УДК 004.056

ПІДХІД ДО ВРАХУВАННЯ РИЗИКУ СПОСТЕРЕЖЕНОСТІ ПРИ ОЦІНЮВАННІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Ю. В. Баришев, асистент
Вінницький національний технічний університет
yuriy.baryshev@gmail.com

Сучасні методики визначення ризиків інформаційної безпеки підприємства передбачають оцінювання поточного стану захищеності відповідно до трьох властивостей інформації: конфіденційності, доступності та цілісності. Збитки, які зазнають власники інформації від втрати кожної з цих властивостей, може визначити власник або користувач цієї інформації. У загальному випадку відомий підхід до визначення ризику описується такою формулою:

$$R = P_c \cdot C_c + P_a \cdot C_a + P_i \cdot C_i,$$

де P_c, P_a, P_i – ймовірність реалізації успішної атаки на конфіденційність, доступність та цілісність відповідно; C_c, C_a, C_i – збитки, які зазнає об'єкт оцінювання від втрати конфіденційності, доступності та цілісності даних відповідно.

Відомо, що, крім конфіденційності, доступності та цілісності, інформація має властивість спостереженості. Однак визначення ризику спостереженості інформації ускладнюється тим, що власники та/або користувачі інформації не можуть визначити величину збитків від порушення цієї властивості. Саме тому дослідження, пов'язані з визначенням ризику спостереженості, є актуальними.

Основною складністю таких досліджень є те, що при порушенні спостереженості інформації зі збереженням конфіденційності, доступності та цілісності інформації власники та/або користувачі інформації не зазнають збитків. З цього випливає, що зловмисникам недоцільно витрачати ресурси на реалізацію атак, направлених лише на порушення спостереженості інформації.

Водночас збереження спостереженості інформації набуває актуальності для користувачів та власників інформації після того, як відбувається атака на інформацію. Саме ця властивість дозволяє в подальшому проводити розслідування інциденту та за його результатами визначати слабкі ланки у системі захисту інформації, а також виявляти суб'єктів зловмисних дій, якщо такі дії мали місце. Отже, з цього випливає, що збереження спостереженості інформації дозволяє підприємству (установі), яке було атаковано, отримати зиск. Таким чином інтегральний ризик для кожного інформаційного ресурсу (або інформаційного потоку) пропонується визначати за такою формулою:

$$R = P_c \cdot C_c + P_a \cdot C_a + P_i \cdot C_i - (1 - P_o) \cdot C_o,$$

де P_o – ймовірність реалізації успішної атаки на спостереженість інформації; C_o – зиск, який отримує атаковане підприємство (установа) від збереження спостереженості інформації.

Із запропонованого підходу випливає, що підприємство, яке було атаковане, за умов збереження спостереженості інформації може отримати зиск від атаки, який переважатиме завдані нею збитки. Зокрема, наведена формула дозволяє пояснити доцільність застосування методу тестування системи захисту інформації "дружній злам".