Міністерство освіти і науки України
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
«ОДЕСЬКА ПОЛІТЕХНІКА»
Кафедра кібербезпеки та програмного забезпечення

КОНСПЕКТ ЛЕКЦІЙ

з дисципліни

«АНАЛІЗ ТА ОЦІНЮВАННЯ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ», частина 1

для здобувачів першого (бакалаврського) рівня освіти
спеціальності - 125 Кібербезпека

Одеса: Одеська політехніка, 2022

Міністерство освіти і науки України
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
«ОДЕСЬКА ПОЛІТЕХНІКА»
Кафедра кібербезпеки та програмного забезпечення

КОНСПЕКТ ЛЕКЦІЙ

з дисципліни

«АНАЛІЗ ТА ОЦІНЮВАННЯ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ», частина 1

для здобувачів першого (бакалаврського) рівня освіти
спеціальності - 125 Кібербезпека

Затверджено
на засіданні кафедри КБПЗ
Протокол № 1 від 26.08.2022р.

Одеса: Одеська політехніка, 2022

Конспект лекцій з дисципліни «Аналіз та оцінювання ризиків інформаційної безпеки», частина 1, для здобувачів першого (бакалаврського) рівня освіти спеціальності 125 Кібербезпека / Укладач Зоріло Вікторія Вікторівна. Одеса: Одеська політехніка, 2022. – 51с.

Укладач: Зоріло Вікторія Вікторівна, к.т.н.

ЗМІСТ

Лекція 1. Вступ. Кібербезпека. Ризики. Основні поняття

У нашому світі з високим ступенем зв'язку розвиток технологій прискорюються експоненціально, надаючи людям нові та швидші способи роботи з інформацією. Разом з цим відбувається зростання рівня загроз інформаційної та/або кібербезпеки. Важко переоцінити значення безпеки в сучасних інформаційних системах.

Термінологія

Кібербезпека стосується захисту особистої чи корпоративної інформації або інформаційних ресурсів від несанкціонованого доступу, атак, крадіжки або пошкодження даних. У контексті кібербезпеки ви зустрінете різні загальні терміни, які мають особливе значення:

- **Актив**: будь-що цінне, що може бути скомпрометовано, викрадено або чому може бути завдано шкоди, включаючи інформацію, фізичні ресурси та репутацію.
- **Загроза**: будь-яка подія чи дія, яка потенційно може спричинити пошкодження активу або переривання послуг.
- **Атака**: навмисна спроба обійти одну або декілька служб безпеки чи засобів керування інформаційною системою.

- **Уразливість**: стан, який робить систему та її активи відкритими для шкоди включно з такими речами як помилки програмного забезпечення, ненадійні паролі, неналежний фізичний захист і погано спроектовані мережі.
- **Експлойт**: техніка, яка використовує вразливість для здійснення атаки. Експлойт також може стосуватися упакованої форми інструментів, таких як програми або скрипти, які автоматизують процес зламу, щоб навіть некваліфікований зловмисник міг використати експлойт для здійснення атаки.
- **Контроль**: контрзахід, який ви застосовуєте, щоб уникнути, зменшити або протидіяти ризикам безпеки через загрози чи атаки.

Складові ризику

Ваша відповідальність як професіонала з кібербезпеки полягає у виявленні ризиків і захисті ваших систем від них. У цьому контексті ризик – це міра вашої схильності до ймовірності пошкодження або втрати. Це означає ймовірність виникнення небезпеки або небезпечної загрози. Ризик часто пов’язаний із втратою системи, живлення чи мережі та іншими фізичними втратами. Однак ризик також впливає на людей, практику та процеси.

Хоча здається, що існує необмежена кількість можливостей і варіацій, коли йдеться про типи атак, які можна влаштувати, на жаль, час і ресурси, які ви можете присвятити захисту активу, не безмежні. Ви повинні визначити, як боротися з різними ризиками, коли плануєте безпеку своїх активів, **що є процесом, який називається управлінням ризиками.** Щоб ефективно управляти ризиком, необхідно враховувати фактори, властиві ризикам, з якими ви маєте справу.

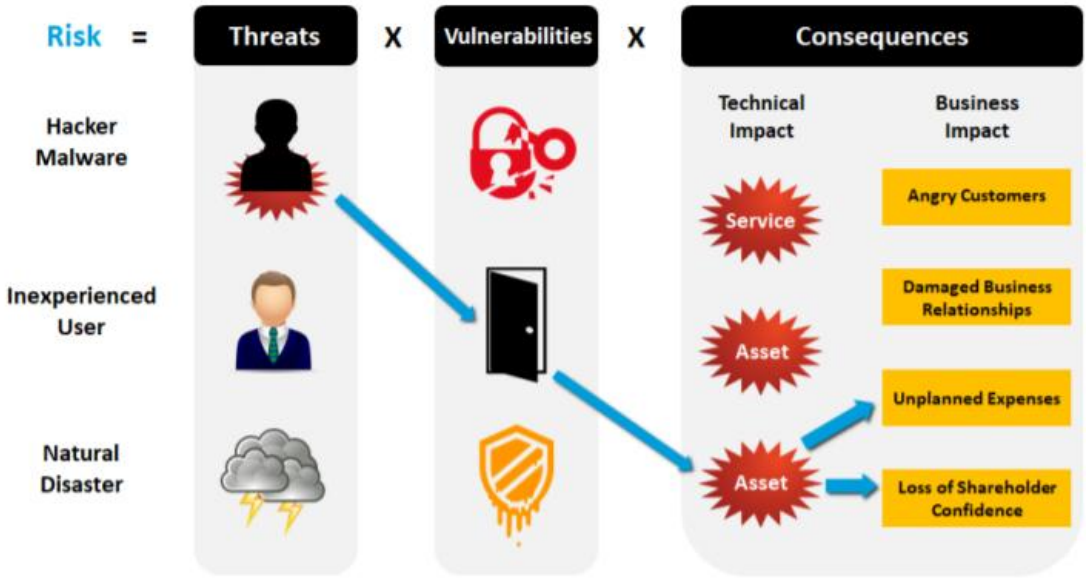
Часто вважається, що ризик складається з трьох факторів, що виражається у такій формулі:

Ризик = Загрози × Вразливі місця × Наслідки

- Загроза: щось або хтось, хто може **скористатися** вразливими місцями**.**
- Вразливість: **слабке** місце або недолік, який дозволяє зловмиснику порушити цілісність системи.
- Наслідком є **збиток**, який виникає через те, що загроза скористалася вразливістю.

У наступному прикладі **хакер** (загроза) використовує **бекдор** (вразливість), щоб установити зловмисне програмне забезпечення на загальнодоступний веб-сервер, що спричиняє **збій сервера** (технічний

наслідок). Це призводить до втрати прибутку та потребує часу та грошей, щоб переконатися, що сервер очищено від «інфекції» (незаплановані витрати). Тоді акціонери компанії можуть втратити впевненість у безпеці громадських послуг організації, що може зменшити ймовірність продовження підтримки компанії.



Технічні та бізнес-впливи ризиків

Наслідки можуть включати як технічні, так і бізнес-наслідки. Наприклад, технічні наслідки атаки можуть включати певну послугу, яка стає недоступною для користувачів (тобто, відмова в обслуговуванні [DoS]) або різні активи, що скомпрометовані, наприклад, видалення даних або надання доступу неавторизованому користувачеві. У свою чергу, ці технічні проблеми можуть призвести до кінцевого впливу на бізнес, наприклад, до розгніваних клієнтів, пошкодження ділових відносин, незапланованих витрат і втрати довіри акціонерів.

Рішення щодо управління ризиками

Оцінивши ступінь трьох факторів, що складають ризик, ви можете визначити ступінь ризику, який керуватиме вашим рішенням щодо того, як з ним боротися. Наприклад, незважаючи на те, що певною вразливістю легко скористатися, і загроза того, що хтось нею скористається, є високою, якщо наслідки тривіальні або взагалі відсутні, ви можете вважати ризик прийнятним, а заходи профілактики непотрібними. З іншого боку, якщо вразливість і загроза низькі, але наслідки досить високі, ви можете вважати

ризик неприйнятним і вирішити витратити час і зусилля на впровадження заходів безпеки.

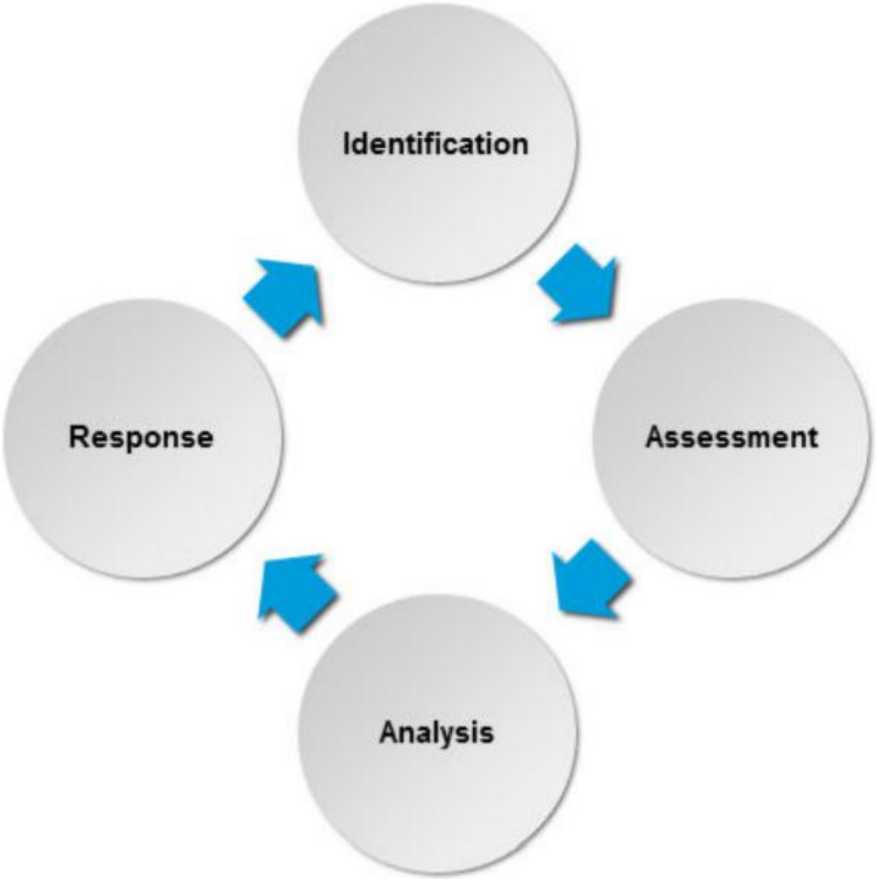
Можливо, ви не в змозі приймати всі рішення щодо управління ризиками. Ці рішення можуть прийматися іншими зацікавленими сторонами або командою управління проектом. Однак ви можете бути в унікальному становищі, щоб зрозуміти, де існують певні технічні ризики, і вам потрібно привернути до них увагу осіб, які приймають рішення.

