Розділ 19. Управління інформаційною та/або кібербезпекою

19.1. Управління кіберінцидентами: Поняття кіберінцидента/ кібератаки. Розслідування кіберінцидентів/кібератак.

19.2. Управління ризиками в інформаційній та/або кібербезпеці: Загальна концепція управління ризиками ІБ. ISO/IEC 27005:2018, IEC 31010:2019, NIST SP 800-39, NIST SP 800-37, NIST SP 800-30, NIST SP 800-137 (Ризики інформаційної безпеки. Аналіз та оцінка ризику. Прийняття ризику. Зменшення ризику. Страхування (перекладання) ризику). Системи класу Incident Response Platform

19.1. Управління кіберінцидентами: Поняття кіберінцидента/кібератаки. Розслідування кіберінцидентів/кібератак

1.1 Поняття кіберінцидента/кібератаки

Інцидент кібербезпеки, (скорочено **кіберінцидент**) – подія або ряд несприятливих подій ненавмисного характеру (природного, технічного, технологічного, помилкового, у тому числі внаслідок дії людського фактора) та/або таких, що мають ознаки можливої (потенційної) кібератаки, які становлять загрозу безпеці систем електронних комунікацій, систем управління технологічними процесами, створюють імовірність порушення штатного режиму функціонування таких систем (у тому числі зриву та/або блокування роботи системи, та/або несанкціонованого управління її ресурсами), ставлять під загрозу безпеку (захищеність) електронних інформаційних ресурсів.

Хакерська атака (кібератака) – спроба реалізації загрози. Тобто, це дії кібер-зловмисників (хакерів) або шкідливих програм, які спрямовані на захоплення інформаційних даних віддаленого комп'ютера, отримання повного контролю над ресурсами комп'ютера або на виведення системи з ладу.

Під **атакою** (англ. *attack*, англ. *intrusion*) **на інформаційну систему** розуміють дії (процеси) або послідовність зв'язаних між собою дій порушника, які приводять до реалізації загроз інформаційним ресурсам шляхом використання уразливостей цієї інформаційної системи.

Типи атак на інформаційні системи:

- Віддалене проникнення (remote penetration).
- Локальне проникнення (local penetration).
- Атака на відмову в обслуговуванні (denial of service).
- Мережні сканери (network scanners).
- Сканери уразливостей (vulnerability scanners).
- Зламувачі паролів (password crackers).
- Аналізатори протоколів (sniffers).
- Спам e-mail (Mailbombing).
- Перехоплення каналу зв'язку (Man-in-the-Middle).

Атака на відмову в обслуговуванні

DoS (від англ. *Denial of Service* – Відмова в обслуговуванні) – атака, що має своєю метою змусити сервер не відповідати на запити. Такий вид атаки не передбачає отримання деякої секретної інформації, але іноді буває підмогою в ініціалізації інших атак. Наприклад, деякі програми через помилки в своєму коді можуть викликати виняткові ситуації, і при відключенні сервісів здатні виконувати код, наданий зловмисником або атаки лавинного типу, коли сервер не може обробити величезну кількість вхідних пакетів.

DDoS (від англ. *Distributed Denial of Service* – Розподілена DoS) – підтип DoS-атаки, що має ту ж мету що і DoS, але що проводяться не з одного комп'ютера, а з декількох комп'ютерів в мережі. У даних типах атак використовується або виникнення помилок, що призводять до відмови сервісу, або спрацьовування захисту, що приводить до блокування роботи сервісу, а в результаті також до відмови в обслуговуванні. DDoS використовується там, де звичайний DoS неефективний. Для цього кілька комп'ютерів об'єднуються, і кожен виробляє DoS-атаку на систему жертви. Разом це називається DDoS-атака.

Будь-яка атака являє собою не що інше, як спробу використовувати недосконаліть системи безпеки жертви або для отримання інформації, або для нанесення шкоди системі, тому причиною будь-якої вдалої атаки є професіоналізм крекерів і цінність інформації, а також недостатня компетенція адміністратора системи безпеки зокрема, недосконаліть програмного забезпечення та недостатня увага до питань безпеки в компанії в цілому.

Аналізатори протоколів *(sniffers)*

Також досить поширений вид атаки, заснований на роботі мережевої карти в режимі promiscuous mode, а також monitor mode для мереж Wi-Fi. В такому режимі всі пакети, отримані мережевою картою, пересилаються на обробку спеціальному додатку, званому сніффером. В результаті зловмисник може отримати велику кількість службової інформації: хто, звідки і куди передавав пакети, через які адреси ці пакети проходили. Найбільшою небезпекою такої атаки є отримання самої інформації, наприклад логінів і паролів співробітників, які можна використовувати для незаконного проникнення в систему під виглядом звичайного співробітника компанії.

Mailbombing

Вважається найстарішим методом атак, хоча суть його проста і примітивна: велика кількість поштових повідомлень роблять неможливими роботу з поштовими скриньками, а іноді і з цілими поштовими серверами. Для цієї цілі було розроблено безліч програм, і навіть недосвідчений користувач може зробити атаку, вказавши всього лише e-mail жертви, текст повідомлення, і кількість необхідних повідомлень. Такі програми дозволяють ховати реальний IP-адрес відправника, використовуючи для розсилки анонімний поштовий сервер. Цій атаці складно запобігти, так як навіть поштові фільтри провайдерів не можуть визначити реального відправника спаму. Провайдер може обмежити кількість листів від одного відправника, але адреса відправника і тема часто генеруються випадковим чином.

Man-in-the-Middle

Вид атаки, коли зловмисник перехоплює канал зв'язку між двома системами, і отримує доступ до всієї інформації, що передається. При отриманні доступу на такому рівні зловмисник може модифікувати інформацію потрібним йому чином, щоб досягти своєї цілі. Мета такої атаки – незаконне отримання, крадіжка або фальсифікування переданої інформації, або ж отримання доступу до ресурсів мережі. Такі атаки вкрай складно відстежити, оскільки зазвичай зловмисник знаходиться всередині організації.

Урядові політики

Уряди різних країн мають різні політики реакції на кібератаки проти інформаційних систем країни.

Україна

Законодавство України визначає: **Кібератака** – спрямовані (навмисні) дії в кіберпросторі, які здійснюються за допомогою засобів електронних комунікацій (включаючи інформаційно-комунікаційні технології, програмні, програмно-апаратні засоби, інші технічні та технологічні засоби і обладнання) та спрямовані на досягнення однієї або сукупності таких цілей:

–порушення конфіденційності;

–цілісності;

–доступності електронних інформаційних ресурсів, що обробляються (передаються, зберігаються) в комунікаційних та/або технологічних системах;

–отримання несанкціонованого доступу до таких ресурсів;

–порушення безпеки, сталого, надійного та штатного режиму функціонування комунікаційних та/або технологічних систем;

–використання комунікаційної системи, її ресурсів та засобів електронних комунікацій для здійснення кібератак на інші об'єкти кіберзахисту.

США

26.07.2016 Президент Сполучених Штатів Америки Барак Обама підписав наказ (директиву) PPD-41, якою доповнив вже чинне законодавство новими правилами реагування на істотні кібератаки на важливі інформаційні системи країни (як урядові, так і приватні). Даним наказом визначено:

1. Кіберінцидент. Подія, що відбулась в, чи спричинена через комп'ютерну мережу, яка ставить під загрозу цілісність, конфіденційність, або доступність комп'ютерів, інформаційних або комунікаційних системи або мереж, реальної або віртуальної інфраструктури контрольованої комп'ютерами або інформаційними системами, або присутньої в них інформації. Також до кіберінцидентів можуть бути віднесені вразливості в інформаційних системах, процедурах кібербезпеки, внутрішньому управлінні або реалізації, які можуть бути використані як загроза.

2. Важливий кіберінцидент. Інцидент або сукупність інцидентів, які можуть завдати істотної шкоди національній безпеці, міжнародним відносинам, економіці Сполучених Штатів або суспільному спокою, громадянським свободам, безпеці та здоров'ю громадян Сполучених Штатів.

Також даним наказом запроваджено градацію рівня загрози від кібератак, аналогічну терористичній. Шкала має 6 градацій: від рівня 0 (білий), до рівня 5 (чорний), з проміжними рівнями 1 (зелений), 2 (жовтий), 3 (помаранчевий) та 4 (червоний).

1.2 Розслідування кіберінцидентів/кібератак

Сьогодні дуже поширене словосполучення «цифрова криміналістика», причому використовують його досить часто. Але що це таке? Взагалі **цифрова криміналістика (digitalforensics)** – це наука про розкриття злочинів, пов'язаних з комп'ютерною інформацією. Разом з тим існує більш повне визначення, яке, на мій погляд, набагато вірніше. **Комп'ютерно-технічна експертиза** – одна з різновидів судових експертиз, об'єктом якої є комп'ютерна техніка й/або комп'ютерні носії інформації, а метою – пошук й закріплення доказів. Прирахування до можливих об'єктів даного виду експертизи віддалених об'єктів, що не перебувають у повному розпорядженні експерта (насамперед, комп'ютерних мереж) поки є спірним питанням, і вирішується він по-різному.

Проводиться така експертиза як за кримінальними справами, так і за цивільними. За кримінальними справами вона може бути призначена слідчим (у рамках досудового наслідку) або судом і поручається конкретному експертові або експертній установі. Результатом експертизи є висновок експерта, який є доказом у справі. За цивільними справами експертиза може бути призначена судом, замовлена однією зі сторін або призначена нотаріусом з ініціативи тієї або іншої сторони.

Звичайно перед експертом ставляться питання такого роду:

– про наявність на досліджуваних об'єктах інформації, що відноситься до справи (у тому числі в неявному, вилученому, схованому або зашифрованому виді);

– про можливість використання досліджуваних об'єктів для певних цілей (наприклад, для доступу в мережу);

– про дії, зроблені з використанням об'єктів;

– про властивості програм для ЕОМ, зокрема про їхню приналежність до числа шкідливих;

– про ідентифікацію знайдених електронних документів, програм для ЕОМ, користувачів комп'ютера.

Разом з тим варто відзначити, що методи комп'ютерно-технічної експертизи часто використовуються при реагуванні на інциденти, пов'язані зі шкідливими програмами. При цьому в ході розслідування, як правило, експерт повинен одержати відповідь на наступні питання:

– Хто зробив атаку?

– Коли відбулася атака?

– Які сервери або робочі станції постраждали?

– Які цілі й мотиви атакуючих?

Стримування

Перше, із чого починається робота над інцидентом, – це його стримування. Фактично від вас потрібно стримати поширення зловреду й тим самим звузити можливий ареал поширення й зменшити збиток.

Чи відключати заражений комп’ютер від мережі фізично? Поширена думка, що це необхідно. Сьогодні думають, що ні. Чому? Так тому що велике поширення дістали засоби інтелектуального керування мережею, і ви сьогодні можете легко вивести будь-який комп’ютер в окрему віртуальну мережу VLAN. Адже насамперед потрібно зробити так, щоб ваша заражена система не могла взаємодіяти з мережею підприємства. А як саме ви це забезпечите, не так уже важливо. Наступним етапом у вашій роботі буде збір інформації.

Збір інформації

На даному етапі від вас буде потрібно зробити повний образ оперативної пам'яті й жорсткого диска зараженого комп'ютера. Саме в цей момент ви зможете одержати інформацію, яка дозволить зрозуміти, як ви будете працювати із зараженням.

Одним з інструментів для одержання повного образа пам'яті й копіювання жорсткого диска є програма FTK Imager Manager. FTK Imager Lite – інструмент попереднього перегляду й візуалізації даних, використовуваний для одержання даних (доказів) у судово-обґрунтованій формі шляхом створення копій даних без внесення змін у вихідні дані.

FTK Imager призначений для:

1. Створення криміналістичних копій:
– локальних жорстких дисків;
– компакт-дисків і DVD;
– флеш-накопичувачів і інших USB-пристроїв;
– папок;
– окремих файлів.
2. Перегляду файлів і папок на окремих жорстких дисках, мережних дисках, zip-дисках, компакт-дисках і DVD, флеш-накопичувачах і інших пристроях USB.
3. Попереднього перегляду вмісту судових дампів, що зберігаються на локальних або мережних дисках.
4. Перегляду в режимі тільки для читання.
5. Експорту файлів і папок із криміналістичних дампів.
6. Відновлення вилучених з «Кошика» файлів, якщо вони не були перезаписані на диску.

Створення ґешів файлів для перевірки цілісності даних з помо щью кожної із двох ґеш-функцій, доступних в FTK Imager: Message Digest 5 (MD5) і Secure Hash Algorithm (SHA-1).

7. Створення ґешів для звичайних файлів і образів дисків (включаючи файли усередині образів дисків), які згодом можна використовувати в якості зразка, щоб підтвердити цілісність ваших доказів. Ґеш, створений FTK Imager, може використовуватися для перевірки того, що ґеш дампа й ґеш диска

збігаються після створення образа й що образ залишається незмінним після створення.

Окремо хотілося б підкреслити, що за допомогою цього програмного забезпечення ви одержуєте побітову копію, включаючи нерозмічені області диска, у яких найчастіше й перебуває шкідлива програма.

Одержання образу оперативної пам'яті

Створити образ оперативної пам'яті можна, вибравши пункти меню File, Capture Memory. Урахуйте, що деякі додатки можуть перешкоджати зняттю образа оперативної пам'яті.

