УДК: 005.7:519.8

ВИЗНАЧЕННЯ ШЛЯХІВ ЩОДО ЗАХИСТУ ІНФОРМАЦІЇ НА ОСНОВІ МОДЕЛЮВАННЯ ПОТЕНЦІЙНОГО КОНФЛІКТУ З ВИКОРИСТАННЯМ ТЕОРІЇ ІГОР

Фукс Максимілліан Андрійович
студент V курсу факультету Інфокомунікацій
Харківський національний університет радіоелектроніки, Україна

Анотація. У статті висвітлюється можливість застосування математичного апарату теорії ігор, а саме пропозиція розгляду конфлікту між керівником відділу IT-безпеки та зловмисником за допомогою біматричних ігор як кращий варіант для визначення оптимальної стратегії захисту інформації.

Ключові слова: біматрична гра, зловмисник, система менеджменту інформаційної безпеки, стратегія, теорія ігор.

Прийняття системи менеджменту інформаційної безпеки (СМІБ) є стратегічним рішенням організації, на проектування та впровадження якої впливають як потреби, так і цілі, розмір, структура, вимоги для безпеки, наявні організаційні процеси у цій організації. СМІБ засновується на підході бізнес-ризику та направлена на створення, реалізацію, експлуатацію, моніторинг, аналіз, підтримку та підвищення ефективності інформаційної безпеки (ІБ). У межах СМІБ розглядають структуру системи, політики, дії щодо планування, обов'язки, практики, процедури, процеси та ресурси організації [1].

Загалом інформаційна безпека може трактуватися як стан захищеності інформаційної середи як від внутрішніх так і від зовнішніх загроз, які спроможні завдати шкоди інтересам особистості, компанії, держави, тощо. Таким чином, захист інформації направлений на забезпечення стану безпеки інформації, яка забезпечується за допомогою її захисту. Інформаційна безпека як механізм захисту забезпечує наступні елементи.

1) Конфіденційність – властивість інформації бути захищеною від несанкціонованого розкриття.

2) Цілісність – властивість інформації бути захищеною від несанкціонованого змінення. При цьому фізична цілісність забезпечує незмінність саме фізичного стану інформації, а логічна – правильність виконання процесів, повноту та її несуперечність.

3) Доступність – властивість інформації бути доступною за певний час авторизованому користувачеві.

Впроваджена СМІБ якраз і забезпечує збереження вищезазначених властивостей за допомогою розгортання процесу управління ризиками, а впроваджені механізми захисту інформації й направлені на підвищення та забезпечення необхідних рівнів моделі Confidentiality, Integrity and Availability (CIA).

СМІБ представляє певну схему, на основі якої є можливість обговорювати, планувати, визначати, відслідковувати проблеми безпеки компанії. Основою СМІБ може слугувати певний стандарт, який забезпечуватиме повноту та узгодженість. Звичайно, компанія сама може змінювати стандарт відповідно до власних потреб для створення найкращої відповідності СМІБ та можливих потреб з урахуванням специфіки бізнесу. Або взяти за основу декілька найпопулярніших і розробити власні внутрішні нормативні документи, політики, процедури, стандарти, інструкції.

Політика – документ, що містить визначені цілі, завдання та шляхи їх досягнення. Важливим є те, що під політикою інформаційної безпеки найчастіше мається на увазі

високорівневий документ, направлений на забезпечення якісного керування ІБ згідно з наявними вимогами бізнеса, клієнтів чи законодавчої бази. Задокументована політика у обов'язковому порядку затверджується керівництвом та доноситься усім співробітникам організації та можливим зовнішнім сторонам, якщо такі є. Окрім розроблених внутрішніх нормативних документів організації, СМІБ може включати в себе умови угод та договорів з третіми сторонами.

Існує велика кількість підходів, на основі яких компанія може розгорнути власну СМІБ, наприклад, стандарти International Organization for Standardization (ISO) та Federal Information Processing Standard (FISP), публікації The National Institute of Standards and Technology (NIST), серія стандартів 8500.x міністерства оборони США, Security Technical Implementation Guide (STIG), документи The European Union Agency for Cybersecurity (ENISA), нормативно-правові акти банку, тощо.

Яскравим прикладом може слугувати лист [2] департаменту інформатизації банкам України, у якому зазначалися питання та можливості забезпечення безпеки інформаційних ресурсів банківської системі України з додаванням вимог із захисту інформації, зумовлених конкретними потребами сфери банківської діяльності і правовими вимогами, які вже висунуто в нормативних документах Національного банку України (НБУ). Прикладом є Постанова №95 від 28.09.2017 Правління НБУ «Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України», мета якої є підвищення рівня захисту інформаційних систем банків. Постанова НБУ №95 засновується на міжнародному стандарті ISO/IEC 27001:2013 та містить вимоги щодо інформаційної безпеки банку [3].