Причина, чому ризиком керують, а не повністю усувають його, полягає в тому, що ризик не завжди суперечить цілям організації. Насправді, якщо ви спробуєте повністю усунути ризик, організація перестане функціонувати. Ви були б повністю відключені, ви б не могли використовувати жодні електронні пристрої, а операції припинилися б. Ось чому управління ризиками – це процес розуміння того, на які ризики ви можете піти, якщо винагорода варта ризику.

Лекція 2. Управління ризиком

Щоб задовольнити постійно зростаючі потреби в інформаційній безпеці та надійності інформації, професіонал повинен мати можливість керувати ризиками, яким піддається його інформація. **Управління ризиками зазвичай визначається як циклічний процес ідентифікації, оцінки, аналізу та реагування на ризики.**

Цей процес не закінчується – поки інформація існує, вона потребуватиме захисту. Таким чином, управління ризиками повторюється безстроково, щоб ви могли завжди зберігати свою інформацію якомога безпечніше. Без управління ризиками ваша безпека буде пасивною; і якщо ви пасивно захищаєте свою інформацію, вона буде залежати від швидких змін технологічного прогресу.



ERM (Корпоративне управління ризиками)

Комплексний процес оцінювання, вимірювання та пом'якшення багатьох ризиків, які пронизують організацію, називається **корпоративним управлінням ризиками (ERM – Enterprise Risk Management).** Процес ERM є важливою частиною будь-якої організації, яка прагне досягти своїх цілей. Традиційно відповідальність за ERM організації покладалася на фінансового та актуарного фахівця (актуарій – спеціаліст з оцінки ризиків, фінансовий аналітик і консультант у сфері страхування, людина, яка застосовує на практиці актуарну математику; офіційно вповноважена особа, яка має відповідну фахову підготовку та обчислює страхові тарифи).

Однак, враховуючи те, що сьогоднішній інформаційний ландшафт зосереджений на інформації та взаємопов'язаних системах у всьому світі, обов'язки ERM також повинен розділити IT-відділ.

Обсяг і складність ресурсів, які надають підприємства, можуть бути величезними, і, безперечно, є викликом для тих, хто відповідає за їх безпеку. Цей корпоративний підхід до наявності та доступності ресурсів спрямований на виявлення ризиків, тобто через мозковий штурм пропонує численні варіанти, за допомогою яких зловмисники можуть скомпрометувати роботу

бізнесу, а також ідентифікує способи, якими середовище підприємства, співробітники, клієнти та партнери можуть ненавмисно зробити те саме.

Розподіливши функції управління ризиками на всіх рівнях організації, ви можете підвищити обізнаність про проблеми кібербезпеки та розглянути всі рівні управління ризиками.

Причин, які спонукають до впровадження ERM, багато. Нижче наведено деякі з них.

- Зберігання конфіденційної інформації про клієнта від несанкціонованого доступу
- Зберігання комерційної таємниці від публічної сфери
- Уникнення фінансових втрат через пошкоджені ресурси
- Уникнення правових проблем
- Підтримання позитивного суспільного сприйняття бренду/іміджу підприємства
- Забезпечення безперервності господарської діяльності
- Встановлення довіри та відповідальності в ділових відносинах
- Виконання вимог стейкхолдерів (зацікавлених сторін)

Якими б не були причини, ERM стає все більш важливою стратегією в діловому світі та складною частиною обов’язків будь-якого спеціаліста із забезпечення захисту інформації.

Схильність до ризику – це властивість, яка визначає, наскільки організація вразлива до втрат. При кількісній оцінці ризик зазвичай визначається як **добуток ймовірності того, що інцидент станеться, і очікуваного впливу або збитку, який настане, якщо він відбудеться.**

Організація наражає себе на ризик у кожній своїй дії. Ці дії відбуваються в процесі ведення бізнесу організацією, постійна потреба в оцінці цих ризиків породила індустрію безпеки в цілому. Без ризику не було б потреби в безпеці, оскільки не було б наслідків для погано виконаних бізнес-процесів. Оскільки підприємства дедалі більше залежать від технологій, зростаюча кількість ризиків пов’язана з професіоналами з комп’ютерної безпеки як основним засобом керування цими ризиками.

Завдяки ERM організація може підтримувати низький рівень ризику, але ніколи не може його повністю уникнути. Ось чому це так важливо для безпеки постійно бути пильними щодо елементів ризику (включаючи загрози, атаки та вразливі місця), які потенційно можуть завдати шкоди активам підприємства. Ігнорування ризику вашої організації обмежить її здатність виживати в будь-якій галузі.

Лекція 3. Аналіз та оцінювання ризиків

При визначенні того, як захистити комп'ютерні мережі, комп'ютерні установки та інформацію, **аналіз ризиків – це процес безпеки, який використовується для оцінки збитків від ризиків, які можуть вплинути на організацію.** Стиль змісту та результатів будь-якого аналізу ризиків має відображати рамки та юрисдикцію, в межах якої працює організація. Наприклад, у Великій Британії аналіз ризиків, який виконується для уряду або як частина державних контрактів, має представляти результати діловою мовою. На противагу цьому, якщо аналіз ризиків проводиться як частина сертифікації ISO 27000, тоді такого обмеження не існує, окрім ймовірності та наслідків ризиків.

Методи аналізу ризику, які використовують для розрахунку ризику, можна розділити на три категорії:

1. **Якісні:** Методи якісного аналізу використовують описи та слова для вимірювання ймовірності та впливу ризику. Наприклад, оцінки впливу можуть бути **серйозними/високими , помірними/середніми** або **низькими.** Подібним чином рейтинги ймовірності можуть бути **ймовірно, малоймовірно** або **рідко**. Якісний аналіз зазвичай базується на сценаріях. Слабкість якісного аналізу ризику полягає в його методології, яка іноді є суб'єктивною та не піддається перевірці. Ви також можете призначити числа від 0 до 9 для вимірювання сили впливу та потенціалу пошкодження. Однак

ви не виконуєте розрахунки за числами, присвоєними ризикам. Метою якісної оцінки є, наприклад, ранжування ризиків за шкалою від 1 до 25 (будь-яке ранжування за будь-якою шкалою).

2. **Кількісні:** кількісний аналіз повністю базується на числових значеннях. Дані аналізуються з використанням історичних записів, досвіду, найкращих галузевих практик і записів, статистичних теорій, тестування та експериментів. Ця методологія може бути слабкою в ситуаціях, коли ризик важко визначити кількісно. **Метою кількісного аналізу є обчислення ймовірних втрат для кожного ризику.**

3. **Напівкількісні (або напівякісні чи змішані):** метод напівкількісного аналізу існує, оскільки неможливо провести суто кількісну оцінку ризику, враховуючи, що деякі проблеми не піддаються цифрам. Наприклад, скільки моральний стан вашого працівника коштує в гривнях? Чого варта ваша корпоративна репутація? Напівкількісний аналіз намагається знайти золоту середину між двома попередніми типами аналізу ризику, щоб створити гібридний метод.

Вплив ризиків на підприємство

Як керівник інформаційного забезпечення, ви, ймовірно, зіткнетеся з ризиком у багатьох різних формах. Перш ніж ви зможете навіть почати пом’якшувати ризики, щоб гарантувати мінімізацію впливу інцидентів, вам потрібно знати, де існують ризики на вашому підприємстві, і визначити, як вони можуть завдати шкоди. Далі класифікуються різні типи ризиків, з якими ви можете зіткнутися на своєму підприємстві. Майте на увазі, що кіберризики впливають на всі сфери та типи корпоративних ризиків і що вони не обов’язково є технічними, але можуть бути сформульовані в термінах бізнесу.

- **Юридичні ризики:** кожне підприємство, незалежно від галузі, повинно дотримуватися певних законів і правил, щоб залишатися в рамках закону. Наприклад, більшість урядів ухвалили закони про захист споживачів, які карають організації, які займаються діяльністю, яка обманює споживача. Інші неетичні методи ведення бізнесу, недобросовісні працівники та недбале

керівництво можуть поставити ваше підприємство під загрозу. Якщо підприємство не дотримується вимог, воно може спочатку отримати сповіщення з більш суворими покараннями, якщо проблему не буде вирішено належним чином і своєчасно. Підприємство може не тільки порушити певні закони, але й бути предметом судового розгляду певними сторонами, які вважають, що заслуговують на компенсацію. Крім того, зростання судових витрат може мати значний грошовий ефект для підприємства.

- **Фінансові ризики:** ваша організація, ймовірно, має очікуваний дохід і прибуток на основі ряду розрахунків, і багато різних загроз можуть призвести до того, що ваш бізнес не зможе відповідати грошовим очікуванням. Фінансові ризики можуть серйозно вплинути на виживання вашого підприємства на конкурентному ринку. Ці ризики можуть мати прямий вплив на ваші фінанси, як-от негайна втрата прибутку, або наслідки можуть бути більш непрямими, як-от вплив на операційні витрати, що може дещо знизити продуктивність через брак витрат на необхідні ресурси. Ви також повинні розглянути, як особливо руйнівна та/або підступна загроза може вплинути на витрати на страхування, оскільки вони часто можуть бути ризиком для себе.
- **Ризики фізичних активів:** залежно від розміру вашого підприємства, ви можете мати багато цінної фізичної власності, що зберігається на різних сайтах компанії. Будь-який фізичний продукт, який продає ваша організація, є вашою головною турботою. Електроніка, така як комп'ютери, промислове обладнання та офісна техніка, також ризикує бути викраденою чи іншим чином пошкодженою. Загрози людини та фактори навколишнього середовища можуть поставити під загрозу ваші фізичні активи.
- **Ризики інтелектуальної власності:** організації, які створюють та володіють інтелектуальною власністю, такою як розважальний контент, програмне забезпечення, комерційні таємниці та дизайн продуктів, усі ризикують втратити інтелектуальну власність через знищення, пошкодження або використання її у несанкціонований спосіб. Хоча інтелектуальну власність зазвичай не викрадають у такому ж сенсі, як фізичну, можуть бути порушені авторські права. Загроза, яка знищує або змінює вашу інтелектуальну власність, може надзвичайно ускладнити або навіть унеможливити її відновлення. Складні методи викрадання даних також можуть ускладнити вам виявлення отримання несанкціонованого доступу або пошкодження вашої інтелектуальної власності.

