УДК 004.056.53
DOI: 10.31673/2409-7292.2025.016743

Хохлачова Ю.Є., Волошин М.П.

МОДЕЛІ ОЦІНЮВАННЯ ЗАЛИШКОВОГО РИЗИКУ В ІНФОРМАЦІЙНИХ СИСТЕМАХ

У статті розглянуто нові моделі оцінювання залишкового ризику в інформаційних системах. Запропоновані моделі дозволяють більш точно оцінювати стан кібербезпеки шляхом урахування різних факторів ризику та механізмів їх впливу. Описано практичне застосування моделей для підвищення ефективності систем захисту інформації. Отримані результати можуть бути використані для вдосконалення кіберзахисту організацій та критичних інформаційних систем. Було представлено нові моделі оцінювання залишкового ризику, які враховують вплив різних типів загроз, рівень захищеності ІС та динаміку змін у середовищі кіберзагроз.

Ключові слова: кібербезпека, інформаційна система, залишковий ризик, моделі оцінювання, кіберзахист.

Вступ

З розвитком цифрових технологій та збільшенням кількості кіберзагроз питання забезпечення надійного захисту інформаційних систем (ІС) набуває особливої актуальності. Незважаючи на впровадження передових заходів кібербезпеки, завжди залишається певний рівень ризику, який визначається як залишковий ризик. Його точне оцінювання є важливим завданням, що дозволяє підвищити ефективність захисту ІС та оптимізувати розподіл ресурсів.

У даній статті представлено нові моделі оцінювання залишкового ризику, які враховують вплив різних типів загроз, рівень захищеності ІС та динаміку змін у середовищі кіберзагроз. Крім того, проаналізовано їх практичне застосування в умовах реальних кіберзагроз. Так стосовно сфери інформаційної безпеки детальний огляд підходів з оцінювання відповідних загроз наведено у Корченко О.Г., Архипова А.Є., Казмірчук С.В. «Аналіз та оцінювання ризиків інформаційної безпеки» та Єрмошина В.В, Невойта Я.В. «Аналіз і оцінка ризиків інформаційної безпеки». Так згідно з даними дослідженнями найбільшого поширення на сьогодні набули метод на основі байєсівських мереж, метод VAR, методика FRAP, стандарт 150/IEC 27005:2008 та ін. Проте багато існуючих моделей мають обмеження, зокрема недостатню точність оцінки ризиків або відсутність врахування динамічних змін у середовищі загроз. Тому розробка моделей, що дозволяють більш об’єктивно оцінювати залишковий ризик та оптимізувати заходи кіберзахисту, є актуальною науковою задачею.

Метою статті є розробка та вдосконалення моделей оцінювання залишкового ризику в інформаційних системах для підвищення ефективності функціонування систем кіберзахисту. Об’єктом дослідження є процес оцінювання залишкового ризику в інформаційних системах. Предмет дослідження – моделі оцінювання залишкового ризику в інформаційних системах.

Виклад основного матеріалу

Загальні підходи до моделювання залишкового ризику

Оцінювання залишкового ризику передбачає аналіз взаємодії кіберзагроз із засобами захисту інформації. Основні підходи до моделювання залишкового ризику включають [1,2]:

- Ймовірнісні моделі, які визначають ризик як ймовірність успішної реалізації загроз при існуючих механізмах захисту.
- Детерміновані моделі, що базуються на аналізі вразливостей системи та рівня її захисту.
- Гібридні моделі, які поєднують ймовірнісні підходи та експертні оцінки.

Модель оцінювання залишкового ризику для забезпечення доступності інформації

Доступність інформаційних ресурсів є критичною характеристикою безпеки ІС. Запропонована модель оцінює рівень ризику шляхом аналізу [3,4]:

- Інтенсивності атак типу DoS/DDoS;
- Надійності механізмів розподілу навантаження;
- Швидкості виявлення та реагування на інциденти.

Ймовірність порушення доступності (P) визначається як сукупність впливу атак (A), ефективності механізмів захисту (Z) та часу відновлення (T):

P=AZ×TP = \frac{A}{Z \times T}.

Чим більша величина P, тим вищий рівень залишкового ризику для доступності ІС.

Модель оцінювання залишкового ризику для забезпечення цілісності інформації

Цілісність інформації може бути порушена внаслідок зловмисних змін даних або програмного забезпечення. Запропонована модель базується на наступних параметрах:

- Кількість вразливостей у програмному забезпеченні (V);
- Частота атак на цілісність (F);
- Надійність механізмів виявлення змін (D).