Іншим прикладом може слугувати методика IT-Grundschutz [4], що описує створення СМІБ і яка розроблена німецьким федеральним відомством з інформаційної безпеки BSI. Насправді стандарт ISO/IEC 27001:2013 містить дуже мало, а то й взагалі не має інструкції щодо застосування та впровадження зазначених у ньому вимог – усе описано доволі абстрактно. Можна зробити припущення, що саме через це німецька команда експертів створила методологію IT-Grundschutz, що містить близько 1500 ясно викладених інструкцій як створити систему керування ІБ. Вимоги зібрані у модулі, що застосовуються до процесів, обладнання, приміщень, додатків, тощо. Вони визначають як ведення необхідної документації, так і застосування засобів захисту інформації й інше.

Ціле сімейство ISO/IEC 27000 включає в себе міжнародні стандарти, що визначають вимоги до СМІБ, управління ризиками, метрикою, вимірами та керівництвом щодо її впровадження. Стандарт ISO/IEC 27003:2017 визначає методологію побудови СМІБ з урахуванням вимог, що зазначені у ISO/IEC 27001:2013. Розгортання СМІБ на основі зазначених у цьому стандарті вимог спирається на модель планування-дія-перевірка-покращення PDCA [5].

Процес визначення прийнятного ризику та вибір оптимальних стратегій для використання CISO – нелегка задача, адже навіть у вищезазначених методологіях відображена лише необхідність розгортання та впровадження засобів захисту інформації, але не представлені рекомендації щодо того, як саме провести оптимізацію вибору, тобто немає ясності яким чином потрібно виконувати зазначені у стандартах вимоги. Зазвичай, на цьому етапі впровадження СМІБ CISO чи навіть ціла команда відповідальних покладаються лише на власний досвід та намагаються якимось недетермінованим чином обрати необхідні засоби захисту. Більш того, працювати вони вимушені при доволі обмеженому фінансуванні, а тому необхідно поєднувати виділені фінансові можливості, потрібні методи захисту і принцип розумної достатності для отримання у результаті ефективної та якісної СМІБ.

Проблемі визначення ефективності проведених інвестицій у кібербезпеку загалом присвячено доволі багато літератури, публікацій та певних методів. Наприклад,

метод аналізу ієрархій Томаса Сааті, теорія корисності чи навіть математичний апарат теорії ігор.

Теорія ігор розглядає взаємовідносини між учасниками, які мають різні чи навіть протилежні мотиви. Використання теоретико-ігрового підходу для моделювання процесу боротьби за реалізацію власних інтересів між CISO та зловмисником є резонним, адже вони обидва є раціональними, розумними і некооперативними, та мають на меті максимізацію власних функцій виграшу шляхом застосування певних стратегії. Тактика кожного з гравців детермінується ходами іншого. Зокрема, коли зловмисник прагне провести атаку на актив, йому обов'язково необхідно проаналізувати можливі контрзаходи впроваджені до системи CISO, і навпаки, для обрання необхідного засобу захисту системи CISO необхідно розглянути можливі атаки на таку систему.

Найчастіше для моделювання використовують найпростішу гру – з нульовою сумою. У антагоністичній грі некооперативні гравці мають повністю протилежні виграші [6]. Але у цьому випадку, насправді, робиться припущення, що втрати організації дорівнюють виграшу зловмисника, що і є грубим спрощенням усієї гри. Для уникнення подальших проблем та некоректних результатів наявна можливість застосування дещо іншого типу ігор, а саме біматричних ігор.

Отже, гра між CISO та зловмисником може бути охарактеризована наступим чином:

- за кількістю учасників: 2 гравці;
- за кількістю стратегій: гра є кінцевою;
- за взаєминами між гравцями: безкоаліційна;
- за властивостями функцій виграшу: гра з ненульовою сумою.

Конкретизація завдання та аналіз характеристик розгортаємої математичної моделі допомагає сконцентруватися на неантагоністичних іграх двох учасників з кінцевим числом стратегій, а саме на біматричних іграх. Ігри такого роду повністю протилежні іграм з нульовою сумою, де один з гравців перемагає за рахунок програшу іншого, а тому розгляд поставленого завдання саме у розрізі біматричних ігор надає можливість приділити увагу не тільки виграшу CISO, а й зловмисника, тим самим описавши функції виграшу для кожної конфліктуючої сторони окремими матрицями.

Можливість використання біматричних ігор у моделюванні взаємодії CISO та зловмисника не суперечить наявним публікаціям та методологіям і може використовуватися як альтернатива, що потребує більше вхідних даних, адже вона розглядає як інтереси CISO, так і зловмисника, а тим самим спроможна представити більш точний результат на основі більшої інформації з обох сторін.

Список джерел:

1. Дорофеев А. Менеджмент информационной безопасности: основные концепции / А. Дорофеев, А. Марков. // Вопросы кибербезопасности. – 2014. – С. 67–73.
2. Національний банк України. Лист 03.03.2011 №24-112/365 Банкам України [Електронний ресурс] / Національний банк України // Департамент інформатизації. – 2011. – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/ v0365500-11#Text.
3. Постанова № 95 Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України [Електронний ресурс] // Правління Національного банку України. – 2017. – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/v0095500-17#Text.
4. BSI-Standard 200-2. // IT-Grundschutz Methodology. – 2017. – №1. – С. 131.
5. Міжнародний стандарт ISO/IEC 27001. – 2013. – №2. – С. 1–34.
6. Колобашкина Л. В. Основы теории игр / Л. В. Колобашкина., 2011. – 199 с.