Якщо ви зіштовхнулися з таким, скористайтеся інструментом Belkasoft Live RAM Capturer.

Наступним кроком буде зняття образа жорсткого диска.

Зняття образа жорсткого диска

Для виконання цього кроку досліджуваний комп'ютер слід відключити. Причому, як не дивно пролунає, потрібно просто витягтися вилку з розетки, а не скористатися стандартною процедурою відключення. Чому? Так тому що при відключенні стандартним способом ви можете втратити частину тимчасових файлів, чого не можна допустити. Створення образа жорсткого диска проводиться тим же інструментом FTK Imager. Виберіть пункт меню File, а потім Createdіskimage. При цьому необхідно скопіювати весь фізичний диск, включаючи невикористовувані сектори, тому що в них можуть зберігатися файли й настроювання шкідливої програми.

Джерела доказів інциденту

Необхідно врахувати, що залежно від типу інциденту вам може знадобитися збір інформації з різних джерел.

Приведу кілька прикладів.

– Журнали міжмережевих екранів дозволять вам довідатися, які з'єднання використовувалися для підключення до зовнішньої мережі.

– Журнали контролера домену містять інформацію про те, до яких ресурсів запитувався доступ з використанням скомпрометованого облікового запису.

– Журнали сервера імен DNS містять доменні імена, які запитували шкідливі програми.

Передача даних

На наступному етапі дані передаються у відділ інформаційної безпеки або стороннім організаціям для проведення розслідування, при цьому необхідно прикладати ґеші образів. якщо образ диска зняти із використанням Ftkimager, то ґеш цього образа втримується у вікні Imagesummary. якщо ж ваша утиліта для збору даних не підтримує обчислення ґеша, то прийдеться скористатися, наприклад, утилітою hashdeep.

На цьому перший етап проведення розслідування можна вважати завершеним.

І далі фахівці з інформаційної безпеки аналізують передані дані.

З юридичної точки зору, задля встановлення змісту та обсягу повноважень суб'єктів, які здійснюють розслідування кіберінцидентів та кібератак, визначимо сутність цієї діяльності. Так, **розслідування кібератак та кіберінцидентів** – структурована сукупність дій та заходів, які здійснюються в межах забезпечення кібербезпеки України поза кримінальним процесом уповноваженими суб'єктами та спрямовані на встановлення механізму, обставин, засобів і знарядь та виконавців кіберінцидентів і кібератак, мінімізацію їх негативного впливу та шкідливих наслідків, а також вжиття заходів з попередження кіберінцидентів та кібератак у майбутньому.

Проведення розслідування кіберінцидентів та кібератак поза межами кримінального процесу означає, що особи, які його проводять, не можуть застосовувати інструментарій процесуальних, слідчих та негласних слідчих (розшукових) дій. Аналіз нормативно-правових актів, які регулюють оперативно-службову діяльність органів СБУ, дає підстави стверджувати, що з метою встановлення обставин, які підлягають з'ясуванню **під час розслідування кібератак та кіберінцидентів, співробітники СБУ мають право**:

– здійснювати опитування осіб (за їх згодою отримуючи від них усні або письмові пояснення), які можуть повідомити будь-яку інформацію, що має значення для досягнення відповідних цілей розслідування;

– отримувати від очевидців кіберінцидента чи кібератаки, службових осіб підприємства, установи, організації або інших громадян речі і документи, що мають значення для встановлення відповідних обставин кіберподії, яка є предметом розслідування;

– отримувати у встановленому порядку дані щодо загроз національній безпеці з використанням кіберпростору або будь-яких інших кіберзагроз об'єктам кібербезпеки, кібератак та/або обставин, інформація про які може сприяти запобіганню, виявленню і припиненню таких загроз, протидії кіберзлочинам, кібератакам та мінімізації їх наслідків;

– у порядку, погодженому із керівником підприємства, установи, організації, проводити візуальний і технічний огляд комп'ютерної та периферійної техніки, яка містить сліди кіберподії;

– ознайомлюватись з документами та даними, що характеризують діяльність підприємств, установ та організацій, вивчати їх, за рахунок коштів, що виділяються на утримання підрозділів, які здійснюють оперативно-розшукову діяльність, виготовляти копії з таких документів, на вимогу керівників підприємств, установ та організацій – виключно на території таких підприємств, установ та організацій;

– застосовувати спеціальне програмне забезпечення або технічні пристрої з метою отримання, збирання та накопичення інформації, необхідної для встановлення обставин кіберінцидента чи кібератаки;

– залучати до проведення окремих заходів фахівців СБУ, проводити з ними консультації та отримувати від них письмові висновки щодо предмета розслідування;

– здійснювати комп'ютерно-технічне дослідження а) зразків цифрової інформації, отриманої у ході ознайомлення з документами та даними, що

характеризують діяльність підприємств, установ та організацій, б) комп'ютерної техніки, мережевих апаратних засобів та їх комплектуючих, залучати до таких досліджень відповідних фахівців;

– за наявності підстав, передбачених ст. 207 КПК України, затримувати особу, в діях якої вбачаються ознаки кримінального правопорушення, та тимчасово вилучати її майно з метою подальшої передачі затриманої особи та вилученого майна уповноваженій службовій особі для вирішення питання про внесення даних про виявлене кримінальне правопорушення в ЄРДР та оформлення процесуального затримання особи в порядку ст. 208 КПК України

Необхідно враховувати також, що розслідування кіберінцидентів та кібератак підрозділами СБУ носить відкритий характер і здійснюється в межах захисту кібербезпеки України. Результати окремих заходів можуть використовуватись в оперативній і контррозвідувальній діяльності, якщо їх зміст відповідає таким потребам. Проте сам процесуальний порядок не визначений ні нормативно-правовими актами СБУ, ні чинним законодавством, що ускладнює реалізацію окремих повноважень та знижує ефективність протидії кіберзагрозам

19.2. Управління ризиками в інформаційній та/або кібербезпеці: Загальна концепція управління ризиками ІБ. ISO/IEC 27005:2018, IEC 31010:2019, NIST SP 800-39, NIST SP 800-37, NIST SP 800-30, NIST SP 800-137 (Ризики інформаційної безпеки. Аналіз та оцінка ризику. Прийняття ризику. Зменшення ризику. Страхування (перекладання) ризику). Системи класу Incident Response Platform

2.1 Загальна концепція управління ризиками ІБ

Управління ризиками дозволяє ефективно та раціонально вибудовувати процеси ІБ та розподіляти ресурси для захисту активів компанії, а оцінка ризиків дозволяє застосовувати доцільні заходи щодо їх мінімізації: для захисту від суттєвих та актуальних загроз логічно застосовуватиме більш дорогі рішення.

Крім цього, вибудований процес управління ризиками ІБ дозволить розробити і в разі потреби застосувати чіткі плани забезпечення безперервності діяльності та відновлення працездатності (Business Continuity & Disaster Recovery): глибока опрацювання різних ризиків допоможе заздалегідь врахувати, наприклад, раптову потребу у віддаленому доступі для великої кількості співробітників, як це може статися у разі епідемій чи колапсу транспортної системи.

Під **ризиком інформаційної безпеки, або кіберризиком**, розуміють потенційну можливість використання вразливостей активів конкретною загрозою заподіяння шкоди організації. Під величиною ризику умовно розуміють добуток ймовірності негативної події та розміру шкоди. У свою чергу, під ймовірністю події розуміється твір ймовірності загрози та небезпеки вразливості, виражені в якісній чи кількісній формі. Умовно ми можемо висловити це логічною формулою:

Величина Ризика = Ймовірність Події

Існують також умовні класифікації ризиків:

– за джерелом ризику (наприклад, атаки хакерів чи інсайдерів, фінансові помилки, вплив державних регуляторів, юридичні претензії контрагентів, негативний інформаційний вплив конкурентів);

– за метою (інформаційні активи, фізичні активи, репутація, бізнес-процеси);

– за тривалістю впливу (операційні, тактичні, стратегічні).

Управління ризиками в інформаційній та/або кібербезпеці як правило включає в себе наступні пункти:

– Визначення ризику інформаційної безпеки.
– Аналіз та оцінка ризику.
– Прийняття ризику.
– Зменшення ризику.
– Страхування (перекладання) ризику).

В цій лекції розглянемо ці пункти як у загальній концепції управління ризиками ІБ так й у відповідних стандартах: ISO/IEC 27005:2018, IEC 31010:2019, NIST SP 800-39, NIST SP 800-37, NIST SP 800-30, NIST SP 800-137.

Рисунок 18.1 – Концепції, підходи та стандарти управління ризиками ІБ

Цілі **аналізу ризиків** ІБ наступні:

1. Ідентифікувати активи та оцінити їх цінність.
2. Ідентифікувати загрози активам та вразливості у системі захисту.
3. Прорахувати ймовірність реалізації загроз та їхнього впливу на бізнес (англ. business impact).

4. Дотриматися балансу між вартістю можливих негативних наслідків та вартістю заходів захисту, дати рекомендації керівництву компанії з обробки виявлених ризиків.

Етапи з 1-го по 3-й є **оцінкою ризику** (англ. risk assessment) і є збиранням наявної інформації. Етап 4 є вже безпосередньо **аналіз ризиків** (англ. risk analysis), тобто, вивчення зібраних даних та видачу результатів/вказівок для подальших дій. У цьому важливо розуміти власний рівень упевненості у коректності проведеної оцінки. На етапі 4 також пропонуються **методи обробки для кожного з актуальних ризиків**:

– передача (наприклад, шляхом страхування);

– уникнення (наприклад, відмова від впровадження тієї чи іншої технології чи сервісу);

– прийняття (свідома готовність завдати шкоди у разі реалізації ризику);

– мінімізація (застосування заходів для зниження ймовірності негативної події, що призводить до реалізації ризику).

Збиток від реалізації атаки може бути **прямим** або **непрямим**.

– Прямий збиток – це безпосередні очевидні й легко прогнозовані втрати компанії, такі як втрати прав інтелектуальної власності, розголошення секретів виробництва, зниження вартості активів або їх часткове або повне руйнування, судові витрати та виплата штрафів і компенсацій тощо.

– Непрямі збитки можуть означати **якісні** або **непрямі** втрати.

Якісними втратами можуть бути призупинення або зниження ефективності діяльності компанії, втрата клієнтів, зниження якості вироблених товарів або послуг. **Непрямі** втрати – це, наприклад, недоотриманий прибуток, втрата ділової репутації, додатково понесені витрати. Крім цього, у зарубіжній літературі зустрічаються також такі поняття, як **тотальний ризик** (англ. total risk), який є присутнім, якщо взагалі ніяких заходів захисту не впроваджується, а також **залишковий ризик** (англ. residual risk), який присутній, якщо загрози реалізувалися, попри впроваджені заходи захисту.

Аналіз ризиків може бути як **кількісним**, і **якісним**.

Розглянемо один із способів **кількісного** аналізу ризиків. Основними показниками вважатимемо такі величини:

– **ALE** – annual loss expectancy, очікувані річні втрати, тобто, **«вартість» всіх інцидентів за рік**.

– **SLE** – single loss expectancy, очікувані разові втрати, тобто, **«вартість» одного інциденту**.

– **EF** – exposure factor, чинник відкритості перед загрозою, тобто, **який відсоток активу зруйнує загроза за її успішної реалізації**.

– **ARO** – annualized rate of occurrence, **середня кількість інцидентів на рік** відповідно до статистичних даних.

Значення SLE обчислюється як добуток розрахункової вартості активу та значення EF, тобто:

$$SLE=AssetValue*EF.$$

При цьому вартість активу слід включати і штрафні санкції за його недостатній захист.

Значення ALE обчислюється як добуток SLE та ARO, тобто:

*ALE=SLE*ARO*.

Значення ALE допоможе проранжувати ризики – ризик із високим ALE буде найкритичнішим. Далі розраховане значення ALE можна буде використовувати для визначення максимальної вартості реалізованих заходів захисту, оскільки, згідно з загальноприйнятим підходом, вартість захисних заходів не повинна перевищувати вартість активу або величину прогнозованої шкоди, а розрахункові доцільні витрати на атаку для зловмисника повинні бути меншими, ніж очікуваний ним прибуток від цієї атаки. Цінність заходів захисту також можна визначити, віднімаючи від розрахункового значення ALE до впровадження заходів захисту значення розрахункового значення ALE після впровадження заходів захисту, а також віднімаючи щорічні витрати на реалізацію цих заходів. Умовно записати цей вислів можна так:

(Цінність заходів захисту для компанії) = (ALE до впровадження заходів захисту) – (ALE після впровадження заходів захисту) – (Щорічні витрати на реалізацію заходів захисту)

Прикладами **якісного** аналізу ризиків можуть бути, наприклад, метод Дельфі, в якому проводиться анонімне опитування експертів у кілька ітерацій до досягнення консенсусу, і навіть мозковий штурм та інші приклади оцінки т.зв. «експертним методом».

Далі наведемо короткий та невичерпний **список різних методологій ризик-менеджменту**, а найпопулярніші з них ми розглянемо далі вже детально.