Ймовірність компрометації цілісності визначається за формулою:

Pint=V×FDP_{int} = \frac{V \times F}{D},

де значення P_{int} показує ймовірність порушення цілісності даних.

Модель оцінювання залишкового ризику для забезпечення конфіденційності

Конфіденційність інформації забезпечується за допомогою криптографічних механізмів та політик доступу. Запропонована модель включає:

- Рівень захисту паролів і аутентифікації (A);
- Надійність криптографічних алгоритмів (C);
- Кількість несанкціонованих спроб доступу (U).

Формула оцінки ризику:

Pconf=UA×CP_{conf} = \frac{U}{A \times C}.

Чим вище значення P_{conf}, тим вищий ризик компрометації конфіденційності.

Практичне застосування розроблених моделей:

1. Оцінювання моделі забезпечення доступності функціонування інформаційних систем на основі залишкового ризику

Модель оцінювання залишкового ризику використовується для аналізу загроз доступності інформаційних ресурсів у системах, зокрема для визначення ймовірності порушення доступності через різні атаки або збої. Основна мета — оцінити залишковий ризик та сформувати стратегії його мінімізації. Залишковий ризик у цій моделі представлений як ймовірність порушення доступності ресурсу:

РД=РЗД(1−РЗУ)P_{Д} = P_{ЗД} (1 - P_{ЗУ})РД=РЗД(1−РЗУ),

де:

- РЗДP_{ЗД}РЗД — ймовірність подолання засобів забезпечення доступності;
- РЗУP_{ЗУ}РЗУ — ймовірність виявлення та усунення загроз доступності.

Приклади обрахунку залишкового ризику:

1. Дата-центр

- Ймовірність подолання системи захисту від DDoS-атак: РЗД=0.4P_{ЗД} = 0.4РЗД=0.4.
- Ймовірність виявлення та нейтралізації загрози: РЗУ=0.8P_{ЗУ} = 0.8РЗУ=0.8.
- Розрахунок залишкового ризику:

РД=0.4×(1−0.8)=0.08P_{Д} = 0.4 \times (1 - 0.8) = 0.08РД=0.4×(1−0.8)=0.08.

2. Банківська система

- Ймовірність успішного злому системи аутентифікації: РЗД=0.3P_{ЗД} = 0.3РЗД=0.3.
- Ймовірність виявлення та блокування атаки: РЗУ=0.9P_{ЗУ} = 0.9РЗУ=0.9.
- Розрахунок залишкового ризику:

РД=0.3×(1−0.9)=0.03P_{Д} = 0.3 \times (1 - 0.9) = 0.03РД=0.3×(1−0.9)=0.03.

3. Хмарний сервіс

- Ймовірність компрометації каналів зв’язку: РЗД=0.5P_{ЗД} = 0.5РЗД=0.5.
- Ймовірність виявлення та запобігання атаці: РЗУ=0.7P_{ЗУ} = 0.7РЗУ=0.7.
- Розрахунок залишкового ризику:

РД=0.5×(1−0.7)=0.15P_{Д} = 0.5 \times (1 - 0.7) = 0.15РД=0.5×(1−0.7)=0.15.

Графік показує залежність залишкового ризику PDP_DPD від ймовірності подолання захисту РЗДP_{ЗД}РЗД при різних рівнях ефективності заходів протидії РЗУP_{ЗУ}РЗУ.

Видно, що при більшому РЗУР_{ЗУ}РЗУ залишковий ризик значно знижується, а при низькому рівні захисту ризик різко зростає.

