СТВОРЕННЯ СИСТЕМИ АНАЛІЗУ ІНФОРМАЦІЙНИХ ЗАГРОЗ ЗА НАЙКРАЩИМИ ПРАКТИКАМИ ТА СТАНДАРТАМИ

ЛИСЕНКО Сергій Олексійович - доктор юридичних наук, професор, ПрАТ «Вищий навчальний заклад «Міжрегіональна Академія управління персоналом», завідувач кафедри правознавства Сєвєродонецького інституту, м. Київ, Україна
ORCID ID: https://orcid.org/0000-0002-7050-5536.
DOI 10.32782/EP.2020.3.12

Статья представляет подход к анализу информационных угроз, основанный на нескольких лучших практиках и стандартах, включая обзор основных жизненных циклов анализа угроз и управления ими.

Преобразование данных о происшествии в информацию об угрозе, требует тщательного планирования и координации между несколькими командами, процессами и структурами. Эта статья раскрывает систему оценки информационных угроз, основанную на лучших практиках и стандартах. Она включает обзор основных жизненных циклов для управления и анализа угроз, а также подробный обзор того, какие показатели необходимы для переноса данных с одного жизненного цикла в другой.

Специалисты в области анализа угроз настаивают на насущной необходимости приоритетного распределения информационных активов, которые нуждаются в защите, поскольку существует слишком много объектов для защиты и значительно меньше мероприятий, которыми их можно защитить. Даже в очень больших финансовых организациях, имеют практически неограниченный бюджет для построения модели информационной безопасности, все равно приходится конкурировать с другими организациями за специалистов, а время, даже для них, всегда будет оставаться ограниченным ресурсом.

Учитывая это, становится понятно, что организациям выгодно использовать данные предварительной информации об угрозах, которые специалисты по информационной безопасности получают, проводя свою деятельность по предотвращению рисков. Аналогичным образом, процесс разведки угроз может быть лучше приспособлен для защиты организации, если специалисты используют заранее собранные данные. Такое сочетание использования данных об угрозах является основой представленной здесь системы анализа. Это выглядит как результат сочетания четырех непонятных систем, каждая из которых имеет свою цель, но для них существует достаточно общего, чтобы быть взаимовыгодными. Конечно, указанные в этой статье циклы механизма и практические шаги по внедрению системы анализа угроз должны быть закреплены административно-правовым путем в соответствующих документах организаций. Поэтому автор останавливается преимущественно на практической стороне вопроса, оставляя нормативный аспект последующим исследователям.

Ключевые слова: информация, угрозы, анализ угроз, система анализа угроз, цикл, циклическая система, правовое регулирование.

Актуальність теми дослідження

Аналіз загроз організації існує з давніх часів, але ще ніколи він не сягав такого системного, науково-обґрунтованого рівня як сьогодні. Така ситуація обумовлена кількома факторами. З одного боку, саме в час розвитку інформаційно-комп'ютерних технологій у працівників безпекової сфе-

ри з'явився достатньо потужний інструментарій, для системного аналізу наявних та потенційних загроз. З іншого ж – ніколи раніше люди не були настільки поінформовані, занурені у потоки даних, як тепер. Це призводить до того, що навіть потужні комплекси не завжди в змозі врахувати всі джерела загроз, без належного програмного та методологічного забезпечення.

Сучасний набір загроз дуже складний і динамічний. На організації часто впливають джерела загроз, які використовують широкий спектр інструментарію та дивовижну мінливість. Чергові заходи протидії загрозам, які могли дуже добре працювати на захист організації ще вчора, можуть уже не мати можливості запобігти тим самим зловмисникам наступного дня, у залежності від того, які нові слабкі сторони в організацій з`явились і які нові можливості та технології відкрили для себе зловмисники. Завдяки такому складному операційному середовищу, організації можуть бути готові відмовитись від спроб створити пріоритетний перелік речей, які потрібно захищати першочергово, і замість цього спробувати захищати все. Але, як відомо з історії військової думки, «хто захищає все, той не захищає нічого». Проблематика визначення пріоритетів у сфері протидії інформаційним загрозам наразі є вкрай гострою, що й обумовило актуальність цього дослідження.

