УДК 0681.3.06
DOI: 10.32626/2308-5916.2019-19.56-62

Б. Я. Корнієнко*, д-р техн. наук,
Л. П. Галата**

*****Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського», м. Київ,
******Національний авіаційний університет, м. Київ

ОПТИМІЗАЦІЯ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ КОРПОРАТИВНОЇ МЕРЕЖІ

Розглядаються основні підходи до розробки алгоритму оптимізації системи захисту інформації корпоративної мережі. Запропоновано перехід від багатокритеріальної задачі оптимізації, до однокритеріальної. При сформульованому понятті захищеності системи оптимізаційна задача полягає в забезпеченні максимального рівня захищеності (як функції вартості інформації, що захищається і ймовірності злому) при обмеженнях вартості системи захисту і впливу на продуктивність системи.

Ключові слова: *оптимізація, критерій, система, захист інформації, загроза, рівень захищеності.*

Вступ. Проблема побудови оптимальної системи захисту інформації у даний час — найбільш актуальна для більшості промислових підприємств. Мета будь-якої системи захисту визначається можливістю сталого функціонування системи в цілому, визначення та нейтралізації загроз безпеки, запобігання витоку інформації по різних каналах. Одною з головних задач стає оптимізація проектування системи захисту. Сьогодні для промислових підприємств інформація являє собою основний комерційний товар. З розвитком інформаційних технологій і доступу до ринків є потреба в її захисті для забезпечення конфіденційності, цілісності і доступності. Для багатьох промислових підприємств впровадження систем захисту є необхідним етапом на шляху до успішного розвитку, кожне з них має свою критичну інформацію, втрата якої може звести до мінімуму конкурентоспроможність і шанси на успішний розвиток на ринку. Поширення такої інформації може призвести до втрати репутації і завдати матеріальної шкоди. Слід зазначити, що активне запровадження автоматизованих інформаційних систем обумовлює виникнення проблем, пов'язаних з інформаційною безпекою. Рішення даних проблем може бути реалізовано з застосуванням спеціальних автоматизованих програмно-технічних засобів [1–4].

Мета роботи — запропоновано алгоритм оптимізації системи захисту інформації корпоративної мережі.

У будь-якій галузі діяльності для вибору ефективної системи, ця система має характеризуватися деякими параметрами, на підставі яких і робиться вибір. Як такі параметри для системи захисту інформації можна виділити наступні: продуктивність, вартість, керованість, сумісність, захищеність тощо. Як зазначено вище, вибір оптимальної системи за такою множиною її характеристик є класичною задачею оптимізації і не завжди може мати ефективне рішення. Тим більше що багато параметрів є суперечливими: із зростанням рівня захищеності, наприклад, зростає вартість, складність настройки, водночас падає продуктивність.

Можна записати критерій якості за вартістю інформації, що захищається, за ймовірністю злому, за вартістю системи захисту інформації, за продуктивністю системи, за захищеністю. З урахуванням сказаного може бути зроблений висновок про багатокритеріальний характер завдання проектування системи захисту інформації. При цьому, крім забезпечуваного рівня захищеності, має враховуватися ще ряд найважливіших характеристик системи. Наприклад, обов'язково має враховуватися вплив системи захисту на завантаження обчислювального ресурсу, що захищається [5–8].

Кінцевою метою вирішення загальної задачі прийняття рішень є вибір з допустимої множини рішень X єдиного найкращого, тобто екстремального за обраними окремими критеріями рішень

$$x^{opt} = \arg \underset{x \in X}{extr} \left\{ k_i \left(x \right) \right\}, \; i = 1, n. \qquad (1)$$

Задача багатокритеріальної оптимізації (1) є некоректною, оскільки в загальному випадку не забезпечує визначення єдиного оптимального рішення з допустимої множини X. Ця некоректність може бути усунена шляхом регуляризації задачі, тобто введенням деякої додаткової інформації, математичних співвідношень або правил, що дозволяють забезпечити вибір єдиного рішення [1].

Одним із шляхів розв’язку багатокритеріальної задачі оптимізації полягає у формуванні зведеного критерію оптимальності, коли використовується згортка частинних критеріїв, чи використання нормативних показників, чи справедливий компроміс, чи оптимальність за Парето.

