**МІНІСТЕРСТВО ОСВІТИ ТА НАУКИ УКРАЇНИ**

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

Навчально-науковий інститут захисту інформації

| | |
|---|---|
| На рецензію | До захисту |
| Завідувач кафедри УІКБ | Завідувач кафедри УІКБ |
| доктор економічних наук, професор | доктор економічних наук, професор |
| _____ С.В. Легомінова | _____ С.В. Легомінова |
| «___» січня 2023 р. | «___» січня 2023 р. |

**КВАЛІФІКАЦІЙНА РОБОТА**

другого магістерського рівня вищої освіти

на тему:

# ПІДХОДИ ДО ОЦІНЮВАННЯ ЕФЕКТИВНОСТІ ПРОЦЕСІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ПІДПРИЄМСТВІ


СТУДЕНТКА: Батуркіна Анастасія Миколаївна _____ (підпис)

КЕРІВНИК: к.в.н., доц. Якименко Юрій Михайлович _____ (підпис)

НОРМОКОНТРОЛЕР: к.держ.упр., доц. Мужанова Тетяна Михайлівна _____ (підпис)


Київ – 2023

**ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ**

**Навчально-науковий інститут захисту інформації**

**Кафедра управління інформаційною та кібернетичною безпекою**

**Спеціальність «Кібербезпека»**

**Спеціалізація «Управління інформаційною безпекою»**

Другого магістерського рівня вищої освіти

«ЗАТВЕРДЖУЮ»
Завідувач кафедри УІКБ
_____ С.В.Легомінова
(підпис)

«___» _____ 2023 р.

**ЗАВДАННЯ на кваліфікаційну роботу**

студентці Батуркіній Анастасії Миколаївні

**1. Тема роботи** «Підходи до оцінювання ефективності процесів інформаційної безпеки на підприємстві», затверджена наказом по університету від "___" _____ 2023 р. № ____.

**2. Термін здачі** студентом оформленої роботи «08» грудня 2022 р.

**3. Об'єкт дослідження:** метрики оцінювання ефективності процесів інформаційної безпеки на підприємстві.

**4. Предмет дослідження:** підходи до оцінювання ефективності процесів інформаційної безпеки**.**

**5. Мета дослідження:** вивчення системи управління інформаційною безпекою на підприємстві.

**6. Перелік питань, які мають бути розроблені:**

1. Проаналізувати вимоги нормативних документів щодо оцінювання ефективності процесів інформаційної безпеки на підприємстві;
2. Проаналізувати практики використання метрик щодо оцінювання ефективності процесів інформаційної безпеки на підприємстві;
3. Провести дослідження і розробити рекомендації щодо використання метрик в оцінюванні ефективності процесів інформаційної безпеки.

**7. Дата видачі завдання** «26» вересня 2022 р.

# КАЛЕНДАРНИЙ ПЛАН

Дата видачі завдання: «26» вересня 2022 р.

| № з/п | Етапи роботи | Термін виконання етапів | Примітка |
|---|---|---|---|
| 1. | Визначення об'єкту, предмету, мети та завдань дослідження. | 26.09.2022 | |
| 2. | Збір та аналіз літератури. | 3.10.2022 | |
| 3. | Розділ 1. Аналіз вимог нормативних документів щодо оцінювання ефективності процесів інформаційної безпеки на підприємстві | 17.10.2022 | |
| 4. | Розділ 2. Аналіз практики використання метрик щодо оцінювання ефективності процесів інформаційної безпеки на підприємстві | 31.10.2022 | |
| 5. | Розділ 3. Дослідження і розробка рекомендацій щодо використання метрик в оцінюванні ефективності процесів інформаційної безпеки | 14.11.2022 | |
| 6. | Формулювання висновків за результатами проведеного дослідження | 01.12.2022 | |
| 7. | Оформлення роботи | 8.12.2022р. | |
| 8. | Оформлення презентації | 15.12.2022р. | |
| 9. | Отримання рецензії на роботу. | 23.12.2022 | |
| 10. | Захист в ДЕК | 17.01.2023 р. | |

Студентка _____ А.М. Батуркіна
(підпис)

Науковий керівник _____ Ю.М. Якименко
(підпис)

# РЕФЕРАТ

Кваліфікаційна робота присвячена дослідженню проблем визначення підходів та безпосередньо метрик оцінювання ефективності процесів інформаційної безпеки на підприємстві. Робота складається зі вступу, трьох розділів, що містять 7 рисунків, висновків та списку використаних джерел, що містить 50 найменувань. Загальний обсяг роботи становить 80 аркушів, з яких 6 аркушів займають перелік умовних скорочень та список використаних джерел.

**Об'єктом дослідження** є метрики оцінювання ефективності процесів інформаційної безпеки на підприємстві.

**Предмет дослідження** - підходи до оцінювання ефективності процесів інформаційної безпеки**.**

**Метою роботи** є дослідження метрик для оцінювання ефективності процесів ІБ на підприємстві. Для цього у роботі використовуються методи аналізу існуючих вимог до оцінювання ефективності процесів ІБ та узагальнення досвіду підприємств щодо використання відповідних метрик.

Як результат у роботі проведено аналіз вимог нормативних документів щодо оцінки ефективності процесів ІБ, зокрема найвідоміших стандартів ; досліджено досвід компаній у використанні різних підходів для оцінки ефективності процесів ІБ; проаналізовані методи оцінювання процесів ІБ, у тому числі використання показників KPI, KRI; проаналізований процес впровадження метрик у СУІБ, окремо розглянуті метрики щодо процесу управління ризиками та інцидентами; розроблено рекомендаційні метрики та показники для підприємства задля оцінки ефективності впроваджених ключових та критичних процесів ІБ.

**Галузь застосування.** Розроблені підходи можуть бути використані при плануванні та реалізації системи управління інформаційною безпекою підприємства у контексті оцінки ефективності впроваджених процесів ІБ.

**Ключові слова:** ІНФОРМАЦІЙНА БЕЗПЕКА ПІДПРИЄМСТВА, ОЦІНКА ЕФЕКТИВНОСТІ, СИСТЕМА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ, ПОКАЗНИКИ, МЕТРИКИ.

**ЗМІСТ**

# ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

ІБ – інформаційна безпека

СУІБ – система управління інформаційною безпекою

ІТ – інформаційні технології

CMMI – Capability Maturity Model Integration

KPI – key performance indicator

KRI – key risk indicator

GRC – governance, risk and compliance.

# ВСТУП

Актуальність теми. Протягом останніх кількох років інтерес до отримання сертифікату ISO 27001 або використання ISO 27001 як найкращої практики швидко зростав. Сьогодні багато компаній, державних установ і муніципалітетів вимагають або сертифікації ISO 27001, або повинні дотримуватися найкращих практик у стандарті. Даний стандарт також все частіше включається в тендерні вимоги або використовується під час закупівель.

Циклічний і ітеративний процес, який ми знаємо як PDCA або Plan-do-Check-Act все ще лежить в основі ISO 27001:2013. Постійне вдосконалення є невід'ємною частиною процесу Plan-do-Check-Act і обов'язковою вимогою ISO 27001:2013.

Організації, які відповідають стандарту ISO 27001:2013, забезпечують постійне вдосконалення своєї системи управління інформаційною безпекою (СУІБ). Пункт 9 стандарту займається конкретно вимірюваннями ефективності СУІБ. У ньому зазначено, що безпосередньо організація визначає і контролює процеси, які буде вимірювати, і повинна описати, як, коли і хто виконує вимірювання. Також необхідно вирішити, хто буде оцінювати результати вимірювань і як це зробити. По суті, потрібно вирішити, чи відповідає результат вимірювань визначеним заздалегідь очікуванням.

Оскільки стандарт не визначає конкретний підхід до вимірювання ефективності впроваджених на підприємстві процесів СУІБ, у роботі пропонується вивчити наявні та актуальні методи оцінювання ефективності процесів СУІБ, а також розглянути метрики оцінювання ефективності на прикладі.

З огляду на зазначене, тема кваліфікаційної роботи є актуальною, а використання її результатів сприятиме підвищенню рівня інформаційної безпеки суб'єктів підприємницької діяльності в умовах інформаційного протиборства.

Мета і завдання дослідження. Мета роботи полягає у дослідженні процесу оцінювання ефективності процесів інформаційної безпеки на підприємстві.

Для досягнення цієї мети в роботі необхідно виконати наступні **завдання**:

1. Проаналізувати вимоги нормативних документів щодо оцінювання ефективності процесів інформаційної безпеки на підприємстві;
2. Дослідити практики використання метрик щодо оцінювання ефективності процесів інформаційної безпеки на підприємстві;
3. Провести дослідження і розробити рекомендації щодо використання метрик в оцінюванні ефективності процесів інформаційної безпеки підприємства.

**Об'єкт дослідження –** метрики оцінювання ефективності процесів інформаційної безпеки на підприємстві.

**Предмет дослідження** – підходи до оцінювання ефективності процесів інформаційної безпеки.

Методи дослідження. Для вирішення означеного вище наукового завдання в роботі використані методи аналізу існуючих вимог до оцінювання ефективності процесів ІБ та узагальнення досвіду підприємств щодо використання відповідних метрик.

Наукова новизна одержаних результатів. Розроблені та наведені в роботі метрики для оцінювання ефективності процесів інформаційної безпеки на підприємстві можуть бути використані при плануванні та реалізації процесу оцінювання ефективності та подальшого вдосконалення процесів на підприємстві.

Практичне значення одержаних результатів. Застосування напрацювань дадуть змогу здійснити обґрунтований вибір методів і засобів оцінювання ефективності процесів інформаційної безпеки на підприємстві.

# РОЗДІЛ 1
# АНАЛІЗ ВИМОГ НОРМАТИВНИХ ДОКУМЕНТІВ ЩОДО ОЦІНЮВАННЯ ЕФЕКТИВНОСТІ ПРОЦЕСІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ПІДПРИЄМСТВІ

## 1.1. Основні вимоги нормативних документів до оцінювання ефективності процесів інформаційної безпеки

Про вимірювання та оцінку ефективності інформаційної безпеки говорять багато стандартів, а саме:

- ISO 27001, ISO 27002
- COBIT
- ITIL
- ISO 13335
- ISO 21827
- GAISP

Поговоримо детальніше про деякі з них та визначимо, що вони нам кажуть про оцінку ефективності в інформаційній безпеці.

Почнемо з ISO 27001, міжнародного стандарту, розробленого Міжнародною організацією з стандартизації та електротехнічною комісією, який надає вимоги до побудови, розвитку та підтримки СУІБ в організації та ефективного управління ризиками ІБ. Ціль СУІБ – визначати та мінімізувати ризики ІБ при роботі з інформацією в рамках існуючих процесів організації так, щоб зберігалась конфіденційність, доступність та цілісність інформації, яка обробляється [1].

**ISO 27001** пропонує Plan, Do, Check, Act (PDCA) методологію прийняття рішень, цикл якої зображений на малюнку 1:


Рис. 1.1. Цикл PDCA

Опис етапів даного циклу:

Планування: фаза створення СУІБ, затвердження політики інформаційної безпеки.

Дія: фаза впровадження контролів ІБ відповідно до затвердженої політики та цілей ІБ.

Перевірка: фаза оцінки й вимірювання продуктивності та ефективності заходів ІБ.

Поліпшення: вживання коригуючих та превентивних заходів відповідно до результатів оцінки ефективності контролів ІБ задля забезпечення постійного вдосконалення СУІБ.

Цей стандарт пропонує методи вимірювання ефективності політики інформаційної безпеки та засобів контролю (Peláez, 2010). Він передбачає реалізацію повного переліку засобів контролю за стандартом ISO 27001. Елементи керування складаються зі змінних, відомих як атрибути, які визначають рівень функціонування цих елементів керування. Стан атрибута контролю можна виміряти за допомогою спеціальних механізмів, деякі з яких включають анкети, інтерв'ю, аудиторські звіти та записи подій.

На основі цих показників створюються ключові показники ефективності (KPI) (Peláez, 2010). Ключові показники ефективності (KPI) — це вимірювання, за допомогою яких можна стежити за зростанням у досягненні важливих цілей у компанії. Можна розробити KPI для всіх видів бізнесу, але тут увага буде зосереджена на KPI, пов'язаних з інформаційною безпекою. Ключові показники ризику (KRI) вимірюють, наскільки ризикованою є діяльність, яка виконується в організації. KRI можна зіставити з KPI, щоб побачити, чи змінилася інтенсивність ризику протягом певного періоду часу. Причина цього зіставлення полягає в аналізі того, як певний KRI або декілька KRI впливають на KPI. Далі визначаються ризики та пропонуються можливі засоби контролю. Нарешті, ефективність політики можна виміряти за допомогою атрибутів. Атрибути допомагають визначити, збільшився чи знизився рівень ризику протягом певного періоду часу.

Як бачимо, дана модель чітко демонструє ідею постійного вдосконалення на основі попередньої перевірки продуктивності СУІБ, так само, як і сам стандарт у пункті 9 "Оцінювання результативності" вимагає регулярного контролю, аналізу та оцінювання результативності СУІБ [1,2].

В рамках цього процесу компанія повинна реалізувати необхідний контроль безпеки і відповідне вимірювання, щоб знизити ризики до прийнятного рівню. Так як багато керівників компаній не розуміють необхідності заходів інформаційної безпеки, отримання ресурсів часто може бути складним завданням, що вимагає значної кількості обґрунтувань, щоб визначити, чи необхідні засоби контролю інформаційної безпеки для бізнесу.

Для того, щоб надати переконливі аргументи керівництву з метою ініціювання програми інформаційної безпеки, співробітники інформаційної безпеки повинні виявити ризики для організаційних процесів і розробити систему вимірювань, здатну визначити ефективність елементів управління, введених згідно з додатком А стандарту ISO 27001 або іншого відповідного стандарту.

Окрім найвідомішого стандарту ISO 27001, слід також згадати NIST SP 800-37 “Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy” («Фреймворк управління ризиками для інформаційних систем та організацій: життєвий цикл систем для забезпечення безпеки та конфіденційності”) [2].

У NIST SP 800-37 зазначено, що Risk Management Framework в цілому вказує на важливість розробки та впровадження можливостей щодо забезпечення безпеки та конфіденційності в IT-системах протягом усього життєвого циклу (SDLC), безперервної підтримки ситуаційної обізнаності про стан захисту IT-систем із застосуванням процесів безперервного моніторингу (англ. 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 [3].

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:

- підготовка, тобто визначення цілей та їхня пріоритизація з точки зору організації та IT-систем;
- категоризація систем та інформації на основі аналізу можливого негативного впливу від 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);
- вибір базового набору заходів захисту та їх уточнення (адаптація) зниження ризику до прийнятного рівня з урахуванням оцінки ризику;
- впровадження заходів захисту та опис того, як саме застосовуються заходи захисту;
- оцінка впроваджених заходів захисту для визначення коректності їх застосування, працездатності та продукування ними результатів, що відповідають вимогам безпеки та конфіденційності;
- авторизація систем або заходів захисту на основі висновку щодо прийнятності ризиків;
- 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 [4].

COBIT (Control Objectives for Information and related Technology) – підхід до управління інформаційними технологіями, створений Асоціацією контролю та аудиту систем (Information Systems Audit and Control Association – ISACA) та Інститутом керівництва IT (IT Governance Institute – ITGI) у 1992 році. Він надає менеджерам, аудиторам та IT користувачам набір затверджених метрик, процесів та найкращих практик з метою допомогти їм у добуванні максимальної вигоди від використання інформаційних технологій та для розробки відповідного керівництва та контролю IT у компанії.

Перша редакція COBIT побачила світ у 1996 році. Версія COBIT 4.1 вийшла у травні 2007 року. В основі COBIT 4.1 лежить процесний підхід, система

збалансованих показників BSC, модель зрілості SEI CMM/CMMI, PMBoK (методологія проектного управління), а також стандарти PRINCE2, TickIT, ITIL® та інші [5].