1. **Фреймворк «NIST Risk Management Framework»** на базі американських урядових документів NIST (National Institute of Standards and Technology, Національного інституту стандартів і технологій США) включає набір взаємопов'язаних т.зв. «спеціальних публікацій» (англ. Special Publication (SP), для простоти сприйняття називати їх стандартами):

1.1. Стандарт **NIST SP 800-39 «Managing Information Security Risk» («Управління ризиками інформаційної безпеки»)** пропонує трирівневий підхід до управління ризиками: організація, бізнес-процеси, інформаційні системи. Цей стандарт описує методологію процесу управління ризиками: визначення, оцінка, реагування та моніторинг ризиків.

1.2. Стандарт **NIST SP 800-37 «Risk Management Framework for Information Systems and Organizations» («Фреймворк управління ризиками для інформаційних систем та організацій»)** пропонує для забезпечення безпеки та конфіденційності використання підходу управління життєвим циклом систем.

1.3. Стандарт **NIST SP 800-30 «Guide for Conducting Risk Assessments» («Посібник з проведення оцінки ризиків»)** сфокусований на IT, ІБ та операційних ризиках. Він описує підхід до процесів підготовки та проведення оцінки ризиків, комунікування результатів оцінки, а також подальшої підтримки процесу оцінки.

1.4. Стандарт **NIST SP 800-137 «Information Security Continuous Monitoring» («Безперервний моніторинг інформаційної безпеки»)** описує

підхід до процесу моніторингу інформаційних систем та IT-середовищ з метою контролю застосованих заходів обробки ризиків ІБ та необхідності їх перегляду.

2. **Стандарти** Міжнародної організації зі стандартизації **ISO** (International Organization for Standardization):

2.1. Стандарт **ISO/IEC 27005:2018 «Information technology – Security techniques – Information security risk management» («Інформаційна технологія. Методи та засоби забезпечення безпеки. Менеджмент ризику інформаційної безпеки»)** входить до серії стандартів ISO 27000 і є логічно взаємопов'язаним ІБ із цієї серії. Цей стандарт відрізняється фокусом на ІБ під час розгляду процесів управління ризиками.

2.2. Стандарт **ISO/IEC 27102:2019 «Information security management – Guidelines for cyber-insurance» («Управління інформаційною безпекою. Посібник з кіберстрахування»)** пропонує підходи до оцінки необхідності придбання кіберстрахування як заходи обробки ризиків, а також до оцінки та взаємодії зі страховиком.

2.3. Серія стандартів **ISO/IEC 31000:2018** описує підхід до ризик-менеджменту без прив'язки до IT/ІБ. Він гармонізований у вигляді **ДСТУ ISO 31000:2018 Менеджмент ризиків. Принципи та настанови (ISO 31000:2018, IDT).** У цій серії варто відзначити стандарт **ISO/IEC 31010:2019 «Risk management – Risk assessment techniques»** – цей стандарт у вітчизняному варіанті **ДСТУ IEC/ISO 31010:2013 Керування ризиком. Методи загального оцінювання ризику (IEC/ISO 31010:2019, IDT).**

3. Методологія **FRAP (Facilitated Risk Analysis Process)** є відносно спрощеним способом оцінки ризиків, з фокусом лише на найкритичніших активах. Якісний аналіз проводиться за допомогою експертної оцінки.

4. Методологія **OCTAVE (Operationally Critical Threat, Asset, Vulnerability Evaluation)** сфокусована на самостійній роботі членів бізнес-підрозділів. Вона використовується для масштабної оцінки всіх інформаційних систем та бізнес-процесів компанії.

5. Стандарт **AS/NZS 4360** є австралійським і новозеландським стандартом з фокусом як на IT-системах, а й у бізнес-здоров'я компанії, тобто, пропонує глобальніший підхід до управління ризиками. Зазначимо, що даний стандарт замінено на стандарт **AS/NZS ISO 31000-2009**.

6. Методологія **FMEA (Failure Modes and Effect Analysis)** пропонує проведення оцінки системи з погляду її слабких місць для пошуку ненадійних елементів.

7. Методологія **CRAMM (Central Computing and Telecommunications Agency Risk Analysis and Management Method)** пропонує використання автоматизованих засобів управління ризиками.

8. Методологія **FAIR (Factor Analysis of Information Risk)** – пропрієтарний фреймворк щодо кількісного аналізу ризиків, що пропонує модель побудови системи управління ризиками з урахуванням економічно ефективного підходу, прийняття поінформованих рішень, порівняння заходів управління ризиками, фінансових показників і точних ризик-моделей.

9. Концепція **COSO ERM (Enterprise Risk Management)** описує шляхи інтеграції ризик-менеджменту зі стратегією та фінансовою ефективністю діяльності компанії та наголошує на важливості їх взаємозв'язку. У документі описані такі компоненти управління ризиками, як стратегія та постановка цілей, економічна ефективність діяльності компанії, аналіз та перегляд ризиків, корпоративне управління та культура, а також інформація, комунікація та звітність.

Спеціальні публікації **NIST SP 800-39, NIST SP 800-37 та NIST SP 800-30** пропонують логічно пов'язаний системний підхід до **оцінки та обробки ризиків**, а **NIST SP 800-53, NIST SP 800-53A** пропонують конкретні заходи щодо **мінімізації ризиків ІБ**. Однак слід мати на увазі, що дані документи за своєю суттю мають лише рекомендаційний характер і не є стандартами (наприклад, на відміну від документів NIST FIPS), а також те, що вони спочатку розроблялися для компаній і організацій зі США. Це накладає певні обмеження їх використання: так, організації що неспроможні отримати міжнародну сертифікацію з виконання положень даних документів, а застосування всього набору пов'язаних фреймворків NIST може виявитися надмірно трудомістким і недоцільним. Найчастіше компанії обирають шлях сертифікації за вимогами Міжнародної Організації зі Стандартизації (International Organization for Standardization, ISO), отримуючи, наприклад, статус «**ISO 27001 Certified**», визнаний у всьому світі. До серії стандартів ISO 27000 входять документи, присвячені інформаційній безпеці та управлінню ризиками. Розглянемо основний документ цієї серії з управління ризиками ІБ: стандарт **ISO/IEC 27005:2018**.

2.2 ISO/IEC 27005:2018

Стандарт **ISO/IEC 27005:2018 «Information technology – Security techniques – Information security risk management» («Інформаційні технології – Техніки забезпечення безпеки – Управління ризиками інформаційної безпеки»)** є вже третьою ревізією: першу версію стандарту було опубліковано у 2005 році, а другу – у 2011. Стандарт гармонізовано в Україні у вигляді **ДСТУ ISO/IEC 27005:2019 Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки (ISO/IEC 27005:2018, IDT)**.

Документ вводить кілька ризик-специфічних термінів. Так, **засобом захисту** (англ. control) називається міра, що змінює ризик. У поняття **контекстів** (англ. context) входять зовнішній контекст, що означає зовнішнє середовище функціонування компанії (наприклад, політичне, економічне, культурне середовище, а також взаємини із зовнішніми стейкхолдерами), і внутрішній контекст, що означає внутрішнє середовище функціонування компанії (внутрішні процеси, політики, стандарти, системи, цілі та культуру організації, взаємини з внутрішніми стейкхолдерами, а також договірні зобов'язання).

Ризик – це результат неточності (англ. uncertainty) при досягненні цілей; при цьому неточність означає стан нестачі інформації, що відноситься до певної події, її наслідків або ймовірності її настання.

Під **рівнем ризику** (англ. level of risk) розуміється величина ризику, виражена у творі наслідків значних подій та ймовірності виникнення цих подій.

Залишковий ризик (англ. Residual risk) – ризик, що залишився після проведення процедури обробки ризиків.

Під **оцінкою ризику** (англ. risk assessment) розуміють загальний процес ідентифікації (тобто пошуку, визначення та описи ризику), аналізу (тобто розуміння природи ризику та визначення його рівня) та оцінки небезпеки (тобто порівняння результатів аналізу ризику з ризик-критеріями визначення допустимості його величини) ризиків.

Обробка ризиків – це процес модифікації ризиків, який може включати:

– уникнення ризику шляхом відмови від дій, які можуть призвести до ризиків;
– прийняття чи збільшення ризику з метою досягнення бізнес-цілей;
– усунення джерел ризику;
– зміна ймовірності реалізації ризику;
– зміна очікуваних наслідків реалізації ризику;
– перенесення (поділ) ризику;
– збереження ризику.

Процес управління ризиками ІБ з погляду авторів стандарту ISO/IEC 27005:2018 має характеризуватися такими особливостями:

1. Оцінка ризиків ведеться з урахуванням наслідків ризиків для бізнесу та ймовірності виникнення ризиків. Здійснюються ідентифікація ризиків, їх аналіз та порівняння (з урахуванням обраного рівня ризик-толерантності).
2. Імовірність та наслідки ризиків доводяться до зацікавлених сторін та приймаються ними.
3. Встановлюється пріоритет обробки ризиків та конкретних дій щодо зниження ризиків.
4. У процес прийняття рішень щодо управління ризиками залучаються стейкхолдери, які потім також інформуються про статус управління ризиками.
5. Оцінюється ефективність проведеної обробки ризиків.
6. Контролюються та регулярно переглядаються ризики і сам процес управління ними.
7. На основі нової інформації процес управління ризиками безперервно покращується.
8. Проводиться навчання співробітників та керівників щодо ризиків та дій для їх зниження.

Сам **процес управління ризиками складається з наступних** кроків (процесів), які відповідають прийнятому в стандарті ISO 27001 підходу **PDCA (Plan – Do – Check – Act)**:

1. Визначення контексту.
2. Оцінка ризиків.
3. Розробка плану обробки ризиків.
4. Ухвалення ризиків.
5. Використання розробленого плану обробки ризиків.

6. Безперервний моніторинг та перегляд ризиків.

7. Підтримка та покращення процесу управління ризиками ІБ.

Розглянемо далі кожен із цих кроків докладніше.

2.2.1. Визначення контексту

Вхідними даними при визначенні контексту є всі релевантні ризик-менеджменту відомості про компанію. В рамках цього процесу вибирається підхід до управління ризиками, який повинен включати критерії оцінки ризиків, критерії оцінки негативного впливу (англ. impact), критерії прийняття ризиків. Крім цього, слід оцінити та виділити необхідні для здійснення даного процесу ресурси.

Критерії оцінки ризиків повинні бути вироблені для оцінки ризиків ІБ у компанії та повинні враховувати вартість інформаційних активів, вимоги до їх конфіденційності, цілісності, доступності, роль інформаційних бізнес-процесів, вимоги законодавства та договірних зобов'язань, очікування стейкхолдерів, можливі негативні наслідки для гудвілу та репутації компанії.

Критерії оцінки негативного впливу повинні враховувати рівень збитків або витрат компанії на відновлення після реалізованого ризику ІБ з урахуванням рівня значущості ІТ активу, порушення інформаційної безпеки (тобто втрати активом властивостей конфіденційності, цілісності, доступності), вимушений простий бізнес-процесів, економічні втрати, порушення планів та дедлайнів, збитки репутації, порушення вимог законодавства та договірних зобов'язань.

Критерії прийняття ризиків можна висловити як ставлення очікуваної бізнес-вигоди до очікуваного ризику. При цьому для різних класів ризиків можна застосовувати різні критерії: наприклад, ризики невідповідності законодавству можуть бути прийняті в принципі, а високі фінансові ризики можуть бути прийняті, якщо вони є частиною договірних зобов'язань. Крім цього, слід враховувати і прогнозований часовий період актуальності ризику (довгострокові та короткострокові ризики). Критерії прийняття ризиків необхідно розробляти, враховуючи бажаний (цільовий) рівень ризику з можливістю прийняття топ-менеджментом ризиків вище за цей рівень за певних обставин, а також можливість прийняття ризиків за умови подальшої обробки ризиків протягом обумовленого часового періоду.

Крім вищезгаданих критеріїв, у рамках процесу визначення контексту слід врахувати межі та обсяг (англ. scope) процесу управління ризиками ІБ: потрібно взяти до уваги бізнес-цілі, бізнес-процеси, плани та політики компанії, структуру та функції організації, застосовні законодавчі та інші вимоги, інформаційні активи, очікування стейкхолдерів, взаємодія з контрагентами. Розглядати процес управління ризиками можна у межах конкретної ІТ-системи, інфраструктури, бізнес-процесу чи межах певної частини всієї компанії.

2.2.2. Оцінка ризиків

У рамках проведення процесу оцінки ризиків компанія має оцінити вартість інформаційних активів, ідентифікувати актуальні загрози та вразливості, отримати інформацію про поточні засоби захисту та їх ефективність, визначити потенційні наслідки реалізації ризиків. В результаті оцінки ризиків компанія повинна отримати кількісну чи якісну оцінку ризиків, а

також пріоритизацію цих ризиків з урахуванням критеріїв оцінки небезпеки ризиків та цілей компанії. Сам **процес оцінки** ризиків складається з дій щодо **ідентифікації** (англ. identification) ризиків, **аналізу** (англ. analysis) ризиків, оцінки **небезпеки** (англ. evaluation) ризиків.