Інший підхід базується на виділенні головного критерію та перетворення всіх інших критеріїв у обмеження. Для цього проводиться аналіз конкретних особливостей багатокритеріальної задачі, з множини окремих критеріїв вибирається один — найважливіший, і він приймається як єдиний критерій оптимізації. Для кожного з інших окремих критеріїв призначається граничне значення, нижче якого він не може опускатися.

Тому в нашому алгоритмі буде проводитися оцінка ефективності системи за параметром захищеності, як основним показником, що характеризує рівень забезпечення захисту системи захисту інформації, а на інші характеристики вводяться обмеження. Будемо оцінюва-

ти захищеність системи (Z) кількісно залежно від вартості інформації, що захищається, ймовірності злому, вартості самої системи захисту, продуктивності системи:

$$Z = f\left(C_{інф}, p_{зл}, B_{сзі}, П\right),$$

де $C_{інф}$ — вартість інформації, що захищається; $p_{зл}$ — ймовірність злому; $B_{сзі}$ — вартість системи захисту інформації; $П$ — продуктивність системи.

З урахуванням введеного поняття захищеності системи оптимізаційна задача полягає у забезпеченні максимального рівня захищеності (як функції вартості інформації, що захищається і ймовірності злому) при обмеженнях вартості системи захисту і впливу на продуктивність системи:

$$Z^{opt} = \max Z(C_{інф}, p_{зл}, B_{сзі}, П).$$

Таким чином, всі окремі критерії, крім одного перетворюються на обмеження, додатково звужують область допустимих рішень X. Тоді вихідна багатокритеріальна задача (1) перетворюється в однокритеріальну вигляду

$$\begin{aligned} x^{opt} &= \arg \underset{x \in X}{extr}\, k^*(x), \\ k_i(x) &\geq (\leq) k_i^B(x), i = 1, n-1, \end{aligned} \qquad (2)$$

де $k^*(x)$ — оптимізаційний скалярний критерій; $k_i^B(x)$ — найгірші допустимі значення окремих критеріїв-обмежень; знак «>» використовується для критеріїв, які необхідно максимізувати, а знак «<» — мінімізувати.

Виведення головного (оптимізаційного) критерію і рівнів обмежень для $k_i^B(x)$ всіх інших критеріїв — суб'єктивна операція, здійснювана експертами. Слід зазначити, що можна розглянути декілька різних варіантів і порівняти результати.

Розглянемо захищеність системи з точки зору ризику. Зауважимо, що використання теорії ризиків для оцінки рівня захищеності на сьогоднішній день є підходом, який найбільш часто використовується на практиці. Ризик (R) — це потенційні втрати від загроз захищеності:

$$R(p) = C_{інф} \cdot p_{зл}.$$

За суттю, параметр ризику тут вводиться як мультиплікативна згортка двох основних параметрів захищеності.

З іншого боку, можна розглядати ризик як втрати в одиницю часу:

$$R(\lambda) = C_{інф} \cdot \lambda_{зл},$$

де $\lambda_{зл}$ — інтенсивність потоку зломів (під зломом будемо розуміти вдалу спробу реалізації загрози інформації).

Ці дві формули пов'язані наступним співвідношенням:

$$p_{зл} = \frac{\lambda_{зл}}{\Lambda},$$

де Λ — загальна інтенсивність потоку несанкціонованих спроб порушення основних властивостей інформації зловмисниками.

Як основний критерій захищеності будемо використовувати коефіцієнт захищеності (D), що показує відносне зменшення ризику в захищеній системі в порівнянні з незахищеною системою:

$$D = \left(1 - \frac{R_{зах}}{R_{нез}}\right) \cdot 100\%, \qquad (3)$$

де $R_{зах}$ — ризик в захищеній системі; $R_{нез}$ — ризик у незахищеній системі.

Для вирішення цієї задачі зведемо її до однокритеріальної за допомогою введення обмежень. В результаті отримаємо:

$$\begin{cases} D(C_{інф}, p_{зл}) \to \max; \\ B_{сзі} \le B_{зад}; \\ П_{сзі} \ge П_{зад}, \end{cases}$$

де $B_{зад}$ і $П_{зад}$ — задані обмеження на вартість системи захисту і продуктивність системи.

Цільова функція обрана виходячи з того, що саме вона відображає основне функціональне призначення системи захисту — забезпечення безпеки інформації [9].