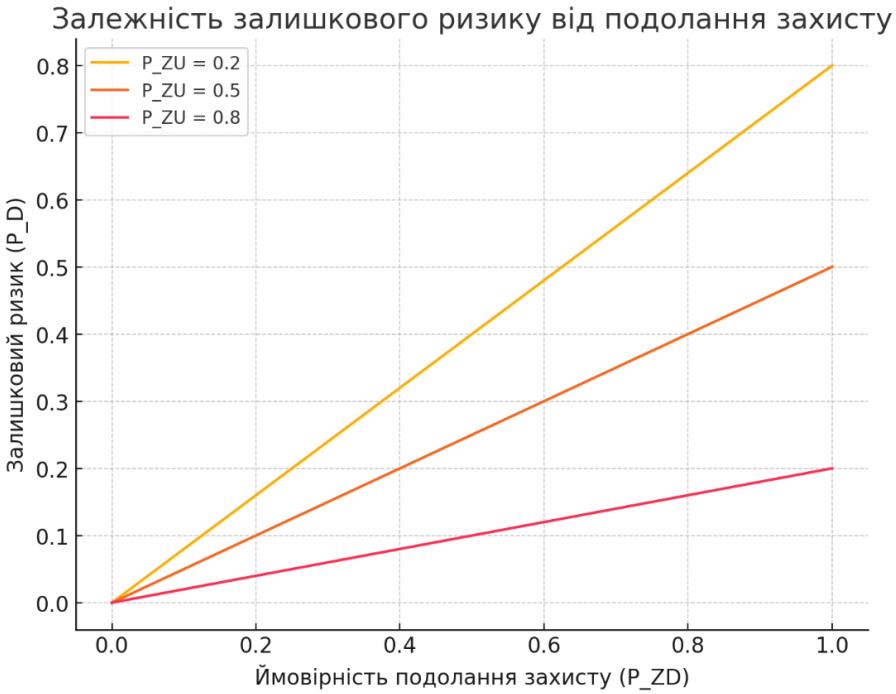

Рис. 1. Графіки залежності залишкового ризику від ймовірностей подолання захисту та ефективності заходів протидії

2. Оцінювання моделі забезпечення цілісності ресурсів інформаційних систем на основі залишкового ризику

Ця модель оцінювання залишкового ризику використовується для аналізу загроз цілісності інформації в інформаційних системах (ІС). Вона дозволяє визначити ймовірність порушення цілісності даних через несанкціоновану модифікацію, знищення або спотворення інформації.

Залишковий ризик у цій моделі представлений як ймовірність порушення цілісності інформації:

РЦ=РЗЦ(1−РЗУ)Р_{Ц} = Р_{ЗЦ} (1 - Р_{ЗУ})РЦ=РЗЦ(1−РЗУ),

де:

- РЗЦР_{ЗЦ}РЗЦ — ймовірність подолання засобів забезпечення цілісності;
- РЗУР_{ЗУ}РЗУ — ймовірність виявлення і усунення загроз цілісності.

Приклади обрахунку залишкового ризику:

1. Корпоративна база даних

- Ймовірність успішного злому та зміни записів у базі: РЗЦ=0.35Р_{ЗЦ} = 0.35РЗЦ=0.35.
- Ймовірність виявлення та відновлення пошкодженої інформації: РЗУ=0.85Р_{ЗУ} = 0.85РЗУ=0.85.
- Розрахунок залишкового ризику:

РЦ=0.35×(1−0.85)=0.0525Р_{Ц} = 0.35 \times (1 - 0.85) = 0.0525РЦ=0.35×(1−0.85)=0.0525.

2. Автоматизована система керування (SCADA)

- Ймовірність успішного внесення змін у критичні дані: РЗЦ=0.4Р_{ЗЦ} = 0.4РЗЦ=0.4.
- Ймовірність виявлення атаки та її нейтралізації: РЗУ=0.9Р_{ЗУ} = 0.9РЗУ=0.9.
- Розрахунок залишкового ризику:

РЦ=0.4×(1−0.9)=0.04Р_{Ц} = 0.4 \times (1 - 0.9) = 0.04РЦ=0.4×(1−0.9)=0.04.