Метою статті є розгляд циклічних механізмів аналізу загроз інформаційній безпеці.

Виклад основного змісту дослідження

Термін «аналіз даних про загрозу» може мати різне значення в різному контексті, але за будь-яких обставин його метою виступає розробка загальної системи збору цих даних з питань інформаційних загроз. Визначення, надане Тілманом, є доволі корисним для розуміння та застосування: «Система аналізу загроз – це організаційна здатність цілісно мислити про загрозу та невизначеність, розмовляти загальноприйнятою мовою загрози, ефективно використовувати перспективні концепції та інструменти загрози для прийняття кращих рішень для знешкодження загроз, розуміти виграш від своїх можливостей і створення стійких пріоритетів» [11].

Початковий життєвий цикл для організації, під час виникнення загроз, складається з наступних етапів: 1) підготовка; 2) виявлення та аналіз; 3) стримування, викорінення та відновлення; 4) післяаварійна діяльність. По закінченні цього чотириступеневого циклу результати мають повернутися на початок життєвого циклу та в інші життєві цикли, як це буде пояснено далі.

Реагування на аварії – це один із тих процесів, який відчутно виграє від належного попереднього планування, і перша фаза цього життєвого циклу це добре ілюструє. Організація повинна заздалегідь розподіляти ресурси, необхідні для відповідної реакції. Це може включати придбання корисних інформаційних технологій, що допоможуть захиститись від загроз, налаштування обчислювальних активів для забезпечення належних доказів у випадку нападу та встановлення правильних тригерів для попередження персоналу, коли напад триває. Нарешті, цей етап процесу включає залучення та навчання відповідного персоналу, для визначення організаційних ресурсів, можливостей та процесів, необхідних у випадку підтвердженого інформаційного нападу [2].

Другий етап – виявлення та аналізу, визначає необхідність організації мати можливість знати, коли в її середовищі розгортається напад. Це означає, відповідно до першого етапу, наявність спеціалістів та технологій, які зможуть фільтрувати та аналізувати інформацію, задля визначення пріоритетності дій на наступному етапі. Такий підхід обумовлено відносно високим ступенем помилкових дій,

які можуть виникнути в результаті прийнятих, стосовно моніторингу, рішень. Як результат, зрілі організації встановлюють систему пріоритетів для того, щоб знати, коли саме найбільш доречно швидко реагувати на певні негативні показники. Таке визначення пріоритетів є чудовою можливістю для інтеграції з системою розвідки загроз. Знання правильних пріоритетів, що базуються на оцінці загрози, на цій ранній фазі реагування на надзвичайні ситуації, є критично важливим для належного управління загрозами.

Третя фаза цього циклу призводить до зупинення нападу. Це означає обмеження розповсюдження нападу (карантин загрози), усунення доступу зловмисника, корисного навантаження або шкідливого програмного забезпечення, а також припинення будь-якого розповсюдження даних, яке триває або незабаром настане. Це також означає спробу налаштувати системи та відновити їх стан роботи на тому рівні, який був до нападу. На цьому етапі також необхідно активно проводити збір даних у цілому та доказів зокрема, оскільки іноді ці дані потрібно буде передавати правоохоронним органам або кадровим та юридичним відділам, для подальшого формування розпоряджень та прийняття рішень.

Заключна фаза життєвого циклу реагування на напад – діяльність після випадків, фактично не є окремою фазою, оскільки має бути інтегрованою з іншими фазами. У рамках цієї фази слід організувати продуманий збір даних та підготовку отриманої інформації для споживання. Це може включати поетапне дослідження того, що сталося, а також висновки аналітиків про те, що саме це означає для організації. Висновок також може включати прогноз, який може бути використаний іншими, щоб знати, де в організації шукати прогалини для появи подібних випадів у майбутньому, а також окреслити кроки, які допоможуть краще запобігти загрозам.

