Секція 1

АНАЛІЗ ІСНУЮЧИХ МОДЕЛЕЙ ЗАГРОЗ І ПОРУШНИКІВ

Овчаренко Н. Д.
Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ»
Науковий керівник: Пєвнєв В. Я.

Актуальність. Зростання кількості технологій та їх використання в різних сферах життя супроводжується також збільшенням кількості кіберзлочинів та інших порушень безпеки. Для забезпечення ефективного кіберзахисту необхідно розуміти, які методи та техніки використовують зловмисники.

Дослідження існуючих моделей порушників дозволяє виявити їхні мотивації, методи та стратегії. Це надає можливість створити більш ефективні заходи кіберзахисту та попередження кіберзлочинів. Також це допомагає виробникам програмного забезпечення та інших технологій покращувати свої продукти, зменшуючи їхню вразливість перед потенційними атаками.

Метою є вивчення та аналіз існуючих моделей поведінки кіберпорушників з метою розкриття їхніх мотивацій, використовуваних технік та стратегій.

Основні положення. В доповіді розглянуто мотивацію, кваліфікацію, технічну оснащеність, обмеження та припущення про характер можливих дій порушників, що дає змогу класифікувати їх за цими критеріями.

Розглядаючи мотивацію, можна виділити різні фактори, що підштовхують особу до порушення закону. Деякі з них можуть бути пов'язані з економічними труднощами, соціальною несправедливістю, амбіціями або навіть психологічними проблемами. У контексті кваліфікації та технічної оснащеності можна зрозуміти які інструменти можуть бути використані та визначити наскільки вірогідно і успішно може бути виконана атака.

Враховуючи обмеження та припущення про характер можливих дій порушника можливо зробити припущення щодо сценаріїв можливих атак. Класифікація порушників за цими критеріями дозволяє визначити спільні тенденції в їхній діяльності та розробляти ефективні стратегії протидії.

У доповіді було розглянуто моделі загроз, які дають нам систематичний підхід до аналізу потенційних небезпек і ризиків, які можуть виникнути у сфері інформаційних технологій або інших сферах. Цей термін може використовуватися в контексті кібербезпеки, фізичної безпеки, бізнес-аналізу та інших областей. Модель загроз допомагає ідентифікувати, класифікувати і аналізувати потенційні загрози для прийняття заходів з їх запобігання чи обмеження.

У доповіді було відзначено, що для кожної загрози потрібно визначити на порушення яких властивостей інформації вона спрямована, користуючись чотирма основними градаціями, а саме: порушення конфідеційності, цілісності, доступності інформації, а також порушення спостереженості та керованості системи. Також потрібно визначити які суб'єкти системи або суб'єкти зовнішні по відношенню до неї, можуть ініціювати загрозу. І наостанок треба визначити можливі способи здійснення загроз.

Висновки. Робота присвячена аналізу існуючих моделей загроз і порушників у кіберпросторі. Було проведено аналіз мотивацій, кваліфікацій, технічної оснащеності, обмежень та припущень про можливий характер дій порушників.

Список літератури

1. 6 Motivations of Cyber Criminals. *Coretech.* URL: https://www.coretech.us/blog/6-motivations-of-cyber-criminals (дата звернення: 10.10.2023);
2. Ramya Mohanakrishnan What Is Threat Modeling? Definition, Process, Examples, and Best Practices. *Spiceworks.* URL – https://www.spiceworks.com/it-security/network-security/articles/what-is-threat-modeling-definition-process-examples-and-best-practices/ (дата звернення: 12.10.2023);
3. Victoria Drake Threat Modeling. *Owasp.* URL – https://owasp.org/www-community/Threat_Modeling (дата звернення: 12.10.2023);
4. Комаров М.Ю. Ониськова А.В. Гончар С.Ф. Аналіз і дослідження моделі порушника безпеки інформації для захищеного вузла інтернет доступу. *Vernadskyjournals.* URL: http://www.tech.vernadskyjournals.in.ua/journals/2018/5_2018/part_1/26.pdf (дата звернення: 12.10.2023).

Відомості про авторів

Овчаренко Нікіта Дмитрович, магістрант кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», n.ovcharenko@student.csn.khai.edu
Пєвнєв Володимир Яковлевич, професор кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», д.т.н, доцент, v.pevnev@csn.khai.edu