2.2.2.1. Ідентифікація ризиків

Метою ідентифікації ризиків є визначення того, що може статися і призвести до потенційних збитків, а також отримати розуміння того, як, де і чому ця шкода може статися. При цьому слід враховувати ризики незалежно від того, чи джерело цих ризиків під контролем організації чи ні. В рамках цього процесу слід провести:

– ідентифікацію (інвентаризацію) активів, отримавши у результаті список IT-активів та бізнес-процесів;

– ідентифікацію загроз, при цьому слід враховувати навмисні та випадкові загрози, зовнішні та внутрішні джерела загроз, а інформацію про можливі загрози можна отримувати як у внутрішніх джерел в організації (юристи, HR, IT тощо), так і зовнішніх (страхові компанії, зовнішні консультанти, статистична інформація тощо);

– ідентифікацію наявних та запланованих до впровадження заходів захисту для виключення їх дублювання;

– ідентифікацію вразливостей, які можуть бути проексплуатовані актуальними загрозами та завдати шкоди активам; у своїй слід враховувати вразливості у програмному чи апаратному забезпеченні, а й у структурі організації, її бізнес-процесах, персоналі, фізичної інфраструктурі, відносинах з контрагентами;

– ідентифікацію наслідків реалізації загроз порушення конфіденційності, цілісності, доступності IT-активів.

2.2.2.2. Аналіз ризиків

Аналіз ризиків може бути проведений з різною глибиною, залежно від критичності активів, кількості відомих уразливостей, а також з урахуванням інцидентів, що відбулися раніше. Методологія аналізу ризиків може бути як якісною, так і кількісною: як правило, спочатку застосовують якісний аналіз для виділення високопріоритетних ризиків, а потім вже для виявлених ризиків застосовують кількісний аналіз, який є більш трудомістким і дає більш точні результати.

При використанні **якісного аналізу** фахівці оперують шкалою описової оцінки небезпеки (наприклад, низька, середня, висока) потенційних наслідків деяких подій та ймовірності настання цих наслідків.

При використанні методів **кількісного аналізу** вже застосовуються чисельні величини, з урахуванням історичних даних про інциденти, що вже відбулися. Слід мати на увазі, що у разі відсутності надійних фактів, що перевіряються, кількісна оцінка ризиків може дати лише ілюзію точності.

При безпосередньо процесі аналізу ризиків спочатку проводиться оцінка потенційних наслідків інцидентів ІБ: оцінюється рівень їхнього негативного впливу на організацію з урахуванням наслідків від порушень властивостей конфіденційності, цілісності, доступності інформаційних активів. Проводяться

перевірка та аудит наявних активів з метою їхньої класифікації залежно від критичності, також оцінюється (бажано у грошових величинах) потенційний негативний вплив порушення властивостей ІБ цих активів на бізнес.

Оцінка вартості активів проводиться в рамках **аналізу негативного впливу на бізнес** (Business Impact Analysis) і може бути розрахована виходячи з вартості заміни або відновлення активів/інформації, а також наслідків втрати або компрометації активів/інформації: розглядаються фінансові, юридичні, репутаційні аспекти.

Далі проводиться оцінка імовірності виникнення інциденту, тобто, всіх потенційних сценаріїв реалізації загроз. Слід врахувати частоту реалізації загрози та легкість експлуатації вразливостей, керуючись статистичною інформацією про аналогічні загрози, а також даними про мотивацію та можливості навмисних джерел загроз (побудова моделі порушника), привабливість активів для атакуючих, наявних уразливостей, застосованих заходів захисту, а у разі розгляду ненавмисно загроз – враховувати місце розташування, погодні умови, особливості обладнання, людські помилки тощо. Залежно від необхідної точності оцінки активи можна групувати або розділяти з точки зору застосовних до них сценаріїв атак.

Нарешті проводиться визначення рівня ризиків для всіх сценаріїв із розробленого списку сценаріїв атак. Величина очікуваного ризику є вірогідністю сценарію інциденту та його наслідків.

2.2.2.3. Оцінка небезпеки ризиків

В рамках процесу оцінки небезпеки ризиків проводиться порівняння отриманих на попередньому етапі рівнів ризиків із критеріями порівняння ризиків та критеріями прийняття ризиків, отриманими на етапі визначення контексту. При прийнятті рішень слід враховувати наслідки реалізації загроз, можливість виникнення негативних наслідків, рівень власної впевненості в коректності проведеної ідентифікації та аналізу ризиків. Слід врахувати властивості ІБ активів (наприклад, якщо втрата конфіденційності нерелевантна для організації, то всі ризики, що порушують дану властивість, можна відкинути), а також важливість бізнес-процесів, що обслуговуються певним активом (наприклад, ризики, що зачіпають малозначущий бізнес-процес, можуть бути визнані низькопріоритетними).

2.2.3. Обробка ризиків ІБ

На початок здійснення цього підпроцесу ми вже маємо список приоритизованих ризиків відповідно до критеріїв оцінки небезпеки ризиків, пов'язаних зі сценаріями інцидентів, які можуть призвести до реалізації цих ризиків. В результаті проходження **етапу обробки** ризиків ми повинні вибрати **заходи захисту**, призначені для **модифікації** (англ. modification), **збереження** (англ. retention), **уникнення** (англ. avoidance) або **передачі** (англ. sharing) ризиків, а також обробити **залишкові ризики** та сформувати **план обробки ризиків**.

Зазначені опції обробки ризиків (модифікацію, збереження, уникнення або передачу) слід вибирати в залежності від результатів процесу оцінки ризиків,

очікуваної оцінки вартості впровадження заходів захисту та очікуваних переваг кожної опції, при цьому їх можна комбінувати (наприклад, модифікувати ймовірність ризику та передавати залишковий ризик). Перевагу слід віддавати легкореалізованим та низькобюджетним заходам, які при цьому дають великий ефект зниження ризиків та закривають більшу кількість загроз, а у разі необхідності застосування дорогих рішень слід давати економічне обґрунтування їх застосування. Загалом слід прагнути максимально знизити негативні наслідки, а також враховувати рідкісні, але руйнівні ризики.

Через війну відповідальними особами може бути сформований план обробки ризиків, який чітко визначає пріоритет і часовий інтервал, відповідно до якими слід реалізувати метод обробки кожного ризику. **Пріоритети** можуть бути розставлені за результатами **ранжирування ризиків** та **аналізу витрат та вигод** (англ. cost-benefit analysis). У разі, якщо в організації вже були впроваджені будь-які заходи захисту, буде розумно проаналізувати їхню актуальність та вартість володіння, при цьому слід враховувати взаємозв'язки між заходами захисту та загрозами, для захисту від яких ці заходи застосовувалися.

Після закінчення плану обробки ризиків слід визначити залишкові ризики. Для цього можуть знадобитися оновлення або повторне проведення оцінки ризиків з урахуванням очікуваних ефектів від запропонованих способів обробки ризиків.

Далі розглянемо докладніше можливі опції обробки ризиків.

2.2.3.1. Модифікація ризиків

Модифікація ризиків має на увазі таке управління ризиками шляхом застосування або зміни заходів захисту, що призводить до оцінки залишкового ризику як прийнятного. При використанні опції модифікації ризиків вибираються виправдані та релевантні заходи захисту, які відповідають вимогам, визначеним на етапах оцінки та обробки ризиків. Слід враховувати різноманітні обмеження, такі як вартість володіння засобами захисту (з урахуванням впровадження, адміністрування та впливу на інфраструктуру), тимчасові та фінансові рамки, потреба в персоналі, що обслуговує ці засоби захисту, вимоги щодо інтеграції з поточними та новими заходами захисту. Також потрібно порівнювати вартість зазначених витрат з вартістю активу, що захищається. До заходів захисту можна віднести: корекцію, усунення, запобігання, мінімізацію негативного впливу,

Результатом кроку «Модифікація ризиків» має стати список можливих заходів захисту з їх вартістю, пропонованими перевагами та пріоритетом впровадження.

2.2.3.2. Збереження ризику

Збереження ризику означає, що за результатами оцінки небезпеки ризику прийнято рішення, що подальші дії його обробці не потрібні, тобто, оцінний рівень очікуваного ризику відповідає критерію ухвалення ризику. Зазначимо, що ця опція суттєво відрізняється від хибної практики ігнорування ризику, за якої вже ідентифікований та оцінений ризик ніяк не обробляється, тобто, рішення про його прийняття офіційно не приймається, залишаючи ризик у «підвішеному» стані.

2.2.3.3. Уникнення (зменшення) ризику

При виборі даної опції приймається рішення не вести певну діяльність чи змінити умови її ведення те щоб уникнути ризику, асоційованого з цією діяльністю. Це рішення може бути ухвалене у разі високих ризиків або перевищення вартості впровадження заходів захисту над очікуваними перевагами. Наприклад, компанія може відмовитися від надання користувачам певних онлайн-послуг щодо персональних даних, виходячи з результатів аналізу можливих ризиків витоку такої інформації та вартості впровадження адекватних заходів захисту.

2.2.3.4. Передача (страхування) ризику

Ризик можна передати тій організації, яка зможе керувати ним найефективніше. Таким чином, на підставі оцінки ризиків приймається рішення про передачу певних ризиків іншій особі, наприклад, шляхом страхування кіберризиків (послуга, що набирає популярності в Україні, проте досі в рази відстає від обсягу цього ринку, наприклад, у США) або шляхом передачі обов'язку з моніторингу та реагування на інциденти ІБ провайдеру послуг MSSP (Managed Security Service Provider) або MDR (Managed Detection and Response), тобто, у комерційний SOC. При виборі опції передачі ризику слід врахувати, як і сама передача ризику може бути ризиком, і навіть те, що можна перекласти в іншу компанію відповідальність управління ризиком, але не можна перекласти її у відповідальність за негативні наслідки можливого інциденту.

2.2.4. Прийняття ризику

Вхідними даними цього етапу будуть розроблені на попередньому етапі плани обробки ризиків та оцінка залишкових ризиків. Плани обробки ризиків повинні описувати те, як оцінені ризики будуть опрацьовані для досягнення критеріїв прийняття ризиків. Відповідальні особи аналізують та погоджують запропоновані плани обробки ризиків та фінальні залишкові ризики, а також вказують усі умови, за яких це погодження виноситься. У спрощеній моделі проводиться банальне порівняння величини залишкового ризику раніше визначеним прийнятним рівнем. Проте слід враховувати, що в деяких випадках може знадобитися перегляд критеріїв прийняття ризиків, які не враховують нові обставини чи умови. У такому разі відповідальні особи можуть бути змушені прийняти такі ризики,

У результаті формується список прийнятих ризиків з обґрунтуванням до тих, які не відповідають раніше певним критеріям прийняття ризиків.

2.2.5. Використання розробленого плану обробки ризиків. Комунікування ризиків ІБ

На даному етапі здійснюється безпосереднє втілення в життя розробленого плану обробки ризиків: відповідно до прийнятих рішень закуповуються та налаштовуються засоби захисту та обладнання, укладаються **договори кібер-страхування** та **реагування на інциденти**, ведеться юридична робота з контрагентами. Паралельно до керівництва та стейкхолдерів доводиться інформація про виявлені ризики ІБ та вживані заходи щодо їх обробки з метою досягнення загального розуміння діяльності, що проводиться.

Розробляються плани комунікації ризиків ІБ для ведення скоординованої діяльності у звичайних та екстрених ситуаціях (наприклад, на випадок великого інциденту ІБ).

2.2.6. Безперервний моніторинг та перегляд ризиків

Слід враховувати, що ризики можуть непомітно змінюватися з часом: змінюються активи та їхня цінність, з'являються нові загрози та вразливості, змінюються ймовірність реалізації загроз та рівень їхнього негативного впливу. Отже, необхідно вести безперервний моніторинг змін, що відбуваються, у тому числі із залученням зовнішніх контрагентів, що спеціалізуються на аналізі актуальних загроз ІБ. Потрібно проводити регулярний перегляд як ризиків ІБ, так і застосовуваних способів їх обробки на предмет актуальності та адекватності ситуації, що потенційно змінилася. Особливу увагу слід приділяти цьому процесу в моменти істотних змін у роботі компанії та бізнес-процесів, що здійснюються (наприклад, при злиттях/поглинаннях, запусках нових сервісів, зміні структури володіння компанією тощо).

2.2.7. Підтримка та покращення процесу управління ризиками ІБ

Аналогічно безперервному моніторингу ризиків слід постійно підтримувати та покращувати сам процес управління ризиками для того, щоб контекст, оцінка та план обробки ризиків залишалися релевантними поточній ситуації та обставинам. Усі зміни та покращення потрібно узгоджувати із зацікавленими сторонами. Критерії оцінки та прийняття ризиків, оцінка вартості активів, наявні ресурси, активність конкурентів та зміни у законодавстві та контрактних зобов'язаннях повинні відповідати актуальним бізнес-процесам та поточним цілям компанії. У разі потреби потрібно змінювати чи вдосконалювати поточний підхід, методологію та інструменти управління ризиками ІБ.

2.3 IEC 31010:2019

Розглянемо тепер стисло стандарт **IEC 31010:2019 «Risk management – Risk assessment techniques» («Менеджмент ризику – Методи оцінки ризику»). ДСТУ IEC/ISO 31010:2013 Керування ризиком. Методи загального оцінювання ризику (IEC/ISO 31010:2019, IDT)**

Цей стандарт входить у серію стандартів з управління бізнес-ризиками без прив'язки безпосередньо до ризиків ІБ. «Найголовнішим» стандартом є документ **ISO 31000:2018 ”Risk management – Guidelines” («Менеджмент ризику – Керівництва»)**, **ДСТУ ISO 31000:2018 Менеджмент ризиків. Принципи та настанови (ISO 31000:2018, IDT)**, який описує фреймворк, принципи та процес управління ризиками. Описаний у цьому документі процес ризик-менеджменту аналогічний розглянутому вище: визначаються контекст, межі та критерії, проводиться оцінка ризиків (що складається з ідентифікації, аналізу, оцінки небезпеки ризиків), далі йде обробка ризиків з подальшою комунікацією, звітністю, моніторингом та переглядом.