Тепер виразимо коефіцієнт захищеності через параметри загроз. У загальному випадку в системі присутня безліч видів загроз. У цих умовах задамо такі величини: W — кількість видів загроз, що впливають на систему; $C_i (i = 1, w)$ — вартість втрати від злому і-го вигляду; $\lambda_i (i = 1, w)$ — інтенсивність потоку зломів і-го вигляду, відповідно; $Q_i (i = 1, w)$ — ймовірність появи загроз і-го вигляду в загальному потоці спроб реалізації загроз, причому $Q_i = \frac{\lambda_i}{\Lambda}$; $p_i (i = 1, w)$ — ймовірність відбиття загроз і-го вигляду системою захисту. Відповідно, для коефіцієнта втрат від зломів системи захисту маємо:

$$R(p) = \sum R_i(p) = \sum C_i \cdot p_{зл\_i};$$

де $R_i(p)$ — коефіцієнт втрат від злому і-го типу; показує, які в середньому втрати припадають на один злом і-го типу. Для незахищеною системи $P_{загр\_i} = Q_i$, для захищеної системи

$$P_{загр\_i} = Q_i \cdot (1 - p_i).$$

Відповідно, для коефіцієнта втрат від зломів системи захисту в одиницю часу маємо:

$$R(\lambda) = \sum_1^w R_i(\lambda) = \sum_1^w C_i \cdot \lambda_{загр\_i},$$

де $R_i(\lambda)$ — коефіцієнт втрат від зломів і-го типу в одиницю часу.

Для незахищеною системи $\lambda_{загр\_i} = \lambda_i$, для захищеної системи $\lambda_{загр\_i} = \lambda_i \cdot (1 - p_i)$. Відповідно, з (3) маємо:

$$D = 1 - \frac{\sum_1^w C_i \cdot Q_i \cdot (1 - p_i)}{\sum_1^w C_i \cdot Q_i} = 1 - \frac{\sum_1^w C_i \cdot \lambda_i \cdot (1 - p_i)}{\sum_1^w C_i \cdot \lambda_i}. \qquad (4)$$

Розглянуту інформаційну систему можна інтерпретувати як систему масового обслуговування, в яку надходять загрози (заявки). Спочатку розглянемо ситуацію, коли на вхід системи надходить загроза одного типу, припускаючи при цьому, що ця загроза не може бути реалізована або наступити кілька разів в один і той же момент часу. Якщо виконані зазначені припущення, то система може перебувати в трьох різних станах:

1) загроза не надходила, а значить, не була реалізована;
2) загроза надходила, але не була реалізована;
3) загроза надходила і була реалізована.

Елементи матриці інтенсивностей переходів можуть бути знайдені за допомогою імітаційної моделі. Для визначення ймовірностей $p_0(t),\ p_1(t),\ p_2(t)$ маємо систему диференціальних рівнянь

$$\begin{cases} \dfrac{dp_0(t)}{dt} = p_0(t) \cdot \lambda_{11} + p_1(t) \cdot \lambda_{21} + p_2(t) \cdot \lambda_{31}, \\ \dfrac{dp_1(t)}{dt} = p_0(t) \cdot \lambda_{12} + p_1(t) \cdot \lambda_{22} + p_2(t) \cdot \lambda_{32}, \\ \dfrac{dp_2(t)}{dt} = p_1(t) \cdot \lambda_{23} + p_2(t) \cdot \lambda_{33} \end{cases} \qquad (5)$$

з початковими умовами

$$p_0(0) = 1;\ p_1(0) = 0;\ p_2(0) = 0.$$

Для оптимізації використовуються кінцеві усталені значення p_i.

Оцінка захищеності з урахуванням наведених вище розрахункових формул і вибір оптимального варіанту системи захисту (необхідного набору механізмів захисту) здійснюється наступним чином.

1. Розрахунок параметрів C_i, λ_i, p_i для оцінки захищеності за вихідними даними.
2. Розрахунок критеріїв захищеності D, $B_{СЗІ}$, $П_{СЗІ}$ ($dП_{СЗІ}$) для кожного варіанту системи захисту (набору механізмів захисту).
3. Вибір системи захисту (набору механізмів захисту при розробці системи) з максимальним коефіцієнтом захищеності D, що задовольняє обмеженням по вартості $B_{СЗІ}$ і продуктивності $П_{СЗІ}$.

Висновки. Запропоновано алгоритм оптимізації системи захисту інформації корпоративної мережі. Здійснено перехід від багатокритеріальної задачі оптимізації, до однокритеріальної. При сформульованому понятті захищеності системи оптимізаційна задача полягає у забезпеченні максимального рівня захищеності (як функції вартості інформації, що захищається і ймовірності злому) при обмеженнях вартості системи захисту і впливу на продуктивність системи.