- **Ризики інфраструктури:** організація повинна залежати від своєї структури, щоб функціонувати з максимальною ефективністю. І фізичні, і абстрактні структури вразливі до ряду загроз. Особливо це стосується будь-якої інфраструктури, яка постачає електроенергію або сприяє транспортуванню. Ризики інфраструктури впливають на бізнес фундаментально і здатні призвести до катастрофічних наслідків.
- **Операційні ризики:** щоденні операції – це те, що забезпечує роботу вашого підприємства та виконання не лише його грошових очікувань, але й його місій або цілей. Навіть якщо при реалізації ризику немає негайних фінансових наслідків, підприємство ризикує втратити свою позицію на ринку, а його продукти чи послуги можуть більше не бути життєздатними. Особливо шкідливими є ризики, які впливають на операційну спроможність організації (тобто на її здатність виконувати багато бізнес-процесів одночасно). Так само операційні ризики можуть вплинути на час, який людина або інші активи витрачають на усунення наслідків ризику – час, який інакше було б витрачено на звичайні бізнес-процеси. Якщо певні процеси кібербезпеки виявляються неефективними для зменшення ризику, тоді можуть знадобитися вдосконалення цих процесів кібербезпеки, що ще більше вплине на загальні бізнес-операції.
- **Репутаційні ризики:** сприйняття організації громадськістю може сильно вплинути на її успіх, а в деяких випадках може приректи її на поразку. Компанії часто повинні підтримувати хороші стосунки зі своїми клієнтами та зважати на те, як на них дивиться суспільство. Бренд вашої організації може бути знецінений, якщо громадськість негативно реагує на такі сценарії, як крадіжка особистих даних, неетична бізнес-практика або зниження якості продуктів і послуг. Ці сценарії також можуть негативно вплинути на ефективність програм управління зв’язками з громадськістю.
- **Ризики здоров’я:** чи то ваші співробітники, чи то клієнти, з якими вони працюють, люди ризикують отримати шкоду в результаті вашої діяльності. Хоча галузі високого ризику, такі як правоохоронні органи тощо, мають очевидні проблеми зі здоров’ям, навіть звичайні підприємства можуть наражати на небезпеку свій персонал і клієнтів, надаючи небезпечні, неперевірені продукти та послуги. Фізичні активи, такі як промислове обладнання та електричне обладнання, можуть становити значний ризик для здоров’я працівників, які ними користуються.

Лекція 4. Інтеграція документації в управління ризиками (частина 1)

Важливою частиною управління ризиками є розробка документації для використання в майбутньому. Написання політики та запис діяльності, пов'язаної з ризиком, перемістить вашу стратегію ERM від концептуальної до конкретної. Ця лекція забезпечить основу для підтримки ваших методів оцінки та пом'якшення наслідків і, зрештою, скерує ваше реагування на інциденти.

Від політики до процедур

Політика визначає наміри організації. Політики тлумачаться та вводяться в дію через **стандарти, настанови (керівні принципи) та процедури.** Що стосується інформаційної безпеки та відповідності, ці терміни використовуються таким чином:

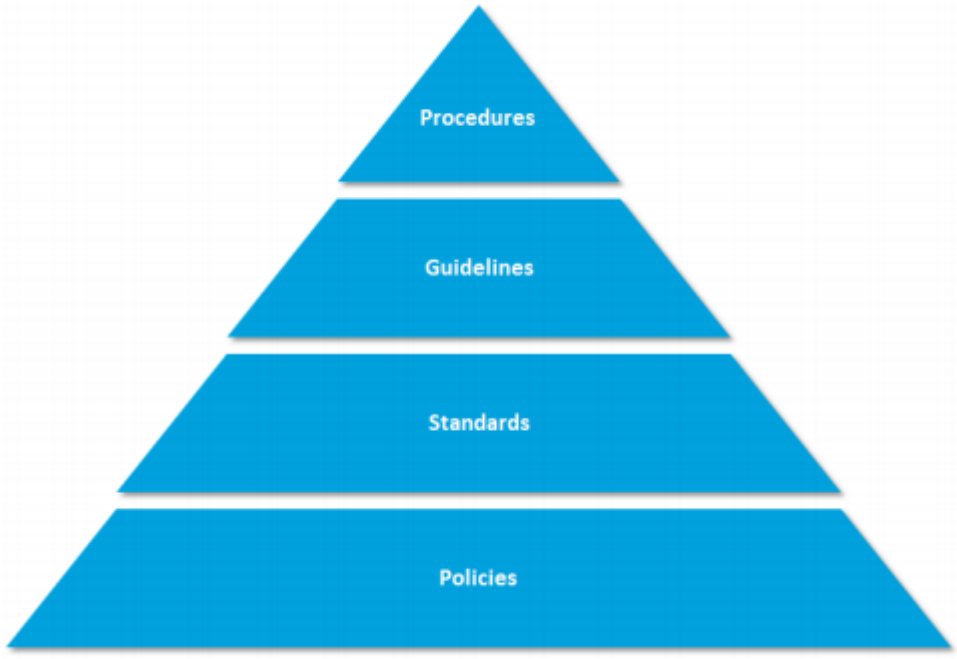


Рисунок 1.1: Політика є основою, на якій будуються стандарти, настанови (керівні принципи) та процедури

Політики – це заяви високого рівня, які визначають наміри організації.

Стандарти складаються з конкретних обов'язкових засобів контролю низького рівня, які допомагають забезпечити виконання та підтримку політики.

Керівні принципи (настанови) є рекомендованими, необов'язковими засобами контролю, які підтримують стандарти або надають посилання для прийняття рішень, коли не існує відповідного стандарту.

Процедури – це покрокові інструкції щодо виконання завдань, необхідних для впровадження різних політик, стандартів і настанов.

Життєвий цикл політики

Життєвий **цикл політики починається, коли організація вирішує, що їй потрібна формальна політика інформаційної безпеки.** Драйвер (пусковий механізм) для розробки або модифікації політики інформаційної безпеки залежить від організації. Це може бути пов'язано зі збільшенням розміру організації, що вимагає письмової політики безпеки для заміни неофіційних інструкцій, для виконання договірних зобов'язань або у відповідь на порушення. Незалежно від причин її розробки, в кінцевому рахунку політика повинна бути затверджена **виконавчим керівництвом,** а в деяких випадках і **радою директорів,** якщо організація досить велика.

Після того як організація визначила потребу, існує кілька способів почати розробку політики. Один із найпростіших методів – завантажити безкоштовний шаблон політики, доступний у різних організаціях безпеки, а потім налаштувати політику відповідно до вашої організації. Також часто організації залучають консалтингову компанію з питань безпеки, щоб допомогти їм у розробці політики.

Незалежно від того, як ви підходите до політики вашої компанії, важливо також порівнювати та протиставляти політику компанії з політикою інших організацій. Можуть існувати теми чи ризики, які ви раніше не розглядали, які впливають на елементи політики.

Не всі політики однакові. Найкраще використовувати чітку та стислу мову в політиці, яку легко зрозуміти. Іншими словами, спробуйте обмежити

формалізм і технічні терміни, які пронизують багато політик. При цьому важливо розуміти, що політика інформаційної безпеки організації є юридичним документом, який ви можете надати співробітникам, клієнтам, а в деяких випадках і суду.

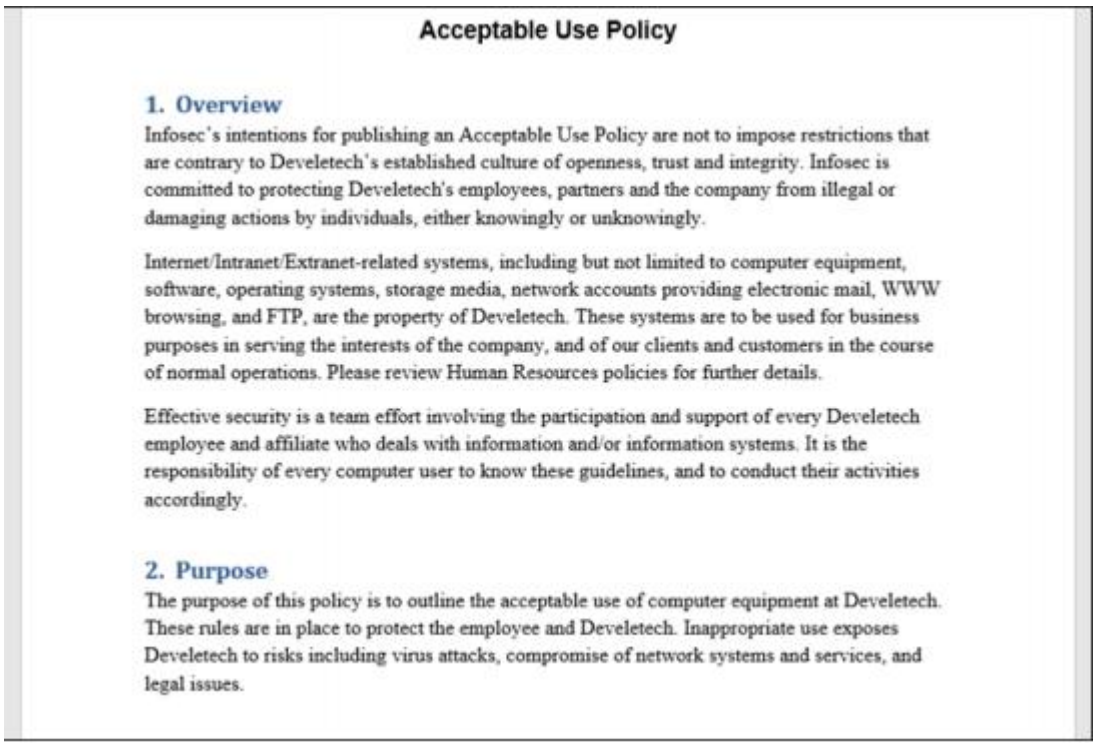
У поєднанні з будь-якими законами чи нормативними вимогами, які можуть діяти в організації, важливо залучати бізнес-лідерів до розробки політики. Якщо політика є надто суворою, це може погіршити здатність працівників вести бізнес, що, у свою чергу, зашкодить організації. **Добре розроблена політика повинна враховувати всі ризики, з якими може зіткнутися бізнес.** Це живий документ, який слід регулярно оновлювати відповідно до того, як змінюються бізнес, технології, середовище та ризики на підприємстві. Коли ідентифікують нові ризики, важливо, щоб ваша політика чітко вказувала, коли повідомляти про інцидент і кому повідомляти про інцидент. Не всі інциденти вимагають судових дій, тому необхідно, щоб політика передбачала, коли повідомляти правоохоронним органам, а коли повідомляти лише внутрішньому персоналу.

Для підтримки політик, розроблених вашою організацією, важливо створити документи про процеси та процедури, які дуже чітко пояснюють, як організація реалізує різні функції безпеки. Це «інструкції», якими користуються системні адміністратори та співробітники компанії, тому вони мають містити необхідні кроки для впровадження та забезпечення дотримання політик. Вони мають бути достатньо конкретними, щоб будь-який користувач, який, як очікується, слідкував за ними, міг це зробити, незалежно від своїх технічних знань. Якщо потрібен заздалегідь визначений рівень технічної майстерності, це має бути чітко зазначено. Наприклад, процедура обробки даних, призначена для використання системними адміністраторами, може передбачати, що адміністратори знайомі з платформою, яку вони підтримують; однак подібна процедура, розроблена для працівників маркетингу та продажів, які мають менше технічних знань, може потребувати більш глибоких, детально розписаних і чітких кроків.

Стиль і зміст цих документів також значно відрізнятимуться між комерційними організаціями та державними органами. Зазвичай документи, що стосуються військових або подібних відомств, наприклад екстрених служб, мають більш інструкційний характер, ніж документи для стандартних підприємств. Іншими словами, ви повинні розуміти свою цільову аудиторію та відповідним чином адаптувати процеси та процедури.