Такий підхід, по суті, перетворює напад, за рахунок його повноцінного вивчення, на дієву інформацію про запобігання загрозам. Рівень, до якого дійде організація, може передбачати усунення окремих технічних деталей, але аналітичний огляд завжди включатиме адміністративно-правовий розділ, який має узагальнити все, що сталося. Таким чином, подія перетворюється на історію, яка допомагає спеціалістам, які схвалюють рішення, зрозуміти, що саме сталося. Крім цього такий підхід додає довіри твердженням аналітиків стосовно того, що слід робити далі, щоб запобігти таким загрозам у майбутньому. Ця інформація може бути використана як вхідні дані до першого етапу, а також у рамках підготовки до наступного нападу. Цю внутрішньо створену інформацію про загрози можна використовувати разом із аналогічно розвідувальною інформацією про загрози із зовнішніх джерел, як важливий внесок у наступний життєвий цикл, для належної інтеграції в модель інформаційної безпеки.

Процес збору інформації про загрози є окремим життєвим циклом. Автор переконаний, що збір інтелектуальної інформації про загрози є процесом відразу двох систем, як це визначив лауреат Нобелівської премії Даніель Канеман у своїй книзі «Мислення швидке і повільне». Науковець докладно описав сучасні види прийняття рішень, які роблять люди, та об'єднав їх у дві головні категорії. Перші рішення швидко приймаються, служать для захисту від шкоди та задовольняють потреби нижчого рівня в «Ієрархії потреб» Маслоу. Другі ж рішення є обдуманими. Вони приходять як результат витрати часу на детальний розгляд вхідних та вихідних даних, а також правильного застосування системи для аналізу результатів [1]. Автор, у свою чергу, пропонує перетворити ці постулати у відповідні адміністративно-правові норми організацій.

Ключова складність полягає у правильному застосуванні кожної зі згаданих систем. Перший тип мислення настільки простий і швидкий, що ми часто застосовуємо його за замовчуванням, практично

інтуїтивно, і це допомагає врятуватися, коли виникає загроза. Очевидно, що перевагою такого типу є швидкість реакції. Однак, його недоліки не менш значущі.- У найкращому випадку воно може призвести до неправильного вибору, а в гіршому – війни, фанатизму та расизму. Безумовно, розвідка загроз повинна бути продуманим комплексом зусиль, розроблених для усунення упереджень та ретельної координації процесу збору інформації, її подальшого аналізу, для досягнення найбільш точного та правильного рішення.

Загальний цикл розвідки загроз організацій, запропонований Лізою Кризан в Об'єднаному коледжі військової розвідки (нині – Національний університет розвідки США), дає приклад періодичного життєвого циклу. Він розроблений з метою забезпечення фахівців постійними даними для запровадження процесу генерування запитань для аналізу та отримання відповідей на них [4]. Перший етап цього життєвого циклу полягає у формуванні повного розуміння того, на які питання повинна відповідати система аналізу загроз і чому. Крім того, такий підхід вимагає від аналітика оцінки, які саме дані потрібно збирати, щоб відповісти на вказані питання. Цей етап повинен здатися дуже знайомим для будь-якого дослідника, оскільки він повторює ті ж самі дії, що передують будь-якому аналітичному проєкту. Наскільки б тавтологічно це не звучало, але вкрай важливо визначити, зрозуміти, які саме дані необхідні для аналізу. Загальна система розвідки ризиків буде надавати інформацію не про дослідження в цілому, а лише про питання для дослідження. Тому, наприклад, дослідник розвідки загроз захоче краще зрозуміти типи атак, які використовують кіберзлочинці в її власній організації та інших подібних [10].

Другий етап – це просто збір даних, і лише іноді – ідентифікація джерел надходження таких даних. При цьому, перший і другий етапи можуть відбуватися паралельно. На цьому етапі, після того, як будуть зібрані необхідні дані, аналітик перегляне їх, обробить і перетворить у робочу інформацію. Іншими словами, відбудеться створення звітів, готових до сприйняття на всіх організаційних рівнях.

Подібно до життєвого циклу реагування на події, даний процес включає подання фактів, висновків та прогнозів з приводу того, що можна очікувати далі. Нарешті, така узагальнена інформація поширюється на різних рівнях організації, включаючи аналітиків загроз. Таким чином, зазначений життєвий цикл знаходиться між циклом реакції випадків та циклом аналізу ризику і, як такий, має доступ до кожного з них.

