УДК 004.056

ДИНАМІЧНІ РИЗИКИ В БІЗНЕС-ПРОЦЕСАХ

Т. А. Іванова[1], О. Є. Архипов[2]

[1] *НТУУ "Київський політехнічний інститут"*
[2] *НТУУ "Київський політехнічний інститут"*

Анотація

В даній роботі визначено поняття ризик, динамічний ризик, бізнес-процес. Також представлено фрагмент типової структури бізнес-процесу виробництва, його можливі загрози. Поняття термінальної ймовірності, сценарний спосіб завдання термінальних ймовірностей.

Ключові слова: ризик, динамічний ризик, інформаційна безпека, бізнес-процес, термінальна ймовірність, загроза, вразливість, атака

Вступ

Інформаційна безпека – основна складова безпеки підприємства та його діяльності в цілому. Вона включає в себе захист і збереження комерційної таємниці підприємства, дані про особливості виробництва і збуту продукції, забезпечення конфіденційності персональних даних співробітників, а також осіб, що надають разові чи регулярні консультації та інформаційно-технічну підтримку. Стан інформаційної безпеки не є постійним, він має динаміку, залежну від постійно змінюваних параметрів зовнішнього та внутрішнього середовища.

Постійно триваючий процес адаптації структури та параметрів системи захисту інформації до поточної трансформації середовища функціонування підприємства становить зміст управління інформаційною безпекою підприємства.

Для всіх процесів (внутрішніх, вхідних, вихідних), які супроводжують діяльність підприємства, характерна наявність інформаційної складової, яка в тій чи іншій мірі з ними взаємодіє і є частиною комерційної таємниці. Незалежно від виду інформації, пов'язаної із забезпеченням функціонування того чи іншого процесу виробництва, для неї характерним є наявність трьох властивостей: конфіденційності, цілісності, доступності.

Конфіденційність чи секретність пояснюється тим, що кожен виконавець повинен знати рівно стільки відомостей, скільки необхідно для виконання його функціональних обов'язків.

Цілісність – властивість інформації, яка забезпечує виконавцю розуміння його місця і ролі в процесі виробництва та дозволяє краще виконувати свої обов'язки.

Доступність – властивість інформації, що дозволяє виконавцю отримувати основні і допоміжні відомості, необхідні в процесі виробництва.

Забезпечення виконуваності всіх властивостей інформації, яка супроводжує весь процес виробництва на підприємстві – *інформаційна безпека підприємства.*

Ризик – діяльність, що пов'язана з подоланням невизначеності у виборі, під час якого є можливість кількісно і якісно оцінити ймовірність досягнення передбачуваного результату, невдачі і відхилення від цілі, *управління ризиками* – процеси, пов'язані з ідентифікацією, аналізом ризиків і прийняттям рішень, які включаю максимізацію позитивних і мінімізацію негативних наслідків при виникненні ризикових подій.

Аналіз ризиків включає в себе:

- Ідентифікацію активів
- Ідентифікацію бізнес-вимог і вимог законодавства, що застосовують до ідентифікованих активів
- Оцінка активів з урахуванням ідентифікованих бізнес-вимог і вимог законодавства, а також наслідків порушення їх конфіденційності, цілісності та доступності
- Ідентифікацію значимих загроз і вразливостей ідентифікованих активів
- Оцінку ймовірності реалізації загроз і величини вразливостей

Оцінка ризиків полягає у визначенні їх кількісного і якісного значення, формування реєстру ризиків і ранжирування ризиків.

1. Об'єкт дослідження

Фрагмент типової структури бізнес-процесу виробництва:

1) Розробка нових і вдосконалення існуючих продуктів
    - Розробка концепції нового продукту

- Розробка стратегії маркетингу і продаж нового продукту
- Розробка конструкції нового продукту

2) Просування і продаж продукції
   - Укладання договору з клієнтом
   - Прийом замовлень від клієнта
   - Виконання замовлення клієнта
3) Відтворення інформаційних систем і устаткування IT-інфраструктури
   - Вибір конфігурації та планування забезпечення компаніїінформаційними системами та обладнанням IT-інфраструктури
   - Розробка або доробка інформаційних систем
   - Введення інформаційних систем або обладнання IT-інфраструктури компанії в експлуатацію
4) Відтворення трудових ресурсів
   - Підбір персоналу
   - Введення персоналу в роботу
   - Рух і вивільнення персоналу
5) Фінансування діяльності та розрахунки
   - Розрахунок витрат
   - Забезпечення фінансовими ресурсами
   - Підготовка фінансової звітності