Розробка процесу та процедури здійснюється майже так само, як і розробка політики. Багато організацій зі стандартизації, наприклад NIST або CIS, мають попередньо визначені процедури або стандартні документи, які можна використовувати як відправну точку, а потім адаптувати їх відповідно до вашої організації. Певні організації матимуть певні типи стандартів, яким вони мають відповідати. Крім того, ви можете залучити консультантів, які допоможуть визначити процедури чи оптимізувати бізнес-процеси, щоб привести їх у відповідність із певною політикою. Незалежно від підходу, завжди доцільно порівняти та зіставити політику з іншими організаціями, щоб побачити, як вони впроваджують інструкції з інформаційної безпеки. Багато організацій, як комерційних, так і державних, публікують свою ключову політику в Інтернеті, щоб дати можливість потенційним користувачам їхніх послуг зрозуміти та отримати впевненість у тому, як організація керує інформацією.

Як і політики, на яких вони базуються, процеси та процедури є живими документами. Якщо політика змінюється у світлі нових ділових, технологічних чи екологічних змін, то так само повинні змінюватися процеси та процедури. Політика, яка оновлює стан безпеки підприємства перед лицем нових загроз і ризиків, марна, якщо її не втілити на практиці через процедурну документацію.



Acceptable Use Policy

1. Overview

Infosec's intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to Develetech's established culture of openness, trust and integrity. Infosec is committed to protecting Develetech's employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

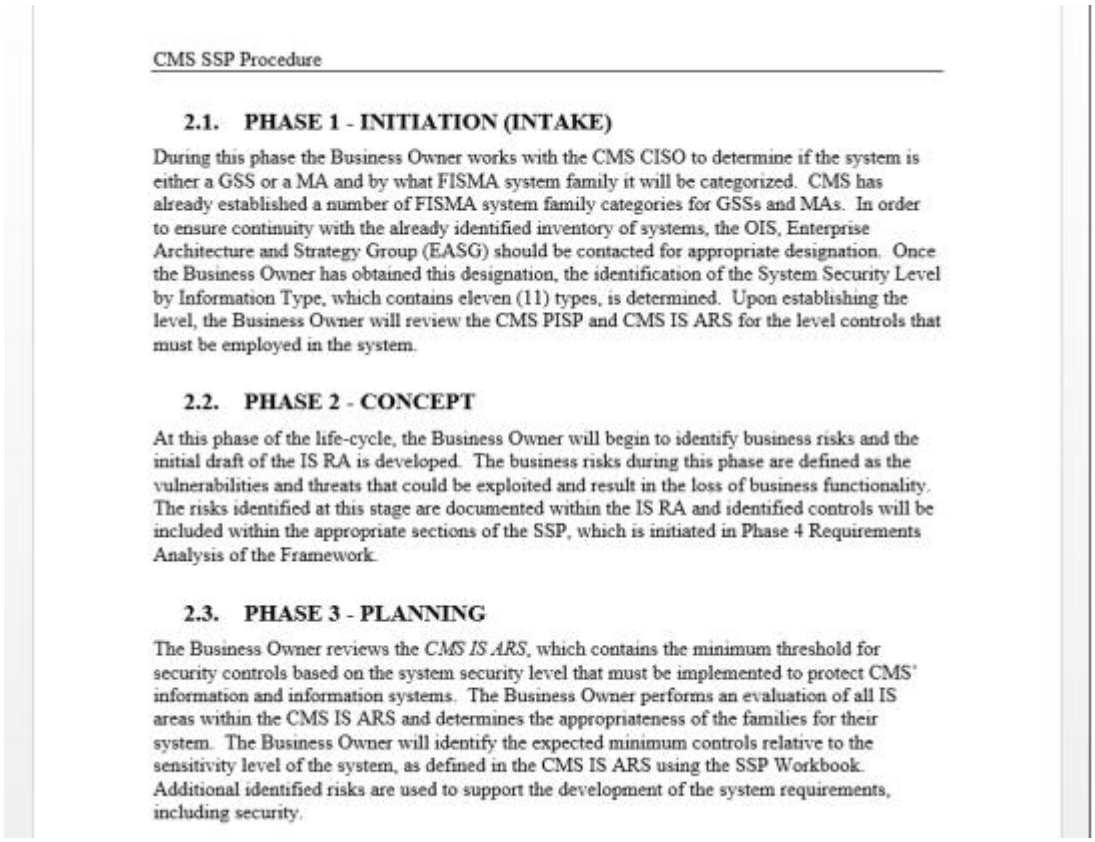
Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of Develetech. These systems are to be used for business purposes in serving the interests of the company, and of our clients and customers in the course of normal operations. Please review Human Resources policies for further details.

Effective security is a team effort involving the participation and support of every Develetech employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

2. Purpose

The purpose of this policy is to outline the acceptable use of computer equipment at Develetech. These rules are in place to protect the employee and Develetech. Inappropriate use exposes Develetech to risks including virus attacks, compromise of network systems and services, and legal issues.

Приклад документа Політики



CMS SSP Procedure

2.1. PHASE 1 - INITIATION (INTAKE)

During this phase the Business Owner works with the CMS CISO to determine if the system is either a GSS or a MA and by what FISMA system family it will be categorized. CMS has already established a number of FISMA system family categories for GSSs and MAs. In order to ensure continuity with the already identified inventory of systems, the OIS, Enterprise Architecture and Strategy Group (EASG) should be contacted for appropriate designation. Once the Business Owner has obtained this designation, the identification of the System Security Level by Information Type, which contains eleven (11) types, is determined. Upon establishing the level, the Business Owner will review the CMS PISP and CMS IS ARS for the level controls that must be employed in the system.

2.2. PHASE 2 - CONCEPT

At this phase of the life-cycle, the Business Owner will begin to identify business risks and the initial draft of the IS RA is developed. The business risks during this phase are defined as the vulnerabilities and threats that could be exploited and result in the loss of business functionality. The risks identified at this stage are documented within the IS RA and identified controls will be included within the appropriate sections of the SSP, which is initiated in Phase 4 Requirements Analysis of the Framework.

2.3. PHASE 3 - PLANNING

The Business Owner reviews the *CMS IS ARS*, which contains the minimum threshold for security controls based on the system security level that must be implemented to protect CMS' information and information systems. The Business Owner performs an evaluation of all IS areas within the CMS IS ARS and determines the appropriateness of the families for their system. The Business Owner will identify the expected minimum controls relative to the sensitivity level of the system, as defined in the CMS IS ARS using the SSP Workbook. Additional identified risks are used to support the development of the system requirements, including security.

Рисунок 1.3: Приклад документа процесу

Теми для включення в політику безпеки та процедури

Усі політики та процедури інформаційної безпеки містять **теми, специфічні для організації та її вимог**. Однак існує рекомендований перелік тем, які має включати ваша документація щодо політик безпеки та процедур. Розробляючи документацію, переконайтеся, що ви отримали схвалення та згоду від вищого керівництва на наступне:

- Сфера дії політики
- Класифікація інформації
- Цілі безпечної обробки інформації
- Як інші політики управління пов’язані з політикою безпеки
- Посилання на підтверджуючі документи
- Конкретні інструкції щодо вирішення питань безпеки
- Особа або група з визначеними обов'язками
- Відомі наслідки недотримання політики безпеки

Кращі практики

Документи безпеки, які містять попередні теми, допоможуть знизити загальний ризик. Крім того, ви повинні підтримувати розробку політик і процедур, які містять найкращі практики, перелічені нижче. Зауважте, що організація не обов’язково зможе або не повинна включити всі ці практики в процес управління ризиками.

Реагування на інциденти: визначає вимоги до моніторингу, реагування та звітності щодо інцидентів, які включають порушення безпеки або підозрювані порушення. Загалом цей набір політик вимагає відповіді на всі інциденти та ймовірні інциденти протягом визначеного періоду часу та відповідно до ієрархії звітності, яка може залежати від серйозності інциденту. І обізнаність у сфері безпеки, і навчання відіграють важливу роль у реагуванні на інциденти, так що особа, чиї основні ролі виходять за межі інформаційної безпеки, знає, до кого та куди звертатися щодо різних рівнів

інцидентів, причому служба обслуговування або довідкова служба є першою лінією в ієрархії звітування. Без своєчасного звітування потрібним людям буде набагато важче знизити ризик порушення безпеки, що завдасть шкоди вашому підприємству.

Криміналістичні завдання: дослідити, звідки почалося порушення, як могло статися порушення та хто міг бути відповідальним за порушення. Політика криміналістичної експертизи повинна включати інформацію про те, кого потрібно повідомляти, коли потрібна судова експертиза, за яких умов вона потрібна та як зв'язатися з особами, відповідальними за ці обов'язки. Важливо залучити юридичного консультанта до формулювання політики криміналістичної експертизи, щоб за необхідності можна було включити відповідні правові вказівки.

Розподіл обов'язків: стверджує, що ніхто не повинен мати занадто багато влади чи відповідальності. Обов'язки та відповідальність слід розподілити між людьми, щоб запобігти етичним конфліктам або зловживанню владою. Такі обов'язки, як авторизація та схвалення, проектування та розробка, не повинні покладатися на одну й ту саму особу, оскільки цій особі було б надто легко обдурити або іншим чином завдати шкоди організації. Наприклад, працівнику було б легше переконатися, що організація використовує лише певне програмне забезпечення, яке містить уразливості, якщо він є єдиним, хто відповідає за це. У багатьох типових IT-відділах ролі оператора резервного копіювання, оператора відновлення та аудитора призначаються різним людям.

Ротація роботи: стверджує, що жодна особа не залишається на життєво важливій посаді надто довго. Обертання окремих осіб на посадах, таких як адміністратор брандмауера чи спеціаліст із контролю доступу, допомагає організації гарантувати, що вона не буде надто міцно прив'язана до однієї особи, оскільки життєво важливі інституційні знання поширюються серед довірених співробітників. Ротація робочих місць також допомагає

зменшити ризик зловживання людьми своєю владою та привілеями, а також запобігає змові між працівниками.

Обов'язкова відпустка: метод запобігання шахрайству, який дає вам можливість переглянути діяльність співробітників. Типова політика обов'язкових відпусток вимагає, щоб працівники брали принаймні одну відпустку на рік із кроком у повний тиждень, щоб вони були відсутні на роботі принаймні п'ять днів поспіль. За цей час ваші відділи корпоративного аудиту та безпеки мають час, щоб дослідити та виявити будь-які невідповідності в діяльності співробітників. Коли працівники розуміють безпеку політики обов'язкових відпусток, ризик шахрайства зменшується.

Найменший привілей: вимагає, щоб користувачі або системи мали лише мінімальний рівень доступу, необхідний для виконання покладених на них обов'язків. Цей рівень мінімального доступу включає засоби, обчислювальне обладнання, програмне забезпечення та інформацію. Коли користувачеві або системі надається доступ, цей доступ має бути лише на рівні, необхідному для виконання необхідних завдань. Якщо ви надаєте користувачеві або системі доступ, який перевищує той, що їм потрібно, то це ще один вектор, який можна використати для компрометації вашої організації.

Процедури працевлаштування та звільнення: визначає процедури прийому на роботу та звільнення, коли працевлаштування починається та закінчується відповідно. Правильна адаптація передбачає привчання нових співробітників до практик безпеки, яких ви очікуєте від них. Це гарантує, що в угоді буде передбачено відповідальність. Подібним чином, коли працівник залишає організацію, ви повинні встановити процес виходу з організації. Звільнений працівник повинен погодитися відмовитися від будь-якого доступу до систем компанії, даних і фізичного обладнання. У деяких випадках звільнення працівника може поставити секрети вашої компанії під загрозу витоку. Щоб підготуватися до цього, ваша політика має визначати, коли ви повинні застосовувати угоди про нерозголошення (NDA).