Стандарт же IEC 31010:2019 примітний тим, що в ньому наведено понад 40 різноманітних технік оцінки ризику, до кожної дано пояснення, зазначено спосіб застосування для всіх підпроцесів оцінки ризику (ідентифікація ризику, визначення джерел та причин ризику, аналіз заходів захисту, аналіз наслідків,

ймовірностей, взаємозв'язків та взаємодій, вимірювання та оцінка рівня ризику, вибір заходів захисту, звітність), а для деяких технік наведено і практичні приклади використання.

2.4 NIST Risk Management Framework

Першим набором документів буде **фреймворк управління ризиками (Risk Management Framework) американського національного інституту стандартів та технологій (NIST)**. Цей інститут випускає документи з ІБ у рамках серії стандартів FIPS (Federal Information Processing Standards, Федеральні стандарти обробки інформації) та рекомендацій SP (Special Publications, Спеціальні публікації) 800 Series. Ця серія публікацій відрізняється логічною взаємопов'язаністю, детальністю, єдиною термінологічною базою. Серед документів, що стосуються управління ризиками ІБ, слід зазначити публікації NIST SP 800-39, 800-37, 800-30, 800-137 та 800-53/53a.

Створення цього набору документів було наслідком ухвалення Федерального закону США про управління інформаційною безпекою (FISMA, Federal Information Security Management Act, 2002 р.) та Федерального закону США про модернізацію інформаційної безпеки (FISMA, Federal Information Security Modernization Act, 2014 р.). Незважаючи на декларовану «прив'язку» стандартів та публікацій NIST до законодавства США та обов'язковість їх виконання для американських державних органів, ці документи цілком можна розглядати і як відповідні для будь-якої компанії, яка прагне покращити управління ІБ, незалежно від юрисдикції та форми власності.

2.5 NIST SP 800-39

Отже, документ **NIST SP 800-39 « Управління ризиком інформаційної безпеки: Рівень організації, місії, інформаційної системи»** пропонує вендоронезалежний, структурований, але гнучкий підхід до управлінню ризиками ІБ у контексті операційної діяльності компанії, активів, фізичних осіб та контрагентів. При цьому ризик-менеджмент повинен бути цілісним процесом, що стосується всієї організації, в якій практикується ризик-орієнтоване прийняття рішень на всіх рівнях. Управління ризиком визначається в даному документі як всеосяжний процес, що включає етапи визначення (frame), оцінки (assess), обробки (respond) і моніторингу (monitor) ризиків. Розглянемо ці етапи докладніше.

1. На **етапі визначення ризиків** організації слід виявити:

- припущення ризики, тобто, ідентифікувати актуальні загрози, уразливість, наслідки, ймовірність виникнення ризиків;
- обмеження ризиків, тобто, можливості здійснення оцінки, реагування та моніторингу;
- ризик-толерантність, тобто, терпимість до ризиків – прийнятні типи та рівні ризиків, а також допустимий рівень невизначеності в питаннях управління ризиками;
- пріоритети та можливі компроміси, тобто, Необхідно пріоритизувати бізнес-процеси, вивчити компроміси, куди може піти організація під час

обробки

ризиків, і навіть тимчасові обмеження та чинники невизначеності, які супроводжують цей процес.

2. На **етапі оцінки ризиків** організації слід виявити:

- небезпеки ІБ, тобто, конкретні дії, осіб чи сутності, які можуть бути загрозами для самої організації або можуть бути спрямовані на інші організації;
- внутрішні та зовнішні вразливості, включаючи організаційні вразливості у бізнес-процесах управління компанією, архітектурі ІТ-систем тощо;
- збитки організації з урахуванням можливостей експлуатації вразливостей загрозами;
- ймовірність виникнення шкоди.

Через війну організація отримує детермінанти ризику, тобто, рівень шкоди та ймовірність виникнення шкоди для кожного ризику.

Для **забезпечення процесу оцінки ризиків** організація заздалегідь визначає:

- інструменти, техніки та методології, що використовуються для оцінки ризику;
- припущення щодо оцінки ризиків;
- обмеження, що можуть вплинути на оцінки ризиків;
- ролі та відповідальність;
- способи збору, обробки та передачі інформації про оцінку ризиків у межах організації;
- методи проведення оцінки ризиків у організації;
- частоту проведення оцінки ризиків;
- способи отримання інформації про загрози (джерела та методи).

3. На **етапі реагування на ризик** організація виконує такі роботи:

- розроблення можливих планів реагування на ризик;
- оцінку можливих планів реагування на ризик;
- визначення планів реагування на ризик, допустимих з погляду ризик-толерантності організації;
- реалізацію прийнятих планів реагування на ризик.

Для забезпечення можливості реагування на ризики організація визначає типи можливої обробки ризиків (прийняття, уникнення, мінімізація, поділ або передача ризику), а також інструменти, технології та методології для розробки планів реагування, способи оцінки планів реагування та методи оповіщення про вжиті заходи реагування в рамках організації та/або зовнішніх контрагентів.

4. На **етапі моніторингу ризиків** вирішуються такі завдання:

- перевірка реалізації прийнятих планів реагування на ризик та виконання нормативних вимог ІБ;
- визначення поточної ефективності заходів реагування на ризики;
- визначення значущих для ризик-менеджменту змін у ІТ-системах та середовищах, включаючи ландшафт загроз, уразливості, бізнес-функції та процеси, архітектуру ІТ-інфраструктури, взаємини з постачальниками, ризик-толерантність організації та ін.

Організації описують методи оцінки нормативної відповідності та ефективності заходів реагування на ризики, а також те, як контролюються зміни, здатні вплинути на ефективність реагування на ризики.

Управління ризиками ведеться на рівнях організації, бізнес-процесів та інформаційних систем, при цьому слід забезпечувати взаємозв'язок та обмін інформацією між даними рівнями з метою безперервного підвищення ефективності здійснюваних дій та комунікації ризиків усім стейкхолдерам. На верхньому рівні (рівні організації) здійснюється ухвалення рішень щодо визначення ризиків, що безпосередньо впливає на процеси, що ведуть на нижчих рівнях (бізнес-процесів та інформаційних систем), а також на фінансування цих процесів.

На рівні організації здійснюються вироблення та впровадження функцій управління, що узгоджуються з бізнес-цілями організації та з нормативними вимогами: створення функції ризик-менеджменту, призначення відповідальних, впровадження стратегії управління ризиками та визначення ризик-толерантності, розробка та реалізація інвестиційних стратегій у ІТ та ІБ.

На рівні бізнес-процесів здійснюються визначення та створення ризик-орієнтованих бізнес-процесів та організаційної архітектури, яка має бути заснована на сегментації, резервуванні ресурсів та відсутності єдиних точок відмови. Крім того, на цьому рівні здійснюється розробка архітектури ІБ, яка забезпечить ефективне виконання вимог ІБ та впровадження всіх необхідних заходів та засобів захисту.

На рівні інформаційних систем слід забезпечити виконання рішень, прийнятих на вищих рівнях, а саме забезпечити управління ризиками ІБ на всіх етапах життєвого циклу систем: ініціалізації, розробки чи придбання, впровадження, використання та виведення з експлуатації. У документі наголошується на важливості стійкості (resilience) ІТ-систем, яка є показником життєздатності бізнес-функцій компанії.

Зазначимо, що у додатку «Н» до аналізованого документа наводиться опис кожного із способів обробки ризиків, перелічених у етапі реагування ризик. Так, зазначено, що в організації повинна існувати як загальна стратегія вибору конкретного способу обробки ризику в тій чи іншій ситуації, так і окремі стратегії кожного способу обробки ризиків. Вказано **основні принципи вибору того чи іншого підходу до обробки ризиків**:

- прийняття (acceptance) ризику має суперечити обраної стратегії ризик-толерантності організації та її можливості відповідати за можливі наслідки прийнятого ризику;
- уникнення (avoidance) ризику є найчастіше найнадійнішим способом обробки ризиків, проте може йти врозріз з бажанням компанії широко застосовувати ІТ-системи та технології, тому рекомендованим підходом є доцільний та всебічно зважений вибір конкретних технологій та ІТ-сервісів;
- поділ (share) та передача (transfer) ризиків – це відповідно частковий або повний поділ відповідальності за наслідки реалізованого ризику з внутрішнім або зовнішнім партнером відповідно до прийнятої стратегії, кінцева мета якої – успішність бізнес-процесів та місії організації;

– мінімізація (або пом'якшення) (mitigation) ризиків передбачає застосування стратегії мінімізації ризиків ІБ на всіх трьох рівнях організації та безпосереднє залучення систем ІБ для пом'якшення можливих наслідків реалізації ризиків. Організації слід вибудовувати бізнес-процеси відповідно до принципів захисту інформації, архітектурні рішення повинні підтримувати можливість ефективної мінімізації ризиків, мінімізація ризиків у конкретних системах має бути реалізована із застосуванням засобів та систем захисту інформації, а політики, процеси та засоби ІБ мають бути досить універсальними та гнучкими для застосування їх у динамічному та різнорідному середовищі організації, з урахуванням безперервно мінливого ландшафту загроз ІБ.

У документі також приділено велику увагу організаційній культурі та довірі постачальникам/контрагентам як факторам успішного управління ризиками. Зокрема, йдеться, що організаційна культура і топ-менеджери компанії безпосередньо впливають на обрані рішення з обробки ризиків, тому загальна стратегія ризик-менеджменту повинна враховувати ризик-апетит компанії і відображати способи управління ризиками, що реально практикуються. Моделі побудови довіри з контрагентами і постачальниками описані в додатку «G» стандарту: перераховані моделі, що базуються на перевірках контрагентів (наприклад, шляхом проведення аудитів), на довірі, що історично склалася (коли за багаторічну історію взаємовідносин контрагент не допускав порушень), на довірі третій стороні (яка проводить незалежну оцінку контрагентів), на мандатній довірі (у разі, коли регуляторними нормами встановлюються вимоги довірі такому постачальнику), і навіть гібридна модель.

2.6 NIST SP 800-37

Тепер перейдемо до документа **NIST SP 800-37 «Risk Management Framework for Information Systems and Organizations»: «Фреймворк управління ризиками для інформаційних систем та організацій: життєвий цикл систем для забезпечення безпеки та конфіденційності»).**

Актуальний документ має ревізію №2 і був оновлений у грудні 2018 для того, щоб врахувати сучасний ландшафт загроз та акцентувати увагу на важливості управління ризиками на рівні керівників компаній, підкреслити зв'язок між **фреймворком управління ризиками (Risk Management Framework, RMF**) та **фреймворком кібербезпеки (Cybersecurity Framework, CSF)**, вказати на важливість інтеграції **процесів керування конфіденційністю (англ. privacy)** та **управління ризиками ланцюжків поставок (англ. supply chain risk management, SCRM)**, а також логічно пов'язати список запропонованих **заходів захисту (контролів, англ. controls)** з документом NIST SP 800-53. Крім цього, виконання положень NIST SP 800-37 можна використовувати за необхідності провести взаємну оцінку процедур ризик-менеджменту компаній у випадках, коли цим компаніям потрібно обмінюватись даними або ресурсами. За аналогією з NIST SP 800-39 розглядається управління ризиками на рівнях організації, місії, інформаційних систем.

У NIST SP 800-37 зазначено, що Risk Management Framework (RMF) в цілому вказує на важливість розробки та впровадження можливостей щодо

забезпечення безпеки та конфіденційності в ІТ-системах протягом усього **життєвого циклу (SDLC)**, безперервної підтримки ситуаційної обізнаності про стан захисту ІТ-систем із застосуванням процесів **безперервного моніторингу (continuous monitoring, CM)** та надання інформації керівництву для прийняття зважених ризик-орієнтованих рішень. У **RMF виділено такі типи ризиків**:

– програмний ризик;
– ризик невідповідності законодавству;
– фінансовий ризик;
– юридичний ризик;
– бізнес-ризик;
– політичний ризик;
– ризик безпеки та конфіденційності (включаючи ризик ланцюжка поставок);
– проектний ризик;
– репутаційний ризик;
– ризик безпеки життєдіяльності;
– ризик стратегічного планування.

Крім цього, **Risk Management Framework**:

- надає повторюваний процес для ризик-орієнтованого захисту інформації та інформаційних систем;
- наголошує на важливості підготовчих заходів для управління безпекою та конфіденційністю;
- забезпечує категоризацію інформації та інформаційних систем, а також вибору, впровадження, оцінки та моніторингу засобів захисту;
- пропонує використовувати засоби автоматизації для управління ризиками та заходами захисту у режимі, близькому до реального часу, а також актуальні тимчасові метрики для надання інформації керівництву для прийняття рішень;
- пов'язує процеси ризик-менеджменту на різних рівнях та вказує на важливість вибору відповідальних за вживання захисних заходів.