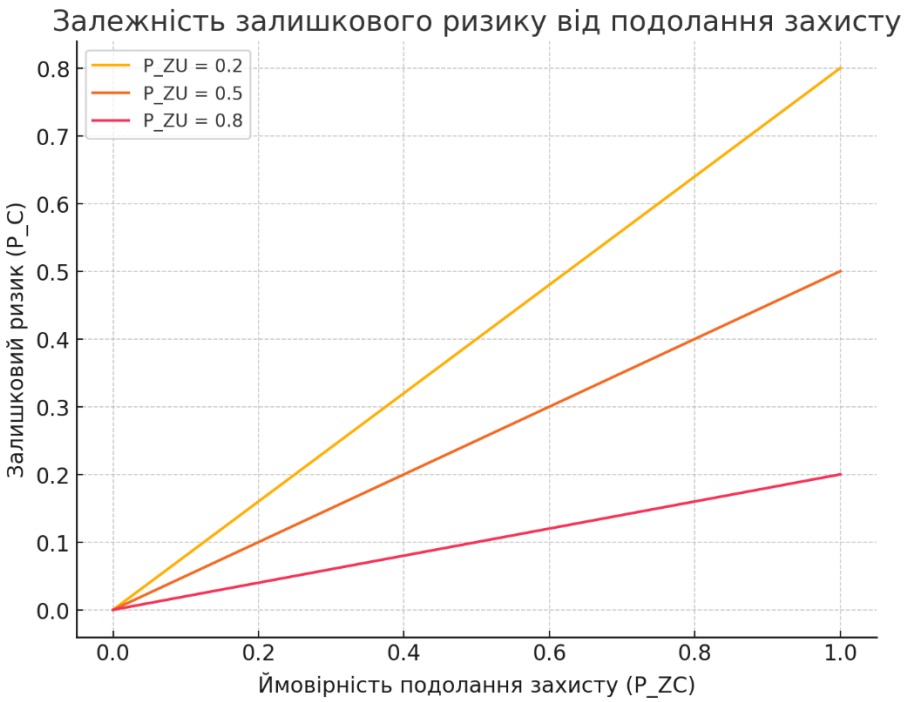

Рис. 2. Графіки залежності залишкового ризику від ймовірностей подолання захисту та ефективності заходів протидії.

3. Хмарне сховище даних

• Ймовірність успішної модифікації файлів користувачів: РЗЦ=0.5Р_{ЗЦ} = 0.5РЗЦ=0.5.

• Ймовірність виявлення загрози та виправлення змін: РЗУ=0.75Р_{ЗУ} = 0.75РЗУ=0.75.

• Розрахунок залишкового ризику:

РЦ=0.5×(1−0.75)=0.125Р_{Ц} = 0.5 \times (1 - 0.75) = 0.125РЦ=0.5×(1−0.75)=0.125.

Графік показує, як змінюється залишковий ризик РСР_СРС залежно від ймовірності подолання захисту РЗЦР_{ЗЦ}РЗЦ при різних рівнях ефективності заходів протидії РЗУР_{ЗУ}РЗУ. При високих значеннях РЗУР_{ЗУ}РЗУ залишковий ризик суттєво зменшується, що підтверджує важливість якісного захисту цілісності інформації.

3. Оцінювання моделі забезпечення конфіденційності ресурсів інформаційних систем на основі залишкового ризику

Ця модель оцінювання залишкового ризику використовується для аналізу загроз конфіденційності інформації в інформаційних системах (ІС). Вона дозволяє оцінити ймовірність порушення конфіденційності через несанкціонований доступ, витік даних або подолання криптографічного захисту.

Залишковий ризик у цій моделі представлений як ймовірність порушення конфіденційності інформації:

РК=РЗК(1−РЗУ)Р_{К} = Р_{ЗК} (1 - Р_{ЗУ})РК=РЗК(1−РЗУ),

де:

• РЗКР_{ЗК}РЗК — ймовірність подолання засобів забезпечення конфіденційності;

• РЗУР_{ЗУ}РЗУ — ймовірність виявлення і усунення загроз конфіденційності.

Приклади обрахунку залишкового ризику:

1. Конфіденційна документація урядової установи

• Ймовірність успішного подолання фізичного та логічного контролю доступу: РЗК=0.3Р_{ЗК} = 0.3РЗК=0.3.

• Ймовірність виявлення несанкціонованого доступу та блокування: РЗУ=0.8Р_{ЗУ} = 0.8РЗУ=0.8.

• Розрахунок залишкового ризику:

РК=0.3×(1−0.8)=0.06P_{K} = 0.3 \times (1 - 0.8) = 0.06РК=0.3×(1−0.8)=0.06.

2. Корпоративна система електронної пошти

• Ймовірність компрометації захисту паролів та витоку інформації: РЗК=0.4P_{ЗК} = 0.4РЗК=0.4.

• Ймовірність виявлення атаки та вжиття заходів: РЗУ=0.85P_{ЗУ} = 0.85РЗУ=0.85.

• Розрахунок залишкового ризику:

РК=0.4×(1−0.85)=0.06P_{K} = 0.4 \times (1 - 0.85) = 0.06РК=0.4×(1−0.85)=0.06.