Постійний моніторинг: описує, які механізми та інструменти використовуються для постійного моніторингу систем на наявність змін, які можуть збільшити ризик для підприємства. Ця практика також точно визначає, які події та середовища слід контролювати на основі попереднього аналізу ризиків. Деякі політики включатимуть положення щодо постійного вдосконалення, щоб підприємство могло взяти на себе активну роль у вирішенні виявлених ризиків.

Навчання та підвищення обізнаності користувачів: без комплексної освіти атаки на користувача (такі як соціальна інженерія) будуть основним джерелом ризику для організації. Окрім навчання користувачів про невід'ємні ризики використання технологій, важливо також навчити їх політикам і процедурам, необхідним для безпечної роботи в системах організації. Навчання також має враховувати типи доступу та ролі, які мають працівники. Наприклад, ви б не навчали продавця ризикам атак SQL-ін'єкцій, але ви б навчили розробників свого веб-сайту цій темі. Спеціальні навчальні механізми можуть варіюватися від нагадувань через повідомлення на екрані під час входу в систему, через паперові брошури на столах співробітників або в зонах загального користування, до навчання конкретним елементам операцій підприємства (пристрої, програмне забезпечення, безпека будівлі тощо).

Вимоги до аудиту та частота: визначає типи аудитів, які проводяться, хто проводить ці аудити та як часто вони проводяться, а також чітко визначає повноваження для усунення проблем аудиту, виявлених у процесі. Політики аудиту зазвичай включають положення про тригери подій, які базуються на оцінці ризиків підприємства. Політика аудиту також повинна визначати вимоги до аудиту для ділових партнерів і субпідрядників, які повинні бути включені в усі контракти з третіми сторонами, які можуть мати вплив на загальну безпеку організації.

Класифікація інформації: інформацію слід класифікувати відповідно до її чутливості та критичності для ділових операцій. Це дає змогу визначати

пріоритети методів захисту даних і застосовувати ці засоби захисту щодо конфіденційності, цілісності та доступності (CIA, confidentiality, integrity, and availability) цих даних. Дані можна розділити на такі категорії: **загальнодоступні**, **приватні**, **обмежені** та **конфіденційні**, що задовольнять потреби більшості організацій, але ви можете створити власну схему категоризації, якщо вона не підходить (наприклад, в Україні прийнято ділити дані на публічну інформацію (яка не становить таємниці) і конфіденційну інформацію – особливої важливості, цілком таємну і таємну).

Лекція 5. Інтеграція документації в управління ризиками (частина 2)

Ця лекція є продовженням **інтеграції документації в управління ризиками (частина 1)**. Розглянемо найкращі практики, політики та процедури, необхідні для інтеграції документації в управління ризиками в організації.

Типи політик безпеки

Нижче наведено приклади **загальних політик безпеки, які можна** знайти в багатьох організаціях.

Політика реагування на інциденти: визначає правила реагування на інциденти безпеки до, під час і після їх виникнення. Ці політики зазвичай відображають інформацію про те, хто відповідає за вирішення конкретних аспектів інциденту, наприклад стримування атак і повідомлення деталей

зацікавленим сторонам. Вони також містять інформацію про ресурси, які доступні для реагування на інциденти.

Політика прийнятного використання: визначає набір правил і обмежень щодо того, як різноманітні внутрішні та зовнішні зацікавлені сторони можуть поводитися щодо активів організації. Ці політики зазвичай окреслюють загальні або конкретні дії, які, на думку організації, зменшать, збільшать або не вплинуть на ризик. У більшості випадків від зацікавлених сторін очікується дотримання політики прийнятного використання, і, якщо вони порушують будь-яку з її умов, до них можуть бути застосовані покарання (наприклад, звільнення).

Політика керування обліковим записом: описує обов'язки адміністраторів щодо забезпечення безпеки різноманітних ідентифікаційних даних і підтримки бізнес-цілей. Такі політики визначають очікувану поведінку щодо того, як створюється, змінюється та видаляється ідентифікаційна інформація зовнішнього або внутрішнього користувача щодо організаційних систем.

Політика паролів: часто ця політика є підмножиною політики керування обліковим записом, яка визначає правила створення та підтримки облікових даних користувачами. Зазвичай встановлюються такі обмеження, як мінімальна кількість символів у паролі, необхідний рівень складності пароля та частота зміни паролів. Політика паролів призначена для того, щоб зменшити ризик спроб злому пароля.

Політика володіння даними: описує, як інформація в організації призначається «власникам» – тобто персоналу, який остаточно відповідає за безпеку цієї інформації та доступ до неї лише уповноваженим особам. Ці типи політик допомагають організації гарантувати, що всі дані обліковуються та що кожен власник розуміє, що від нього очікується.

Політика класифікації даних: визначає, як організація вирішує класифікувати різні рівні конфіденційності даних. Організація може

сортувати свої заходи безпеки на основі того, які дані становлять найбільший ризик у разі їх витоку чи підробки.

Політика збереження даних: визначає, як і коли організація повинна зберігати дані у своїх системах, а також як і коли організація має видаляти ці дані. Це особливо важливо, якщо організація обробляє **ідентифікаційну інформацію (Personally Identifiable Information, PII)** або **захищену інформацію про здоров'я (Protected Health Information, PHI)**, яка часто підпадає під нормативні та юридичні обмеження.

Типи процедур

Нижче наведено приклади **загальних процедур безпеки, які можна** знайти в багатьох організаціях.

Видобуток доказів: щоб підтримати процес судового розслідування, коли це необхідно після інциденту безпеки, організація повинна розробити процедури для збору та надання доказів. Залежно від обставин інциденту ці докази можуть зберігатися всередині компанії, але їх також може знадобитися надати третій юридичній особі. Процедури повинні гарантувати, що докази підтримують цілісність і підтверджуються на кожному етапі процесу, щоб їх актуальність і точність не могли бути поставлені під сумнів.

Виправлення: дослідники безпеки, групи розробників і зловмисники постійно виявляють нові вразливості програмного забезпечення, навіть якщо це програмне забезпечення існує роками. **Таким чином, виправлення є життєво важливою процедурою, яка запобігає використанню цих уразливостей зловмисником.** В організації процедури виправлення часто не є простим натисканням кнопки оновлення чи навіть автоматизованим процесом. Службі безпеки та іншому персоналу може знадобитися ретельно перевірити виправлення, перш ніж вони надішлють їх у робочі системи, переконавшись, що зміни в програмному забезпеченні не вплинуть на роботу негативно.

Розвиток компенсаційного контролю: компенсаційний контроль – це захід безпеки, який використовується для зменшення ризику, коли основний контроль безпеки не працює або не може повністю відповідати очікуванням. Наприклад, основним контролем може бути те, що хост генерує сповіщення для адміністратора, коли виявляє підозрілу поведінку, як-от повторні невдалі спроби входу. Однак існує ймовірність, що сповіщення не дійде до адміністратора з будь-якої причини або що хост взагалі не попередить про дію. Таким чином, перегляд журналів вручну, таких як системний журнал/журнали подій, журнали автентифікації та журнали брандмауера, є компенсаційним контролем, оскільки людина може помітити підозрілу поведінку, яку автоматизована система не помітила. Ви також можете розробити компенсаційні елементи керування для підтримки первинних елементів керування, а не просто замінити їх у разі необхідності. Наприклад, залучення до аналізу даних може допомогти зміцнити існуючий інструмент або систему. Співробітники служби безпеки можуть виконувати аналіз тенденцій і історичний аналіз, щоб передбачити майбутню поведінку певної системи, яку статичний інструмент може бути не в змозі передбачити, а також персонал може збирати в одне ціле та співвідносити дані, щоб надати інструменту повнішу перспективу подій.

Контрольні процедури тестування: так само, як тестування патчів (виправлень), організаціям може знадобитися окреслити процедури тестування запланованих або існуючих засобів контролю безпеки. Ці процедури мають перевірити ефективність контролю щодо зниження ризику та зважити це проти його вартості. Процедури тестування контролю краще виконувати не один раз, а постійно, щоб ви могли визначити, коли засіб керування відстає від сучасних технологій або коли він більше не відповідає мінливим потребам бізнесу.

Планування виправлення: коли оцінка безпеки або інший огляд визначає проблемні області в організації, має бути розроблений план усунення цих проблем. Плани виправлення зазвичай включають кроки з

видалення або призупинення роботи системи на час усунення помилки; це має бути зроблено таким чином, щоб максимально уникнути збоїв. Плани виправлення можуть також включати загальні кроки для реалізації самого виправлення, припускаючи, що це відоме рішення. В іншому випадку план може потребувати надання більш узагальнених кроків для нового та неперевіреного рішення.

Управління винятками: у цьому контексті винятком є будь-яка обставина, яка ускладнює для організації виконання стандартних процедур усунення. Наприклад, організація може мати застаріле програмне забезпечення, яке є невід'ємною частиною бізнес-операцій. Оцінка безпеки визначає кілька вразливостей в інтерфейсах прикладного програмування (API) і бібліотеках, які він використовує. Зазвичай коригувальною дією буде лише оновлення цих API та бібліотек, але це, по суті, порушить застарілу програму. Переписування коду в застарілій програмі, щоб вона працювала з цими оновленнями, теж не зовсім здійсненне. Це виняток із процесу відновлення.

Суворі процедури керування винятковими ситуаціями передбачатимуть подібні проблеми та інструктуватимуть персонал щодо найкращих дій. У наведеному вище прикладі працівникам служби безпеки знадобиться план, щоб повідомити керівникам вищого рівня про їхній вибір: або прийняти ризик, або відмовитися від застарілої програми та шукати нове рішення. План керування винятковими ситуаціями також може надати персоналу служби безпеки компенсаційні засоби контролю, які не зовсім пом'якшують ризик, але принаймні дещо його зменшують або переносять в інше місце (страхування ризику).

Документи підтримки бізнесу

Існує кілька поширених типів ділових документів, з якими спеціалісти із забезпечення інформації повинні стикатися під час виконання своїх

звичайних обов’язків. Багато з них зосереджені на ділових партнерствах і альянсах. Оскільки всі організації ведуть бізнес з іншими організаціями, існує багато типів **спільних угод**, які використовуються для регулювання цих відносин. Деякі з цих угод конкретно стосуються безпеки, управління ризиками та реагування на інциденти, тоді як інші можуть включати їх у другорядному порядку або не включати їх зовсім.

Генеральна угода про надання послуг (Master Service Agreement, MSA): закладає основу для будь-яких майбутніх ділових документів, які можуть узгодити дві сторони. Метою MSA є прискорення процесу укладання угоди в міру розвитку відносин між кожним діловим партнером. Організації можуть використовувати MSA, щоб усунути надмірності, які виникають, коли організації-партнери укладають кілька угод, подібних до перелічених у решті таблиці.