Список використаних джерел:

1. Korniyenko B. Y., Galata L. P. Design and research of mathematical model for information security system in computer network. *Науковий журнал «Наукоємні технології».* 2017. № 2 (34). С. 114–118.
2. Корнієнко Б.Я. Дослідження моделі взаємодії відкритих систем з погляду інформаційної безпеки. *Наукоємні технології.* 2012. № 3 (15). С. 83–89. doi.org/10.18372/2310-5461.15.5120 (ukr).
3. Korniyenko B. Y., Yudin O., Novizkij E. Open systems interconnection model investigation from the viewpoint of information security. *The Advanced Science Journal*. 2013. Issue 8. P. 53–56.
4. Корниенко Б. Я. Информационная безопасность и технологии компьютерных сетей: монография. ISBN 978-3-330-02028-3, LAMBERT Academic Publishing, Saarbrucken, Deutschland. 2016. 102 с.
5. Korniyenko B., Galata L., Kozuberda O. Modeling of security and risk assessment in information and communication system. *Sciences of Europe*. 2016. Vol. 2. № 2 (2). P. 61–63.
6. Korniyenko B., Yudin A., Galata L. Risk estimation of information system. *Wschodnioeuropejskie Czasopismo Naukowe*. 2016. № 5. P. 35–40.
7. Корнієнко Б. Я., Юдін О. К., Снігур О. С. Безпека аутентифікації у web-ресурсах. *Науково-практичний журнал «Захист інформації».* 2012. № 1 (54). С. 20–25. doi.org/10.18372/2410-7840.14.2056 (ukr).
8. Корнієнко Б. Я., Максімов Ю. О., Марутовська Н. М. Прикладні програми управління інформаційними ризиками. *Науково-практичний журнал «Захист інформації»*. 2012. № 4 (57). С. 60–64. doi.org/10.18372/2410-7840.14.3493 (ukr).
9. Корниенко Б. Я. Кибернетическая безопасность — операционные системы и протоколы. ISBN 978-3-330-08397-4, LAMBERT Academic Publishing, Saarbrucken, Deutschland. 2017. 122 с.

OPTIMIZATION OF THE INFORMATION SYSTEM OF THE CORPORATE NETWORK

The main approaches to the algorithm of optimization of the information security system of the corporate network are considered. The transition from the multicriterion optimization problem to the one-criterion is proposed. With the formulation of the concept of system security optimization problem is to provide the maximum level of security (as a function of the value of information, protects and probability of breaking) with the limitations of the value of the system of protection and impact onproductivity of the system.

Key words: *optimization, criterion, system, information protection, threat, security level.*

Одержано 31.01.2019

УДК 681.3:519.72:003.26:004.056
DOI: 10.32626/2308-5916.2019-19.62-68

А. М. Кудін*, **, д-р техн. наук,
Л. В. Ковальчук*, д-р техн. наук,
Б. А. Коваленко***

*Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського», м. Київ,
**Національний банк України, м. Київ,
***ООО «GlobalLogic Ukraine», м. Київ

ТЕОРЕТИЧНІ ЗАСАДИ ТА ЗАСТОСУВАННЯ БЛОКЧЕЙН-ТЕХНОЛОГІЙ: ІМПЛЕМЕНТАЦІЯ НОВИХ ПРОТОКОЛІВ КОНСЕНСУСУ ТА КРАУДСОРСІНГ ОБЧИСЛЕНЬ

Наведено аналіз існуючих блокчейн-технологій, їх алгоритмів консенсусу та стійкості до відомих атак підміни блоку. Наведені основні ідеї та варіанти практичних реалізацій нового протоколу консенсусу «Proof-of-accuracy», розробленого авторами. Наведено проект блокчейн-системи, яка надає послуги обчислень в режимі краудсорсінгу.

Ключові слова: *блокчейн, протоколи консенсусу, атаки подміни блоку, краудсорсінг.*

Вступ. Сталою сучасною тенденцією розвитку IT-технологій є зростання частки децентралізованих систем зберігання та обробки даних, що визначає актуальність дослідження блокчейн-технології. Важливою складовою технології є протоколи узгодження. В роботі вирішено задачу вдосконалення протоколів узгодження в розподілених системах за рахунок застосування принципово нових схем залу-