Оцінка ризиків інформаційної безпеки клієнтів телекомунікаційних підприємств

Бакалаврська кваліфікаційна робота · спеціальність 125 «Кібербезпека»

Автор	Зінченко Максим Романович
Освітня програма	Безпека інформаційних і комунікаційних систем
Науковий керівник	Ізмайлова Ольга Василівна, к.т.н., доцент

Робота поєднує методику оцінювання ризиків із програмним прототипом, який автоматизує розрахунки первинного та залишкового ризику.

Актуальність теми

Телекомунікаційні підприємства накопичують у CRM-середовищі персональні, фінансові та технічні дані клієнтів. Порушення їх безпеки напряму впливає на якість обслуговування, фінансові операції та довіру абонентів.

Критичні дані

- ідентифікаційні та контактні дані
- фінансові записи та тарифи
- технічні параметри підключення
- історія звернень у підтримку

Можливі наслідки

- витік персональних даних
- шахрайські дії
- некоректні нарахування
- збої в обслуговуванні
- репутаційні втрати

Проблема управління

Без формалізованої оцінки складно визначити, які ризики є критичними, які контрзаходи пріоритетні та який залишковий ризик залишається після захисту.

Потрібна методика, яка переводить якісні ознаки ризику у зрозумілу числову оцінку та дозволяє порівнювати ризикові сценарії між собою.

Мета, об’єкт, предмет і завдання роботи

Мета роботи

Підвищення обґрунтованості управління інформаційною безпекою клієнтів шляхом розроблення методики оцінювання ризиків і програмного прототипу.

Об’єкт

Процеси обробки та захисту клієнтських даних у телекомунікаційному підприємстві.

Предмет

Методи, критерії та програмні засоби оцінювання ризиків інформаційної безпеки.

Завдання роботи

01 проаналізувати предметну область і підходи до оцінювання ризиків

02 визначити активи, загрози, вразливості та ризикові сценарії

03 сформувати критерії, шкали та формули розрахунку ризику

04 реалізувати програмний модуль оцінювання ризиків

05 перевірити ефективність контрзаходів на сценаріях

Логіка роботи: від аналізу CRM-середовища — до методики, програмної реалізації та оцінки ефективності зниження ризику.

Ключові ризикові сценарії

Ризик у роботі розглядається як конкретний сценарій: актив, загроза, вразливість, процес обробки даних і можливі наслідки для клієнта та підприємства.

1. Слабка автентифікація
прості паролі та відсутність блокування після невдалих входів

2. Надлишкові права доступу
ролі мають більше прав, ніж потрібно для виконання роботи

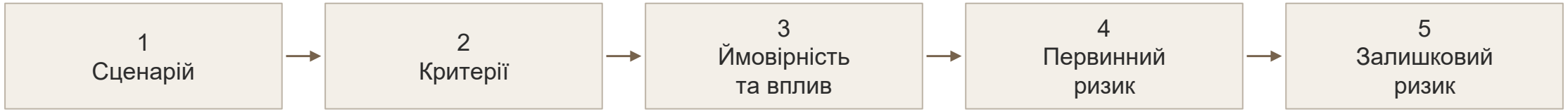
3. Масовий експорт без контролю
відсутність лімітів, погодження та аудиту вивантаження

4. Проблеми backup-відновлення
резервні копії створюються, але не перевіряються відновленням

Саме ці сценарії надалі оцінюються за єдиними критеріями та порівнюються за рівнем залишкового ризику.

Загальна логіка методики

Методика перетворює опис ризикового сценарію у послідовний розрахунок: від вхідних критеріїв до первинного ризику, залишкового ризику та рівня небезпеки.



Вхідні дані

- актив і процес
- загроза та вразливість
- оцінки F, V, A, C, I, D, J, R
- ефективність контрзаходів K

Розрахунок

- P — ймовірність
- Impact — сукупний вплив
- Rprimary — ризик до захисту
- Rresidual — ризик після контрзаходів

Вихідний результат

- числове значення ризику
- рівень ризику
- пріоритет реагування
- пріоритетні дії

Критерії та шкали оцінювання

Щоб різні ризики можна було порівнювати між собою, кожен критерій переводиться в єдину шкалу 1–5. Далі критерії об’єднуються через вагові коефіцієнти.

Ймовірність P

F — частота реалізації загрози
V — рівень вразливості системи
A — привабливість активу

Вплив Impact

C — конфіденційність
I — цілісність
D — доступність
J — юридичні наслідки
R — репутаційна шкода

Контрзаходи K

K показує силу захисту після впровадження контрзаходів: парольна політика, RBAC, контроль експорту, backup, аудит.

Шкала 1–5

1 — низький рівень
3 — середній рівень
5 — високий рівень

Приклад інтерпретації

Якщо актив містить паспортні або фінансові дані, оцінки конфіденційності та цілісності будуть вищими, ніж для менш чутливої інформації.

