УДК 681.3.067

А. В. Дудатьєв, к. т. н., доц.;
Ю. В. Баришев , асп.

РОЗШИРЕННЯ ЕКОНОМІЧНОЇ СКЛАДОВОЇ ПОНЯТТЯ РИЗИКУ В ТЕОРІЇ ЗАХИСТУ ІНФОРМАЦІЇ

Розглянуто місце ризику в теорії захисту інформації та його значення у проектуванні системи захисту інформації. Зроблено аналіз сучасного розуміння ризику, на основі якого визначено ряд недоліків. Запропоновано шляхи усунення цих недоліків. Наведено математичну модель, яка дозволяє врахувати запропоновані підходи. Визначено перспективи подальшого дослідження.

Вступ

В межах вирішення проблеми забезпечення інформаційної безпеки виникає задача оцінювання захищеності інформаційних ресурсів (ІР). Оцінювання інформаційної безпеки дозволяє визначити найслабші ланки об'єкта дослідження, а також зпрогнозувати ефективність впровадження тих чи інших засобів та заходів захисту. В результаті інженеру бажано отримати оцінки ресурсів, виражених у вартісній формі, оскільки йому необхідно визначити суму коштів, які варто витрачати на удосконалення наявної або проектування нової системи захисту інформації. Таким показником є ризик.

Сучасне розуміння ризику

Зазвичай ризик, пов'язаний з деяким ІР, визначають так [1, С. 385]:

$$R = PC, \tag{1}$$

де R — ризик; P — ймовірність реалізації загрози на даний ресурс; C — вартість максимальних збитків власника ресурсу від успішної реалізації атаки на цей ресурс.

За останній показник, у більшості випадків, використовують вартість самого ресурсу. Якщо ж втрата даного *IP* приводить до зупинки виробничого процесу, то в якості вартості максимальних збитків використовують збитки, спричинені цим простоєм, та вартість самого ресурсу. В конкретних випадках можуть різнитися підходи до визначення типів цієї вартості, але всіх їх можна формалізувати у такому вигляді:

$$C = \sum_{i=1}^{q} C_i, \tag{2}$$

де C_i — вартість i-тих збитків власника від успішної реалізації атаки на *IP*; q — кількість видів збитків власника.

Даний підхід до розрахунку ризиків може бути ефективними, якщо мова йде про фізичні ресурси. У випадку, коли необхідно оцінити саме інформаційні ресурси, можуть виникнути проблеми в його застосуванні, пов'язані зі специфікою безпосередньо інформації.

В літературі, пов'язаній з теорією захисту інформації [2], виділяють такі основні її характеристики:

— цілісність — характеристика безпеки інформації, що відображає її здатність протистояти несанкціонованій модифікації;

— доступність — характеристика безпеки інформації, яка відображає її властивість, що полягає у можливості використання відповідних ресурсів у заданий момент часу згідно пред'явлених повноважень;

— конфіденційність — характеристика безпеки інформації, що відображає її властивість нерозкритості та доступності без відповідних повноважень. Іншими словами конфіденційність — це «прихованість» інформації від осіб, які не мають права доступу до неї.

Таким чином, якщо порушується перша характеристика, то можна визначити вартість збитків власника даної інформації від такої атаки за формулою 2. У випадку, коли порушується доступність, то збитки також несе власник і їх також можна врахувати, але в зв'язку з тим, що дані збитки мають інший характер, ніж збитки, отримані від втрати цілісності інформації, для більш достовірних результатів їх варто формалізувати.

Часто ж в зловмисникам необхідно лише ознайомитися із засекреченою інформацією, наприклад, із виробничим ноу-хау, яке дозволяє його власнику виготовляти унікально кращу продукцію, ніж конкуренти. Якщо ж відбулася тільки втрата конфіденційності інформації, яка захищається, то виникає складність визначення розмірів збитків, які зазнав власник. Дана складність лише зростає у випадку, коли попит на цю унікальну продукцію на певному ринку вище за пропозицію, оскільки прямих збитків одразу власник не зазнає, а ринок забезпечуватиме реалізацію продукції в повному обсязі без зміни ціни на неї. Отже одразу, після успішної реалізації зловмисником атаки, власник інформації збитків не зазнав.

