УДК 004.056

# ДЕЯКІ ПОГЛЯДИ НА ПОБУДОВУ МОДЕЛІ ЗАГРОЗ В ІНТЕРЕСАХ ОЦІНКИ РИЗИКУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ КОМПАНІЇ

Магдаліна М.І.
Науковий керівник – доцент Снігуров А.В.
Харківський національний університет радіоелектроніки, каф. ІКІ,
м. Харків, Україна
тел. +38(097) 933-78-40.

In the report, an analysis of problems in building a model of threats and an intruder in the assessment of information security risks of companies is carried out. The report analyzes the content of the threat model, presents problems in solving the task of building a threat model. A classification and integral indicator of intentional threats is proposed.

При оцінці ризиків інформаційної безпеки одним з ключових завдань є побудова моделі загроз і її складової – моделі порушника. Оцінка ризиків інформаційної безпеки (ІБ) вимагає розуміння рівня загроз (можливості - Likelihood, ймовірності – Probability, або щорічної кількості - Annualized rate of occurrence). Ця оцінка є різною для різних компаній, різних ризикових ситуацій, різної безпекової ситуації.

Відомо, що усі загрози поділяються відповідно джерела загрози на загрози від антропогенних джерел, загрози від природних джерел та загрози від техногенних джерел. До перших відносяться загрози від людини. Такою людиною може бути зловмисник, який реалізує або таргетовану (цільову) атаку, або нетаргетовану атаку. Такою людиною може бути зловмисник, який по необережності або халатності порушує інформаційну безпеку компанії. Зловмисники можуть бути зовнішні та внутрішні (інсайдери). До типів зовнішніх зловмисників можуть відноситися представники спеціальних служб іншої держави, кримінальні структури, потенційні злочинці і хакери, несумлінні партнери, представники аварійних служб і наглядових організацій, технічний персонал телекомунікаційних послуг. До інсайдерів можуть відноситися основний персонал компанії (програмісти, розробники, користувачі), представники служби захисту інформації, допоміжний склад (охорона, прибиральники тощо), технічний персонал (експлуатація, життєзабезпечення).

Під природними загрозами розуміються пожежі, землетруси, повені, урагани, магнітні бурі, радіоактивне випромінювання, інші форс-мажорні обставини. Під техногенними загрозами розуміються технічні проблеми з засобами зв'язку, мережами інженерних комунікацій (каналізація, водопостачання), транспортом, неякісними технічними засобами обробки інформації, неякісними програмними засобами обробки інформації, проблеми з допоміжними засобами (охоронна сигналізація, телефони) тощо.

Модель загроз та модель порушника мають дати відповідь на одне з головних питань при оцінці ризиків ІБ – який порушник реальний для

конкретної компанії, яка природна або техногенна загроза реальна для компанії.

При аналізі поставленого питання необхідно зрозуміти, по – перше, що таке модель. Модель — це абстрактне представлення (опис) реальності в певній формі (наприклад, у математичній, фізичній, символічній або графічній), призначене для розвитку розуміння цієї реальності. В доповіді приводяться приклади моделі загроз ІБ, яка представлена в текстовій формі, та приклади математичної моделі таких загроз. В доповіді аналізуються проблеми адекватності та точності моделі загроз. Важливим поняттям при побудові моделі загроз є класифікація загроз. Класифікація — це система групування об'єктів дослідження або спостереження відповідно до їх загальних ознак. Класифікація загроз дозволяє їх поділити по певним класам, східним по значенням параметрів моделі. Це дає змогу виділити для кожного класу загроз східні механізми їх реалізації та побудувати механізми захисту від цих загроз.

При побудові моделі ненавмисних загроз – природних та техногенних в більшості випадків вистачає статистики реалізації цих загроз у світі, країні та регіоні компанії, історія реалізації цих загроз в самій компанії. Методи експертного аналізу загроз з використанням такої інформації дають можливість з певною якістю побудувати модель даних загроз. Складніше ситуація є з побудовою моделі зловмисника. Параметрами моделі мають бути: мотивація зловмисника та його потенціал. Під потенціалом зловмисника розуміється наявність у нього певної кваліфікації та обладнання для реалізації конкретної атаки.

Що ми маємо отримати після побудови моделі зловмисника для оцінки ризиків ІБ. По-перше інтегрований показник, який би об’єднував мотивацію та потенціал зловмисника. Необхідність такого показника обумовлена тим, що потенціал може у зловмисника і бути, але мотивації немає. І навпаки. Тому в доповіді пропонується ввести інтегральний показник зловмисника – рівень небезпечності зловмисника. По друге, класифікація типів зловмисників по інтегральному показнику. В доповіді пропонується класифікація на підставі 3-х рівнів по шкалі: високий, середній, низький.

Такий підхід дозволяє отримати інформацію про можливість реалізації тих чи інших каналів атаки на критичні активи організації з урахуванням того, хто може здійснити таку атаку.

Список використаних джерел:

1. ISO/IEC 27005:2022 Інформаційна безпека, кібербезпека та захист конфіденційності — Настанови щодо управління ризиками інформаційної безпеки [Електронний ресурс] / ISO. – 2022. – Режим доступу до ресурсу: https://www.iso.org/ru/standard/80585.html.