Заява про застосовність (Statement of Applicability, SOA): визначає засоби контролю, які існують в організації, і пояснює їх призначення. Оскільки SOA визначають, чому використовується той чи інший засіб керування, вони часто знаходяться під прямим впливом висновків, зроблених під час оцінки ризику. SOA має посилатися на політику та процедури, які використовуватимуть визначені засоби контролю. Може бути корисним не лише пояснити, чому було включено певний елемент керування, але й пояснити, чому певні елементи керування було виключено.

Аналіз впливу на бізнес (Business Impact Analysis, BIA): Визначає поточні організаційні ризики та визначає вплив на поточні, критично важливі

для бізнесу операції та процеси, якщо такі ризики дійсно виникають. BIA містить оцінки вразливості та оцінки для визначення ризиків та їх впливу. BIA має включати всі фази бізнесу, щоб забезпечити надійну стратегію продовження бізнесу.

Угода про оперативну сумісність (Interoperability Agreement, IA): загальний термін для будь-якого документа, який описує ділове партнерство або співпрацю, у якому всі організації обмінюються деякими ресурсами під час спільної роботи.

Угода про безпеку взаємозв'язку (Interconnection Security Agreement, ISA): спрямована на інформаційні системи партнерських організацій, щоб гарантувати, що використання міжорганізаційних технологій відповідає певним стандартам безпеки для CIA. Оскільки вони зосереджені на безпеці, ISA часто пишуться як юридично обов'язкові. ISA також можуть підтримувати меморандуми про взаєморозуміння для підвищення життєздатності їх безпеки. NIST надає спеціальну публікацію 800-47 для розробки плану взаємозв'язку під назвою Керівництво з безпеки для взаємозв'язних систем інформаційних технологій.

Меморандум про взаєморозуміння (Memorandum of Understanding, MOU): зазвичай не має обов'язкової юридичної сили та зазвичай не передбачає фінансових зобов'язань. Меморандум про взаєморозуміння є менш формальним, ніж традиційні контракти, але все ж має певну важливість для всіх залучених сторін. Зазвичай вони вводяться як спосіб виразити бажання всіх сторін досягти тієї самої мети узгодженим способом. Документ може містити довідкову інформацію про кожну організацію; історія відносин між двома організаціями та обставини, які призвели до партнерства; і загальний або конкретний графік для спільної ділової діяльності. Оскільки вони зазвичай не мають правової основи, меморандуми про взаєморозуміння не є найбезпечнішою угодою для партнерства.

Угода про рівень обслуговування (Service-Level Agreement, SLA): чітко визначає, які послуги мають надаватися клієнту та яку підтримку, якщо

така є, буде надано. Послуги можуть включати все: від обладнання та програмного забезпечення до людських ресурсів. Сильний SLA окреслить основні очікувані послуги для цілей відповідальності. Документ може містити часові рамки, протягом яких несправності будуть виправлені або обслуговуватися, гарантії безвідмовної роботи або, у випадку мережевого провайдера, гарантії швидкості завантаження та завантаження даних.

Угода операційного рівня (Operating-Level Agreement, OLA): виявляє та визначає робочі відносини між групами або підрозділами організації, оскільки вони розподіляють відповідальність за виконання однієї чи кількох угод SLA зі своїми внутрішніми чи зовнішніми клієнтами.

Угода про нерозголошення (Non-Disclosure Agreement, NDA): угода між організаціями, яка передбачає, що вони не будуть ділитися конфіденційною інформацією, знаннями чи матеріалами з неавторизованими третіми сторонами. У NDA також зазвичай вказується, у яких випадках, якщо такі є, дані можуть бути використані або оброблені суб'єктом-одержувачем. Для даних, отриманих із відкритих джерел, NDA не підлягає виконанню.

Угода про ділове партнерство (Business Partnership Agreement, BPA): визначає, як буде здійснюватися партнерство між суб'єктами господарювання та що саме очікується від кожного суб'єкта з точки зору послуг, фінансів і безпеки. З міркувань безпеки BPA має точно описувати, чим партнери готові ділитися один з одним, і як оброблятиметься будь-який міжорганізаційний доступ.

Примітка. Прикладом стандарту з'єднання є Код з'єднання PSN (Code of Interconnection, CoICo). Цей урядовий стандарт Великобританії застосовується до послуг підключення, які надають комерційні постачальники. Стандарт можна знайти за адресою https://www.gov.uk/government/publications/psn-code-of-interconnection-coico .

Невиконання

Недотримання певних ділових документів, особливо тих, які мають юридичну силу, може призвести до серйозних покарань для організації чи особи. Наприклад, припустімо, що ваша організація має ISA з іншою організацією. Якщо ваша безпека надто сильно відхиляється від вимог, з якими ви погодилися в ISA, і станеться порушення, ваша організація не лише нестиме відповідальність за порушення, але й суб'єкт господарювання, з яким ви співпрацюєте, також може подати позов проти вашої організації. Це може призвести до великих штрафів, які серйозно вплинуть на бізнес-операції та прибутковість. Ви можете нести значну відповідальність навіть за юридично необов'язкові угоди. Негативні наслідки часто більш нематеріальні. Ваша організація може втратити повагу в очах зацікавлених сторін і потенційних партнерів, що може вплинути на її репутацію на ринку. Навіть фізичні особи можуть бути притягнуті до відповідальності за невиконання, особливо таких документів, як NDA. Якщо ваш роботодавець змусить вас підписати NDA і ви розголошуєте конфіденційну інформацію неавторизованим сторонам, ви можете втратити роботу та отримати позов про відшкодування збитків.

Дотримуйтесь цих вказівок під час інтеграції документації у ваші стратегії ERM:

Завантажте безкоштовні шаблони політики, щоб спростити створення політики.

Розгляньте можливість найняти консультанта, якщо ваша організація не може підтримувати внутрішню розробку політики.

Використовуйте пряму, стислу мову та уникайте юридичного жаргону в політиках.

Залучайте бізнес-лідерів до розробки політики та переконайтеся, що виконавче керівництво схвалює політику перед тим, як її застосовувати.

Підтримка політики з чітко визначеними процесами та процедурами.

Зробіть процеси та процедури легкими для дотримання та пристосуйте їх до технічних можливостей вашої аудиторії.

Порівняйте політику, процеси та процедури з політиками інших організацій.

Розглядайте політики, процеси та процедури як живі документи, які можуть змінюватися в міру розвитку бізнесу та технологій.

Включіть найкращі практики, такі як ротація робочих місць, обов’язкові відпустки та навчання користувачів, у свою політику на основі конкретних вимог підприємства.

Залучайте HR, юрисконсультів, керівництво та інші організації до процесу розробки політики, щоб отримати унікальні перспективи.

Переконайтеся, що політика містить положення щодо відповідності законодавству та нормам.

Визначте будь-яку конфіденційну ідентифікаційну інформацію, яку обробляє ваша організація.

Відверто повідомляйте своїм клієнтам, як і з якою метою використовуватиметься їхня ідентифікаційна інформація.

Порадьте своїх клієнтів щодо найкращих практик збереження конфіденційності.

Розробіть план безперервності бізнесу (business continuity plan, BCP), щоб підтримувати повсякденну роботу в разі інциденту.

Визначте в BCP, які компоненти знаходяться під загрозою та як їх слід зберігати в безпеці.

Перевіряйте свій BCP і перевіряйте його регулярно.

Визначте різноманітні ділові документи та угоди, які стосуються потреб вашого підприємства.

Використовуйте таку угоду, як SLA, у будь-якому партнерстві, яке потребує надійної безпеки та юридичної та фінансової відповідальності.

Оцінка ризику

Оцінка ризику використовується для виявлення, аналізу та обчислення ризиків. Вона виконується для ідентифікації будь-яких інформаційних активів, які можуть стати ціллю кібератаки: апаратне забезпечення, програмне забезпечення, дані клієнтів та інтелектуальну власність. Після визначення типів даних оцінка ризику визначить типи ризиків, пов’язані з кожним типом ідентифікованого ризику. Потім буде запроваджено засоби контролю, щоб запобігти виникненню будь-якого із зазначених ризиків. Цей процес буде постійним циклом, який слід виконувати регулярно, оскільки система та активи організації постійно змінюватимуться.

Під час проведення оцінки ризику необхідно враховувати такі речі:

- Яка є загроза ?
- Чи вразлива система до цієї загрози?
- Як цей ризик вплине на організацію (репутаційні або матеріальні збитки)?

Використовуючи цю просту структуру, можна розробити високорівневий розрахунок кіберризику:

Кіберризик = Загроза × Вразливість × Цінність інформації

Види оцінки ризиків

Після того, як усю цю інформацію, згадану вище, буде зібрано, ви можете розпочати розробку плану оцінки ризиків для задоволення потреб конкретного тесту. Існує кілька різних типів оцінки ризику, які залежатимуть від типу організації, з якою ви маєте справу, та її цілей.

- **Юридичний ризик (ризик комплаєнсу або ризик дотримання норм)** ґрунтується на порушеннях законодавства, зокрема законів, правил і нормативних актів, або, з іншого боку, на внутрішніх політиках або бізнес-стандартах певної організації.
- **Репутаційний ризик –** це будь-який вид негативної реклами, суспільного сприйняття або будь-яка неконтрольована подія, яка може вплинути на репутацію організації.
- **Трансакційний ризик** – це будь-який ризик, пов’язаний із наданням послуг або продукту. Наприклад, це може бути пов’язано з коливаннями курсу іноземної валюти на продукт, продаж якого завершено, але ще не розраховано.
- **Стратегічний ризик** – це все, що може статися внаслідок бізнес-рішень, прийнятих працівниками на основі бізнес-цілей. Це можна розглядати як ризик недосягнення цих цілей.
- **Операційний ризик** – це будь-яка зміна в бізнес-процесах, людях, системах або зовнішніх подіях, які можуть завдати збитків організації.

***Розділення ризиків на дані категорії не є універсальним, згідно з різними класифікаціями можна виділити ще багато інших видів ризиків (екологічні, фінансові тощо).**

Крім цього, існує 2 типи методів оцінки ризиків, які можна виконати.

Кількісний: це аналіз ризиків з найвищим пріоритетом, який використовує числову рейтингову систему для визначення їхньої ймовірності. Це оцінить результат певного процесу за ймовірністю того, що він дійсно досяжний і досягає бізнес-цілей. Це може бути корисно під час спроби оцінити рішення, коли є певна невизначеність щодо теми, і це може створити реалістичну та досяжну вартість, графік або цільовий обсяг.

Якісний: це найпоширеніший тип оцінки ризику. Він базується на судженні оцінювача (експерта). Оцінювачем зазвичай є людина з досвідом у цій галузі, яка зможе використовувати власні судження та знання для оцінки та аналізу ризиків.

Лекція 6. Документування ризиків

Оцінка ризиків буде основою стратегії управління ризиками для організації, тому це фундаментальна частина процесу. Нижче наведено кроки, які ви можете виконати під час проведення оцінки ризику.