Ключові галузі управління IT:

- Відповідність стратегії наголошує на зв'язку між планами бізнесу та IT; виявленні, підтримці та контролі за ціннісною пропозицією IT; а також на відповідності IT та бізнес операцій.
- Корисність являє собою реалізацію ціннісної пропозиції, контроль за тим, щоб IT забезпечували певні стратегії переваги, зосередження на оптимізації витрат та підтвердження справжньої цінності IT.
- Управління ресурсами присвячене питанням, пов'язаним з управлінням критичними IT ресурсами, а саме, оптимізацією інвестицій та належним керівництвом додатками, інформацією, інфраструктурою та персоналом. Ключові питання стосуються оптимізації знань та інфраструктури.
- Управління ризиками вимагає поінформованості вищого керівництва у сфері ризиків, чіткого розуміння корпоративного підходу щодо них, відповідності вимогам прозорості щодо істотних ризиків, включення функції чи системи управління ризиками у практику організації.
- Оцінка ефективності є контроль за реалізацією стратегії, результатами проектів, використанням ресурсів, ефективністю процесів і сервісним обслуговуванням. Для цього застосовуються, зокрема, системи збалансованих показників, які перетворюють стратегію на послідовність дій, результати яких вимірюються іншими, порівняно з бухгалтерським обліком, методами.

Концептуальне ядро стандарту COBIT 4.1 сформовано з 34 високорівневих процесів (які покривають близько 200 цілей контролю), згрупованих у 4 домени (сфери діяльності), один з яких Моніторинг та оцінка: якість та відповідність IT процесів вимогам контролю повинні оцінюватися на регулярній основі. Цей домен включає нагляд з боку керівництва за процесами управління в організації,

а також незалежний контроль з боку внутрішніх та зовнішніх аудиторів. Регламентовані процеси:

- ME1 Відстежувати та оцінювати продуктивність IT
- ME2 Відстежувати та оцінювати внутрішні контролі
- ME3 Гарантувати відповідність регулюючим вимогам
- ME4 Забезпечувати керівництво IT [6]

Що стосується нормативних документів України, можна зазначити Положення про здійснення контролю за дотриманням банками вимог законодавства з питань інформаційної безпеки, кіберзахисту та електронних довірчих послуг від 16.01.2021 №4 та положення №95 .

## 1.2. Досвід використання підходів до оцінювання ефективності процесів інформаційної безпеки

Компанії використовують різні підходи до оцінювання ефективності своєї ІБ. Це залежить від масштабу компанії, її бюджету та зрілості ІБ в цілому. Проаналізуємо підходи, які обирають сучасні компанії, щоб оцінити ефективність використаних та обраних заходів безпеки.

Процес управління ефективністю інформаційної безпеки допомагає організації зрозуміти, наскільки добре вона виконує свої цілі інформаційної безпеки. Оскільки звичайні показники керування ефективністю (такі як вартість або дохід) можуть мати меншу релевантність у контексті безпеки, важливо мати методологію оцінки, адаптовану до конкретних потреб безпеки. Ця структура також допомагає організаціям зрозуміти рівень інвестицій (з точки зору фінансового чи людського капіталу), необхідних для створення міцної позиції безпеки, яка допомагає досягти цілей організації.

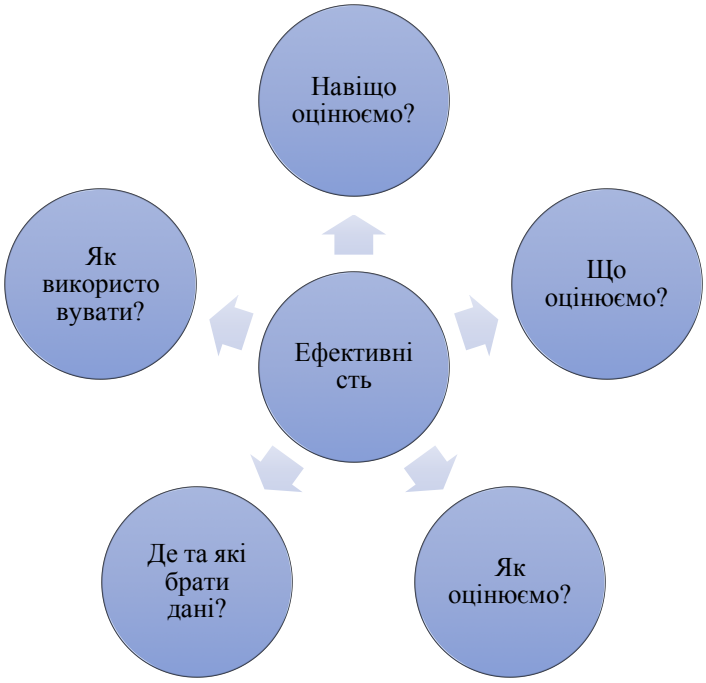


Рис. 1.2. Оцінка ефективності ІБ

Інформаційна безпека сумно відома своєю складністю та постійними змінами. Крім того, що ці атрибути ускладнюють захист ключових активів, вони також ускладнюють точну оцінку ефективності заходів безпеки організації.

Управління продуктивністю інформаційної безпеки намагається вирішити цю проблему, запровадивши структуру, за допомогою якої можна точно оцінити програму інформаційної безпеки. Якщо все зроблено правильно, керування кіберефективністю допоможе вам зрозуміти, де ви слабкі, а де сильні, і які кроки ви можете вжити, щоб покращити ті сфери, де вашій програмі бракує, створивши цілі ефективності інформаційної безпеки [7].

Як правило, програма буде оцінюватися за допомогою ключових показників ефективності, таких як:

- Скільки часу потрібно для виявлення інцидентів безпеки
- Час реагування після виявлення інцидентів
- Кількість інцидентів
- Рівень підготовленості
- Усвідомлення загрози
- Результати навчання безпеки

Розміщення цих показників у контексті також є надзвичайно важливим. Наприклад, організація може успішно виявляти та перешкоджати тисячам атак щодня, що може створити враження високоефективної програми безпеки. Однак глибший розгляд може виявити, що ці атаки нескладні, їх легко запобігти та не становлять жодного ризику для критично важливих активів. Хоча це може створювати зовнішній вигляд успіху програми, набагато небезпечніші ризики можуть вирувати під поверхнею, непоміченими [8].

Організації іноді оцінюють свою ефективність інформаційної безпеки на щорічній або піврічній основі за допомогою стороннього постачальника або внутрішньої команди. Одним із недоліків цієї форми управління кіберпродуктивністю є її епізодичний, тимчасовий характер. Зважаючи на те, як швидко все змінюється, дуже легко виникнути проблеми під час тривалих періодів між тестуваннями.

Ручне оцінювання також може ускладнити оцінку ефективності з часом, оскільки члени команди повинні екстраполювати датовані сторонні оцінки або статичні результати для вимірювання прогресу. Зважаючи на те, наскільки багато команд безпеки перевантажені своїми повсякденними обов’язками, часто стає важко підтримувати точну довгострокову оцінку ефективності.

Програмне забезпечення, яке пропонує безперервне автоматичне звітування (наприклад, платформи керування шляхом атаки), допомагає вирішити цю проблему, пропонуючи більш повну картину ефективності програми безпеки в будь-який момент часу. Програмне забезпечення такого роду може виявляти проблеми, генерувати вказівки щодо їх усунення та надавати постійну видимість того, як з часом змінюється ефективність інформаційної безпеки [9, 10].

Як правило, великі компанії у сфері виробництва, телекомунікацій чи хостингу значною мірою залежать від процесів вимірювання та рівня обслуговування, чи то LEAN, ITIL, ISO 9001 чи аналогічні. Ці вимірювання часто бувають напівавтоматичними і зводяться в єдиний інструмент звітності, подібний до панелі звітності.

ISO 27001 не вимагає використання конкретних інструментів. Це було б природнім розвитком, коли компанія досягла певної зрілості та пройшла через низку послідовних ітерацій поліпшення задля автоматизації процесу.

Найкращі практики рекомендують почати з вибору кількох вимірювань з кожного процесу, та включити їх як частину робочих процедур організації ІТ [11].

Збір вихідних даних щодо окремих процесів СУІБ можна легко здійснювати у вигляді електронної таблиці або аналогічного та зведеного документа для використання в управлінській звітності [12, 13].

**Висновки до Розділу 1**

Вимірювання ефективності інформаційної безпеки є важливою частиною системи управління інформаційною безпекою в організаціях. Дослідження в минулому в основному були зосереджені на створенні підходів до якісного вимірювання. Оскільки це може призвести до неоднозначних висновків, кількісні показники все частіше пропонуються як корисна альтернатива. Тим не менш, літератури щодо кількісних підходів залишається мало. Таким чином, дослідження щодо оцінки продуктивності інформаційної безпеки є складним завданням, особливо тому, що багато підходів не перевіряються в організаційних умовах. Стандарти безпеки, хоча і зосереджують увагу на важливості оцінки впроваджених процесів ІБ, не дають конкретних вимог щодо безпосередньої оцінки ефективності.

Наразі, найпоширенішим підходом на підприємствах для оцінки ефективності процесів ІБ є використання метрик для кількісного вимірювання ефективності.

# РОЗДІЛ 2
# АНАЛІЗ ПРАКТИКИ ВИКОРИСТАННЯ МЕТРИК ЩОДО ОЦІНЮВАННЯ ЕФЕКТИВНОСТІ ПРОЦЕСІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ПІДПРИЄМСТВІ

## 2.1. Методи оцінювання ефективності процесів інформаційної безпеки

Вимірювання трьох нематеріальних вимірів, таких як знання, ставлення та поведінка, може здатися непростим завданням. Паула Девіс у «Вимірюванні ефективності тренінгів з питань інформаційної безпеки» [3] опублікувала деякі з найефективніших методів, які допомагають виміряти обізнаність співробітників щодо безпеки.

Паула Девіс пропонує використовувати різні методи для вимірювання ефекту програми підвищення обізнаності. При вимірюванні ставлення, наприклад, передбачається, що найкращий результат, який можна отримати, це використання: опитування, інтерв’ю або фокус-груп, залежно від потреб організації (беручи до уваги кількість співробітників, робочі зусилля, час і витрати).

Фокус-групи - це форма групового інтерв'ю, яка реалізується в спілкуванні між учасниками з метою збору інформації. Цей спосіб зручний для збору даних від кількох учасників одночасно. Інтерв'ю використовуються для збору якісних даних. Учасникам дозволяється відповідати на відкриті запитання без обмеження часу та обсягу. Основна перевага інтерв’ю полягає в тому, що можна отримати корисні дані про речі, які нелегко виявити (наприклад, почуття, емоції та ставлення).

Методологія дослідження відіграє важливу роль у формуванні кінцевого результату будь-якого дослідження. Це може можна визначити як «загальний процес, що керує всім дослідницьким проектом» (Пальвія, Мао, Салам та Соліман, 2003). Два найбільш часто використовувані підходи - це кількісний і якісний.

Кількісне дослідження передбачає збір фактів і вивчення зв'язку між цими фактами. Це методологія включає в себе методи та прийоми, які здатні давати кількісні та узагальнені дані висновки (Bell, 2005). Тому це вважається формалізованим і контрольованим підходом.

«Якісне дослідження — це ситуаційна діяльність, яка знаходить спостерігача у світі. Він складається з набору інтерпретаційні, матеріальні практики, які роблять світ видимим. Ці практики змінюють світ. Вони перетворити світ на ряд уявлень, включаючи польові нотатки, інтерв'ю, розмови, фотографії, записи та пам'ятки для себе. (Дензін, 2005) «Якісне дослідження дозволяє свобода шукати відповіді на запитання, а також знаходити рішення на основі попередньо визначеного набору процедур.

Ця методологія більше зосереджена на розумінні індивідуального сприйняття світу. Воно шукає розуміння, а не статистичне сприйняття світу.

Існують різні види якісних методів. Майерс обговорює чотири методи дослідження, які є дослідження дії, тематичні дослідження, етнографія та обґрунтована теорія (Myers, 2011). Ці методи коротко пояснюються нижче.

Вимірюючи ефективність інформаційної безпеки, організації визначають ступінь задовільності їхніх потреб у безпеці. Такі вимірювання можуть стосуватися всієї СУІБ або окремих її елементів. Окрім продуктивності систем, також можуть бути досліджені організаційні, поведінкові та кримінологічні аспекти або інші більш вузькі операційні, програмні та технічні сфери. Загалом методики, що використовуються для вимірювання ефективності інформаційної безпеки, поділяються на кількісні та якісні категорії [14, 37], при цьому можлива комбінація підходів.

Кількісний аналіз інформаційної безпеки є традиційним підходом до вимірювання. Серед них [9, 14, 27, 30, 38]:

- технічний аналіз і тестування інформаційних систем, напр. тестування на проникнення,
- математичні моделі або статистичні розрахунки ризиків, напр. аналіз ризиків і

- економічний аналіз обґрунтування інвестицій — напр. ROI.

Такі аналізи дозволяють організаціям визначити, чи зможуть зловмисники обійти засоби контролю безпеки, наскільки ймовірно матеріалізація певних загроз і чи окупляться інвестиції в конкретні заходи. Переваги таких аналізів, за умови їх належного проведення, можна знайти в їх точності та надійності, але їхні окремі процедури дуже складні та вимагають багато часу та знань. Крім того, такі аналізи необхідно проводити в поєднанні з іншими типами аналізів, оскільки дуже важливо спочатку визначити окремі вразливі місця або обсяг інвестицій. Оскільки безпека є складною системою, що робить неможливим передбачити всі загрози та вразливості, кількісні аналізи є дещо неповними та недостатніми, якщо розглядати їх ізольовано, незважаючи на їхню точність [9]. Тому деякі автори [11, 35, 39] дедалі частіше зазначають, що економічно орієнтовані моделі є занадто упередженими, оскільки рентабельність заходів не може бути єдиним критерієм ефективності інформаційної безпеки. Тим не менш, техніко-економічні моделі не можна заперечувати в їх достовірності, особливо якщо врахувати, що заходи, реалізовані на операційних рівнях, являють собою найпоширеніший і найбільш розроблений підхід до забезпечення інформаційної безпеки. Однак слід усвідомлювати, що прийняття самих технічних та оперативних заходів недостатньо, оскільки продуктивність організацій в епоху складних питань інформаційної безпеки також залежить від інших тактичних і стратегічних аспектів [8, 32, 40, 41].

Дедалі більша увага, яка приділяється менеджменту, культурі, політикам і стосункам з користувачами, спрямована на роз’яснення питань, пов’язаних з інформаційною безпекою, покращує наші знання та усвідомлення її складної природи. Це також впливає на моделі вимірювання, які все частіше набувають якісного характеру та включають систематичні оцінки заздалегідь визначених критеріїв з метою визначення рівня реалізації стратегій безпеки [14]. На додаток до класичних списків контролів інформаційної безпеки, якісні моделі також включають підходи, які аналізують інформаційну безпеку з соціально-психосоціальної, організаційної та кримінологічної точок зору. Ці нові та сучасні

підходи досліджуються дедалі більшою кількістю експертів [8, 10, 40, 42, 43, 44]. У цьому контексті моделі інформаційної безпеки спираються на такі теорії:

*Поведінкові:* теорія раціонального вибору, теорія запланованої поведінки та теорія мотивації захисту [40, 41, 45].

*Організаційні:* структура TOE, організаційна складність, продуктивність, стратегія та культура [33, 35, 46, 47].

*Кримінологічні:* загальна теорія стримування, ситуативна теорія запобігання злочинності [13, 27, 48, 49].