Але зловмисник, який ознайомився з даною інформацію зможе також виготовляти цю унікальну продукцію та реалізовувати її на ринку, підвищуючи власні виробничі можливості. Через певний проміжок часу, коли ринок насититься даною продукцією і попит на неї спаде, власник інформації отримає серйозного конкурента на ринку в особі зловмисника, який колись дізнався цей виробничий секрет. Саме тут власник інформації і буде зазнавати збитків.

Постановка задачі

Таким чином актуальною є задача розширення поняття ризику, яке б дозволило враховувати збитки власника від порушення конфіденційності інформації, представленої у вигляді *IP*, та інтегрувати їх в поняття загального ризику.

Розширення поняття ризику

У зв'язку з тим, що оцінювання інформаційної безпеки відбувається в умовах невизначеності, у цій статті будемо використовувати нечіткі оцінки ймовірності появи тієї чи іншої події. Розглянемо атаки на порушення кожної з характеристик інформації.

При атаках, що направлені на порушення цілісності, основною особливістю є те, що результати такої атаки можуть лишитись непоміченими протягом певного періоду часу. Отже збитки при порушенні цілісності інформаційного ресурсу власник може зазнати два різні типи збитків, які не варто додавати, оскільки ймовірність порушення цілісності шляхом її помітного пошкодження та ймовірність атаки типу заміни даних суттєво відрізняються. Відповідно пропонується розглядати дві складові ризику цілісності окремо:

— ризик втрати інформаційного ресурсу;

— ризик дезінформації.

Збитки, які зазнає власник від втрати інформаційного ресурсу пропонується визначати за допомогою вартості відновлення *IP*. Відновлення *IP* може бути здійснене за допомогою резервних копій, придбання аналогічного зразка та інших шляхів, які залежать від конкретного ресурсу, що розглядається.

$$\tilde{R}_i^l = \tilde{P}_i^l \cdot C_i^l, \tag{3}$$

де $\tilde{R}_i^l$ — ризик втрати *i*-го *IP*; $\tilde{P}_i^l$ — оцінка ймовірності втрати *i*-го *IP*; C_i^l — вартість відновлення *i*-го *IP*.

Оскільки оцінюючи, необхідно передбачити максимальні збитки, які може понести власник, то період, протягом якого реалізована атака дезінформації, будемо вважати рівним періоду між двома перевірками цілісності *IP*. Будемо вважати, що погодинно власник цього ресурсу втрачає однакову величину вартості, яка дорівнює максимальній з можливих, які залежать від фази виробничого процесу, сезону та інших умов для конкретного підприємства. Виходячи з цих міркувань, ризик дезінформації пропонується визначати з формули

$$\tilde{R}_i^d = \tilde{P}_i^d v_i^d t_i^d, \tag{4}$$

де $\tilde{R}_i^d$ — ризик дезінформації для *i*-го *IP*; $\tilde{P}_i^d$ – оцінка ймовірності дезінформації для *i*-го *IP*; v_i^d — питомі збитки при дезінформації, спрямованої на *i*-й IP;

t_i^d — період дезінформації для *i*-го *IP*.

Аналогічним чином формалізуємо ризик, пов'язаний з порушенням доступності, для *i*-го *IP*

$$\tilde{R}_i^a = \tilde{P}_i^a v_i^a t_i^a, \tag{5}$$

де $\tilde{R}_i^a$ — ризик порушення доступності для *i*-го *IP*; $\tilde{P}_i^a$ — оцінка ймовірності реалізації атаки зловмисником на *i*-й *IP*, спрямованої на порушення доступності; v_i^a — питомі збитки від реалізації атаки, спрямованої на порушення доступності *i*-го *IP*; t_i^a — тривалість відновлення доступу до *i*-го *IP*.

Перед визначенням вартості збитків від порушення конфіденційності інформаційного ресурсу варто провести попередній аналіз характеру інформації. Під характером інформації розуміється причина, яка стала в основі рішення про присвоєння грифу секретності. Зазвичай грифи секретності надають інформації, яка містить такі відомості:

— відомості, які надають перевагу підприємству над конкурентами;

— відомості, витік яких нанесе збитки підприємству.

До першого типу можна віднести різного роду виробничі секрети. До другого типу — інформація про забруднення навколишнього середовища, факти порушення законодавства, угод, негативні економічні показники підприємства тощо. Іноді трапляються випадки, коли обидві причини зумовили присвоєння грифу секретності, наприклад, факт отримання надприбутків від забруднення навколишнього середовища. Відповідно до даної класифікації пропонується і визначати збитки.