1. Будьте **в курсі системи:** що це таке, що вона робить, хто нею користується тощо.
2. **Визначте загрози:** несанкціонований доступ, неправомірне використання інформації, витік даних, втрата даних або порушення роботи служби.
3. Визначте ризик і **вплив ризику:** ризик матиме високий, середній чи низький вплив на систему?
4. **Проаналізуйте контрольне середовище:** ви можете зробити це, переглянувши кілька категорій інформації та оцінивши середовище. Ви

шукаєте все, що може допомогти запобігти загрозам, будь-яку форму пом’якшення, процеси виявлення або будь-який тип контролю, який можна використовувати для виявлення загроз у системі. Знову ж таки, кожен з цих засобів можна категоріювати згідно з такими категоріями: **задовільний, задовільний із рекомендаціями, потребує покращення, невідповідний**.

5. **Визначте оцінку ймовірності:** визначте, наскільки ймовірна кожна подія, проаналізувавши засоби контролю, які ваша організація має на місці для запобігання цим проблемам. Це також можна класифікувати на високий, середній і низький рівень ймовірності.

6. Нарешті, ви зможете **розрахувати рейтинг ризику:**

*Вплив (якщо експлуатується) * Імовірність (експлойту в оцінюваному контрольному середовищі) = Рейтинг ризику*

Наприклад: є ризик порушення доступності інформації, якщо зловмисники перехоплять керування і змінять логіни та паролі облікових записів. Це може призвести до матеріальних збитків розміром 1 000 000 грн. Ймовірність реалізації даного ризику складає 2%.

Рейтинг1=1 000 000*0,02=20 000

Крім того існує ризик порушення цілісності і конфіденційності інформації, якщо зловмисник зможе отримати доступ до неї. Це призведе до матеріальних збитків розміром 500 000 грн, ймовірність реалізації такого ризику 10%.

Рейтинг2= 500 000*0,1=50 000

Таким чином ризик 2 має вищий рейтинг, ніж ризик 1, і потребує першочергового опрацювання.

Є багато корисних документів для оцінки ризиків, але найпоширенішим є **реєстр ризиків**. Реєстр ризиків використовується для

документування ризиків і дій, необхідних для управління ними. Це життєво важлива частина успішного управління ризиками в організації. Це допомагає вести облік усіх виявлених ризиків разом із способами їхнього керування, пом’якшення чи реагування на них.

Реєстр ризиків зазвичай міститиме такі відомості:

- Дата виявлення ризику
- Назва ризику
- Власник ризику (той, хто відповідає за керування цим ризиком)
- Реакцію на ризик (що робити, якщо ризик реалізувався)
- Опис ризику
- Ймовірність реалізації ризику
- Потенційний вплив ризику (матеріальні, моральні збитки, їх кількісна або якісна оцінка)
- Рейтинг ризику

Інша документація:

- Політика ризиків
- План пом’якшення (покращення, зменшення) ризиків
- План комунікації ризиків
- План реагування на ризики
- Процес ризику

Реєстрація ризику

Розглянемо вміст реєстру ризиків і побачимо, для чого його можна використовувати.

Публікація Міжнародної організації зі стандартизації (ISO) 73:2009 «Управління ризиками — Словник» визначає *реєстр ризиків* як:

запис інформації про виявлені ризики.

Від Recipro City Labs

Реєстр ризиків може бути представлений у кількох форматах, включаючи електронну таблицю, таблицю або список на інформаційній панелі. Ризики можна класифікувати за рейтингом:

- **Серйозний:** термінова загроза для організації та зменшення ризику або виправлення мають бути негайними.
- **Підвищений:** для організації існує обґрунтована загроза, яку слід усунути в прийнятний час.
- **Низький:** загроза має досить низький рейтинг і зазвичай прийнятна, що все ще може становити ризик для організації. Можливо, знадобиться запровадити додаткові процедури безпеки, щоб запобігти подальшій загрозі.

Після виконання кроків, згаданих у попередніх цілях, ви повинні мати знання та зібрану інформацію для заповнення реєстру ризиків. Кожен ідентифікований вами ризик слід помістити в реєстр ризиків разом із усією необхідною інформацією, щоб ви могли розрахувати рейтинг ризику та зробити наступний крок для захисту організації (як зазначено в попередній меті).

Кроки:

Базовий приклад

Нижче наведено приклад реєстру ризиків, взятий із Tyler Cybersecurity . Його завершено та внесено всю відповідну інформацію залежно від виявленого ризику.

Identified Threat	Impact	Likelihood	Value	Risk Calculation
Unauthorized access (Malicious or Accidental)	High (100)	High (1.0)	100*1.0=100	Severe
Misuse of Information by Authorized Users	High (100)	Medium (.5)	100*.5=50	Elevated
Data leakage/Unintentional Exposure of Customer information	High (100)	Medium (.5)	100*.5=50	Elevated
Failed Processes	High (100)	Low (.1)	100*.1=10	Low (Normal)
Loss of data	High (100)	Low (.1)	100*.1=10	Low (Normal)
Disruption of Service or Productivity	High (100)	Low (.1)	100*.1=10	Low (Normal)

- **Виявлена загроза 1:** несанкціонований доступ буде мати високий вплив, оскільки якщо це станеться, це може спричинити багато ризиків для системи. Імовірність цього також висока. Через те, що обидві ці категорії оцінюються як високі, ризик вважається **серйозним**, що дає вам зрозуміти, що це вимагає негайних дій. За даними PurpleSec у 2020 році Magellan Health постраждала від атаки програм-вимагачів і витоку даних, згідно з якими 365 000 пацієнтів постраждали від складної кібератаки.
- **Виявлена загроза 2:** зловживання інформацією шляхом несанкціонованого доступу матиме великий вплив, оскільки критично важливо, якщо будь-яка конфіденційна інформація доступна будь-кому, хто не повинен мати до неї доступу. Імовірність цього вважається середньою. Це означає, що це не зовсім неможливо, але якщо в організації є правильні процедури безпеки в певних місцях, шансів на це буде менше. Через це розраховане значення становить 50, а розрахунок ризику **підвищений**. Це означає, що він вимагає дій, але не таких негайних, як попередній ризик.

Виявлена загроза 6: порушення роботи служби або продуктивності матиме значний вплив, якщо організації потрібна ця служба для функціонування, тобто доступ до файлів у спільному мережевому ресурсі або

в онлайн-магазині. Вплив є високим, оскільки деякі організації не могли б функціонувати без певних подібних послуг. Імовірність цього вважається низькою, оскільки зазвичай це трапляється не надто часто. Зазвичай існує також процедура, якої слід дотримуватися, якщо це станеться, що знижує пов’язані з цим ризики. Через це розраховане значення є досить низьким, а остаточний розрахунок ризику є **низьким.**

Лекція 7. Ризик-менеджмент

Ризик-менеджмент – це не автономна діяльність, ізольована від основних видів діяльності. Ризик-менеджмент є частиною обов’язків керівництва та невід'ємною частиною всіх організаційних процесів, включаючи стратегічне планування, проекти і процеси.

Ризик-орієнтоване управління передбачає створення необхідної культури та інфраструктури бізнесу для:

виявлення причин і основних факторів виникнення ризиків;

ідентифікації, аналізу та оцінки ризиків;

прийняття рішень на основі проведеної оцінки;

вироблення антиризикових керуючих впливів;

зниження ризику до прийнятного рівня;

організації виконання протиризикової програми;

контролю виконання запланованих дій;

аналізу та оцінки результатів.

Методи реагування на ризики

УХИЛЕННЯ ВІД РИЗИКІВ.

ПРИЙНЯТТЯ РИЗИКІВ.

РОЗПОДІЛ ТА АУТСОРСИНГ РИЗИКУ.

ПОПЕРЕДЖЕННЯ РИЗИКУ.

ЗНИЖЕННЯ СТУПЕНЯ РИЗИКУ.

УХИЛЕННЯ ВІД РИЗИКУ

УХИЛЕННЯ ВІД РИЗИКУ передбачає відмову від вчинення певних дій та прийняття рішень, що характеризуються високим ризиком, зокрема:

від ризикованих інвестиційних та інноваційних проектів;

від послуг ненадійних (сумнівних) партнерів і контрагентів;

від послуг некомпетентних, недобросовісних співробітників;

від прийняття ризикованих рішень;

від здійснення операції, рівень ризику за якими надмірно високий;

від використання у значних обсягах позикового капіталу;

від надмірного використання оборотних активів в низьколіквідних формах;

від використання вільних грошових активів в короткострокових вкладеннях

Відмова від ризику дозволяє повністю уникнути можливих втрат, але позбавляє підприємство додаткових джерел формування прибутку, а відповідно негативно впливає на темпи його економічного розвитку, ефективність використання власного капіталу та вільних грошових активів в короткострокових вкладеннях.

УХИЛЕННЯ ВІД РИЗИКУ повинно здійснюватися дуже виважено за таких умов: якщо відмова від одного ризику не спричиняє виникнення іншого ризику вищого рівня; якщо рівень ризику незалежний з рівнем дохідності операції за шкалою «дохідність-ризик»; якщо втрати за даним видом ризику перевищують можливості їх відшкодування за рахунок власних фінансових коштів підприємства; якщо розмір доходу від операції, яка генерує певні види ризику, є несуттєвим, тобто має невідчутну питому вагу у формуванні грошового потоку підприємства; якщо операція є нехарактерною для діяльності підприємства, носить інноваційний характер і

за нею відсутня інформаційна база, необхідна для визначення рівня ризиків та прийняття відповідних управлінських рішень.

ПРИЙНЯТТЯ РИЗИКУ

ПРИЙНЯТТЯ РИЗИКУ передбачає взяття ризику на свою відповідальність або його збереження та не передбачає вживання жодних заходів щодо захисту від нього. Застосовується у випадках, коли рівень ризику знаходиться на прийнятному рівні, а вплив на нього є неможливим або економічно неефективним і за умови настання ризику призводить до втрат.

ПРИЙНЯТТЯ РИЗИКУ Втрати у разі настання ризику можуть покриватись за рахунок: поточного грошового потоку; отримання кредитів, позик; державних дотацій; використання додаткових коштів, що вносяться власниками бізнесу з метою його підтримки; спонсорства; резервування власних коштів для непередбачених випадків; самострахування.

ПРИЙНЯТТЯ РИЗИКУ може бути запланованим (свідомим) та незапланованим (несвідомим)

Незаплановане прийняття ризику виникає, якщо: джерело небезпеки не було виявленим; страхового покриття виявилося недостатньо; третя сторона не виконала взятих на себе зобов'язань щодо компенсації збитків від ризиків; втрати виявилися поза рамками пункту контракту про передачу ризику третій стороні; можливість зниження ризику була проігнорована через низьку ймовірність його реалізації.

Заплановане прийняття ризику передбачає два підходи до покриття можливих втрат: покривати втрати по мірі їх виникнення; резервувати певну суму доходу в кожен період.

Резервування коштів полягає в тому, що на підприємстві створюються відокремлені фонди відшкодування збитків за рахунок частини власних коштів (фінансові резерви, резервні фонди). Залежно від призначення фонди створюються в формах: натуральна форма – підприємства створюють

страхові запаси сировини, матеріалів та комплектуючих, залишають вільні потужності, встановлюють додаткові контакти. грошова форма – резервні грошові фонди створюються головним чином для непередбачених витрат, пов'язаних зі зміною цін і тарифів, оплатою ризиків, покриттям кредиторської заборгованості, збитків щодо ліквідації господарського суб'єкта, збитків від стихійних лих. Найважливішою умовою створення резервів є визначення необхідного в кожному конкретному випадку обсягу резервного запасу і порівняння витрат на їх створення з витратами на страхування.