Вони пояснюють, як організаційні та особистісні фактори, соціальний контекст, організаційна культура, міжособистісні стосунки, зовнішнє середовище, заходи профілактики та реагування та санкції впливають на поведінку користувачів і, отже, сприяють безпеці інформаційних систем. Незважаючи на широку сферу застосування, якісні методи також мають ряд недоліків. Наукові дослідження часто зосереджуються на вимірюванні ізольованих елементів і взаємозв'язків, тому їхні результати мають вузьку сферу практичного застосування. Крім того, як і кількісних моделей, якісних методів також недостатньо, оскільки вони не можуть точно виміряти всі сфери, ідентифікувати всі загрози та узгодити часто розбіжні точки зору або потреби експертів і користувачів. Результати такого аналізу можуть бути вкрай суб’єктивними або відносними, особливо коли окремі сфери оцінюються на основі інтуїції чи упередженої логіки [34, 40].

Окрім вищезазначених методів, організації нерідко звертаються до стандартів або рекомендаційних збірок, які пропонують свої методи оцінки ефективності процесів ІБ. Так, наприклад, стандарт ISO/IEC 27004:2016 ”Monitoring, measurement, analysis and evaluation” (“Моніторинг, вимірювання, аналіз та оцінка”) є спадкоємцем першої версії цього документа, яка була випущена у 2009 році. Цей документ логічно пов'язаний із стандартами серії ISO 27000, використовує єдиний з ними термінологічний апарат та використовується для перевірки відповідності СУІБ вимогам оцінки ефективності, як зазначено у п.9.1 стандарту ISO/IEC 27001:2013. Зокрема, цей пункт вимагає, щоб організації

оцінювали ефективність функції інформаційної безпеки та побудованої СУІБ шляхом визначення об'єктів вимірювання (включаючи процеси та заходи ІБ), вибору методів для оцінки та аналізу ефективності, а також затвердження термінів та відповідальних із збереженням документальних результатів оцінки [31].

Метою оцінки ефективності СУІБ є перевірка того, що збудовані процеси та дії, що виконуються, дійсно ведуть до виконання вимог стандарту ISO 27001. Основними завданнями при оцінці ефективності СУІБ є збір релевантної інформації, її коректна обробка та аналіз, а також забезпечення відтворюваності результатів. Перевагами впровадження процесів оцінки ефективності СУІБ є підвищення прозорості СУІБ (виявлення некоректних, неефективних або взагалі не впроваджених заходів захисту), забезпечення кількісної оцінки прогресу ефективності СУІБ та процесів ІБ, документальне свідчення виконання вимог стандарту ISO 27001, а також підтримка ризик-орієнтованих процесів прийняття рішень , зокрема обґрунтування виділення бюджетів на ІБ.

Для отримання релевантної інформації, придатної для подальшого аналізу, стандарт ISO/IEC 27004:2016 пропонує використовувати моніторинг наступних дій, процесів та систем:

1. Впровадження процесів СУІБ
2. Управління кіберінцидентами
3. Управління вразливістю
4. Управління конфігураціями
5. Програми з підвищення обізнаності
6. Збір подій ІБ
7. Аудит ІБ
8. Процеси оцінки та обробки кіберризиків
9. Управління кіберризиками третіх осіб
10. Управління безперервністю діяльності
11. Управління процесами фізичної безпеки
12. Моніторинг ІТ-інфраструктури.

У стандарті ISO/IEC 27004:2016 наведено такі процеси СУІБ, які можна аналізувати для вимірювання ефективності ІБ:

1. Планування

2. Підтримка з боку керівництва компанії

3. Ризик-менеджмент

4. Управління політиками ІБ

5. Управління ресурсами

6. Обмін інформацією

7. Оцінка з боку керівництва

8. Документування

9. Аудит [45].

У документі також пропонуються такі ролі, які можуть бути призначені відповідальним особам компанії в рамках процесу вимірювання ефективності СУІБ:

1. Клієнт – запитує інформацію про ефективність СУІБ та заходів захисту інформації, включаючи СЗІ

2. Планувальник - зіставляє одержувані з СУІБ або СЗІ дані з параметрами, які застосовуються для оцінки ефективності СУІБ, створюючи модель вимірювання

3. Рецензент - перевіряє коректність моделі вимірювання та релевантність зіставлення даних з параметрами

4. Власник інформації - передає дані із компонентів СУІБ або СЗІ, що знаходяться у сфері його відповідальності

5. Збиральник інформації - відповідає за збирання, запис та зберігання даних для вимірювання

6. Аналітик – проводить аналіз зібраних даних

7. Комунікатор – повідомляє результати аналізу заінтересованим уповноваженим особам.

Стандарт ISO/IEC 27004:2016 пропонує наступний процесний PDCA-підхід для оцінки ефективності СУІБ:

1. Визначення вхідних даних, які будуть використовуватись для оцінки та аналізу; при цьому використовується високорівневий опис СУІБ та бізнес-процесів компанії.

2. Створення та підтримка вимірних параметрів, що передаються з компонентів СУІБ, із СЗІ, від співробітників в результаті опитувань, наприклад, події ІБ, звіти про сканування, статистика з пройдених awareness-тренінгів, статистика з інцидентів ІБ, результати аудитів, результати навчальних тривог щодо забезпечення безперервності діяльності та відновлення працездатності.

3. Запуск процедур для оцінки ефективності СУІБ, що включає оповіщення задіяних осіб та підрозділів, вибір та налаштування систем для збору даних, налаштування правил перевірки одержуваних даних на коректність, аналіз даних та надання звітності в заданому форматі, включаючи звіти, дашборди, діаграми [48].

4. Моніторинг та вимірювання, що включають ручний та/або автоматизований збір даних, перевірку отриманих даних на коректність, надійне зберігання.

5. Аналіз результатів та інтерпретація результатів аналізу, які мають відображати недоліки СУІБ та відхилення між очікуваними та фактичними результатами вимірювання параметрів СУІБ.

6. Оцінка ефективності СУІБ та процесів ІБ на основі аналізу отриманих результатів.

7. Перегляд та покращення процесів моніторингу, вимірювання, аналізу, оцінки СУІБ на основі отриманого зворотного зв'язку, аналізу вивчених уроків, даних бенчмарків, перегляду процедур оцінки ефективності СУІБ.

8. Збереження звітних документів, передання їх для ознайомлення заінтересованим уповноваженим особам.

У додатку «В» до стандарту ISO/IEC 27004:2016 наведено приклад набору безпосередньо метрик ІБ, які можна використовувати для кількісної оцінки ефективності СУІБ відповідно до вимог, зазначених у стандарті ISO 27001.

## 2.2. Аналіз метрик для вимірювання ефективності процесів інформаційної безпеки

З цієї нагоди визначення метрики буде взято зі стандартів ISO, відповідно до яких: - метрика визначає систему вимірювання або стандарт; шкали вимірювання та одиниці вимірювання для моніторингу ефективності, а вимірювання – це акт визначення кількості, розміру ступеня (чогось) за допомогою стандартної групи заходів та процедур вимірювання, визначених метрикою. Метрики можуть відповісти на такі запитання: «Що вимірюється, чому це вимірюється і хто це вимірює?». Є численні результати щодо використання метрик безпеки та їх ролі. Він використовується для документування (стану безпеки) та координації результатів, які слід виправити, для вимірювання результатів програм безпеки, для розуміння та керування вимогами безпеки, як інструмент для оцінки засобів контролю безпеки результати, встановлення розміру ризику, а також для позитивного впливу на поведінку співробітників. Поняття метрики завжди присутнє в критеріях, стандартах і концепціях безпеки. У цьому контексті термін метрики здебільшого згадується як інструмент для оцінки, оцінки, координації та узгодження з вимогами безпеки.

Наприклад, норма ISO/IEC у виданні Кодексу правил управління інформаційною безпекою говорить про необхідність прийняття універсального та збалансованого вимірювальна система як умова успішної реалізації програм безпеки. Коли ми говоримо про стандарт ISO і, зокрема, норму ISO/IEC 27001, прямо вимагається, щоб інформація, отримана шляхом вимірювання за допомогою метрик, була включена в процес прийняття рішень щодо дій, які слід вжити для покращення стану безпеки. Конкретні вказівки щодо їх використання доступні в інструкціях ISO BIP 0074, які визначають класи метрик і вимірювань ISMS (Система управління інформаційною безпекою).

NIST (Національний інститут стандартів і технологій) у своїй публікації NIST SP 800-55 «Посібник для розробки, вибору і впровадження метрик рівня

IT-системи», визначив спосіб застосування та розробки конкретних метрик безпеки для застосування в різних сферах результатів вимірювання безпеки. Згідно з моделлю зрілості CMMI, вимірювання та показники є складовою частиною процесу моніторингу зрілості програм безпеки. Існують також деякі інші джерела використання показників, як-от. метрики, як того вимагає Common Criteria (CC), і важливо зазначити результати інституту ISACA, перетворені на критерії COBIT, які об'єднують метрики під час оцінювання та оцінки характеристик технологічних областей. Однак факт полягає в тому, що використання метрик все ще недостатньо і використовується лише на обмеженій кількості груп індикаторів. Авторами стверджується, що найбільша кількість даних про якість програм безпеки відноситься до метрик для виявлення шкідливого коду, статистиці входу в кімнати та даних про якість спам-повідомлень. І людський фактор як фактор часто ігнорується.

Проблема полягає в неадекватній стандартизації метрик і невідомих силах про спосіб їх використання в ширшому контексті управління безпекою. Існуюча група метрик також не об'єднана в єдину систему, тому її навряд чи можна застосовувати для всієї організації. Таким чином, здається, що показники ризику все ще є «незрілою» дисципліною, яку пояснюють і розуміють по-різному. Неясним також є питання про групу змінних, які використовуються для вимірювання безпеки, і про те, які характеристики системи вимірюються, і це ще менше відомо, що представляють виміряні результати та спосіб їх збору (зокрема тих факторів, які вимірюються опосередковано), кількісна оцінка описаних індикаторів тощо.

Проблеми виникають через той факт, що стан безпеки, не лише описуваний безпосередньо вимірюваними атрибутів, часто описується абстрактними показниками. Що також залишається невизначеним, так це область базової термінології (метрики, вимірювання, вимірювання, індикатори) і область (домен), у якій метрики пов'язані з нею. Отже, це причина, чому незрозуміло, що описують метрики, як це інтерпретувати та оцінювати. У кожному випадку неузгоджена термінологія і складний збір даних для деяких метрик (наприклад,

для оцінки інтелектуальної власності) роблять Подальший розвиток показників безпеки складний і повільний.

Використання метрик вважається наразі найпоширенішим методом оцінки ефективності процесів ІБ на підприємстві, тому поговоримо та проаналізуємо метрики.

Метрикою вважається система вимірювання, така як наприклад температурна шкала за Цельсієм, яка забезпечує метричну шкалу, за якою можна виконувати вимірювання. Інші приклади включають шкали такі як відсотки, цифри, невдача/успіх або шкали зрілості, такі як шкала зрілості CMMI (Capability Maturity Model Integration) або Cobit.

Це може бути навіть така проста шкала, як градуйована шкала рівня задоволеності або кольорові шкали.

Цілями використання метрик для вимірювання ефективності процесів ІБ можна назвати наступне:

- Забезпечення відповідності бізнес-стратегії:
  - відповідність стратегічним цілям
  - забезпечення IT підтримки бізнесу
- Досягнення цілей:
  - CSF (критичні фактори успіху)
- Обґрунтування витрат:
  - при звітності керівництву
  - ведення бюджету
- Вдосконалення:
  - не ефективний, тому потребує вдосконалення
  - занадто ефективний
  - уникнення невідповідностей / зменшення рикзику
  - покращення показників або зміна підходу

Коли йдеться про захист конфіденційних даних, запобігання витоку даних і виявлення кібератак, слід дотримуватися контрольного списку, щоб відстежувати свої зусилля [15].

Показник ефективності або ключовий показник ефективності (KPI) є типом вимірювання ефективності. KPI оцінюють успіх організації або певної діяльності (наприклад, проектів, програм, продуктів та інших ініціатив), в якій вона бере участь. Ключові показники ефективності забезпечують стратегічне й операційне вдосконалення, створюють аналітичну основу для прийняття рішень і допомагають зосередити увагу на найважливішому. Ключові показники ефективності (KPI) — це ефективний спосіб вимірювання успіху будь-якої діяльності (включаючи кібербезпеку) і допомога в прийнятті рішень [16].

Також для оцінки процесів ІБ часто використовують ключовий показник ризику (KRI) — міру, яка використовується в менеджменті для визначення того, наскільки ризикованою є діяльність. Ключові показники ризику – це показники, які використовуються організаціями для раннього сигналу про збільшення ризику в різних сферах діяльності підприємства. Він відрізняється від ключового показника ефективності (KPI) тим, що останній означає, наскільки добре щось робиться, тоді як перший є індикатором можливості майбутнього негативного впливу. KRI надає раннє попередження для виявлення потенційних подій, які можуть зашкодити безперервності діяльності/проекту.

Важливість оцінки та її постійного моніторингу ефективності діяльності та безпосередньо інформаційної безпеки безумовна. Як сказав Пітер Друкер, те, що вимірюють, тим керують – і інформаційна безпека не виняток. Ви повинні мати заходи, щоб регулярно та відслідковувати оцінювати ефективність захисних заходів, у які ви інвестували.

Це важливо з двох причин:

- Аналіз ключових показників ефективності, ключових індикаторів ризику (KRI) і положень безпеки надає миттєвий знімок того, як ваша команда безпеки функціонує з часом. Допомога вам краще зрозуміти, що працює, а що погіршується, покращення прийняття рішень щодо майбутніх проектів.
- Показники надають кількісну інформацію, яку можна використовувати, щоб показати керівництву та членам правління, що ви

серйозно ставитеся до захисту та цілісності конфіденційної інформації та активів інформаційних технологій [17].

Звітність і надання контексту щодо показників ефективності інформаційної безпеки є важливою частиною роботи багатьох керівників інформаційної безпеки (CISO) і керівників інформаційних технологій (CIO), що спонукає зростаючий інтерес до звітності на рівні акціонерів, регуляторних органів і правління. Найкращі професіонали з інформаційної безпеки використовують показники, щоб розповісти історію, особливо коли звітують нетехнічним колегам [18].

## 2.3. Впровадження метрик в систему управління інформаційною безпекою

Для того, щоб впровадити метрики в існуючу СУІБ, необхідно виділити процеси, які будуть оцінюватись та визначити безпосередньо самі метрики для вимірювання ефективності цих процесів. Проаналізуємо існуючі рекомендації щодо визначень метрик для ключових процесів ІБ для подальшої їх оцінки.
Один із способів створення хорошої метрики дотримання вимог системи SMART (Specific, Measurable, Achievable, Repeatable, Timely). Показник, який за визначенням охоплює всі наведені нижче цілі можна назвати SMART метрикою:

1. Специфічні: Метрики мають передавати інформацію, яка має відношення до мети, для якої вони були створені

2. Вимірність: Метрика має піддаватися кількісному виміру та виводитися з фактичних чисел. Важливо уникати показників, які базуються на оцінках

3. Досяжні: Досяжні показники – це ті, для яких є все, щоб відповідати генерації показників

4. Повторюваність: повторювана метрика – це така, яку можна чітко визначити, передати, а необроблені дані можуть бути зібрані та звітовані однаково всіма залученими працівниками

5. Своєчасність: частота, з якою метрика звітує про дані, має відповідати швидкості змін, очікуваних від базових даних, або мети, з якою метрика узгоджується [19].

У цьому різноманітному світі кібербезпеки, який постійно розвивається, CISO часто стикаються з проблемою використання та відстеження даних, доступних з різних інструментів безпеки, розгорнутих у кількох доменах безпеки.

Вони постійно ставлять перед собою такі запитання:

• Чи маємо ми достатньо інформації про різні сфери безпеки?

• Чи достатньо консолідованих/історичних даних для управління IT-безпекою та прийняття стратегічних рішень?

• Чи можемо ми встановити рівні зрілості та порівняти з ними наші досягнення?

Відповідь на вищезазначене полягає в зборі показників, які більше підходять для потреб CEO.

