y.m.virsjkyy@student.csn.khai.edu
Тецький Артем Григорович, доцент кафедри комп’ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», к.т.н., a.tetskiy@csn.khai.edu