Гнучкість методики

За потреби набір критеріїв можна розширити фінансовими, юридичними або галузевими показниками та задати для них окремі ваги.

Формули методики: від критеріїв до результату

Формули не вводять нові дані, а узагальнюють оцінки за критеріями. Спочатку визначаються ймовірність і вплив, потім первинний ризик і залишковий ризик після контрзаходів.

1. Ймовірність

P = 0,35F + 0,35V + 0,30A

F — частота
V — вразливість
A — привабливість активу

2. Вплив

Impact = 0,30C + 0,20I + 0,20D + 0,15J + 0,15R

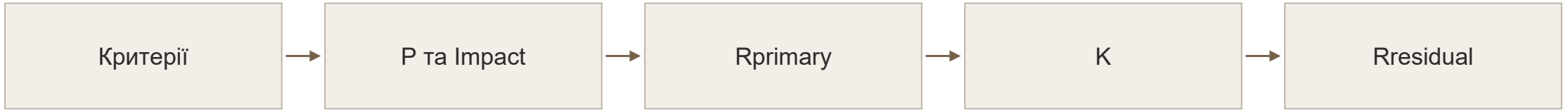
C/I/D — безпекові наслідки
J/R — правові та репутаційні наслідки

3. Ризик

Rprimary = P × Impact

Rresidual = Rprimary × (6 − K) / 5

K — ефективність контрзаходів



Первинний ризик показує небезпеку до захисних заходів, а залишковий ризик показує, що залишається після врахування ефективності контрзаходів.

Ймовірність (P)

Ймовірність ризику визначається через три критерії: частоту виникнення загрози, експлуатованість вразливості та доступність активу для порушника. Кожен критерій оцінюється за шкалою 1–5, після чого ці оцінки об’єднуються у показник P.

Рівень	Частота/передумови (F)	Експлуатованість (V)	Доступність активу (A)
1	Передумови виникають винятково рідко	Вразливість важко використати без спеціальних умов	Актив практично недоступний для джерела загрози
2	Подія малоймовірна, але можлива за поодиноких умов	Потрібні суттєві зусилля або спеціальні знання	Доступ обмежений і добре сегментований
3	Передумови з’являються періодично	Використання можливе за наявності мотивації або помірних ресурсів	Актив доступний частині користувачів чи каналів
4	Подія може виникати регулярно	Вразливість використовується відносно просто	Актив доступний широкому колу користувачів у процесі роботи
5	Передумови присутні постійно або майже постійно	Використання дуже просте і майже не потребує додаткових умов	Актив безпосередньо доступний порушнику або масовому колу осіб

Така шкала дозволяє формалізувати експертну оцінку ймовірності та зробити різні ризикові сценарії порівнюваними між собою.

Вплив (Impact)

Вплив ризику оцінюється через наслідки для конфіденційності, цілісності, доступності, юридичної відповідальності та репутації підприємства. Кожен критерій оцінюється за шкалою 1–5, після чого ці оцінки об’єднуються у показник Impact за ваговою формулою.

Рівень	Конфіденційність C	Цілісність I	Доступність D	Юридичні наслідки J	Репутаційна шкода R
1	Розкриття незначної або нечутливої інформації	Дані майже не змінюються або легко перевіряються	Короткочасне порушення без впливу на роботу	Юридичні наслідки практично відсутні	Репутаційний вплив мінімальний
2	Можливе розкриття обмеженого набору клієнтських даних	Незначні помилки в окремих записах	Тимчасові незручності для частини користувачів	Можливі внутрішні зауваження або скарги	Невелике невдоволення окремих клієнтів
3	Розкриття персональних або контактних даних групи клієнтів	Помилки можуть вплинути на обслуговування або фінансові операції	Помітне порушення роботи окремого сервісу	Можливі скарги клієнтів або перевірки	Помітне зниження довіри частини клієнтів
4	Витік значного обсягу персональних або фінансових даних	Спотворення критичних клієнтських або фінансових записів	Тривале порушення роботи важливих сервісів	Можливі штрафи, претензії або офіційні перевірки	Значні репутаційні втрати для підприємства
5	Масовий витік критичних клієнтських даних	Критичне порушення достовірності бази клієнтів або платежів	Масова недоступність CRM або ключових сервісів	Серйозні правові наслідки, регуляторні санкції	Критична втрата довіри клієнтів і публічний резонанс

Чим вищий рівень впливу, тим серйозніші наслідки для клієнтських даних, бізнес-процесів, юридичної відповідальності та довіри клієнтів.

Як коефіцієнт K зменшує залишковий ризик

K відображає ефективність контрзаходів за шкалою 1–5. Чим сильніші контрзаходи, тим менший коефіцієнт у формулі залишкового ризику.