Наступний список демонструє запитання, які варто собі поставити при формулюванні та визначенні метрик для вимірювання ефективності процесів ІБ:

- Що вимірюється?
- Ціль вимірювання?
- Як вимірюється та яка частота?
- Хто відповідальний за вимірювання?
- Як відбувається документування та звітування вимірювань?
- Оцінка впроваджених вимірювань (зміни у бізнесі, стратегії, ландшафту ризиків можуть вплинути на базу вимірювань) [20]

Що стосується процесів, на які варто звернути увагу в рамках оцінювання ефективності ІБ, то універсального підходу тут нема і кожна організація повинна відштовхуватись від визначеної стратегії, як самого бізнесу, так і ІБ.

Розглянемо рекомендації міжнародних організацій щодо процесів, на яких варто зосередитись. Дані процеси взяті із зрозуміння основ, від яких залежить ефективність СУІБ в цілому. Ці процеси наступні:

- Узгодження IT та бізнесу
- Процес управління ризиками інформаційної безпеки
- Процес підтримки відповідності
- Процес підвищення обізнаності персоналу щодо ІБ
- Процес аудитів / перевірок [21]

Проаналізуємо метрики, які можна використати для оцінки деяких вищезазначених процесів. Цілі, знахідки та плани дій відрізняються від компанії до компанії, але ми проаналізуємо приклади, які можуть бути доречними до більшості компаній [25, 40].

Узгодження IT та бізнесу – як ми гарантуємо, що стратегія інформаційної безпеки та впроваджені процеси інформаційної безпеки належним чином підтримують і враховують потреби та вимоги бізнес-стратегій і цілей?

Ми можемо поставити собі такі питання:

- Чи стратегія інформаційної безпеки та IT-послуги приносять користь бізнесу?
- Чи зобов’язується керівництво забезпечити постійний внесок у стратегії інформаційної безпеки та IT-послуги?

Таблиця 2.1

Приклад метрик до процесу узгодження ІТ та бізнесу

| Метрика | Цілі | Знахідки / Невідповідності | Плани дій |
|---|---|---|---|
| % підтриманих бізнес-стратегічних цілей і вимог стратегічними цілями та рішеннями інформаційної безпеки.<br>**Метод/джерела:**<br>Переглянути бізнес-стратегічні рішення та переконатись, що вони були оцінені з т. з ризиків відносно питань ІТ та інформаційної безпеки. Так, усі основні стратегічні рішення щодо ІБ мають переглядатися та затверджуватися вищим керівництвом, щоб забезпечити узгодженість із бізнес-послугами та стратегіями. | **Цілі**<br>Усі бізнес-рішення мають підтримуватися ІТ-рішеннями, зокрема, питаннями інформаційної безпеки. Якщо це не актуально, це потрібно задокументувати та затвердити на етапі проекту.<br>**Знахідки / Невідповідності**<br>Наші останні рішення щодо аутсорсингу та ІТ-закупівель не узгоджувалися з нашою ІТ-стратегією і, зокрема, з вимогами інформаційної безпеки.<br>**Плани дій**<br>Переконайтеся, що ІТ-вимоги є обов'язковими для порядку денного, а всі відповідні вимоги до інформаційної безпеки та потенційні проблеми визначені та розглянуті. | | |
| Рівень задоволеності бізнесу (зацікавленими сторонами) пропонованими послугами інформаційної безпеки та внутрішньою підтримкою. Чи приносить інформаційна безпека цінність зацікавленим сторонам?<br>**Метод/джерела:**<br>Дані, зібрані за допомогою інтерв'ю або анкет, надісланих відповідним зацікавленим сторонам кожного бізнес-підрозділу, бізнес-процесу тощо. | **Ціль**<br>Наш базовий рівень вище середнього, напр. високий рівень задоволеності пропонованими послугами інформаційної безпеки (шкала від низького до середнього, високого до відмінного).<br>**Знахідки / Невідповідності**<br>У порівнянні з минулим роком ми підвищили рівень задоволеності з середнього до високого.<br>**Плани дій**<br>Жодних планів дій | | |

Продовження табл. 2.1

Приклад метрик до процесу узгодження IT та бізнесу

| | |
|---|---|
| % змін стратегії інформаційної безпеки, яка затверджена керівництвом.<br>Метод/джерела:<br>Перегляньте поточну стратегію інформаційної безпеки або основні стратегічні рішення щодо інформаційної безпеки та переконайтеся, що керівництво їх офіційно схвалило. | **Ціль**<br>Усі стратегічні рішення щодо інформаційної безпеки мають бути затверджені керівництвом.<br>**Знахідки / Невідповідності**<br>Деякі стратегічні IT-рішення щодо передачі на аутсорс критичних IT-систем протягом 2013 року не були оцінені з точки зору ризиків та не були схвалені керівництвом.<br>**Плани дій**<br>Переконатись, що всі основні IT-стратегічні рішення схвалені керівництвом. Встановити деякі базові вимоги для схвалення керівництва. Наприклад:<br>• Критичні IT-послуги<br>• Конфіденційні дані<br>• Специфічні питання інформаційної безпеки<br>• Обсяг бюджету |

Відповідність. Питаннями, які ми повинні поставити, можуть бути:

- Чи достатньо ми дотримуємося наших зобов'язань щодо інформаційної безпеки, конфіденційності, управління та відповідних зобов'язань?

- Чи витрати, пов'язані з досягненням і підтримкою відповідності, є меншими, ніж бізнес-вигоди (не лише уникнення штрафів, але й цінність бренду від того, що вас бачать як правильно)?

- Чи успішно ми керуємо ризиками бути спійманими, наприклад, через інциденти невідповідності, чи негативні оцінки відповідності, або неспроможність оцінити нові чи зміни зобов'язань щодо дотримання?

Ефективність процесів підтримки відповідності може включати оцінку того, чи ефективно та результативно ми вирішуємо проблеми невідповідності, які фінансові витрати пов'язані із стимулюванням процесу відповідності, ступінь розуміння керівництвом, підтримки, участі тощо [26, 38].

Таблиця 2.2

Приклад метрик до процесу управління відповідністю ІБ

| **Метрика** | **Цілі** | **Знахідки / Невідповідності** | **План дій** |
|---|---|---|---|
| Кількість невідповідностей та похідних витрат на рік (наприклад, зовнішні вимоги, політики та процедури)<br>**Метод/джерела:**<br>Перегляд списків інцидентів на кінець року, а також значні результати/згнахідки зовнішнього аудиту. | **Ціль**<br>Немає серйозних проблем із невідповідністю, фінансових чи іміджевих наслідків.<br>**Знахідки / Невідповідності**<br>Наш аутсорсинговий постачальник знайшов виток даних<br>**План дій**<br>Перегляньте відповідні процеси інформаційної безпеки та контракт з постачальником. | | |
| Час між виявленням невідповідностей та впровадженням виправлень.<br>Допомагає виявити проблеми з ефективністю процесу відповідності.<br>**Метод/джерела:**<br>Співставити час повідомлених проблем невідповідності / інцидентів безпеки з фактичним часом впровадження виправлень. | **Ціль**<br>Залежно від складності питання необхідно вирішити протягом двох робочих днів.<br>**Знахідки / Невідповідності**<br>У нас було два інциденти, які досі не вирішені.<br>**План дій**<br>Нам потрібно оцінити ефективність відділу внутрішнього комплаєнсу. Чи потрібно перебудовувати процес? Чи є якісь обмеження ресурсів чи внутрішня опозиція? | | |

Продовження табл. 2.2

Приклад метрик до процесу управління відповідністю ІБ

| | |
|---|---|
| Витрати на усунення проблем, пов'язаних із невідповідністю, наприклад, адміністративна робота, пов'язана з усуненням проблем (оптимізація процесів, процедури, створення / вдосконалення політик чи IT-контроль).<br>**Метод/джерела:**<br>Переглянути загальні витрати, пов'язані з усуненням невідповідності у річному бюджеті. | **Ціль**<br>За звичайних обставин на вирішення проблем, пов'язаних з безпекою, можна виділити максимум 20% річного бюджету.<br>**Знахідки / Невідповідності**<br>Витрати, пов'язані з проблемою невідповідності, перевищують ліміт у 20%. Сюди входить проведення нового пентесту та переробка політик за допомогою зовнішніх консультантів.<br>**План дій**<br>Знайти відповіді на питання:<br>Чи було проведено економічне обґрунтування та аналіз витрат і вигод? Хто розглядав і затверджував витрати? |

Обізнаність. Важливо переконатися, що зусилля з підвищення обізнаності базуються на «реальних проблемах», виявлених в організації, або актуальних поточних тенденціях безпеки. Питання наступні:

- Як ми гарантуємо, що зусилля з підвищення обізнаності досягнуть відповідних зацікавлених сторін/працівників?
- Вони чогось навчилися?

Одна з цілей обізнаності полягає в тому, щоб співробітники поводилися більш безпечно і ненавмисно не наражали організацію на ризики.

Нам також потрібно підтвердити, що результати інформування використовуються для покращення нашої безпеки [40].

Таблиця. 2.3

Приклад метрик до процесу обізнаністю ІБ

| Метрики | Ціль | Знахідки / Невідповідності | План дій |
|---|---|---|---|
| % відхилення при порівнянні встановлених факторів успіху кампаній з підвищення обізнаності із результатами реалізованих кампаній.<br>**Метод/джерела:**<br>Порівняння результатів програми підвищення обізнаності/навчання з результатами фізичних перевірок або опитувань/тестів для працівників. | **Ціль**<br>Гарантувати, що мінімум 80% працівників успішно завершили тест/вікторину після кампанії.<br>Фізичний огляд робочих місць показує значне зменшення фізично чутливих робочих паперів, розблокованих робочих станцій, USB-пристроїв тощо.<br>**Знахідки / Невідповідності**<br>Менше 60% працівників відповіли правильно щодо політик безпеки, щодо мобільних пристроїв і використання хмарних сервісів. Під час нашого внутрішнього аудиту ми виявили незаблоковані робочі станції та конфіденційні документи, які лежали в кімнаті для друку.<br>**План дій**<br>Нам потрібно переоцінити те, як подається інформація під час навчання. Можливо, ми зможемо зробити його більш “сюжетним” і краще використовувати внутрішню мережу, як інструмент поширення інформації. | | |
| % ІТ-користувачів, які цього місяця відвідали інтранет-сайт з інформацією про безпеку.<br>**Метод/джерела:**<br>Задокументуйте місячну кількість відвідувань у розділі інформаційної безпеки внутрішньої мережі. | **Ціль**<br>Наш середній рівень відвідувань не повинен опускатися нижче 70%.<br>**Знахідки / Невідповідності**<br>Останнє оновлення з попередженням про шкідливе програмне забезпечення бачили 90% ІТ-співробітників.<br>**План дій**<br>Жодного | | |

Продовження табл. 2.3

Приклад метрик до процесу обізнаністю ІБ

| Метрики | Ціль | Знахідки / Невідповідності | План дій |
|---|---|---|---|
| % співробітників, які пам'ятають навчання з ІБ. Можна виміряти, виконавши тести/вікторини на теми попередньої кампанії з підвищення обізнанності. **Метод/джерела:** Порівняйте результати тестів, проведених через короткий проміжок часу після завершення, з результатами тестування після більш тривалого періоду часу, напр. 2-6 міс. | **Ціль** Рівень успіху: 60% співробітників пам'ятають теми попереднього ознайомлення/навчання. **Знахідки / Невідповідності** Знання тем різко падає через 6 місяців, порівняно з тестами, які проводяться одразу після завершення навчання обізнаності. **План дій** Нам потрібно підтримувати обізнаність і знання щодо важливих тем безпеки, збільшуючи частоту зустрічей/кампаній з підвищення обізнаності. | | |

Процес аудиту та перевірок. Крім того, щоб внутрішній аудит проводився структуровано, нам також потрібно визначити, як стан безпеки змінюється з часом, і як змінюється наш рівень ефективності по відношенню до зусиль із пом'якшення, що випливають із спостережень аудиту.

Чи зменшують витрати, спрямовані на усунення невідповідностей, кількість невідповідностей та інцидентів безпеки?

Також важливо переглядати результати аудиту з плином часу, щоб переконатися, що обсяг аудиту безпосередньо пов'язаний із фактичним рівнем ризику, а також переконатися, що розглядаються сфери високого ризику та вилучаються області з невеликою кількістю критичних зауважень або без них.

Таблиця 2.4

Приклад метрик до процесу аудиту та перевірок ІБ

| Метрики | Ціль | Знахідки / Невідповідності | План дій |
|---|---|---|---|
| % критичних зауважень у порівнянні з останнім аудитом. Які тенденції у порівнянні даних з попередніми аудитами?<br>**Метод/джерела:**<br>Порівняйте кількість критичних спостережень. Прикладами можуть бути спостереження, що стосуються пріоритетів 1 і 2, а також оцінка CVSS, що перевищує встановлений поріг. | **Ціль**<br>Скорочення числа критичних зауважень і відсутність критичних зауважень, що повторюються.<br>**Знахідки / Невідповідності**<br>Критичні зауваження цього року є ідентичними зауваженням попереднього року.<br>**План дій**<br>Необхідно забезпечити облік критичних зауважень / невідповідностей. Потрібна ефективніша управлінська та бюджетна підтримка для виправлення критичних зауважень / невідповідностей. | | |
| Обсяг ресурсів, виділених для проведення критичних спостережень, тобто часу, грошей та робочої сили.<br>**Метод/джерела:**<br>Порівняйте загальний обсяг ресурсів, витрачених на вирішення проблем, пов'язаних із критичними спостереженнями. Це можна порівняти із витратами за попередній рік.<br>Чи окупаються витрачені гроші меншою кількістю зауважень ревізорів чи меншою кількістю інцидентів у сфері безпеки? | **Ціль**<br>Доки в інфраструктурі не відбудуться серйозні зміни, витрати на проведення спостережень повинні становити не більше 10% бюджету на IT.<br>**Знахідки / Невідповідності**<br>Витрати на ресурси зросли на 15% порівняно з минулим роком, але це очікується завдяки технологічним інвестиціям та змінам у системі ERP.<br>**План дій**<br>Жодних дій наразі не потрібно. | | |

### 2.3.1 Метрики в управлінні ризиками

Оцінка ефективності є ключовим елементом будь-якої системи управління та належної практики управління. Він включає шість ключових видів діяльності:

моніторинг, вимірювання, аналіз, оцінка, внутрішній аудит і аналіз керівництва. Оцінка ефективності системи управління ризиками організації забезпечує постійну відповідність процесу управління ризиками бізнес-стратегіям і цілям організації. Організації повинні прийняти програму метрик для офіційного проведення оцінки ефективності. Ефективна програма вимірювання допомагає вимірювати безпеку та управління ризиками з точки зору управління.

Простіше кажучи, метрики – це вимірні показники ефективності. Двома ключовими показниками, які використовуються, є ключові показники ризику (KRI) і ключові показники ефективності (KPI). COBIT 5 для ризиків визначає KRI як показники, здатні показати, що підприємство є або має високу ймовірність бути підданим ризику, який перевищує визначену схильність до ризику. Вони мають вирішальне значення для вимірювання та моніторингу ризику та оптимізації продуктивності. Ці показники допомагають ефективно повідомляти зацікавленим сторонам результати ефективності управління ризиками (повідомлення про ризики) і дозволяють керівництву приймати обґрунтовані рішення щодо управління ризиками [36]. У той час як KPI зосереджені на ефективності бізнесу, KRI зосереджені на ефективності управління ризиками.