Розглянемо перший тип конфіденційної інформації. При її витоку конкуренти-злов-мисники зможуть також її використовувати для покращення власної продукції. Так на ринку з'явиться ще один виробник аналогічної продукції. Крім того, підприємство-зловмисник зможе виробляти дану продукцію в обсязі більшому або меншому за підприємство-власника інформації, що також необхідно врахувати при оцінюванні даного типу збитків. Будь-яка унікальна продукція з часом може бути витіснена іншою, ще кращою продукцією, таким чином є визначений проміжок часу t_{life}, протягом якого продукцію буде економічно доцільно реалізовувати.

Збитки, які зазнає підприємство від витоку конфіденційної інформації другого типу, можна спрогнозувати власникам підприємства, виходячи з особливостей конкретної інформації та очікуваних наслідків, з метою запобігання яких і було надано інформації гриф секретності.

$$\tilde{R}_i^c = \tilde{P}_i^c \left(C_i^c + rkp_i (1+\delta)^{t_{life} - t_{impl}} \right), \tag{6}$$

де $\tilde{R}_i^c$ — ризик порушення конфіденційності *i*-го *IP*; $\tilde{P}_i^c$ — оцінка ймовірності реалізації атаки зловмисником на *i*-ий *IP*, спрямованої на порушення конфіденційності; C_i^c — прогнозовані прямі збитки від витоку конфіденційної інформації; r — відносна частка ринку, яку займає власник для реалізації унікальної продукції; p_i — величина прибутку власника від унікальності продукції, забезпеченої за рахунок відомостей *i*-го інформаційного ресурсу; δ — відносний приріст обсягу виготовленої продукції; t_{life} — час, протягом якого буде реалізовуватись дана продукція; t_{impl} — час впровадження продукції у виробництво зловмисником; k — щорічний обсяг виготовлення продукції, який визначається з формули

$$k = \min\left(k_{owner}, k_{\text{intruder}}\right), \tag{7}$$

де k_{owner} — щорічний обсяг виготовлення продукції власника; k_{intruder} — прогнозований щорічний обсяг виготовлення продукції зловмисником.

Таким чином, ризик — це не тільки збитки власника, отримані від реалізації атаки, але і прибутки зловмисника, які він може «вкрасти» у власника інформації.

Інтегральний ризик для *N IP* визначатиметься за формулою:

$$\tilde{R} = \sum_{i=1}^{N} \left(\tilde{R}_i^l + \tilde{R}_i^d + \tilde{R}_i^a + \tilde{R}_i^c \right), \tag{8}$$

За допомогою (8) можна розрахувати значення інтегрального ризику для об'єкта оцінювання ін-

формаційної безпеки. Причому такий підхід дозволяє спростити експертам задачу оцінювання ймовірності реалізації атак, внаслідок конкретизації об'єктів цього оцінювання.

Висновки

В статті запропоновано новий підхід до визначення ризиків власника інформаційних ресурсів, виходячи з прибутків, отриманих зловмисником, внаслідок успішної реалізації атаки. Також запропоновано шлях використання цього розширеного поняття ризику в процесі оцінювання інформаційної безпеки, що дозволить отримати підвищення достовірності результатів внаслідок спрощення процесу експертного оцінювання ймовірностей успішної реалізації атак. В подальшому передбачається уточнення процесу оцінювання ймовірностей реалізації атак та впровадження запропонованого підходу в процес проектування систем захисту інформації.

СПИСОК ЛІТЕРАТУРИ

1. ІНТЕРНЕТ—ОСВІТА—НАУКА—2008: шоста міжнародна конференція ІОН. — 2008, 7 — 11 жовтня, 2008: збірник матеріалів конференції. Том 2 / Від. ред. В. В. Грабко. — Вінниця: УНІВЕРСУМ–Вінниця, 2008 — 298 с. — ISBN 978-966-641-268-6.

2. Корченко А. П. Построение систем защиты информации на нечетких множествах. Теория и практические решения / А. П. Корченко — К.: МК-пресс, 2006. — 316 с.

Рекомендована кафедрою обчислювальної техніки

Надійшла до редакції 8.09.08
Рекомендована до друку 20.10.08

Дудатьєв Андрій Веніамінович — доцент, ***Баришев Юрій Володимирович*** — аспірант.
Кафедра захисту інформації Вінницького національного технічного університету