Основа для життєвого циклу аналізу ризиків, представлена нами, була взята зі звіту RAND (Research and Development – «Дослідження і розробка») американської некомерційної організації, яка виконує функції стратегічного дослідницького центру, що працює на замовлення уряду США, їх збройних сил і пов'язаних з ними організацій. Зазначений звіт було присвячено проблемі перетворення аналізу ризику в аналітичну систему. Для адаптації до структури інформаційних загроз було модифіковано кілька частин циклу. Крім того, проведені моделювання загроз були взяті з четвертої системи для кількісної оцінки інформаційних ризиків. Такий підхід надає нам можливість управляти загрозами окремо, але при цьому надавати кожному суб`єкту робочу інформацію, необхідну йому для безперебійної роботи [8].

Загалом, аналіз загрози є менш чутливим до тактики та техніки агресора, ніж розвідка загроз. Причиною цього є те, що, хоча можуть існувати різні способи, якими джерело загроз може знайти шлях до обчислювального середовища організації, наслідковий ризик, як правило, є більш фіксованим. Як приклад можна навести ситуацію у сфері роздрібної торгівлі, де здатність зловмисника використовувати слабкі місця в точках роздрібного продажу може з часом змінюватися. Однак результат, скоріше за все, буде однаковим,

наприклад – подальша компрометація та розповсюдження даних кредитних карток, з метою вчинення шахрайства.

Є кілька змінних показників, які необхідні для правильного моделювання загрози. Загалом, аналіз загроз корисно сприймати як абстракцію тих деталей розвідки загроз, які є дуже корисними для повсякденного блокування та вирішення питань, необхідних для захисту сучасних мереж.

Використовуючи інформацію, що була зібрана у певний час і у певному місці, можна накопичити дані, необхідні для моделювання двох змінних показників, що називаються «Частота подій загроз» (TEF) та «Можливість загроз» (TCap). Ці дві змінні показників дають нам модель, яка демонструє, наскільки часто атакують агресори або (якщо мова йде про внутрішній персонал) як часто вони роблять помилки і коли вони це роблять. Додатково можна спрогнозувати, яку шкоду вони можуть принести. Супроводжуватись збір даних повинен через профіль спільноти загроз, який надає організації тему для спілкування про спільноту загроз [12].

Дані з профілю загрози розподіляються між цими двома змінними (TEF і TCap), які використовуються як похідні дані до моделі аналізу загроз із міжнародним позначенням «FAIR» (factor analysis of information risk). Модель FAIR використовується у середовищі професіоналів безпекової аналітики та призначена для кількісної оцінки ризику настання інформаційних загроз та перспектив завдання збитків, з використанням економічних показників. Одночасно, якісний профіль загрози буде перетворений у показник частоти спроб втрат з плином часу (TEF) та виміру того, на що здатні джерела загрози (TCap). Хоча частота є природною кількісною величиною, можливості в моделі FAIR виражаються через рівень джерела загрози. По суті, зловмисники, які можуть використати найбільше сил у своїх атаках з точки зору часу, навичок та ресурсів, мають найважливіше значення TCap. Ці значення також слід зберігати разом із профілем загроз, щоб організації могли чітко усвідомлювати, які саме джерела загроз найбільш важливі для них [3].

Слід зазначити, що опис не є необхідною передумовою для побудови профілів загроз та їх подальшого аналізу. Дійсно, позитивна атрибуція неймовірно складна та відносно непотрібна для цілей процесу розвідки загроз. Замість того, щоб чітко покладатися на аналіз, який стверджує, що атака певного типу вплинула на інформаційні можливості (наприклад – окремої країни), FAIR лише запитує, чи може атака такого типу бути частиною ширшої, абстрагованої групи (у цьому випадку – нападників на певну організацію, або навіть державу). Деякі користувачі FAIR можуть обрати модель можливостей загрози для конкретної країни, але це не становить інтересу для аналізу ризиків у наших умовах [9]. Принципи FAIR також беруть інформацію про стан контролю та економічний вплив на організацію, щоб забезпечити точний аналіз загроз. Однак, повна обробка моделі FAIR виходить за рамки предмету нашого дослідження, тому ми не будемо на цьому зосереджуватись [6].