Слабкий контроль

K = 1
коефіцієнт = 1,0
Rresidual = Rprimary

Середній контроль

K = 3
коефіцієнт = 0,6
Rresidual = 60% від Rprimary

Сильний контроль

K = 5
коефіцієнт = 0,2
Rresidual = 20% від Rprimary

Обґрунтування K

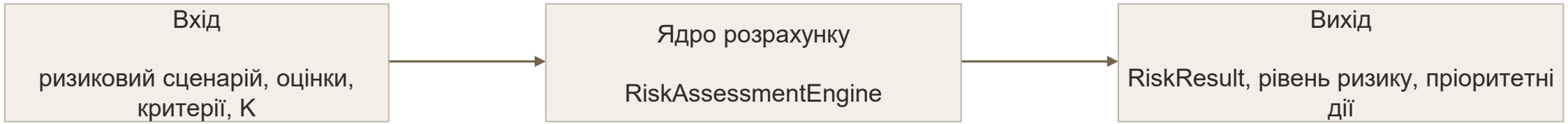
Значення K пов’язане з наявністю конкретних заходів: парольна політика, блокування входу, рольова модель доступу, погодження експорту, аудит дій, тестове відновлення backup.

Практичний зміст

Контрзаходи не скасовують сам факт загрози, але зменшують імовірність реалізації або масштаб наслідків. Тому оцінка переходить із критичної зони в контрольовану або прийнятну.

Архітектура програмної реалізації

Програмний прототип не є повноцінною CRM-системою. Його призначення — автоматизувати оцінювання ризикових сценаріїв і показати ефект контрзаходів.




```
RiskScenario("R1", "Компрометація облікового запису через слабку автентифікацію",
             "Обліковий запис CRM", "Зовнішній порушник", "Слабка парольна політика",
             "Вхід до CRM", 4, 4, 3, 5, 3, 2, 4, 4, 2),
```

Основні класи

RiskScenario — опис сценарію та оцінки
RiskAssessmentEngine — виконання формул
RiskResult — підсумковий результат

Контрольні модулі

AuthenticationControl — автентифікація
AccessMatrixValidator — права доступу
ExportControlService — експорт даних
BackupControlService — резервне відновлення

Алгоритм розрахунку в коді

Програмна логіка повторює математичну методику: сценарій перевіряється, показники розраховуються послідовно, результат класифікується за рівнем ризику.

1. **Створення сценарію**
   задаються F, V, A, C, I, D, J, R, K у межах 1–5
2. **Валідація**
   перевіряється коректність вхідних оцінок
3. **Розрахунок P та Impact**
   обчислюються зважені суми критеріїв
4. **Розрахунок ризику**
   визначаються Rprimary і Rresidual
5. **Класифікація**
   сценарій отримує рівень і пріоритет реагування

Псевдокод

```
probability = 0.35F + 0.35V + 0.30A
impact = 0.30C + 0.20I + 0.20D + 0.15J + 0.15R
primary = probability × impact
residual = primary × (6 − K) / 5
level = classify(residual)
```

Реалізація дозволяє додавати нові сценарії без зміни загальної логіки програми: змінюються лише вхідні дані та оцінки.

Контрольні модулі як контрзаходи

Контрольні модулі показують, які саме практичні заходи можуть зменшити ризик. Вони обґрунтовують підвищення K у покращених сценаріях.

AuthenticationControl

перевіряє складність паролів, блокування після невдалих входів

AccessMatrixValidator

виявляє надлишкові права доступу та порушення рольової моделі

ExportControlService

контролює масове вивантаження клієнтських даних через ліміти, погодження та аудит

BackupControlService

перевіряє актуальність резервних копій, checksum, тестове відновлення

Зв’язок із методикою: якщо контроль реально зменшує вразливість або наслідки, оцінка K зростає, а залишковий ризик знижується.

Порівняння до і після контрзаходів

Для перевірки ефективності створено два набори сценаріїв: базовий стан до впровадження захисту та покращений стан після застосування контрзаходів.

```
BASELINE
R2 16.0 Критичний
R3 16.0 Критичний
R1 12.8 Значний
R5 12.8 Значний
R4 7.2 Контрольований
R6 7.2 Контрольований
```

```
IMPROVED
R2 4.8 Прийнятний
R3 4.8 Прийнятний
R5 4.8 Прийнятний
R6 3.6 Прийнятний
R1 3.2 Прийнятний
R4 2.4 Прийнятний
```

Висновки

1. Аналіз предметної області
визначено клієнтські дані, CRM-процеси, загрози, вразливості та ризикові сценарії

2. Методика оцінювання
сформовано критерії, шкали та формули для первинного і залишкового ризику

3. Програмна реалізація
реалізовано прототип з класами RiskScenario, RiskAssessmentEngine і RiskResult

4. Контрольні модулі
показано контрзаходи для автентифікації, доступу, експорту та резервного відновлення

5. Перевірка ефективності
після контрзаходів сумарний залишковий ризик знизився з 72,0 до 23,6

Мету роботи досягнуто: методику оцінювання ризиків розроблено, програмно реалізовано та перевірено на практичних ризикових сценаріях.