У документі вказано **7 етапів застосування RMF**:

1. Підготовка, тобто, визначення цілей та їхня пріоритизація з точки зору організації та ІТ-систем.
2. Категоризація систем та інформації на основі аналізу можливого негативного впливу внаслідок втрати інформації (крім негативного впливу, NIST SP 800-30 також вказує ще 3 фактори ризику, що враховуються при проведенні оцінки ризику: загрози, уразливість, ймовірність події).
3. Вибір базового набору заходів захисту та їх уточнення (адаптація) зниження ризику до прийнятного рівня з урахуванням оцінки ризику.
4. Впровадження заходів захисту та опис того, як саме застосовуються заходи захисту.
5. Оцінка впроваджених заходів захисту для визначення коректності їх застосування, працездатності та продукування ними результатів, що відповідають вимогам безпеки та конфіденційності.

6. Авторизація систем або заходів захисту на основі висновку щодо прийнятності ризиків.

7. Безперервний моніторинг систем та застосованих заходів захисту для оцінки ефективності застосованих заходів, документування змін, проведення оцінки ризиків та аналізу негативного впливу, створення звітності щодо стану безпеки та конфіденційності.

Далі у публікації NIST SP 800-37 перераховуються завдання, які слід виконати кожному з етапів застосування RMF. Для кожного із завдань вказується назва задачі (контролю), перераховуються вхідні та вихідні (результуючі) дані процесу з прив'язкою до категорій відповідних контролів CSF, наводиться список відповідальних та допоміжних ролей, додатковий опис задачі, а також при необхідності даються посилання на пов'язані документи NIST.

Далі перерахуємо завдання для кожного з етапів застосування RMF.

Завдання етапу «**Підготовка**» на **рівні організації** включають:

- визначення ролей управління ризиками;
- створення стратегії управління ризиками, з урахуванням ризик-толерантності організації;
- проведення оцінки ризиків;
- вибір цільових значень заходів захисту та/або профілів із документа Cybersecurity Framework;
- визначення для ІТ-систем загальних заходів захисту, які можуть бути успадковані з більш високих рівнів (наприклад, з рівня організації чи бізнес-процесів)
- пріоритизацію ІТ-систем;
- розробку та впровадження стратегії безперервного моніторингу ефективності заходів захисту.

Завдання етапу «**Підготовка**» на **рівні ІТ-систем** включають:

- визначення бізнес-функцій та процесів, які підтримує кожна ІТ-система;
- ідентифікацію осіб (стейкхолдерів), зацікавлених у створенні, впровадженні, оцінці, функціонуванні, підтримці, виведенні з експлуатації систем;
- визначення активів, які потребують захисту;
- визначення межі авторизації для системи;
- виявлення типів інформації, що обробляються/передаються/зберігаються в системі;
- ідентифікацію та аналіз життєвого циклу всіх типів інформації, що обробляються/передаються/зберігаються в системі;
- проведення оцінки ризиків на рівні ІТ-систем та оновлення списку результатів оцінки;
- визначення вимог щодо безпеки та конфіденційності для систем та середовищ функціонування;
- визначення розташування систем у загальній архітектурі компанії;
- розподіл точок застосування вимог щодо безпеки та конфіденційності для систем та середовищ функціонування;

– формальну реєстрацію ІТ-систем у відповідних департаментах та документах.

Завдання етапу «**Категоризація**» включають:

– документування параметрів системи;

– категоризацію системи та документування результатів категоризації за вимогами безпеки;

– перегляд та узгодження результатів та рішень щодо категоризації за вимогами безпеки.

Завдання етапу «**Вибір набору заходів захисту**» включають:

– вибір заходів захисту для системи та середовища її функціонування;

– уточнення (адаптація) обраних заходів захисту для системи та середовища її функціонування;

– розподіл точок застосування заходів забезпечення безпеки та конфіденційності до системи та середовища її функціонування;

– документування запланованих заходів забезпечення безпеки та конфіденційності системи та середовища її функціонування у відповідних планах;

– створення та впровадження стратегії моніторингу ефективності вживаних заходів захисту, яка логічно пов'язана із загальною організаційною стратегією моніторингу та доповнює її;

– перегляд та узгодження планів забезпечення безпеки та конфіденційності системи та середовища її функціонування.

Завдання етапу «**Впровадження заходів захисту**» включають:

– впровадження заходів захисту відповідно до планів забезпечення безпеки та конфіденційності;

– документування змін до запланованих заходів захисту постфактум, виходячи з реального результату впровадження.

Завдання етапу «**Оцінка впроваджених заходів захисту**» включають:

– вибір оцінювача або команди з оцінки, відповідних типу оцінки, що проводиться;

– розроблення, перегляд та узгодження планів щодо оцінки впроваджених заходів захисту;

– проведення оцінки заходів захисту відповідно до процедур оцінки, описаних у планах оцінки;

– підготовку звітів з оцінки, що містять знайдені недоліки та рекомендації щодо їх усунення;

– виконання коригувальних дій із заходами захисту та переоцінку відкоригованих заходів;

– підготовку плану дій на підставі знайдених недоліків та рекомендації зі звітів з оцінки.

Завдання етапу «**Авторизація**» включають:

– збір авторизаційного пакета документів та відправлення його відповідальній особі на авторизацію;

– аналіз та визначення ризику використання системи або застосування заходів захисту;

– визначення та впровадження кращого плану дій при реагуванні на виявлений ризик;

– визначення прийнятності ризику використання системи чи застосування заходів захисту;

– повідомлення про результати авторизації та про будь-яку нестачу заходів захисту, що становить значний ризик для безпеки або конфіденційності.

Завдання етапу «**Безперервний моніторинг**» включають:

– моніторинг інформаційної системи та середовища її функціонування на наявність змін, що впливають на стан безпеки та конфіденційності системи;

– оцінку заходів захисту відповідно до стратегії безперервного моніторингу;

– реагування на ризик на основі результатів безперервного моніторингу, оцінки ризику, плану дій;

– оновлення планів, звітів щодо оцінки, планів дій на підставі результатів безперервного моніторингу;

– повідомлення про стан безпеки та конфіденційності системи відповідній посадовці відповідно до стратегії безперервного моніторингу;

– перегляд стану безпеки та конфіденційності системи для визначення прийнятності ризику;

– розробку стратегії виведення системи з експлуатації та виконання відповідних дій після закінчення терміну її служби.

2.7 NIST SP 800-30

Спеціальна публікація **NIST SP 800-30 Guide for Conducting Risk Assessments (Посібник з проведення оцінок ризику)** присвячена процедурі проведення оцінки ризику, яка є фундаментальним компонентом процесу управління ризиком в організації відповідно до NIST SP 800-39, поряд з визначенням, обробкою та моніторингом ризиків. Процедури оцінки ризиків використовуються для ідентифікації, оцінки та пріорітизації ризиків, що породжуються використанням інформаційних систем, для операційної діяльності організації, її активів та працівників. **Цілями оцінки ризиків** є інформування осіб, які приймають рішення, та підтримка процесу реагування на ризик шляхом ідентифікації:

– актуальних загроз як самої організації, і опосередковано іншим організаціям;

– внутрішніх та зовнішніх уразливостей;

– потенційних збитків організації з урахуванням можливостей експлуатації вразливостей загрозами;

– ймовірності виникнення цієї шкоди.

Кінцевим наслідком є обчислення детермінанти (значення) ризику, тобто, функції від розміру шкоди та ймовірності виникнення шкоди. **Оцінку ризику можна проводити на всіх трьох рівнях управління ризиками** (рівні організації, місії, інформаційних систем) за аналогією з підходом, що

застосовується в NIST SP 800-39 та NIST SP 800-37. Наголошується, що **оцінка ризиків** – це безперервний процес, що стосується всіх рівнів управління ризиками в організації, а також вимагає включення в **життєвий цикл розробки систем (SDLC)** і проводиться з частотою, адекватною цілям і обсягу оцінки.

Процес оцінки ризиків включає:

- підготовку до оцінки ризиків;
- проведення оцінки ризиків;
- комунікування результатів оцінки та передачу інформації всередині організації;
- підтримка досягнутих результатів.

У документі йдеться про важливість складання методології оцінки ризику, що розробляється організацією на етапі визначення ризиків. Вказано, що організація може вибрати одну або кілька методологій оцінки ризику, залежно від наявних ресурсів, фази SDLC, складності та зрілості бізнес-процесів, критичності/важливості інформації, що обробляється. При цьому створенням коректної методології організація підвищує якість і відтворюваність оцінок ризику, що реалізуються.

Методологія оцінки ризику зазвичай включає:

- опис процесу оцінки ризику;
- модель ризиків, що описує оцінювані фактори ризику та взаємозв'язку між ними;
- спосіб оцінки ризиків (наприклад, якісний або кількісний), що описує значення, які можуть набувати факторів ризику, і те, як комбінації цих факторів можуть бути оброблені;
- спосіб аналізу (наприклад, загрозливо-центричний, орієнтований на активи чи вразливості), що описує, як ідентифікуються та аналізуються комбінації факторів ризику.

Модель ризиків описує оцінювані фактори ризику та взаємозв'язку між ними. **Фактори ризику** – це характеристики, які використовуються в моделях ризику як вхідні дані для визначення рівнів ризиків при проведенні оцінки ризиків. Крім цього, фактори ризику використовуються при комунікуванні ризиків для виділення тих факторів, які відчутно впливають на рівні ризиків у певних ситуаціях та контекстах. **Типові фактори ризику** включають:

- загрози;
- вразливості;
- негативний вплив;
- ймовірність;
- попередні умови.

При цьому деякі фактори ризику можуть бути декомпозовані до більш детальних характеристик, наприклад, загрози можна декомпозувати до **джерел загроз (англ. threat sources)** та **подій загроз (англ. threat events).**

Загроза – це будь-яка обставина чи подія, що має потенціал негативного впливу на бізнес-процеси чи активи, співробітників, інші організації шляхом здійснення несанкціонованого доступу, руйнування, розголошення чи

модифікації інформації та/або відмови в обслуговуванні. Події загроз породжуються джерелами загроз. **Джерелом загроз** може бути навмисна дія, спрямована на експлуатацію вразливості, або ненавмисну дію, внаслідок якої вразливість була проексплуатована випадково. В цілому, **типи джерел загроз** включають:

- ворожі кібератаки чи фізичні атаки;
- людські помилки;
- структурні помилки в активах, підконтрольних організації;
- природні чи техногенні аварії чи катастрофи.

Детальність визначення подій загроз залежить від глибини побудови моделі ризиків. У разі детального розгляду моделі ризиків можна будувати сценарії загроз, які є набором з кількох подій загроз, що призводять до негативних ефектів, атрибутованих до певного джерела загроз (або кількох джерел) та впорядкованих за часом; при цьому розглядається потенційна ймовірність послідовної експлуатації кількох уразливостей, що призводить до успішної реалізації атаки. Події загроз у кібер- або фізичних атаках характеризуються набором **тактик, технік та процедур (англ. tactics, techniques, and procedures, TTPs),** про які ми вже говорили раніше.

Розглянутий документ також говорить про таке поняття, як «**зміщення загрози**» (англ. threat shifting), під яким розуміється зміна атакуючими своїх TTPs залежно від заходів захисту, вжитих компанією та виявлених атакуючими. Зміщення загрози може бути здійснено в тимчасовому домені (наприклад, спроби атакувати в інший час або розтягнути атаку в часі), цільовому домені (наприклад, вибір менш захищеної цілі), ресурсному домені (наприклад, використання атакуючими додаткових ресурсів для злому цілі), домені планування або методу атаки (наприклад, використання іншого інструментарію хакера або спроби атакувати іншими методами). Крім цього, підкреслюється, що атакуючі часто воліють шлях найменшого опору задля досягнення своєї цілі, тобто, вибирають найслабшу ланку в ланцюзі захисту.

Вразливість – це слабкість в інформаційній системі, процедурах забезпечення безпеки, внутрішніх способах захисту або особливостях конкретної реалізації/впровадження тієї чи іншої технології чи системи. Уразливість характеризується своєю небезпекою у тих розрахункової важливості її виправлення; при цьому небезпека може бути визначена залежно від очікуваного негативного ефекту експлуатації цієї вразливості. Більшість уразливостей в інформаційних системах організації виникають або через не застосовані (випадково чи навмисно) заходи ІБ, або застосовані невірно. Важливо також пам'ятати і про еволюцію загроз і самих систем, що захищаються – і в тих, і в інших згодом відбуваються зміни, які слід враховувати при проведенні переоцінки ризиків. Крім уразливостей технічного характеру в IT-системах,

Попередня умова (англ. predisposing condition) у контексті оцінки ризиків – це умова, що існує в бізнес-процесі, архітектурі або IT-системі, що впливає (знижує або збільшує) на ймовірність заподіяння шкоди загрозою. Логічними синонімами будуть терміни «схильність» (англ. susceptibility) або

«відкритість» (англ. exposure) ризику, що означають, що вразливість може бути проексплуатована загрозою заподіяння шкоди. Наприклад, SQL-сервер потенційно схильний до вразливості SQL-ін'єкції. Окрім технічних попередніх умов, слід враховувати і організаційні: так, місце розташування офісу в низині збільшує ризик підтоплення, а відсутність комунікації між співробітниками під час розробки IT-системи збільшує ризик її злому надалі.