Ефективна програма вимірювання ризику дає кілька переваг, зокрема:

- Уможливлення регулярного перегляду тенденцій ризиків і кращої видимості технологічних ризиків і вразливостей
- Підвищення підзвітності та підвищення ефективності управління технологічними ризиками
- Допомога в аналізі керівництва та надання індикаторів рішень для постійного вдосконалення управління технологічними ризиками
- Надання вхідних даних для визначення пріоритетності рішень щодо розподілу ресурсів
- Допомога в упорядкуванні інформації про ризики
- Внесок у загальну економію витрат і підвищення ефективності управління ризиками

Ключовими кроками в програмі вимірювання ризику є:

- Вибір і розробка метрик
- Збір даних метрик
- Аналіз даних метрик
- Звітність результатів метрик

Набір метрик ризику, вибраний для початкового впровадження, повинен ґрунтуватися на поточному рівні зрілості управління ризиками організації та сприяти вдосконаленню високопріоритетних напрямків управління ризиками. Показники також повинні охоплювати різні категорії зацікавлених сторін в організації. Збір і аналіз даних метрик, а також звітування про результати метрик можна автоматизувати (див. розділ цієї статті під назвою «Автоматизація — роль інструментів GRC у програмі метрик»). Пропонується модель із трьома лініями захисту для встановлення відповідальності за ризики та забезпечення підзвітності [22, 23, 24].

Бізнес-менеджери схильні думати, що технологічні ризики належать і управляються IT або відділом ризиків в організації. COBIT 5 для ризиків визначає IT-ризик як бізнес-ризик, зокрема бізнес-ризик, пов’язаний із використанням, володінням, функціонуванням, залученням, впливом і впровадженням IT на підприємстві.

Модель із трьома лініями захисту може бути використана як основний засіб для структурування ролей і відповідальності за прийняття рішень, пов’язаних із ризиками, і контроль для досягнення ефективного управління ризиками, управління та забезпечення:

Першою лінією захисту є управлінські команди окремих напрямків діяльності (LoB), які відповідають за виявлення та управління ризиком, притаманним продуктам, послугам, процесам і системам у своїх LoB.

Другою лінією захисту є незалежна корпоративна служба ризиків, яка відповідає за розробку системи управління ризиками; визначення ролей і обов'язків; а також забезпечення нагляду, підтримки, моніторингу та звітності.

Третя лінія захисту — це функція внутрішнього аудиту, яка відповідає за незалежний огляд засобів контролю, процесів і систем управління ризиками організації.

У табл. 2.5 наведено огляд ролей і обов’язків трьох ліній захисту з прикладами KRI.

Таблиця 2.5

Три лінії захисту та їх ролі і обов’язки

| **Лінія захисту** | **Перша лінія** | **Друга лінія** | **Третя лінія** |
|---|---|---|---|
| Організаційний відділ | Напрямки бізнесу | Відповідний за ризики | Внутрішній аудит |
| Роль | Менеджери / Власники ризиків | Покриття ризиків | Незалежна перевірка |
| Обов’язки | Визначати ризики та керувати ними.<br>Оцінювати та посилювати контроль.<br>Відстежувати та повідомляти про профіль ризику.<br>Дотримуватись політик та фреймворків ризиків. | Допомога у визначенні стратегії з управління ризиками, політики та структури для управління ризиком.<br>Надавати керівництва управління ризиками.<br>Визначати ролі та обов'язки.<br>Забезпечувати нагляд, підтримку, моніторинг та звітність. | Надати незалежну та об’єктивну впевненість щодо загальної ефективності управління ризиками.<br>Повідомляти результати незалежних перевірок усім зацікавленим сторонам. |
| Приклади KRI | Відсоток інцидентів, де задіяні персональні дані клієнтів | Відсутність плану наступності для ключових ролей | Недостача ефективної звітності |

Пов’язування KRI з KPI дає змогу бізнес-менеджерам оцінити зв’язок між ризиком і ефективністю бізнесу, а також відповідність KRI бізнес-цілям організації та схильності до ризику. Це допомагає в міжфункціональній

співпраці та впровадженні міркувань ризику в бізнес-рішення. Пов’язування KRI з KPI також допомагає отримати підтримку бізнесу для інвестицій у заходи зі зменшення ризиків. У табл. 2.6 показані кілька прикладів KRI, пов’язаних з KPI, і вплив KRI на бізнес.

Таблиця 2.6

Зв’язок KRI та KPI

| **KRI** | **KPI** | **Наслідки/Вплив на бізнес** |
|---|---|---|
| Відсутність плану успадкування ключових ролей | Своєчасне впровадження послуги або здача проекту | Відсутність резервного копіювання для визначених ключових ролей впливає на безперервність обслуговування, що призводить до проблем із відповідністю та можливого недотримання угод про рівень обслуговування (SLA). |
| Відсоток інцидентів із залученням особистих даних клієнтів | Дотримання правил, політики чи процесів | Це вказує на невиконання зобов’язань щодо відповідності або процесів і може призвести до перевірки з боку регуляторних органів або ЗМІ, що може негативно вплинути на репутацію організації. |
| Кількість послуг, скасованих або відкладених через простої, пов’язані з безпекою | Кількість простоїв служби, пов'язаної з безпекою | Інциденти безпеки, що впливають на критичні системи, потенційно можуть спричинити переривання роботи служби або її погіршення. |
| Відсоток бізнес-додатків/систем, які не підтримуються резервним планом | Кількість бізнес-додатків/систем, які не підтримуються резервним планом | Відсутність резервного копіювання даних для бізнес-додатків/систем призводить до втрати даних і негативно впливає на безперервність обслуговування в разі будь-якого переривання. |

Продовження табл. 2.6

Зв’язок KRI та KPI

| **KRI** | **KPI** | **Наслідки/Вплив на бізнес** |
|---|---|---|
| Кількість невідповідностей, виявлених під час випробувань безпеки/аудитів, які залишаються невирішеними після запланованого періоду часу | Відсоток невідповідностей, виявлених під час випробувань/перевірок безпеки, але не усунених протягом запланованого часу | Затримка в усуненні вразливостей, виявлених під час тестів/аудитів безпеки, робить організацію легкою мішенню для зловмисних атак |
| Кількість інцидентів безпеки, пов’язаних із вразливістю сторонніх систем/співробітників | Неадекватне стороннє управління | Інформація організації може бути піддана ризику третіми сторонами з неадекватним управлінням інформаційною безпекою. |
| Кількість систем без оновлених патчів | Відсутність адекватних часових рамок планового простою систем | Затримка в оновленні систем робить організацію легкою мішенню для зловмисних атак. |
| Відсутність ефективного звітування про ключовий ризик | Відсутність перегляду процесів управління ризиками | За відсутності перегляду процесів управління ризиками ці процеси можуть і надалі залишатися неефективними, що призведе до невиявлення вразливостей/ризику. |

COBIT 5 for Risk — це професійний посібник COBIT 5, у якому розглядаються ризики, пов’язані з IT, і надаються детальні практичні вказівки для спеціалістів із ризиків. Конкретно для KRI, у ньому визначаються KRI, перераховуються параметри та критерії вибору KRI, описується модель із трьома лініями захисту, перераховуються переваги KRI, які надають підприємству, а також окреслюються загальні проблеми, з якими стикаються під час успішного впровадження KRI [28, 29].

COBIT 5 для ризиків містить перелік деяких можливих KRI для різних зацікавлених сторін — директора з інформації (CIO), відділу ризиків і головного

виконавчого директора (CEO)/ради директорів (BoD). Деякі з цих KRI показані у табл. 2.7.

Таблиця 2.7

Приклад KRI з COBIT 5 для оцінки ефективності процесу управління ризиками

| **Тип події** | **CIO** | **Відповідний за ризики** | **(CEO)/Рада директорів (BoD)** |
|---|---|---|---|
| Інвестиції/проекти, пов'язані із прийняттям рішень | Відсоток проектів, які були виконані вчасно та згідно з бюджетом<br>Кількість та тип відхилень від плану технічної інфраструктури | Відсоток IT проектів, перевірених та схвалених службою забезпечення якості; які відповідають цілям якості<br>Відсоток проектів із заздалегідь визначеними перевагами | Відсоток IT інвестицій, які перевищили або відповідають заздалегідь визначеній вигоді для бізнесу<br>Відсоток витрат до IT, які мають відношення до бізнес-стратегії |
| Бізнес події, пов'язані із залученням 3х сторін | Ступінь схвалення бізнесом IT стратегії, тактики | Частота зустрічей із залученням керівництва підприємства, на яких обговорюється внесок IT у підвищенні вартості | Частота звітності IT директора або відвідування засідань виконавчої влади, на яких обговорюється внесок IT у досягненні цілей підприємства |
| Безпека | Відсоток користувачів, які не дотримуються стандартів паролів | Кількість і тип підозрюваних і фактичних порушень доступу | Кількість інцидентів, що впливають на бізнес |

Продовження табл. 2.7

Приклад KRI з COBIT 5 для оцінки ефективності процесу управління ризиками

| | | | |
|---|---|---|---|
| Вимушені дії персоналу: руйнування | Кількість рівнів обслуговування, на які вплинули операційні інциденти<br>Відсоток IT персоналу, який виконує річний план | Кількість інцидентів, викликаних недостатньою документацією<br>Кількість критично важливих для бізнесу процесів, які залежать від IT та не охоплені планом забезпеченні безперервності IT | Вартість невідповідності IT, включаючи розрахунки та штрафи<br>Кількість проблем невідповідності, про які було повідомлено правлюнню |

Рішення для управління ризиками з управління, ризиків і відповідності (GRC) надає організації консолідоване уявлення про ризики. Рішення дозволяє оцінювати ризики та надає уповноваженому персоналу можливість призначати показники ризику, збирати зміни в профілі ризиків організації та контролювати ризики та показники щодо цільових показників і порогів допустимості.

Корпоративні цілі та політика, визначені вищим керівництвом, разом з іншими авторитетними джерелами та стандартами сприяють розробці реєстру ризиків. Реєстр ризиків використовується для формування анкет оцінки ризиків, які використовуються для проведення оцінки ризиків. Результати оцінки ризику керують розробкою та впровадженням планів усунення ризиків або їх зменшення. Ці плани, а також результати доводяться до вищого керівництва [30, 31].

Корпоративні цілі та реєстр ризиків використовуються для розробки показників — KPI та KRI відповідно. Панель показників або результати регулярно повідомляються вищому керівництву. На рисунку 2.1 наведено огляд робочого процесу автоматизації показників ризику в типовому рішенні GRC.

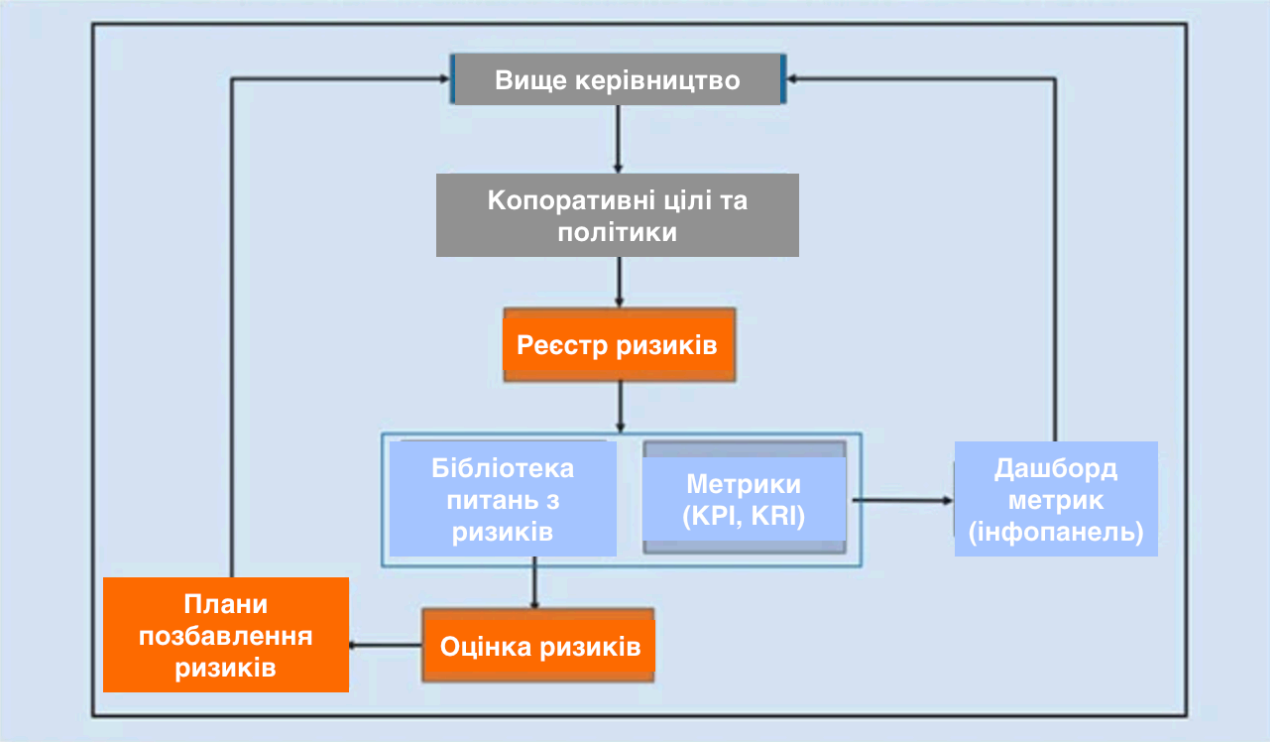


Рис. 2.1. Огляд робочого процесу автоматизації показників ризику в типовому рішенні GRC

Важливо усвідомлювати загальні проблеми, пов'язані зі збиранням показників ризику та KPI. Ось три основні проблеми, які ускладнюють збирання показників ризику:

*Неясність обов'язків:* Найчастіше керівники управління ризиками не розподіляють обов'язки між відповідними членами команди. В результаті стає незрозумілим, хто відповідає за збір показників та звітність [41, 42].

*Відсутність доступності даних:* Вкрай важливо зберігати та мати доступ до правильних видів даних, тому що це рушійна сила процесу прийняття стратегічних рішень. На жаль, багато груп безпеки стикаються з проблемами якості даних - працюючи з суперечливими даними, відсутніми даними або надмірними даними. Внаслідок цього членам груп доводиться витрачати значну кількість часу та ресурсів на збір даних, що призводить до неефективності та непродуктивності процесу управління ризиками.

*Недостатнє вивчення загроз:* Коли потенційна загроза виникає, необхідно діяти швидко. Оперативна інформація про загрози може стимулювати ефективні процеси прийняття рішень, але тільки в тому випадку, якщо відповідна

інформація надається швидко. Ґрунтуючись на застарілому програмному забезпеченні та інструментах, які вони використовують, багато фахівців безпеки зазнають затримки між тим, коли порушення відбувається і коли воно виявлено. На жаль, затримка загрози може призвести до значних витрат на відновлення та значного підриву репутації.

*Відсутність довіри:* Багато організацій не впевнені в точності своїх показників. Якщо група з питань безпеки перевіряє неповні або застарілі дані з одного джерела, це може призвести до неточностей у звітності та висновках [49].

Як тільки команди безпеки матимуть змогу вирішати ці проблеми, вони зможуть ефективно визначати метрики для оцінки ефективності процесу управління ризиками ІБ.

### 2.3.2 Метрики в управлінні інцидентами

У світі безперервної роботи систем технічні інциденти ведуть до серйозних наслідків.

Щогодини простою в роботі системи обходиться компаніям у середньому 300 тисяч доларів США втраченої вигоди, втраченої продуктивності співробітників та витрат на технічне обслуговування. У разі масштабних відмов витрати можуть зростати як на дріжджах (можна згадати компанію Delta Airlines, яка втратила близько 150 млн. доларів США через збій у роботі IT у 2017 році). Клієнти, які не можуть сплатити рахунки, провести важливу відеоконференцію або купити авіаквиток, швидко йдуть до конкурентів.