Наступні ризики є специфічними для внутрішніх процесів:

Управління кадровими ресурсами. Ризик інформаційної безпеки виникає при взаємодії співробітників та інформаційних систем. Отже, всі співробітники відіграють важливу роль у справах з ризиками в організації. Ці ризики повинні враховуватися при наймі, навчанні, покаранні, а також при звільненні чи переводі на іншу роботу.

Дослідження та розробка. Ці види діяльності можуть представляти собою значний ризик у випадку, якщо існує неконтрольований зв'язок між середовищем розробки та середовищем виробництва/експлуатації. Дослідження і розробка можуть також виробляти строго конфіденційну інформацію, яка є складовою комерційної таємниці, і відноситься до продуктів розробки. Тому учасники цих процесів повинні усвідомлювати ризики і свою відповідальність за управління ними.

Адміністрування і IT. Ці процеси часто розглядаються у якості процесів, що несуть відповідальність за оцінку і управління ризиками інформаційної безпеки. Проте важливо, щоб усвідомлювався зв'язок між інформаційними ризиками і ризиками організації і, як наслідок, оцінка ризиків інформаційної безпеки виконувалась усіма функціональними підрозділами.

Фінанси і бухгалтерія. Оцінка ризиків інформаційної безпеки має першочергове значення для фінансових і бухгалтерських процесів в будь-якій організації. Якісне корпоративне управління потребує злагодженої і точної фінансової інформації, яка можу бути відстежена з моменту свого походження до моменту її використання за допомогою зрозумілого журналу аудиту. У відповідності з вимогами бізнесі і нормативної бази повинна забезпечуватися конфіденційність цінової інформації, фінансових результатів і прогнозів.

Наступні ризики є специфічними для окремих зовнішніх процесів:

Продаж і маркетинг. Ці види діяльності представляють собою життєво важливий інтерфейс між організацією та суспільством. В будь-якій організації існує потенціальний ризик порушення конфіденційності інформації по ходу торгових і маркетингових операцій, а також нанесення збитків репутації організації по причині того, що не були забезпечені точність і доступність інформації.

Виробництво і експлуатація. Інформація, яка використовується в процесах виробництва і експлуатації, повинна бути дуже точною і узгодженою, а також доступною по першому запиту. Для тих ресурсів, які є критичними для процесів виробництва і експлуатації, відповідні ризики повинні бути чітко ідентифіковані і опрацьовані.

Підтримка . Цей процес потребує точної інформації, доступної до першого запиту. Наслідками порушення є заподіяння шкоди репутації організації.

2. Методологія аналізу динамічних інформаційних ризиків

Термінальні ймовірності. Особливістю бізнес-процесу є кінцевий цикл реалізації окремих бізнес-процедур, з яких складається процес. При виконанні бізнес-процедур використовуються різноманітні системи інформаційних технологій, загрози та вразливості яких мають змінних характер. Тому структура моделі загроз є динамічною і має такі особливості:

- Змінний склад моделі загроз бізнес-процесу, залежність від конкретики виконуваної задачі
- Обмежений час існування загроз (пов'язано з розвитком бізнес-процесу, портфелем замовлень, їх тривалістю)
- Розподілення ймовірності кожної загрози в межах проміжку часу τ, що відповідає часу існування загрози

Вважаючи ці особливості вводиться поняття термінальної ймовірності реалізації загрози $P(t)$, яка розподілена на проміжку часу τ за деяким законом:

$$P(t) = P_m \int_0^t p(t)dt = P_m \int_{t_1}^{t_1+t} p(t)dt$$

і відповідає значенню ймовірності реалізації загрози $P(t)$ за певний проміжок часу t$\leq\tau$, за який було почато реалізацію загрози. При чому $\int_0^\tau p(t)dt = 1$, а значить $P(\tau)= P_m$. Приклад зміни термінальної ймовірності показано на Рис. 1.