Після того, як проведено декілька аналізів актуальної загрози, організація отримає пріоритетний список основних потенційних негативних сценаріїв. Важливо зазначити, що FAIR фокусується саме на сценаріях, а це означає, що існують повні дані про збитки, включаючи сукупність загроз, слабкі сторони контролю та тип економічного впливу, що виникне у майбутньому. Ці сценарії настання найвищих збитків можуть бути використані разом із деякими прогнозованими планами атак, яким можуть допомогти результати з життєвого циклу розвідки загроз [7].

Кожен із попередніх життєвих циклів має свої сильні сторони та корисність у різних частинах загальної моделі інформаційної безпеки. Однак, лише поєднуючи їх разом, ми можемо побачити, що саме зріла система аналізу інформаційних загроз здатна зробити для організації. Зро-

зумілим стає механізм взаємодії цих життєвих циклів, а також – де саме вхідні та вихідні дані можуть бути взаємовигідними кожному учаснику подій та як оптимізувати їх використання.

Висновки і перспективи подальших досліджень

На практиці часто має місце відстань між функцією управління ризиками та операціями в моделі інформаційної безпеки, орієнтованої на протидію загрозам. При цьому, необхідність у співпраці цих сфер діяльності, обумовлена потребою кращого зрозуміння ролі одне одного та вирішення щоденних життєвих ситуацій. Команда управління загрозами потребує бізнес-пріоритети, які може запропонувати команда аналітиків. Проте команда аналітиків повинна краще розуміти загрози, для оцінки палітри ризиків та пріоритетів бізнесу. Адміністративно-правове закріплення системи розвідки інформаційних загроз, як плану їх співпраці, дає чіткі права та обов'язки звітування для кожної команди. Це може змусити співпрацювати там, де взаємодії взагалі може не бути, і створити професійні зобов'язання, які сприятимуть кращій роботі в команді та призведуть до вищої якості продуктів розвідки і аналізу загроз.

Багато організацій працюють над проблематикою покращення своєї звітності, стосовно інформаційної безпеки, перед вищим керівництвом (правліннями, радами директорів, акціонерів тощо). Для цих організацій ключовим питанням є пошук правильного способу інформування про безліч методів реалізації негативних сценаріїв, а також наглядного відображення прогнозів потенційних інформаційних збитків. Адміністративно-правова координація обміну даними між групами операцій з інформаційної безпеки та групами з аналізу загроз може не тільки допомогти забезпечити більш уніфікований підхід до повсякденної роботи цих команд, але і сприятиме єдності у наскрізних історіях інформаційних загроз, про які слід говорити окремо. Усе це обумовлює нагальність подальших досліджень адміністративно-правового механізму протидії загрозам інформаційній безпеці організацій у контексті окресленої автором моделі.

Література

1. Канеман Даніель, Мислення швидке та повільне. К. *Наш формат*, 2017. 387с.

2. Лисенко С.О. Особливий погляд на інформаційну безпеку. К.- Людмила, 2020. 375 с.

3. Freund J., Jones J. (2014). Measuring and Managing Information Risk: A FAIR Approach. Portsmouth, NH: *Butterworth-Heinemann*.

4. Krizan L. (1999). Intelligence Essentials for Everyone. Joint Military Intelligence College. URL: https://apps.dtic.mil/dtic/tr/fulltext/u2/a476726.pdf.

5. NIST SP 800-61 Rev. 2, Computer Security Incident Handling Guide, URL: https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final.

6. OpenGroup FAIR Risk Taxonomy Standard. URL: https://publications.opengroup.org/c13k.

7. OpenGroup FAIR Risk Analysis Standard. URL: https://publications.opengroup.org/c13g.

8. RAND's 2007 publication, Using Risk Analysis to Inform Intelligence Analysis.

9. The OpenGroup's cyber risk quantification (CRQ) standards, (Open FAIR or just FAIR). URL: https://www.opengroup.org/forum/security-forum-0/openFAIRandquantitativerisk

10. The threat intelligence cycle, adapted from Krizan's 1999 book, Intelligence Essentials for Everyone.

11. Tilman L. (2013). Risk Intelligence: A Bedrock of Dynamism and Lasting Value Creation. URL: https://www.europeanfinancialreview.com/risk-intelligence-a-bedrock-of-dynamism-and-lasting-value-creation/.