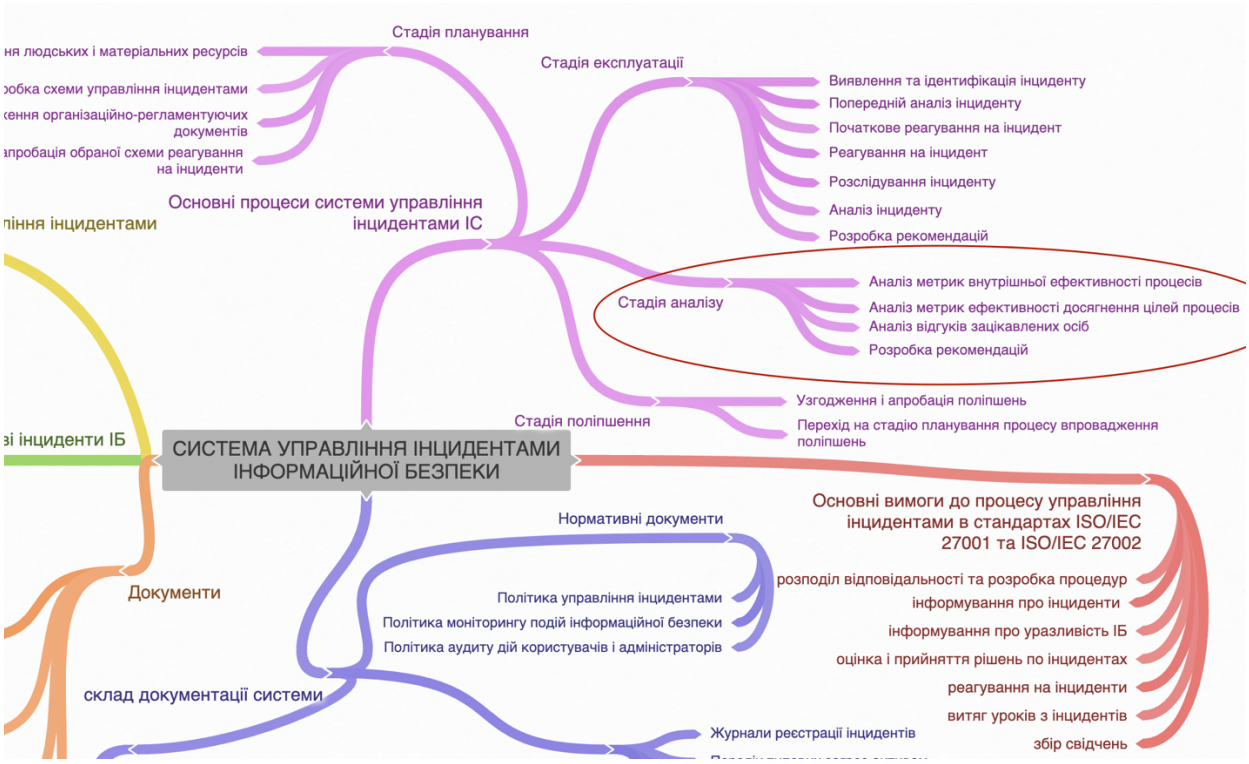


Рис. 2.2. Стадія аналізу управління інцидентами ІБ

На рис. 2.2 ми бачимо візуалізація системи управління інцидентами інформаційної безпеки, яка є у відкритому доступі. Як можна помітити, невід'ємним етапом системи є етап аналізу, який включає в себе аналіз метрик внутрішньої ефективності процесів, аналіз метрик ефективності досягнення цілей процесів і т.д.

На карту поставлено дуже багато. Тому командам дуже важливо відстежувати KPI управління інцидентами, а також використовувати результати для виявлення, діагностики, виправлення та, нарешті, запобігання інцидентам.

Позитивний момент полягає в тому, що при обробці інцидентів у веб-сфері та програмному забезпеченні (на відміну від механічних поломок та відключення систем) команди зазвичай отримують набагато більше даних. Тому вони можуть ефективніше розібратися в ситуації та провести покращення.

Але є і мінуси. Іноді стає складніше зрозуміти проблему за наявності великого обсягу даних.

Ключові показники ефективності (KPI) допомагають компаніям визначити, чи вони досягають конкретних цілей. У контексті управління інцидентами цими

показниками може бути кількість інцидентів, середній час розв'язання або середній час між інцидентами [43, 44].

Під час відстеження KPI керування інцидентами можна виявити та діагностувати проблеми з процесами та системами, визначити орієнтири та поставити реалістичні цілі для роботи команди, а також знайти відправну точку для вирішення масштабних питань.

Припустимо, що компанія прагне вирішення всіх інцидентів протягом 30 хвилин, але команді це вдається в середньому за 45 хвилин. Без конкретних показників важко зрозуміти, у чому проблема. Система оповіщення спрацьовує надто повільно? У процесі щось працює? Потрібні сучасніші діагностичні інструменти? Ця проблема пов'язана з командою чи обладнанням?

Тепер додайте показники. Якщо відомо, скільки часу потрібно системі оповіщення для спрацьовування, ви зможете зрозуміти, чи є вона причиною проблеми. Якщо діагностика займає більше половини часу, ви можете зосередитись на усуненні несправностей у ній. Якщо команда B працює на 25 % повільніше, ніж команди A, C та D, можна спробувати зрозуміти, чому це відбувається [45].

KPI не усунуть ваші проблеми автоматично, але вони допоможуть зрозуміти суть неполадок і вкажуть, куди потрібно звернути увагу та зусилля.

Якщо ви використовуєте інструмент оповіщення, корисно знати, скільки оповіщень генерується протягом певного періоду часу. За допомогою рішення Jira Service Management ви зможете надсилати оповіщення, а також створювати звіти та дашбоарди для їх відстеження.

Шукайте періоди, коли спостерігається значне чи нетипове зростання чи падіння, і навіть позитивна динаміка. При виявленні таких змін проаналізуйте причини та способи реагування ваших команд на них.

Кількість інцидентів за певний період. Відстеження кількості інцидентів за певний період передбачає підрахунок середньої кількості інцидентів за певний період. Цим періодом може бути тиждень, місяць, квартал, рік чи навіть день.

Згодом інциденти відбуваються частіше чи рідше? Кількість інцидентів вважається прийнятною чи її можна скоротити? Після того, як ви зрозумієте, в чому полягає проблема з кількістю інцидентів, ви зможете припустити, чому це число зростає або залишається високим і що команда може зробити для вирішення проблеми.

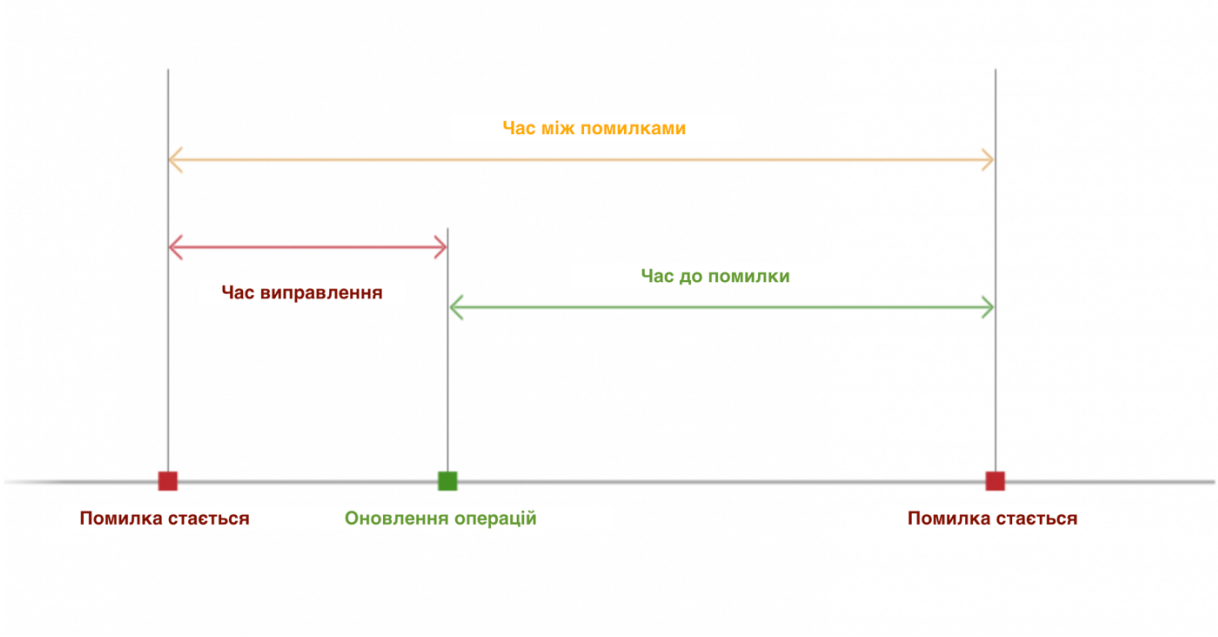


Рис. 2.3. Метрики в управлінні інцидентами ІБ

MTBF (середнє напрацювання на відмову/помилку) — середній час роботи технічного продукту між усунутими збоями. За допомогою цього показника можна відстежувати доступність та надійність усіх продуктів.

Як і інші показники, він наводить на серйозніші питання. Якщо значення MTBF недостатньо високе, варто задуматися, чому системи так часто виходять з ладу і як можна зменшити чисельність майбутніх збоїв або запобігти їм.

MTTA (середній час підтвердження) - це середній час, який проходить між отриманням оповіщення та моментом, коли учасник команди підтвердить інцидент і почне працювати над його усуненням. Цей показник є важливим тим, що за його допомогою можна зрозуміти, наскільки швидко ваша команда реагує на інциденти.

Якщо з'ясувалося, що швидкість реагування недостатньо висока, можна поставити нові питання. Чому значення MTTA таке велике? Команди перевантажені, відволікаються чи можуть зрозуміти, кому адресовано

оповіщення? За допомогою MTTA можна визначити проблему, а подібні питання допоможуть дістатися її суті.

MTTD (середній час виявлення) – це середній час, необхідний вашій команді, щоб виявити проблему. Цей термін часто використовується у сфері кібербезпеки командами, які зосереджені на виявленні атак та випадків несанкціонованого доступу.

Якщо значення цього показника різко змінюється чи залишається недостатньо високим, варто з'ясувати причину.

MTTR може означати середній час виправлення, рішення, реагування чи відновлення. Мабуть, найбільшу користь становить середній час рішення. Цей показник дозволяє зафіксувати не лише час, витрачений на діагностику та усунення безпосередньої проблеми, а й час на запобігання повторенню такої проблеми у майбутньому. Відновлення є основним показником DevOps; саме його, на думку програми DevOps Research and Assessment (DORA), можна використовуватиме оцінки стабільності команди DevOps.

Цінність цього показника найкраще проявляється під час діагностики. Чи дозволяються інциденти так швидко і ефективно, як ви очікували? Якщо ні, потрібно з'ясувати причину, через яку час вирішення не відповідає цільовому значенню [32, 47].

Відновлення є основним показником DevOps; саме його, на думку програми DevOps Research and Assessment (DORA), можна використовуватиме оцінки стабільності команди DevOps. Це сукупний час, що йде на виявлення проблеми, пом'якшення її наслідків та повне усунення.

Час безвідмовної роботи - це кількість часу (у відсотках), протягом якого системи доступні та працездатні.

З розширенням взаємозв'язків онлайн-сервісів та зростанням складності самих систем стало зрозуміло, що гарантія безвідмовної роботи протягом 100% часу неможлива. У випадку більшості продуктів прагнуть забезпечити високу доступність, тобто створити таку систему або продукт, які можуть працювати без перерви протягом тривалого часу. Згідно з галузевим стандартом, безвідмовна

робота протягом 99,9% часу – це дуже добрий результат, а протягом 99,99% – відмінний.

Відстежувати значення цього показника обов'язково до виконання обіцянок, даних клієнтам. Як і інші показники, він становить лише відправну точку. Якщо безвідмовну роботу не вдається забезпечувати на рівні 99,99 %, для розуміння причини потрібно буде глибше вивчити проблему, поговорити з командою, а також проаналізувати процес, структуру, доступ чи технологію.

«Інциденти набагато унікальніші, ніж прийнято про них думати. Два інциденти, дозволити які можна за один проміжок часу, можуть значно відрізнятися за тим, наскільки вони несподіваними і незбагненними виявилися для відповідальних фахівців. Крім того, заходи щодо пом'якшення наслідків або виправлення ситуації можуть нести абсолютно різні ризики у різних інцидентах. Інциденти — це не деталі з конвеєра, у яких показником якості є обмежений розкид фізичних розмірів»,

— Джон Оллспоу, «Як уникнути малозмістовних даних про інциденти» (John Allspaw, Moving Past Shallow Incident Data)

KPI є ефективним способом для оцінки ефективності процесу управління інцидентами, але лише KPI недостатньо. Їх потрібно використовувати як відправну точку. Вони допоможуть виявити причину проблеми та стануть першим кроком на складному шляху до ефективного покращення [50].

**Висновки до Розділу 2**

Показники/метрики ризику та ключові показники ризику (KRI) є способом вимірювання ефективності. Важливість даних показників пов'язана з тим, що менеджери з управління ризиками повинні довести, що вони відповідають очікуванням не лише регуляторів, експертів та їхньої ради директорів, а й їхніх клієнтів, інвесторів, колег та спільнот.

В епоху прозорої економіки швидкий розвиток та поширення таких технологій, як соціальні мережі, не залишили компаніям жодного місця

сховатися. Ми живемо в епоху прозорості, коли громадськість має право впливати на репутацію компанії.

Без вимірювання будь-якого ключового показника ризику навряд чи можна продемонструвати цінність програми управління ризиками компанії або ступінь пом'якшення раніше невстановлених ризиків.

Однак, такі метрики як KPI, KRI мають недоліки. Так, можна легко потрапити у залежність від малозмістовних даних. Якщо ваша команда дозволяє інциденти недостатньо швидко, для вирішення проблеми знадобиться щось більше, ніж просте усвідомлення цього факту. Вам потрібно розуміти, як і чому команда вирішує чи не вирішує проблеми. Крім того, потрібно знати, чи можна порівняти проблеми, які ви порівнюєте.

На підставі KPI не можна зрозуміти, як ваші команди підходять до вирішення складних завдань, чому інциденти відбуваються все частіше або чому на дозвіл інциденту А пішло втричі більше часу, ніж інцидент Б.

Для цього потрібні аналітичні висновки. Однак дані можуть стати не лише відправною точкою на шляху до цих висновків, а й перешкодою. Через них може скластися помилкове враження ефективної роботи, коли показники не покращуються. Показники не враховують відмінності (іноді дуже суттєві) між інцидентами або підходами до їх вирішення. Крім того, за кадром залишається досвід ваших команд та фундаментальна складність самих інцидентів.

Завдяки вивченому у розділі два, можна зробити висновок, що ефективнішим підходи до оцінювання ефективності процесів ІБ є комплексний аналіз показників таких як KPI, KRI.

Приклади, наведені у Розділі 2 є джерелом натхнення і можуть, з невеликими змінами, застосовуватися до більшості організацій, які включили всі або деякі з п'яти процесів СУІБ, які були розглянуті.

Підсумуємо, у чому інтегровані в СУІБ показники ефективності процесів ІБ можуть допомогти команді з ІБ:

- Відстежувати кількісну інформацію, щоб вони могли продемонструвати свої зусилля щодо захисту даних організації та інших технологічних активів;

- Переглянути, які з їхніх зусиль виявилися корисними, які потребують додаткової роботи, а які потребують капітального перегляду;

- Отримувати ширшу та чіткішу картину ситуації безпеки своєї організації, щоб приймати кращі та більш обґрунтовані рішення щодо загальної безпеки своєї організації.

# РОЗДІЛ 3
# ДОСЛІДЖЕННЯ І РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ВИКОРИСТАННЯ МЕТРИК В ОЦІНЮВАННІ ЕФЕКТИВНОСТІ ПРОЦЕСІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

## 3.1 Опис підприємства та постановка задачі на використання метрик на прикладі

Для використання метрик на прикладі, візьмемо реальне підприємтсво та спробуємо дослідити ефективність впроваджених процесів ІБ.