Момент виникнення загрози - t_1, час її існування – τ, $p(t)$ – густина термінальної ймовірності, рівномірно розподілена на часовому проміжку $[t_1,t_2]$, що обумовлює лінійне зростання в цьому проміжку термінальної ймовірності $P(t)$ від 0 до її максимального значення P_m з подальшим збереженням свого значення до моменту $t_1+\tau$ завершення бізнес-процесу.

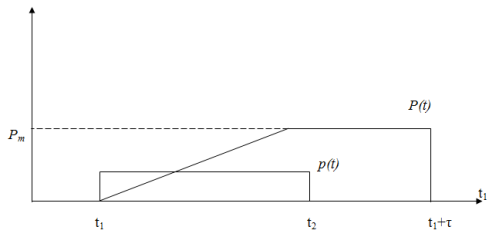

Рис. 1. Залежність значення ймовірності *P(t)* від густини розподілу *p(t)* і часу τ існування загрози.

В момент $t_1+\tau$ ймовірність різко спадає до 0. Це пояснюється спадом інтересу атакуючої сторони до інформації, що була об'єктом атаки.

Використання термінальних ймовірностей дозволяє врахувати динаміку розвитку атак, яку зазвичай опускають при проведенні аналізу загроз. Очевидно, що ймовірності реалізації загроз залежать від часу, тоді і значення ризиків не будуть постійними в часі. Ризики бізнес-процесів мають динамічний та процесний характер.

Сценарний спосіб завдання термінальних ймовірностей. Ймовірність реалізації загрози визначається за формулою:

$$P(t) = P_T(t)P_V(t),$$

де $P_T(t)$ - це ймовірність виникнення загрози, $P_V(t)$ - ймовірність реалізації атаки.

Нехай є зловмисник , загроза T відносно деякої інформації сторони B, вразливість V. $P_T(t)$ - зловмисник оцінює свої можливості, тобто досвід K, грошові ресурси G і час t. При $t = 0$ початковий досвід також дорівнює 0. g – вигода, яку отримає , визначається цінністю інформації. Тоді

$$P_T = \frac{GK}{g}t$$

Це означає, що при нестачі досвіду грошові можливості A не мають ніякої ваги для виникнення загрози. При t_{max}: $K = max, G = min, g = max$.

Можна припустити, що зі зростанням t, яке атакуюча сторона тратить на організацію, підготовку і проведення атаки, росте термінальна ймовірність $P_v(t)$ успішного використання вразливості V:

$$P_V(t) = p_v t,$$

де густина ймовірності p_v розподілена рівномірно на проміжку $(0,\ t_v)$, $t_v > t_{max}$, $p = const$. Тоді ймовірність реалізації загрози визначається виразом:

$$P(t) = P_T(t)P_V(t) = \left(\frac{GK}{g}t\right)p_v t = \frac{GKp_v}{g}t$$

Висновок

При широкому застосуванні підприємством інформаційних технологій та електронної комерції його успішне функціонування значною мірою пов'язане із рівнем захищеності інформації. Загрози, які стосуються використовуваних ресурсів IT, напряму впливають на конкурентоспроможність, інноваційність, подальший розвиток підприємства. Також вразливості систем, людський фактор мають безпосереднє відношення до убезпечення інформації.

Бізнес-процеси – невід'ємна частина діяльності підприємства. Саме вони визначають напрямок діяльності, успішність, подальше планування і розвиток. Загрози бізнес-процесів визначають ризики, які можливі при реалізації цих загроз.

Динамічні ризики характеризуються часовим проміжком, на якому виконується бізнес-процес. Визначення та підрахунок динамічних ризиків є важливим етапом у формуванні політики захисту інформації.

Тому без визначення загроз, побудови моделі загроз, знаходження вразливостей, остаточному підрахунку ризиків неможлива бізнес-діяльність з використанням інформаційних технологій. Адже інформація, що циркулює під час процесу, повинна бути захищеною задля подальшого успіху та економічної вигоди підприємства.

Література

1. Архипов А. Е. Особенности анализа рисков в информационно-коммуникационных системах.
2. Астахов А. Искусство управления рисками.
3. Кузнецова Е. С. Управление операционными рисками на основе процессного подхода.
4. Ахметханов Р. С., Дворецкая Т. Н., Куксова В. И., Юдина О. Н. Динамические риски и безопасность техническиех систем.