12. Willis, H. (2007). Using Risk Analysis to Inform Intelligence Analysis. RAND. URL: https://www.rand.org/dam/rand/pubs/working_papers/2007/RAND_WR464.pdf.

АНОТАЦІЯ

Стаття представляє підхід до аналізу інформаційних загроз, заснований на кількох найкращих практиках та стандартах, що включає огляд основних життєвих циклів аналізу загроз та управління ними.

Перетворення даних про подію в інформацію про загрозу, вимагає ретельного планування та координації між кількома командами, процесами та структурами. Ця стаття розкриває систему оцінки інформаційних загроз, засновану на найкращих практиках та стандартах. Вона включає огляд основних життєвих циклів для управління та аналізу загроз, а також детальний огляд того, які показники необхідні для перенесення даних з одного життєвого циклу в інший.

Спеціалісти у сфері аналізу загроз стверджують, що нагальною є потреба пріоритетного розподілу інформаційних активів, які потребують захисту, оскільки існує надто багато об`єктів для захисту та значно менше заходів, якими їх можна захистити. Навіть у дуже потужних фінансових організаціях, які мають практично необмежений бюджет для побудови моделі інформаційної безпеки, все одно доводиться конкурувати з іншими організаціями за спеціалістів, а час, навіть для них, завжди залишатиметься обмеженим ресурсом.

З огляду на це зрозуміло, що організаціям вигідно використовувати дані попередньої інформації про загрози, які спеціалісти з інформаційної безпеки отримують, проводячи свою діяльність щодо запобігання ризиків. Аналогічним чином, процес розвідки загроз може бути краще пристосовано для захисту організації, якщо спеціалісти використовують заздалегідь зібрані дані. Таке поєднане використання даних про загрози є основою представленої тут системи аналізу. Це виглядає як результат поєднання чотирьох незрозумілих систем, кожна з яких має свою мету, але для них існує достатньо спільного, щоб бути взаємовигідними. Звичайно, що окреслені в цій статті цикли механізму та практичні кроки по запровадженню системи аналізу загроз повинні бути закріплені адміністративно-правовим шляхом у відповідних документах організацій. Тому автор зупиняється здебільшого на практичній стороні питання, лишаючи нормативний аспект подальшим дослідникам.

Ключові слова: інформація, загрози, аналіз загроз, система аналізу загроз, цикл, циклічна система, правове регулювання.

SUMMARY

In the article presents an approach to information threat analysis based on several best practices and standards, which includes an overview of the main life cycles of threat analysis and management.

Transforming event data into threat information requires careful planning and coordination between multiple teams, processes, and structures. This article discloses an information threat assessment system based on best practices and standards. It includes an overview of the main life cycles for threat management and analysis, as well as a detailed overview of what indicators are needed to transfer data from one life cycle to another.

Experts in the field of threat analysis argue that there is an urgent need to prioritize the distribution of information assets that need protection, because there are too many objects for protection and far fewer measures to protect them. Even in very large financial organizations, which have a virtually unlimited budget to build a model of information security, still have to compete with other organizations for professionals, and time, even for them, will always be a limited resource.

Given this, it is clear that organizations benefit from using prior information about the threats that information security professionals receive in carrying out their risk prevention activities. Similarly, the threat intelligence process may be better adapted to protect the organization if professionals use pre-collected data. This combined use of threat data is the basis of the analysis system presented here. This looks like a combination of four obscure systems, each with its own purpose, but for them there is enough in common to be mutually beneficial. Of course, the cycles of the mechanism outlined in this article and the practical steps to implement a threat analysis system should be enshrined administratively in the relevant documents of organizations. Therefore, the author dwells mostly on the practical side of the issue, leaving the normative aspect to future researchers.

Key words: information, threats, threat analysis, threat analysis system, cycle, cyclic system, legal regulation.