Прикладом підприємтсва слугуватиме холдинг “Назва груп”. Компанія активно розвивається у різних сферах бізнесу, постійно освоюючи нові напрямки та галузі. Та основними сферами діяльності компанії “Назва груп” є: дистрибуція та логістика, виробництво, рітейл, транспортно-експедиційні послуги, імпорт та створення нових продуктів та просування на внутрішньому і зовнішніх ринках.

Організація поділена на наступні відділи:

- Відділ безпеки
- Відділ ІТ
- Служба обліку та аудиту
- Фінансовий відділ
- Відділ маркетингу
- Служба логістична
- Відділ дистрибуції

Для кращого розуміння процесів, що відбуваються всередині компанії, наведено список основних бізнес-процесів організації:

- Корпоративне управління
- Стратегічний менеджмент
- Постачання
- Виробництво
- Маркетинг

- Збут
- Бухгалтерський облік
- Управління кадрами
- Забезпечення ІТ
- Забезпечення ІБ
- Підтримка клієнтів

Штат – більш ніж 2500 співробітників. Географія роботи – північна, центральна та західна частина України (18 областей).

## 3.2 Дослідження і розробка рекомендацій по використанню метрик в оцінюванні ефективності процесів інформаційної безпеки

Оскільки для прикладу ми розглядаємо материнську компанію холдингу, основною задачою є контроль дочірніх компаній, забезпечення їх необхідними ресурсами та збереження високої репутації.

Після останнього аудиту за CMM компанія отримала рівень 3, який відповідає рівню зрілості процесів, як “визначені”. Отже, ми розуміємо, що процеси ІБ чітко визначені та проактивні. Однак, в компанії ніколи не оцінювалась ефективність впроваджених процесів кількісно.

Для оцінки ефективності впроваджених процесів інформаційної безпеки, пропонується обрати наступні процеси, як найбільш критичні для такого типу та масштабу організації:

- Контроль доступу
- Управління обізнанітю
- Управління інцидентами
- Управління ризиками
- Управління вразливостями
- Управління змінами

Для оцінки ефективності вищезазначених процесів, обираємо використання показників KPI та KRI в комплексі для кращого розуміння тенденції процесу ІБ.

Для вибору KPI будемо використовувати метод, описаний у Розділі 2 SMART. Процес управління показниками KPI для організації пропонується наступний:

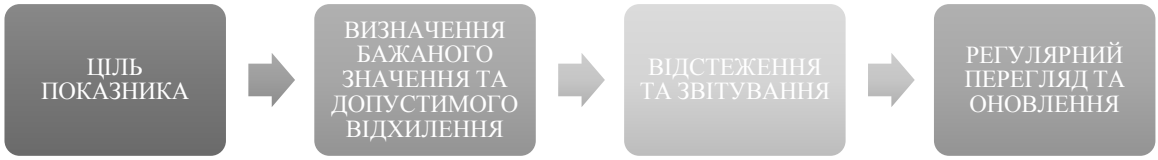


Рис. 3.1. Процес управління показниками KPI

Процес управління показниками KRI для організації пропонується наступний:

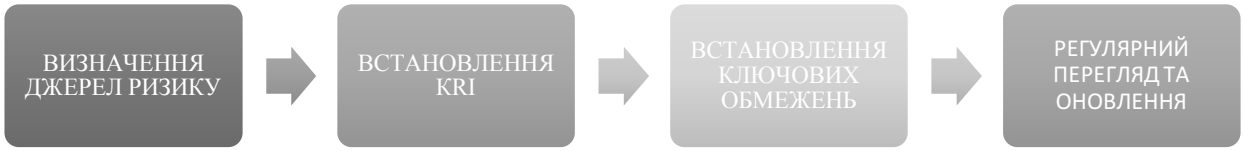


Рис. 3.2. Процес управління показниками KRI

За допомогою досліджених найкращих практик, вимог стандартів та досвіду використання метрик для оцінювання ефективності процесів ІБ, створимо таблиці із запропонованими для організації показниками KPI та KRI для ключових процесів ІБ з поясненням до кожного.

Показники процесу керування доступом мають значення, оскільки IT-безпека постійно змінюється. Зовнішнє середовище безпеки змінюється щороку. В організації щомісяця приходять і йдуть співробітники. Згідно з даними уряду США, середній термін перебування співробітників в Америці становить близько чотирьох років. Таким чином, навчання та процеси, які ви створили кілька років тому, можуть бути недостатніми.

По суті, метрики щодо керування доступом важливі з кількох причин. Як ми розглядали раніше, по-перше, вони посилають сигнал співробітникам і керівникам, що проблеми з керуванням доступом відстежуються і що проблеми будуть виявлені. По-друге, показники керування доступом допомагають оцінювати прогрес у порівнянні з вашими цілями та стратегією. У сфері IT-

безпеки іноді важко визначити успіх. Ми можемо продемонструвати успіх, щоб показати, що наша організація досягає або перевищує показники з процесу керування доступом. Отже, нижче наведено приклад таких показників.

Таблиця 3.1

Метрики вимірювання ефективності процесу управління доступом на підприємстві

| **Показники** | **Можливі вимірювання** | **Оцінювання** |
|---|---|---|
| Кількість неактивних облікових записів користувачів | Загальна кількість неактивних облікових записів користувачів | Ефективність процесу. Неактивні / без власника облікові записи користувачів. |
| Кількість користувачів з адміністративним доступом | Кількість користувачів з адміністративним доступом | Ключові ризики. |
| Огляди привілеїв доступу | Кількість переглядів доступу на рік | Ефективність процесу. Ключові ризики. Дозволи / привілеї , які використовуються і є ефективними, та які не використовуються на регулярній основі. |
| Кількість програм, інтегрованих у поточну систему контролю доступу | Кількість програм, інтегрованих у поточну систему контролю доступу | Ефективність процесу. Ключові ризики. |
| Час надання доступу після запиту менеджера | Години<br>Доби | Швидкість / ефективність процесу |
| Кількість неактивних облікових записів | Кількість користувачів, які не входили в систему протягом 3 місяців | Неактивні / без власника |
| Невизначені прилади у внутрішній мережі | Кількість невизначениз приладів у внутрішній мережі | Ключові ризики. |

Продовження табл. 3.1

Метрики вимірювання ефективності процесу управління доступом на підприємстві

| Показники | Можливі вимірювання | Оцінювання |
|---|---|---|
| Спроби авторизації | Кількість невдалих спроб входу (або відсоток) на місяць | Ризики зламу. Зверніть увагу, коли цей показник з часом зростає. |
| Облікові записи користувачів із простроченими паролями | Кількість облікових записів користувачів із простроченими паролями | Відповідність вимогам політики паролів. |
| Кількість привілейованих облікових записів без власника | Кількість привілейованих облікових записів без власника | Ключові ризики. |
| Кількість інцидентів безпеки через критичну роль і комбінації прав доступу | Кількість інцидентів безпеки через критичну роль і комбінації прав доступу | Ключові ризики. |
| Час до деактивації прав доступу співробітника | Години<br>Доби | Ключові ризики. |
| Облікові записи користувачів із прямими повноваженнями, не призначеними через ролі | Кількість облікових записів користувачів із прямими правами, не призначеними через ролі | Гігієна надання доступу. |
| Відсоток паролів, оновлених за останні 12 місяців | Кількість облікових записів з паролями, оновленими за останні 12 місяців / загальна кількість облікових записів | Ефективність процесу. Кількість співробітників, які дотримуються вимог щодо пароля. |
| Відсоток паролів, що відповідають правилам складності | Кількість облікових записів з паролями, що відповідають правилам складності / загальна кількість облікових записів | Ефективність процесу. Кількість співробітників, які дотримуються вимог щодо пароля. Відповідність вимогам політики паролів. |

Наступний процес, який ми розглянемо буде управління обізнаністю з ІБ. Важливим питанням стає, на яких саме ризиках і поведінці нам слід зосередитися, оскільки ризики часто унікальні для кожної організації. Після аналізу літератури стає ясним , що більшість організацій поділяють однакові три найбільші людські ризики – фішинг, паролі та оновлення. Таким чином, я збираюся визначити ці ризики, поведінку, яка керує цими ризиками, і як виміряти цю поведінку. Також варто зазначити, що в залежності від організації слід вирішити заздалегідь, чи ціль вимірювати та відстежувати поведінку окремої особи чи ролі/відділу/підрозділу в цілому. У разі відстеження на індивідуальному рівні необхідно переконатись, що вживаються заходи для захисту інформації та конфіденційності кожної особи. Залежно від розміру організації та обсягу даних, які вона збирає, також може знадобитися співпрацювати з кимось в організації, хто спеціалізується на аналітиці даних / бізнес-аналітиці, щоб допомогти компанії нормалізувати / проаналізувати результати. Отже, спробуємо визначити рекомендовані показники ефективності процесу з управління обізнаністю персоналу щодо питань ІБ.

Таблиця 3.2

Метрики вимірювання ефективності процесу управління обізнаністю ІБ на підприємстві

| **Показники** | **Можливі вимірювання** | **Оцінювання** |
|---|---|---|
| Участь в інформаційних тренінгах | Кількість учасників / загальна кількість працівників | Відсоток участі в курсах. Ефективність процесу. |
| Відсоток невдалих тестів | Кількість непройдених тестів / загальна кількість тестів | Відсоток нескладених тестів після тренінгів/курсів з інформаційної безпеки. Ефективність процесу. |
| Обізнаність з аспектами кібербезпеки | Відсоток учасників, які пройшли навчання | Збільшення відвідуваності. Ефективність процесу. |
| Співробітники задоволені змістом навчання/курсу | Кількість працівників, задоволених змістом курсу | Ефективність процесу. |

Продовження табл. 3.2

Метрики вимірювання ефективності процесу управління обізнаністю ІБ на підприємстві

| Показники | Можливі вимірювання | Оцінювання |
|---|---|---|
| Зменшення кількості інцидентів, які є наслідком електронної атаки | Кількість зафіксованих інцидентів або зловмисного програмного забезпечення, які є результатом фішингу | Ефективність процесу. Ключові ризики. |
| Збільшення кількості співробітників, які повідомляють про фішингову діяльність | Кількість зареєстрованих фішингових атак | Збільшення кількості співробітників, які повідомляють про фішингову діяльність. Ключові ризики. Ефективність процесу. |
| Персональні дані обробляються відповідно до принципів конфіденційності, встановлених у Банку | Кількість порушень, пов'язаних з правилами конфіденційності | Ефективність процесу. Ключові ризики. |
| Зменшення кількості слабких паролів | Кількість інцидентів, пов’язаних зі слабкими паролями після навчання (курсу) / Кількість інцидентів, пов’язаних із слабкими паролями до навчання (курсу) | Ефективність процесу. Ключові ризики. |

Є два рівні ефективного управління змінами. Співробітники компанії вносять зміни у свою роботу, а компанія надає їм процеси, інструменти та системи, які згладять зміну. Вимірювання успіху в управлінні змінами починається з розгляду кількох ключових показників ефективності на обох рівнях. Вимірювання успішності змін має бути не останнім кроком у процесі управління змінами, а найкращою практикою, важливою на кожному етапі. Оцінка зусиль на цьому шляху дозволить компанії бути проактивною і виправляти невдачі та непорозуміння, перш ніж вони стануть справжніми

проблемами, отже не доведеться повертатися назад і скасовувати нові процеси, системи чи способи роботи після їх впровадження. Рекомендовані метрики для оцінювання ефективності процесу управління змінами наступні:

Таблиця 3.3

Метрики вимірювання ефективності процесу управління змінами ІБ на підприємстві

| **Показники** | **Можливі вимірювання** | **Оцінювання** |
|---|---|---|
| Кількість несанкціонованих змін | Кількість несанкціонованих змін / кількість внесених змін<br>Кількість несанкціонованих змін / кількість несанкціонованих змін за попередній місяць (або рік) | Ефективність процесу |
| Зміна використання робочої сили | Загальна кількість робочих годин, витрачених на координацію змін / Загальна кількість доступних робочих годин на координацію (не впровадження) змін | Наявні витрати робочої сили |
| Кількість невдалих змін<br>Зміна рівню успіху | Кількість невдалих змін за місяць<br>Кількість невдалих змін на рік<br>Кількість невдалих змін / Кількість реалізованих змін<br>Час впровадження зміни певного типу (год.) | Ефективність процесу<br>Вдосконалення |
| Середній час, витрачений на впровадження змін залежно від типу, терміновості чи пріоритету | Час впровадження зміни певного типу (год.)<br>Час впровадження зміни з певним пріоритетом (годин) | Ефективність процесу<br>Вдосконалення |
| Зміни внесені в робочий час | Кількість змін, внесених протягом робочого часу на тиждень<br>Кількість невдалих змін, внесених під час діяльності / успішних змін, внесених під час діяльності | Успішне обслуговування |
| Коефіцієнт впровадження змін | Загальна кількість впроваджених змін / Загальна кількість змін у процесі розробки | Ефективність обробки змін |

Продовження табл. 3.3

Метрики вимірювання ефективності процесу управління змінами ІБ на підприємстві

| Показники | Можливі вимірювання | Оцінювання |
|---|---|---|
| Коефіцієнт перепланованих змін | Кількість перепланованих змін / Загальна кількість змін у потоці задачі | Впровадження змін за графіком |
| Частка термінових змін | Кількість аварійних змін / загальна кількість змін у потоці задач | Ефективність процесу<br>Ключові ризики |
| Кількість інцидентів, викликаних змінами<br>Частка інцидентів у результаті змін | Кількість змін, що призвели до інцидентів / загальна кількість впроваджених змін | Ефективність процесу<br>Ключові ризики |
| Кількість змін, що спричинили перерву в будь-якій службі протягом робочого часу | Кількість змін, які призводять до перерв у робочий час<br>Кількість змін, що призвели до переривання будь-якої послуги / загальна кількість впроваджених змін | Ключові ризики |
| Кількість несанкціонованих змін | Кількість виявлених несанкціонованих змін / кількість внесених змін | Зміни, які обійшли процес управління змінами<br>Ефективність процесу<br>Ключові ризики |

Показники вразливості мають вирішальне значення для успішного вимірювання програми керування вразливостями. Розглядаючи, які показники розглядати, підхід не повинен полягати в простому зборі статистичних даних і діаграм, але він повинен зосереджуватися на визначенні пріоритетів для виправлення найбільш критичних систем і програм компанії.

Кроки для збору правильних показників для організації потребують ретельного планування ІТ-командами та відділами безпеки. Цього можна

досягти, розуміючи важливість збору показників. Наступні метрики можуть допомогти оцінити ефективність впровадженого на підприємстві процесу управління вразливостями:

Таблиця 3.4

Метрики вимірювання ефективності процесу управління вразливостями ІБ на підприємстві

| **Метрики** | **Можливі вимірювання** | **Оцінювання** |
|---|---|---|
| Середній час виявлення | Години<br>Доби | Середній проміжок часу до виявлення відомих вразливостей у всій організації.<br>Ефективність процесу. |
| Середній час для вирішення | Години<br>Доби | Середній проміжок часу, витрачений на усунення/виправлення вразливостей після виявлення за допомогою оцінки вразливості.<br>Ефективність процесу. |
| Середнє вікно експозиції | Години | Час, коли вразливість вперше стала загальнодоступною, до часу виправлення заражених систем.<br>Ефективність процесу.<br>Ключові ризики. |
| Покриття сканера | ІТ-активи, які скануються / Кількість важливих ІТ-активів, % | Співвідношення активів, які фактично скануються, до відомих активів (наприклад, із рішення для керування активами).<br>Ключові ризики. |

Продовження табл. 3.4

Метрики вимірювання ефективності процесу управління вразливостями ІБ на підприємстві

| Метрики | Можливі вимірювання | Оцінювання |
|---|---|---|
| Кількість наданих винятків | Кількість вразливостей, які не були усунені з певних причин | Кількість вразливостей, які не були усунені з різних причин.<br>Ключові ризики. |
| Швидкість повторного відкриття вразливості | Частота повторюваних (знову відкритих) уразливостей | Ефективність процесу санації. Високий показник означає, що процес виправлення є помилковим.<br>Ключові ризики. |
| % систем без відкритої високої/критичної вразливості | Кількість виправлених систем без відкритих високих уразливостей / загальна кількість ключових систем | Який % систем повністю виправлено та не має високої вразливості.<br>Ключові ризики.<br>Ефективність процесу. |
| Кількість відкритих критичних/високих уразливостей | Кількість відкритих критичних/високих уразливостей | Ключові ризики.<br>Ефективність процесу. |

Підсумуємо та виберемо із запропонованих метрик найбільш підходящі для підприємства, яке було взято за приклад, та сформулюємо рекомендації щодо їх використання.