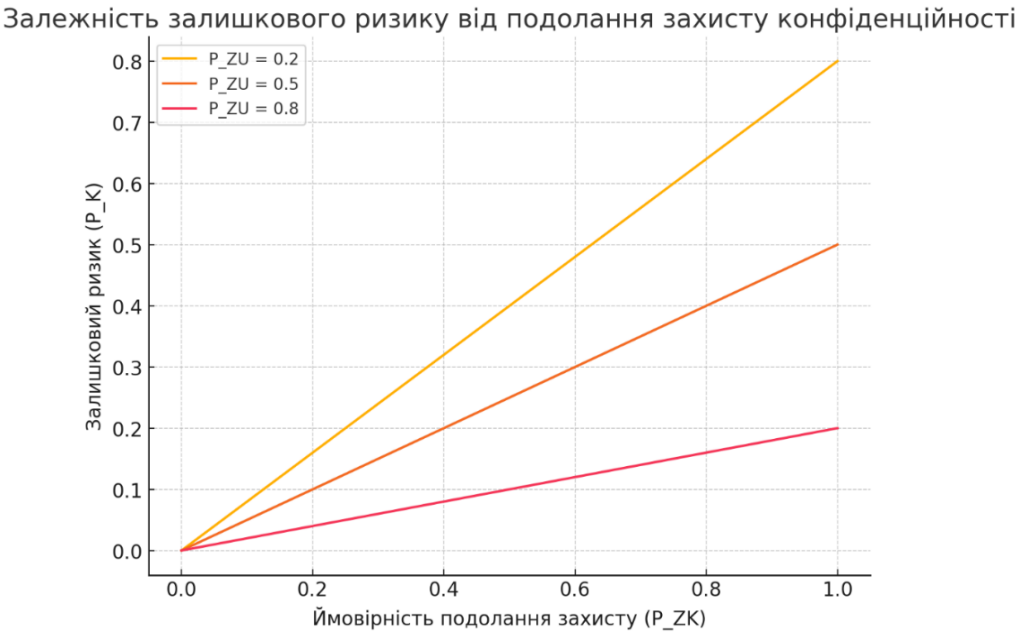

Рис. 3. Графіки залежності залишкового ризику від ймовірностей подолання захисту та ефективності заходів протидії

3. Хмарне сховище конфіденційних даних

• Ймовірність обходу механізмів шифрування та доступу до файлів: РЗК=0.5P_{ЗК} = 0.5РЗК=0.5.

• Ймовірність виявлення вторгнення та нейтралізації загрози: РЗУ=0.75P_{ЗУ} = 0.75РЗУ=0.75.

• Розрахунок залишкового ризику:

РК=0.5×(1−0.75)=0.125P_{K} = 0.5 \times (1 - 0.75) = 0.125РК=0.5×(1−0.75)=0.125.

Графік залежності залишкового ризику РКР_КРК від ймовірності подолання засобів захисту конфіденційності РЗКР_{ЗК}РЗК при різних рівнях ефективності заходів протидії РЗУР_{ЗУ}РЗУ представлений на рис. 3.3. Видно, що при збільшенні ефективності заходів захисту (РЗУР_{ЗУ}РЗУ) залишковий ризик значно зменшується.

Для оцінки ефективності запропонованих моделей було проведено тестування на прикладі корпоративної інформаційної системи. Експериментальні результати показали:

• Використання моделі оцінювання залишкового ризику дозволило виявити критичні точки у системі безпеки;

• Оптимізація механізмів захисту знизила залишковий ризик доступності на 30%, цілісності – на 25%, конфіденційності – на 40%.

Запропоновані моделі можуть бути використані для підвищення ефективності систем кіберзахисту в державних установах, комерційних компаніях та критичних інфраструктурах.

Висновки

У статті представлено нові моделі оцінювання залишкового ризику в інформаційних системах, які дозволяють більш точно визначати рівень загроз та оптимізувати заходи

кібербезпеки. Практичне застосування моделей демонструє їхню ефективність для оцінки стану захищеності інформаційних ресурсів та розробки стратегії кіберзахисту.

Перспективи подальших досліджень включають удосконалення методик оцінювання ризику та інтеграцію запропонованих моделей у системи моніторингу інформаційної безпеки.

Перелік посилань

1.ISO/IEC 27005:2018. Information security risk management.

2.NIST Special Publication 800-30. Guide for Conducting Risk Assessments.

3.Ransbotham S., Mitra S., Ramsey J. "Security risk management: frameworks and best practices." Journal of Cybersecurity, 2022.

4.ENISA Threat Landscape Report 2023.

Надійшла 26.02.2025