При резервуванні важливо правильно визначити розмір фонду. Малий розмір фонду призведе до того, що його буде недостатньо для компенсації збитків. Велийкий розмір фонду відволікає значні кошти, які не залучаються в обіг, є мертвим капіталом і не приносять прибутку. Для прийняття правильного рішення щодо розміру фонду слід враховувати: прийнятний для підприємства рівень ризику; розміри фонду, достатні для забезпечення компенсації втрат від збереженого ризику; часовий масштаб накопичення і функціонування фонду. Періодично розмір фонду повинен переглядатися.

Самострахування полягає в створенні власних страхових фондів, призначених для покриття збитків, за типом фондів страхових компаній. Самострахування зазвичай реалізується через створення кептивних страхових компаній (страхові компанії, які входять в групу нестрахових організацій (промислових, фінансово-промислових груп тощо) і страхують ризики всієї групи).

Кептивне страхування ПЕРЕВАГИ дозволяє інвестувати кошти фондів в межах об'єднаної ділової одиниці; дозволяє зберегти прибуток всередині групи; дозволяє отримати пільги по оподаткуванню (передбачається законодавством певних країни); Дозволяє уникнути бюрократичної тяганини при оформленні страхування. НЕДОЛІК додається новий ризик погіршення загальних фінансових результатів, пов'язаний з настанням великих, катастрофічних ризиків.

РОЗПОДІЛ РИЗИКУ

РОЗПОДІЛ РИЗИКУ передбачає розподіл відповідальності за ризик між підприємством та третіми особам при збереженні його загального існуючого рівня. Застосовується у випадках, коли вплив на ризик з боку підприємства є неможливим або економічно не виправданим, а рівень ризику не є прийнятним для підприємства. СПОСОБИ РОЗПОДІЛУ РИЗИКУ:

1. Шляхом укладання договорів.
2. Через використання диверсифікації.
3. Через організаційну форму бізнесу.

Типи договорів, що використовуються для розподілу ризику: будівельні контракти; договори на зберігання і перевезення вантажів; договори на продаж, обслуговування, постачання; договір оренди, лізингу; договір гарантії та поруки; договір застави майна; договір факторингу; договір хеджування; договір страхування.

Порука – договір, що застосовується для забезпечення зобов'язань при взаєминах кредитора як з юридичною так і з фізичною особою.У договорі поруки фігурують три сторони: принципал – зобов'язується повернути борг; поручитель – бере на себе відповідальність за виконання зобов'язань принципала; кредитор – особа, щодо якої укладено договір. Гарантія – договір, що застосовується для забезпечення зобов'язань при взаєминах між юридичними особами. При використанні гарантії з гаранта стягується тільки сума гарантії, спеціально обумовлена в документі про гарантії. Вона може бути меншою від суми боргу.

Факторинг дозволяє фірмі, що передає свої боргові зобов'язання фактор-посереднику, отримати гарантію на отримання всіх платежів, зменшуючи таким чином кредитний ризик підприємства. У факторингових операціях беруть участь три сторони: фактор-посередник – банк або організація, що мають ліцензію на здійснення такої діяльності; підприємство-постачальник; підприємство-покупець.

Хеджування (Hedging) передбачає передачу ризиків, викликаних несприятливими змінами курсів валют, товарних цін та процентних ставок шляхом укладання строкових контрактів. Існують два типи операцій хеджування: хеджування на підвищення; хеджування на зниження.

Хеджування (Heaging) Під строковим контрактом розуміється контракт, виконання якого за укладеною угодою відкладається на певний термін. До строкових контрактів відносять: форвардні контракти – взаємне зобов'язання сторін провести купівлю-продаж товару за заздалегідь узгодженою (форвардної) ціною в заздалегідь обумовлений термін. ф'ючерсні контракти – зобов'язання купити або продати певну кількість фінансових інструментів або товарів за ціною, погодженою у вільному біржовому торзі. На відміну від форвардних ф'ючерсні контракти можуть укладатись тільки на біржі. Однією з сторнон таких угод є розрахункова палата біржі. опціон – право (а не зобов’язання) щось купити або продати за заздалегідь обумовленою ціною у встановлений термін.

Диверсифікація полягає в дробленні активів, інвестицій між непов'язаними один з одним об'єктами вкладень, розподіл зусиль між декількома непов'язаними між собою, видами діяльності («не класти всі яйця в один кошик»). Форми диверсифікації: диверсифікація діяльності; диверсифікація портфеля цінних паперів диверсифікація програми реального інвестування диверсифікація кредитного портфеля диверсифікація постачальників сировини та матеріалів; диверсифікація ринків збуту; диверсифікація валютного кошика підприємства; диверсифікація в банківській системі.

АУТСОРСИНГ РИЗИКУ

АУТСОРСИНГ РИЗИКУ передбачає покладання відповідальності за зниження можливості виникнення несприятливих подій на сторонню організацію (інший суб'єкт). Найчастіше така передача здійснюється на основі договору. Підприємство концентрується на основних функціях, що

приносять дохід. Для аутсорсерів надання допоміжних функцій є основним бізнесом, вони вміють ефективно і якісно їх надавати, самі послуги стандартизуються. Аутсорсери навчилися управляти ризиками допоміжних функцій, на яких вони спеціалізуються. Для підприємства сотні ризиків перетворюються в кілька ризиків управління постачальником послуг.

ПОПЕРЕДЖЕННЯ РИЗИКУ

ПОПЕРЕДЖЕННЯ РИЗИКУ передбачає проведення превентивних заходів, спрямованих на зниження ймовірності настання несприятливої події. інструменти попередження ризику: заходи, що підвищують надійність функціонування та поліпшують якісні характеристики підприємства; заходи, що покращують реакцію підприємства на вплив зовнішнього середовища; заходи, що дозволяють змінити параметри впливу зовнішнього середовища на підприємство.

Заходи, що підвищують надійність функціонування та поліпшують якісні характеристики підприємства: превентивні заходи щодо запобігання аварій основних технічних засобів; система поточного та капітальний ремонту техніки; постійний контроль за забезпеченням збереження майна; система якості; удосконалення системи управління підприємством; ретельний відбір персоналу; підвищення кваліфікації, рівня освіти співробітників; впровадження гнучких технологій.

Заходи, що покращують реакцію підприємства на вплив зовнішнього середовища: вивчення кон'юнктури ринку; маркетингові дослідження; прогнозування та планування діяльності; впровадження системи стратегічного управління; використання додаткової інформації для прийняття рішень; ретельна перевірка партнерів; використання нових інформаційних технологій тощо.

Перевірка бізнес-партнерів: аналізуються установчі та інші документи; перевіряються факти реєстрації підприємства, отримання ліцензії, постановки на облік у податковій інспекції та регулярності сплати податків;

при виникненні сумнівів встановлюються факти можливої втрати паспортів особами, відомості про яких містяться у поданих документах; встановлюється факт розташування за вказаною фактичною адресою підприємства; перевіряються виробничі і фінансові можливості щодо виконанню умов договору; з незалежних джерел з'ясовується репутація керівника і головного бухгалтера підприємства.

Заходи, що дозволяють змінити параметри впливу зовнішнього середовища на підприємство: пошук нових ринків збуту; активний маркетинг; формування свого споживача; посилення санкцій за невиконання договірних зобов'язань.

ЗНИЖЕННЯ СТУПЕНЯ РИЗИКУ

ЗНИЖЕННЯ СТУПЕНЯ РИЗИКУ (ЛОКАЛІЗАЦІЯ) передбачає проведення превентивних заходів, спрямованих на зниження розміру потенційних збитків.

МЕТОДИ ЗНИЖЕННЯ СТУПЕНЯ РИЗИКУ: створення венчурів; лімітування ризиків; дублювання значущих об'єктів, схильних до ризику; ефективний менеджмент в процесі реалізації ризикованих рішень; навчання персоналу роботі в екстрених ситуаціях; соціально-психологічні заходи щодо виховання чутливості до ризику; розвиток корпоративної культури; активна протидія тощо.

Література

1. Друкер, Питер, Ф. Эффективное управление предприятием.: Пер. с англ. – М.: ООО «И.Д. Вильямс», 2008. – 224с.: ил. Парал. тит. англ.

2. Дж. М. Кейнс. Общая теория занятости, процента и денег.

3. Альгин А.П. Грани экономического риска. – М.: Знание, 1991. – 64с. – (Новое в жизни, науке, технике. Сер. «Практика хозяйствования и управления»; №1).

4. В.В. Черкасов Проблемы риска в управленческой деятельности: Монография, М.: «Рефл-бук», Киев: «Валер», 1999.

5. Валдайцев С.В. Оценка бизнеса: учеб.: 3-е изд. перераб. и доп. – М.: ТК Велби, Изд-во Проспект, 2008. – 576с.

6. Балабанов И.Т. Риск-менеджмент. М. – Финансы и статистика, 1996. – 192с.: ил.

7. Гранатуров В.М. Экономический риск: сущность, методы измерения, пути снижения: Учебное пособие. – 2е изд., перераб. и доп. – М.: Издательство «Дело и Сервис», 2002 – 160с.

8. Вітлінський В.В., Наконечний С.І. Ризик у менеджменті. – К.: ТОВ «Борисфен-М», 1996. – 336с.

9. Тэпман Л.Н. Риски в экономике: Учеб. пособие для вузов / Под ред. проф. В.А. Швандара. – М.: ЮНИТИ-ДАНА, 2002. – 380 с.

10. Ризик у ринковій економіці: Навчальний посібник/ Андрєєва Т.Є., Петровська Т.Е. – Харків: Бурун Книга, 2005. – 128с.: 12іл.

11. Устенко О.Л. Теория экономического риска: Монография. – К.: МАУП, 1997. – 164с.

12. Ілляшенко С.М. Економічний ризик: Навчальний посібник. 2-ге вид., доп. перероб. – К.: Центр навчальної літератури, 2004. – 220с. 11

13. Хохлов Н.В. Управление риском: Учеб. Пособие для вузов. – М.: ЮНИТИ-ДАНА, 2001. – 239с.

14. Райзберг Б.А. Предпринимательство и риск. – М.: Знание, 1992. – 62с. – (Новое в жизни, науке, технике. Сер. «Экономика», №4).

15. ВітлінськийВ. В. Аналіз, моделювання та управління економічним ризиком / В. В. Вітлінський, П. І. Верчено. - К. : КНЕУ, 2000. - 292 с.

16. Вітлінський В. В. Ризикологія в економіці та підприємництві : монографія / В. В. Вітлінський, Г. І. Великоіваненко. - К. : КНЕУ, 2004. - 480 с.

17. Клименко С. М. Обґрунтування господарських рішень та оцінка ризиків / С. М. Клименко, О. С. Дуброва. - К. : КНЕУ, 2005. - 252 с.

18. Лук’янова В. В. Економічний ризик / В. В. Лук’янова, Т. В. Головач. - К. : Академвидав, 2007. - 464 с.

19. Tom Demarko. Waltzing with Bears: Managing Risk on Software Projects.