Ймовірність виникнення загрози (англ. likelihood of occurrence) – фактор ризику, що розраховується на основі аналізу ймовірності того, що певна вразливість (або група вразливостей) може бути проексплуатована певною загрозою, з урахуванням ймовірності того, що загроза завдасть реальної шкоди. Для навмисних загроз оцінка ймовірності виникнення зазвичай оцінюється на підставі намірів, можливостей та цілей зловмисника. Для ненавмисних загроз оцінка ймовірності виникнення, як правило, залежить від емпіричних та історичних даних. При цьому можливість виникнення оцінюється на певну часову перспективу – наприклад, на наступний рік або на звітний період. У разі, якщо загроза практично повністю буде ініційована або реалізована протягом певного часового періоду, в оцінці ризиків слід враховувати очікувану частоту її. При оцінці ймовірності виникнення загрози слід враховувати стан управління та бізнес-процесів організації, попередні умови, наявність та ефективність існуючих заходів захисту. Імовірність негативного впливу означає можливість того, що при реалізації загрози буде завдано будь-якої шкоди, незалежно від її величини.

При **визначенні загальної ймовірності виникнення подій загроз** можна використовувати такі три етапи:

1. Оцінка ймовірності того, що подія загрози буде кимось ініційована (у разі навмисної загрози) або станеться сама (у разі ненавмисної).
2. Оцінка ймовірності того, що загроза, що виникла, призведе до шкоди або завдасть шкоди організації, активам, співробітникам.
3. Загальна можливість розраховується як комбінація перших двох отриманих оцінок.

Окрім цього підходу, у документі дається рекомендація не шукати абсолютно всіх взаємопов'язаних загроз і вразливостей, а сконцентруватися на тих з них, які дійсно можуть бути використані в атаках, а також на бізнес-процесах та функціях з недостатніми заходами захисту.

Рівень негативного впливу (англ. impact) події загрози – це величина шкоди, яка очікується від несанкціонованого розголошення, доступу, зміни, втрати інформації чи недоступності інформаційних систем. Організації явно визначають:

1. Процес, який використовується визначення негативного впливу.
2. Припущення, що використовуються визначення негативного впливу.
3. Джерела та методи отримання інформації про негативний вплив.
4. Логічне обґрунтування, використане визначення негативного впливу.

Крім цього, при розрахунку негативного впливу організації повинні враховувати цінність активів та інформації: можна використовувати прийняту в

компанії систему категорування інформації за рівнем значущості або результати оцінок негативного впливу на конфіденційність (Privacy Impact Assessments).

При оцінці ризиків важливим фактором є **ступінь неточності** (англ. uncertainty), що виникає через наступні, загалом, природні обмеження, такі як неможливість з точністю спрогнозувати майбутні події; недостатні наявні відомості про загрози; невідомі вразливості; нерозпізнані взаємозалежності.

З урахуванням вищесказаного **модель ризику** можна описати як наступну логічну структуру:

джерело загрози (з певними характеристиками) з певною *часткою ймовірності* ініціює *подію загрози*, яка *експлуатує вразливість* (що має певну частку небезпеки, з урахуванням попередніх умов та успішного обходу захисних заходів), внаслідок чого створюється *негативний вплив* (з певною величиною ризику як функції від розміру шкоди та ймовірності) виникнення шкоди), що породжує *ризик*.

Документ дає також рекомендації щодо використання процесу **агрегування ризиків** (англ. risk aggregation) з метою об'єднання кількох роз'єднаних або низькорівневих ризиків в один загальніший: наприклад, ризики окремих IT-систем можуть бути агреговані в загальний ризик для всієї підтримуваної ними бізнес-системи. При такому об'єднанні слід враховувати, що деякі ризики можуть реалізовуватися одночасно чи частіше, ніж це прогнозувалося. Також слід враховувати взаємозв'язки між роз'єднаними ризиками і об'єднувати їх, або, навпаки, роз'єднувати.

У NIST SP 800-30 також описані основні **способи оцінки ризиків**: кількісний (англ. quantitative), якісний (англ. qualitative) та напівкількісний (англ. semi-quantitative).

Кількісний аналіз оперує конкретними цифрами (вартістю, часом простою, витратами тощо) і найкраще підходить для проведення аналізу вигод та витрат (англ. Cost-benefit analysis), проте є досить ресурсомістким.

Якісний аналіз застосовує описові характеристики (наприклад, високий, середній, низький), що може призвести до некоректних висновків через малу кількість можливих оцінок та суб'єктивність їх виставлення.

Напівкількісний спосіб є проміжним варіантом, що пропонує використовувати більший діапазон можливих оцінок (наприклад, за шкалою від 1 до 10) для більш точної оцінки та аналізу результатів порівняння. Застосування конкретного способу оцінки ризиків залежить як від сфери діяльності організації (наприклад, у банківській сфері може застосовуватися суворіший кількісний аналіз), так і від стадії життєвого циклу системи (наприклад, на початкових етапах циклу може проводитися лише якісна оцінка ризиків, а на більш зрілих) – вже кількісна).

Нарешті, у документі також описано три основні **способи аналізу** факторів ризиків: загрозливо-центричний (англ. threat-oriented), орієнтований на активи (англ. asset/impact-oriented) або вразливість (англ. vulnerability-oriented).

Загрозо-центричний спосіб сфокусований на створенні сценаріїв загроз та починається з визначення джерел загроз та подій загроз; далі, вразливості

ідентифікуються у тих загроз, а негативний вплив пов'язують із намірами зловмисника.

Спосіб, **орієнтований на активи**, передбачає виявлення подій загроз і джерел загроз, здатних вплинути на активи; на чільне місце ставиться потенційний збиток активам.

Застосування способу, **орієнтованого на вразливість**, починається з аналізу набору попередніх умов та недоліків/слабкостей, які можуть бути проексплуатовані; далі визначаються можливі події загроз та наслідки експлуатації ними знайдених уразливостей. Документ містить рекомендації щодо комбінування описаних способів аналізу для отримання більш об'єктивної картини загроз при оцінці ризиків.

Отже, як ми вже вказали вище, NIST SP 800-30 **процес оцінки ризиків** розбивається на 4 кроки:

- підготовка до оцінки ризиків;
- проведення оцінки ризиків;
- комунікування результатів оцінки та передача інформації всередині організації;
- підтримка досягнутих результатів.

Розглянемо докладніше завдання, які виконуються на кожному з етапів.

1. Підготовка до оцінки ризиків

У межах підготовки до оцінки ризиків виконуються такі:

1.1. Ідентифікація цілі оцінки ризиків: яка інформація очікується в результаті оцінки, які рішення будуть продиктовані результатом оцінки.

1.2. Ідентифікація області (англ. scope) оцінки ризиків у контексті застосування до конкретної організації, тимчасового проміжку, відомостей про архітектуру та технології, що використовуються.

1.3. Ідентифікація специфічних припущень та обмежень, з урахуванням яких проводиться оцінка ризиків. В рамках цього завдання визначаються припущення та обмеження в таких елементах, як джерела загроз, події загроз, уразливості, попередні умови, ймовірність виникнення, негативний вплив, ризик-толерантність та рівень неточності, а також обраний спосіб аналізу.

1.4. Ідентифікація джерел попередньої інформації, джерел загроз та вразливостей, а також інформації про негативний вплив, яка використовуватиметься для оцінки ризиків. У цьому процесі джерела інформації можуть бути як внутрішніми (такими, як звіти щодо інцидентів та аудитів, журнали безпеки та результати моніторингу), так і зовнішніми (наприклад, звіти CERTів, результати досліджень та інша загальнодоступна релевантна інформація).

1.5. Ідентифікація моделі ризиків, способу оцінки ризиків та підходу до аналізу, які використовуватимуться в оцінці ризиків.

2. Проведення оцінки ризиків

У межах оцінки ризиків виконуються такі:

2.1. Ідентифікація та характеризування актуальних джерел загроз, включаючи можливості, наміри та цілі навмисних загроз, а також можливі ефекти від ненавмисних загроз.

2.2. Ідентифікація потенційних подій загроз, релевантності цих подій та джерел загроз, які можуть ініціювати події загроз.

2.3. Ідентифікація вразливостей та попередніх умов, які впливають на ймовірність того, що актуальні події загроз призведуть до негативного впливу. Її метою є визначення того, наскільки аналізовані бізнес-процеси та інформаційні системи вразливі перед ідентифікованими раніше джерелами загроз та наскільки ідентифіковані події загроз дійсно можуть бути ініційовані цими джерелами загроз.

2.4. Визначення ймовірності того, що актуальні події загроз призведуть до негативного впливу, з урахуванням характеристик джерел загроз, уразливостей та попередніх умов, а також схильності організації до цих загроз, беручи до уваги впроваджені заходи захисту.

2.5. Визначення негативного впливу, породженого джерелами загроз, з урахуванням характеристик джерел загроз, уразливостей та попередніх умов, а також схильності організації до цих загроз, беручи до уваги впроваджені заходи захисту.

2.6. Визначення ризику від реалізації актуальних подій загроз, беручи до уваги рівень негативного впливу від цих подій та ймовірність настання цих подій. У Додатку «І» до цього стандарту наведено таблицю І-2 для розрахунку рівня ризику залежно від рівнів ймовірності та негативного впливу.

3. Комунікування результатів оцінки ризиків та передачі інформації

У рамках комунікування результатів оцінки ризиків та передачі інформації виконуються такі завдання:

3.1. Комунікування результатів оцінки ризиків особам, які приймають рішення, для реагування на ризики.

3.2. Передача заінтересованим особам інформації щодо ризиків, виявлених в результаті оцінки.

4. Підтримка досягнутих результатів

У межах підтримки досягнутих результатів виконуються такі задачі:

4.1. Проведення безперервного моніторингу факторів ризику, які впливають на ризики в операційній діяльності організації, її активи, співробітників, інші організації. Цю задачу присвячено стандарт NIST SP 800-137, який ми розглянемо далі.

4.2. Актуалізація оцінки ризиків з використанням результатів безперервного моніторингу факторів ризику.

Як бачимо, документ NIST SP 800-30 пропонує досить детальний підхід до моделювання загроз та розрахунку ризиків. Цінними є також додатки до цього стандарту, що містять приклади розрахунків по кожній із підзадач оцінки ризиків, а також переліки можливих джерел загроз, подій загроз, уразливостей та попередніх умов.

2.8 NIST SP 800-137

Перейдемо тепер до огляду документа **NIST SP 800-137 «Information Security Continuous Monitoring for Federal Information Systems and Organizations» («Безперервний моніторинг інформаційної безпеки для федеральних інформаційних систем та організацій»).**

Завданням побудови стратегії безперервного моніторингу інформаційної безпеки є оцінка ефективності заходів захисту та статусу безпеки систем з метою реагування на виклики, що постійно змінюються, та завдання у сфері інформаційної безпеки. Система безперервного моніторингу ІБ допомагає надавати ситуаційну поінформованість про стан безпеки інформаційних систем компанії на підставі інформації, зібраної з різних ресурсів (таких як активи, процеси, технології, співробітники), а також наявні можливості щодо реагування на зміни ситуації. Ця система є однією з тактик у загальній стратегії управління ризиками.

Як і інші документи серії SP, у цій публікації наведено рекомендований **процесний підхід до вибудовування системи моніторингу ІБ**, що складається з:

- визначення стратегії безперервного моніторингу ІБ (включає в себе вибудовування стратегії на рівні організації, бізнес-процесів та інформаційних систем; призначення ролей та відповідальних; вибір тестового набору систем для збору даних);
- розробки програми безперервного моніторингу ІБ (включає визначення метрик для оцінки та контролю; вибір частоти проведення моніторингу та оцінки; розробку архітектури системи моніторингу);
- запровадження програми безперервного моніторингу ІБ;
- аналізу знайдених недоліків та звіту про них (включає аналіз даних; звітність з оцінки заходів захисту; звітність з моніторингу статусу захисту);
- реагування на виявлені недоліки;
- перегляду та оновлення стратегії та програми безперервного моніторингу ІБ.

У документі також надаються такі рекомендації щодо **вибору інструментів** забезпечення безперервного моніторингу ІБ:

- підтримка ними великої кількості джерел;
- використання відкритих та загальнодоступних специфікацій (наприклад, SCAP – Security Content Automation Protocol);
- інтеграція з іншим програмним забезпеченням, таким як системи Help Desk, системи управління інвентаризацією та конфігураціями, системами реагування на інциденти;
- підтримка процесу аналізу відповідності застосовним законодавчим нормам;
- гнучкий процес створення звітів, можливість «провалюватися» (англ. drill-down) у глибину даних, що розглядаються;
- підтримка систем Security Information and Event Management (SIEM) та систем візуалізації даних.

2.9 Системи класу Incident Response Platform

Як ми знаємо, на даний момент кількість інцидентів ІБ, особливо у великих компаніях, досить велика, і при реагуванні на них рахунок йде буквально на хвилини. При цьому далеко не всі можуть дозволити собі найняти велику кількість висококласних спеціалістів.

Виникає питання: як допомогти аналітикам ІБ (передусім на L1 та L2) при реагуванні на інциденти та зняти з них рутинне навантаження щодо виконання однотипних операцій?

Уявімо ситуацію, коли SIEM-система показує, що відбувається можлива атака на фінансову систему дистанційного банківського обслуговування. Зловмисники можуть викрасти гроші з рахунків фірми з хвилини на хвилину і після цього повернути кошти буде важко.

Аналітик SOC, побачивши такий інцидент, повинен за сценарієм реагування зібрати великий **обсяг допоміжної інформації:**

– ім'я атакованого сервера;

– назва фінансової системи;

– уточнити прізвище та контактні дані відповідального;

– отримати у нього додаткову інформацію.