Для процесу управління доступом пропонується обрати наступні метрики для оцінки ефективності даного процесу:

- Кількість перевірок привілеїв для кожної критичної системи, порівняно з минулим роком
- Кількість інцидентів ІБ, пов’язаних із доступом, порівняно з минулим роком
- Відсоток паролів, що відповідають правилам складності, порівняно з минулим півріччям

- Час, необхідний на деактивацію облікового запису користувача після його звільнення або зміни посади
- Кількість невдалих спроб авторизації в облікові записи адміністратора критичних систем на місяць

Для компанії, яка раніше не використовувала практику оцінки ефективності процесів ІБ, даних критеріїв буде достатньо. Ці показники допоможуть команді зосередитись на проблемах, які є у процесі управління доступом та вжити необхідних заходів щодо усунення наявних пробілів.

Так само надаймо рекомендаційні метрики для інших процесів ІБ підприємства, які були визначені як критичні. Наступний процес, який ми розглянемо, буде управління обізнаністю персоналу щодо питань ІБ:

- Кількість працівників, що приймали участь у тренінгах за останні півроку (зручніше порахувати у відсотках відносно сумарної кількості співробітників)
- Відсоток невдалих тестів порівняно з минулими тестами
- Кількість зафіксованих інцидентів, які виникли у результаті фішингу або використання соціальної інженерії
- Кількість зафіксованих інцидентів, які виникли у результаті невиконання інструкція та політик безпеки
- Кількість зафіксованих інцидентів, які виникли у результаті використання слабких паролів (зручніше оцінювати як частку кількості таких інцидентів після відповідного тренінгу і до)

Для процесу управління змінами рекомендованими метриками для регулярної оцінки ефективності даного процесу пропонуються:

- Частка інцидентів, викликаних змінами
- Кількість несанкціонованих змін
- Коефіцієнт перепланованих змін
- Кількість змін, що були успішно впроваджені, порівняно з минулим півріччям
- Кількість змін, що були впровадженні у визначені терміни, порівняно з минулим півріччям

Для останнього критичного процесу управління вразливостями ІБ, пропонуються наступні рекомендаційні критерії щодо оцінки ефективності існуючого процесу:

- Середній час виявлення вразливості

- Середній час вирішення вразливості
- Покриття сканера, що використовується в компанії
- Кількість інцидентів ІБ після впровадження нового сканеру
- Кількість інцидентів ІБ після заощадження команди з пентестів

Слід також пам’ятати, що ефективний процес оцінки ефективності полягає у порівнянні результатів з попередніми оцінками, тому регулярність та збір даних у цьому процесі є ключовими.

Вивчення тенденцій дозволяє підприємству відстежувати ефективність безпеки з часом і визначати місця, які вимагають коригування у системі безпеки. На більш високому рівні шляхом впровадження рекомендацій допоможуть підприємству досягнути наступних своїх цілей:

- Оцінка його відповідності законодавству та нормам
- Покращення ефективності впроваджених заходів безпеки
- Відповіді на бізнес-питання високого рівня щодо безпеки, сприяння прийняттю стратегічних рішень найвищим керівництвом організації.

**Висновки до Розділу 3**

Завдяки вивченим нормативним документам та їх вимогам до оцінювання ефективності процесів ІБ та дослідженому досвіду використання підходів до оцінювання ефективності на підприємствах, а також дослідженим метрикам та способам їх грамотного визначення, було проаналізовано процеси ІБ на підприємстві та запропоновано метрики для кожного з них. Серед цих процесів були: процес управління доступом, процес управління обізнаністю персоналу щодо питань ІБ, управління змінами та управління вразливості. Дані процеси були визначені як ключові та критичні для компанії, оскільки компанія є холдингом, та її основна ціль позбутися або зменшити ризики саме у питаннях взаємодії з дочірніми компаніями. Для всіх вищезазначених процесів були запропоновані показники та вимірювання для оцінки ефективності кожного з процесів, а також наведені помітки щодо результатів використання тієї чи іншої метрики.

У ході розробки рекомендацій щодо використання метрик в оцінюванні ефективності процесів інформаційної було розроблено 4 таблиці з показниками та метриками для оцінювання ефективності процесів ІБ та підприємстві.

# ВИСНОВКИ

Сучасні загрози дуже різноманітні, і сучасні зловмисники зосереджуються не лише на великих організаціях. Кожна людина піддається ризику, і великим і малим організаціям необхідно мати належний захист, а також знання та ресурси, необхідні для оцінки їхньої ефективності. На щастя, оцінка таких речей, як видимість мережі, керування правами доступу та звітування про інциденти та помилкові тривоги, може допомогти організаціям визначити загальний стан мережі та ефективність захисту.

Інформація щодо ефективності впроваджених процесів безпеки також може допомогти групам безпеки залучити додаткову підтримку з боку CISO та правління компаній під час покращення та розширення своїх можливостей захисту. У міру того як зловмисники розвиваються, інструменти захисту мережі розвиваються разом з ними, і допомога сучасним бізнес-лідерам зрозуміти кроки, необхідні для того, щоб бути на крок попереду кіберзлочинців, є важливою.

У першому розділі магістерської роботи було досліджено вимоги нормативних документів щодо оцінки ефективності процесів ІБ та досвід використання підходів до оцінки ефективності. Про вимірювання та оцінку ефективності інформаційної безпеки говорять багато стандартів, а саме:

- ISO 27001, ISO 27002
- COBIT
- ITIL
- ISO 13335
- ISO 21827
- GAISP

Сурових конкретних вимог щодо самого процесу оцінки ефективності нормативні документи не фіксують.

У другому розділі було проаналізовано використання метрик в системі управління інформаційної безпеки та безпосередньо метрики для оцінки

ефективності процесів управління ризиками та інцидентами. Було досліджено та розглянуто впровадження метрик в систему управління інформаційною безпекою та способи грамотного визначення та вибору метрик.

Третій розділ розглядає розробку рекомендацій щодо використання метрик оцінювання ефективності процесів ІБ на підприємстві. Наведено приклад підприємства та за допомогою досліджених у попередніх розділах методів вибору та підбору метрик, розроблено метрики та показники для оцінки ефективності процесів управління змінами, обізнаністю, доступом та вразливостями.

Розроблені та наведені в роботі рекомендаційні метрики для оцінювання ефективності процесів інформаційної безпеки на підприємстві можуть бути використані при плануванні та реалізації процесу оцінювання ефективності та подальшого вдосконалення процесів на підприємстві.

# СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ


1) How to measure ISO 27001 ISMS efficiency with KPIs https://www.neupart.com/good-enough-it-risk-management/27001-isms-kpi-metrics
2) 4 Steps Toward Successfully Measuring the Effectiveness of Your Security Controls https://www.sentinelone.com/blog/4-steps-toward-successfully-measuring-the-effectiveness-of-your-security-controls/
3) Guidelines and standards for measuring the effectiveness of pr programs and activities https://instituteforpr.org/effectiveness-programs-activities/
4) Обзор стандарта COBIT (Control Objectives for Information and related Technology) v. 4.1. Методология, процессы, критерии, внедрение Cobit. https://www.itexpert.ru/rus/biblio/detail.php?ID=16161
5) ISO/IEC 27001:2022(en) Information security, cybersecurity and privacy protection — Information security management systems — Requirements
6) Измерение эффективности процессов кибербезопасности. Метрики ИБ. Часть 3 https://www.securityvision.ru/blog/izmerenie-effektivnosti-protsessov-kiberbezopasnosti-metriki-ib-chast-3/
7) Как посчитать эффективность информационной безопасности? Алексей Лукацкий, Бизнес-консультант по безопасности CISCO
8) Методы оценки информационной безопасности https://sky-dynamics.ru/stati/metody-ocenki-informacionnoj-bezopasnosti/
9) Оценка эффективности информационной безопасности, Рустэм Хайретдинов, CEO компании Appercut Security
10) Конференція «Світ інформації та телекомунікацій», Батуркіна Анастасія, Теза «Застосування комп'ютерних інформаційних технологій в галузі кібербезпеки»
11) 27 жовтня 2022, Всеукраїнська науково-практична конференція «Актуальні проблеми кібербезпеки» Батуркіна Анастасія, Information security management. Measuring ISMS processes

12) Mishra S, Chasalow L. Information security effectiveness: A research framework. *Issues in Information Systems*. 2011; 12(1): 246–255. Available: http://iacis.org/iis/2011/246-255_AL2011_1677.pdf. [Google Scholar]

13) Kong HK, Kim TS, Kim J. An analysis on effect of information security investments: A BSC perspective. *Journal of Intelligent Manufacturing*. 2012; 23(4): 941–953. 10.1007/s10845-010-0402-7 [CrossRef] [Google Scholar]

14) Rhee HS, Ryu YU, Kim CT. (2012). Unrealistic optimism on information security management. *Computers & Security*. 2012; 31(2): 221–232. 10.1016/j.cose.2011.12.001 [CrossRef] [Google Scholar]

15) Baskerville R, Spagnoletti P, Kim J. Incident—centred information security: Managing a strategic balance between prevention and response. *Information & Management*. 2014; 51(1): 138–151. 10.1016/j.im.2013.11.004 [CrossRef] [Google Scholar]

16) Elizabeth Chew, Marianne Swanson, Kevin Stine, Nadya Bartol, Anthony Brown, and Will Robinson, NIST Special Publication 800-55 Revision 1, INFORMATION SECURITY, 2009.

17) How Do You Measure Security Control Effectiveness https://bestpractice.biz/how-do-you-measure-security-control-effectiveness/

18) Н.А. Маслова, Донецкий национальный технический университет, г. Донецк, Украина, Методы оценки эффективности систем защиты информационных систем

19) 14 Cybersecurity Metrics + KPIs You Must Track in 2022 https://www.upguard.com/blog/cybersecurity-metrics

20) Top 15 Cybersecurity Metrics and KPIs for Better Security https://cybertalents.com/blog/top-15-cybersecurity-metrics-and-kpis-for-better-security

21) Infosys.com | NYSE: INFY, Information security metrics, 1-4 p, 2021

22) Що таке MTTR, MTBF, MTTF і MTTA? Посібник з показників управління інцидентами, https://www.motadata.com/uk/blog/incident-management-metrics/

23) Risk management metrics to track, https://tensix.com/7-risk-management-metrics-to-track/

24) 7 KPIs You Can Use for Risk Management https://www.indeed.com/career-advice/career-development/kpi-for-risk-management

25) How to Measure Risk Management Performance: KPI & Metrics https://securityscorecard.com/blog/how-to-measure-risk-management-performance

26) Risk Management Metrics & Key Risk Indicators [Best Practices] https://www.logicmanager.com/resources/erm/risk-metrics-for-governance-effectiveness/

27) Как выбрать ключевые показатели эффективности и метрики управления инцидентами https://www.atlassian.com/ru/incident-management/kpis

28) Source: What Is KPI? (Key Performance Indicator) - SEO & Digital Marketing Blog (https://www.dopinger.com/blog/what-is-kpi)

29) What Is KPI Management? https://www.splunk.com/en_us/data-insider/kpi-management.html

30) How to Measure the Success of IAM Deployment https://www.spiceworks.com/it-security/identity-access-management/guest-article/how-to-measure-the-success-of-iam-deployment/

31) Are You Completing These Access Management Metrics Every Month? https://www.avatier.com/blog/are-you-completing-these-access-management-metrics-every-month/

32) What is Cybersecurity Performance Management? https://www.xmcyber.com/uncategorized/what-is-cybersecurity-performance-management/

33) Security Metrics – Reasons Why You Should Measure Them https://www.proserveit.com/blog/security-metrics-program

34) What is Security Metrics Management in information security? https://www.tutorialspoint.com/what-is-security-metrics-management-in-information-security

35) Lance Spitzner, Security Awareness Metrics – What to Measure and How https://www.sans.org/blog/security-awareness-metrics-what-to-measure-and-how/

36) Metrics for Measuring Change Management https://www.prosci.com/resources/articles/measuring-change-management-effectiveness-with-metrics

37) Metrics & KPIs for measuring change management, according to 2 change leaders https://www.zendesk.com/blog/measuring-change-management-success/

38) Vulnerability & Patch Management Metrics: Top 10 KPIs to Measure Success, https://purplesec.us/learn/vulnerability-management-metrics/

39) Jacobs MA. Complexity: Toward an empirical measure. *Technovation*. 2013; 33(4–5): 111–118. 10.1016/j.technovation.2013.01.001 [CrossRef] [Google Scholar]

40) Sqiure R, Song H. Cyber-physical systems opportunities in the chemical industry: A security and emergency management example. *Process Safety Progress*. 2014; 33(4): 329–332. 10.1002/prs.11676 [CrossRef] [Google Scholar]

41) Xu J, Ge H, Juanjuan X, Yangrui G. Study on the mode of intelligent chemical industry based on cyber-physical system and its implementation. *Advances in Engineering software*. 2016; 99: 18–26. 10.1016/j.advengsoft.2016.04.010 [CrossRef] [Google Scholar]

42) Institute Ponemon. Security effectiveness framework study; 2010. Available: http://trionlogics.com/wp-content/uploads/Security-Effectiveness-Framework-Study.pdf.

43) Ernst&Young. Global information security survey. Get ahead of cybercrime. Insight on governance, risk and compliance; 2014. Available: http://www.ey.com/Publication/vwLUAssets/EY-global-information-security-survey-2014/$FILE/EY-global-information-security-survey-2014.pdf.

44) PricewaterhouseCoopers [PWC]. Global state of information security survey 2014;. Defending yesterday; 2013. Available: http://www.pwc.com/gx/en/consulting-services/information-security-survey/download.jhtml.

45) European Union Agency for Network and Information Security. ENISA threat landscape: Overview of current and emerging cyber-threats; 2013. Available: https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape/enisa-threat-landscape-2013-overview-of-current-and-emerging-cyber-threats.

46) The Department for Business Innovation & Skills [BIS], PricewaterhouseCoopers [PWC]. Information security breaches survey; 2014. Available: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/307296/bis-14-767-information-security-breaches-survey-2014-technical-report-revision1.pdf.

47) Verizon. Data breach investigation report; 2014. Available: http://www.verizonenterprise.com/DBIR/2014/reports/rp_dbir-2014-executive-summary_en_xg.pdf.

48) Sansage. State of security information and event management processes. The burried truth; 2012. Available: http://www.firmenpresse.de/pdf-pressrelease178292.pdf.

49) Hewlett Packard Development Company [HP]. State of security operations. Report of capabilities and maturity of cyber defense organizations, Business white paper;: 2015. Available: http://h30499.www3.hp.com/t5/HP-Security-Products-Blog/State-of-Security-Operations-2015-Report/ba-p/6697279#.VXbfk0ZqG2m.

50) Hua M, Bapna S. Who can we trust? The economic impact of insider threats. *Journal of Global Information Technology Management*. 2013; 16(4): 47–67. 10.1080/1097198X.2013.10845648 [CrossRef] [Google Scholar]