Якщо не залишилося сумнівів у тому, що цей інцидент – »бойовий», а не хибнопозитивний, **то аналітику потрібно якнайшвидше**:

– ізолювати атакований сервер від мережі компанії;

– заблокувати скомпрометований обліковий запис,

Як бачимо, завдань – багато, і всі їх слід виконати за суворо відведений нормативами та KPI час, наприклад, за 10 хвилин. І саме тут допоможе нашому аналітику може прийти платформа **Incident Response Platform (IRP) – система автоматизації реагування на інциденти інформаційної безпеки**. Система IRP допомагає:

– виконати ряд рутинних операцій зі збору додаткової інформації;

– здійснити невідкладні дії зі стримування (англ. contain) та усунення (англ. eradicate) загрози;

– відновити (англ. recover) атаковану систему;

– оповістити зацікавлених осіб;

– зібрати та структурувати дані про розслідувані інциденти інформаційної безпеки.

Крім того, IRP дозволяє роботизувати та автоматизувати однотипні дії оператора-фахівця ІБ, які він робить при реагуванні на інциденти інформаційної безпеки, що допомагає знизити навантаження співробітника щодо виконання рутинних операцій. Давайте докладніше зупинимося на задачах реагування на інциденти інформаційної безпеки, що виконуються системами IRP.

Процеси реагування на інциденти ІБ

Для того, щоб зрозуміти, як і де коректно застосовувати та впроваджувати системи IRP, нам слід побачити процес реагування на інциденти інформаційної безпеки загалом та подумати, як можна його автоматизувати. Для цього звернімося до документа **NIST SP 800-61 «Computer Security Incident Handling**

Guide» («Посібник з обробки інцидентів комп'ютерної безпеки»). Відповідно до нього, **реагування на інциденти ІБ** складається з кількох взаємопов'язаних процесів:

1. Підготовка
2. Детектування
3. Аналіз
4. Стримування/локалізація
5. Усунення
6. Відновлення
7. Пост-інцидентні дії

Розглянемо ці процеси докладніше у тих застосування IRP-систем їх автоматизації.

1. Підготовка

Етап підготовки є попереднім та одним із ключових. На даному етапі слід зробити всю організаційну роботу, щоб дії команди реагування на інциденти ІБ були документально підтверджені та узгоджені. Політики, процедури та інструкції з реагування повинні бути максимально чіткими, докладними та зручними, щоб у разі високопріоритетного інциденту у аналітиків команди реагування було чітке розуміння того, що слід зробити в тій чи іншій ситуації. Слід регулярно проводити тренування з відпрацювання кроків, визначених у написаних документах, а також навчати персонал компанії та команду реагування коректним технічним та організаційним діям під час інциденту.

На етапі підготовки також створюються та налаштовуються playbooks або runbooks – сценарії реагування, відповідно до яких команда реагування та IRP-система будуть робити заздалегідь задані дії в залежності від деталей інциденту. Наприклад, у разі настання високопріоритетного інциденту ІБ на особливо критичній системі відповідно до playbook, член групи реагування повинен зв'язатися з керівником та відповідальною за систему особою, а IRP-платформа повинна дати команду на ізоляцію цієї системи від мережі компанії для проведення подальших розглядів.

Крім того, на етапі підготовки слід забезпечити групу реагування на інциденти всім необхідним програмним та апаратним забезпеченням (тобто видати ноутбуки, смартфони, встановити на них необхідні утиліти), а також виконати превентивні дії щодо запобігання інцидентам (захистити мережу та пристрої компанії, встановити засоби захисту інформації, провести навчання співробітників основам ІБ). У цей час платформа IRP налаштовується для ефективного застосування: до неї підключаються IT-системи та засоби захисту, з якими належить взаємодіяти при реагуванні на інциденти. Як правило, забезпечують підключення тих систем, які здатні надати фахівцю додаткову інформацію в контексті інциденту, наприклад, відомості про порушених інцидентом користувачів (контактні дані, посада, структурний підрозділ, повноваження) та пристрої (тип операційної системи, встановлене ПЗ, виконувана функція). Крім цього, підключаються і засоби захисту, які в рамках реагування на інцидент виконуватимуть завдання зі стримування та усунення загроз, наприклад, засоби захисту кінцевих точок, міжмережевих екранів та системи управління мережею.

Таким чином, до моменту виникнення інциденту інформаційної безпеки в компанії слід приходити у всеозброєнні: фахівці з реагування та система IRP повинні знаходитись у повній бойовій готовності. Це є запорукою того, що навіть якщо інцидент трапиться, його можна буде швидко локалізувати, і його наслідки не будуть надмірно руйнівними.

2. Детектування

На етапі детектування слід визначити список можливих типів інцидентів ІБ та сформулювати перелік ознак можливих інцидентів. Ознаки можна умовно поділити на прекурсори та індикатори інцидентів інформаційної безпеки:

- *прекурсор* – це ознака того, що інцидент ІБ може статися у майбутньому;
- *індикатор* – це ознака того, що інцидент уже стався або відбувається прямо зараз.

Прикладами прекурсорів інциденту інформаційної безпеки можуть бути зафіксоване інтернет-сканування відкритих портів веб-серверів компанії або виявлення вразливості в IT-системі. Прикладами індикаторів інциденту інформаційної безпеки можуть бути поява повідомлень від засобів захисту (антивіруса, міжмережевого екрану тощо) про можливу атаку, несанкціоноване видалення або модифікація даних, появу помилок та збоїв у роботі IT-систем. Слід уважно ставитися до аномалій у мережевому трафіку: несподівані сплески певного типу трафіку (наприклад, DNS) можуть свідчити про шкідливу активність. Нетипова поведінка користувачів також слід аналізувати: віддалене підключення в неробочий час із незвичайної локації може бути ознакою компрометації облікового запису.

3. Аналіз

Під час етапу аналізу інциденту основне навантаження лягає на досвід і експертизу аналітика – він має прийняти рішення, чи був зафіксований інцидент «бойовим», чи все ж таки це було хибнопозитивне спрацювання. Слід провести ідентифікацію та первинну обробку (тріаж, англ. triage): визначити тип інциденту та категорувати його. Далі визначаються **індикатори копрометації (англ. Indicators of Compromise, IoCs)**, аналізується можливий масштаб інциденту та порушені ним компоненти інфраструктури, проводиться обмежене форензик-обстеження для уточнення типу інциденту та можливих подальших кроків щодо реагування.

На цьому етапі безцінну допомогу надасть IRP-платформа завдяки тому, що вона може надати важливу контекстну інформацію, що стосується інциденту. Наведемо приклад: SIEM-система повідомляє про те, що веб-сервер компанії зазнав атаки, при цьому вразливість, що використовувалася, застосовна тільки до ОС Windows. Аналітик, подивившись у консоль IRP, відразу побачить, що атакований веб-сервер працює на ОС Linux, отже атака не могла бути успішною. Інший приклад: антивірусна система на одному з ноутбуків повідомила про вірусне зараження і про звернення до певних IP-адрес. Аналітик, скориставшись даними IRP-системи, побачить, що аналогічна мережна активність спостерігається і на кількох інших пристроях у мережі компанії, що говорить не про одиничний вірус, а про масоване зараження. Інциденту буде надано більш пріоритетний статус, він буде ескалований відповідно до матриці ескалації, і на його усунення будуть направлені додаткові ресурси. Платформа IRP допоможе

запротоколувати всі дії, виконані в рамках реагування, а також автоматизує дії щодо комунікування та ескалації інциденту.

4. Стримування/локалізація

На етапі стримування (або локалізації) інциденту головним завданням є оперативна мінімізація потенційної шкоди від інциденту ІБ та надання тимчасового вікна для ухвалення рішення щодо усунення загрози. Цього можна досягти, наприклад, оперативно включивши суворіші заборонні правила на міжмережевому екрані для зараженого пристрою, ізолювавши заражений хост від локальної мережі компанії, відключивши частину сервісів та функцій, або, нарешті, повністю вимкнувши заражений пристрій.

На даному етапі використовуються відомості про інцидент, отримані на етапі аналізу, а також дані про те, яку функцію виконує порушений інцидентом ІТ-актив, оскільки, наприклад, вимкнення критично важливого сервера може призвести до істотніших негативних наслідків для компанії, ніж просте перезавантаження некритичного сервісу на ньому. У цій ситуації IRP-платформа знову ж таки підкаже, які функції виконує сервер, як і коли його можна вимикати або ізолювати (за умови, що на етапі підготовки дана інформація була занесена до IRP). Крім цього, у playbooks IRP-системи на етапі підготовки також мають бути закладені сценарії стримування, які застосовуються для кожного конкретного типу інциденту. Наприклад, у випадку DDoS-атаки, можливо, немає сенсу вимикати атаковані сервера, а у разі вірусного зараження усередині одного сегмента мережі можна не ізолювати пристрої в іншому сегменті. На етапі стримування також проводиться аналіз подробиць атаки: яка система була першою атакована, якими тактиками, техніками та процедурами користувалися атакуючі, які командні сервери використовуються в цій атаці і т.д. Вказану інформацію допоможе зібрати IRP-система: інтеграція з **джерелами кіберрозвідки (англ. Threat Intelligence feeds)** та спеціалізованими пошуковими системами (наприклад,VirusTotal, Shodan, Censys і т.д.) дасть більш чітку і збагачену картину інциденту, що відбудеться, що допоможе ефективніше впоратися з ним. У деяких випадках може знадобитися отримати форензик-дані для подальшого проведення комп'ютерної криміналістичної експертизи, і IRP-платформа допоможе зібрати таку інформацію з атакованих пристроїв.

5. Усунення

На етапі усунення інциденту проводяться вже активні дії з видалення загрози з мережі та запобігання повторній атакі: видаляється шкідливе ПЗ, змінюються зламані облікові записи (їх можна тимчасово заблокувати, змінити пароль або, наприклад, перейменувати), встановлюються оновлення та патчі для проексплуатації налаштування засобів захисту (наприклад, для блокування IP-адреси зломщиків). Зазначені дії виконуються для всіх порушених інцидентом сутностей – і для пристроїв, і для облікових записів, і для програм.

Надзвичайно важливо ретельно усунути вразливості, які використовувалися зловмисниками, оскільки найчастіше, успішно зламавши якусь компанію, хакери повертаються в надії використовувати ті самі недоліки її захисту. При виконанні цього процесу платформа IRP дасть необхідні команди засобам захисту і збере дані про всі зачеплені інцидентом пристрої. Таким чином, швидкість реагування на інцидент інформаційної безпеки щодо усунення самої

загрози істотно зростає при використанні IRP-системи, яка буде чудовою підмогою аналітику ІБ.

6. Відновлення

На етапі відновлення слід перевірити надійність вжитих заходів захисту, повернути системи в нормальний режим роботи (business as usual), можливо, відновивши якісь системи з резервних копій або встановивши і налаштувавши їх заново. На даному етапі системи IRP допоможуть не забути всі пристрої і хронологію подій, що брали участь в інциденті, оскільки ці дані зберігаються і накопичуються в IRP протягом усього циклу розслідування інциденту.

7. Пост-інцидентні дії

На етапі пост-інцидентних дій (англ. post-incident activities) слід проаналізувати причини інциденту (англ. root cause analysis) для того, щоб звести до мінімуму ймовірність повторного аналогічного інциденту в майбутньому, а також оцінити коректність та своєчасність дій персоналу та засобів захисту, і, можливо, оптимізувати якісь процедури реагування та політики ІБ. У разі серйозного інциденту слід провести позачергове сканування інфраструктури на наявність уразливостей, пен-тесту та/або позапланового аудиту інформаційної безпеки. Логічно використовувати агреговану базу знань для ведення накопиченого досвіду реагування, що також можна зробити в IRP-платформі, в якій вже зберігається докладна інформація про інциденти ІБ, що відбулися, і про вжиті заходи реагування. У деяких випадках потрібне складання офіційного звіту щодо інциденту, особливо якщо він був серйозним або торкнувся важливих даних. Як бачимо, IRP – це ще й універсальне сховище відомостей про інциденти інформаційної безпеки з можливістю роботизування рутинних дій фахівця з інформаційної безпеки.

Висновки з застосування IRP

Підведемо підсумок. Системи IRP є автоматизованими засобами реагування на інциденти інформаційної безпеки, що реалізують контрзаходи для протидії загрозам інформаційної безпеки відповідно до заздалегідь заданих сценаріїв реагування. Сценарії реагування називаються playbooks або runbooks і є набором автоматизованих завдань з детектування загроз і аномалій в інфраструктурі, реагування і стримування загроз в режимі реального часу. Сценарії реагування діють на основі налаштовуваних правил і типів інцидентів, виконуючи ті чи інші дії в залежності від даних, що надходять із засобів захисту або інформаційних систем. Платформи IRP допомагають проводити структуроване та журнальне реагування на інциденти інформаційної безпеки на підставі правил та політик. Узагальнюючи сказане, можна зробити висновок, що система IRP – це платформа реагування на інциденти кібербезпеки, призначена для захисту інформації шляхом систематизації даних про інциденти інформаційної безпеки та роботизацію дій оператора-аналітика ІБ. Завдяки IRP-платформам команди реагування на інциденти інформаційної безпеки можуть суттєво заощадити час та зусилля при розслідуванні інцидентів ІБ, що підвищує операційну ефективність діяльності департаментів ІБ та SOC-центрів.