УДК 004.056.55

# ПОРІВНЯЛЬНИЙ АНАЛІЗ МЕТОДИК ОЦІКИ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

**Бакалов Ю. М., Косарєва Д. І.,** здобувачі вищої освіти гр. КБ-181
Науковий керівник: **Синенко М. А.**, к.ф.м.-н., доцент
*Національний університет «Чернігівська політехніка»*

Інтенсивний розвиток комп'ютерних технологій сприяв широкому їх впровадженню у більшість сфер людської діяльності, що, з одного боку, спростило і прискорило процеси аналізу, зберігання та обробки інформації. Разом з тим збільшення об'єму інформації, яка підлягає обробці, розширення кола користувачів інформаційними джерелами приводять до нових можливостей для несанкціонованого доступу до даних та появи нових вразливостей. У зв'язку з цим задачі, пов'язані з гарантуванням інформаційної безпеки залишаються на сьогодні досить актуальними.

Одним із обов'язкових елементів дослідження існуючих та створення нових систем захисту інформації (СЗІ) є оцінка ризиків. Існує думка, що процеси оцінки ризиків є фундаментом для побудови ефективної СЗІ організації. На даний час відома значна кількість методів та моделей оцінки інформаційної безпеки, які використовують якісні та кількісні підходи для визначення оптимальних способів обробки ризиків, у тому числі стандарти (ISO/IEC 27005, EBIOS, NIST SP800-30, OCTAVE та ін.) та спеціалізовані програмні продукти (CRAMM, Counter Measures, Гриф, РискМенеджер, Risk Watch та ін.) Однак проблема пов'язана з оцінкою ризиків не є остаточно вирішеною, відповідні моделі та методи продовжують розвиватись та удосконалюватись.

Існуючі методики можна поділити на декілька груп в залежності від способу оцінювання ризику:

−методики, що використовують оцінку ризику на якісному рівні, як то «високий», «сердній», «низький». До таких методик відноситься, наприклад, FRAP;

−методики, які оцінюють ризик кількісно числовим значенням. Наприклад, методика RiskWatch, де для оцінки ризику використовують значення можливих річних втрат;

−методики, які застосовують змішані оцінки. До таких методик відносять CRAMM, методики Microsoft та інші.

У загальному випадку для кількісного розрахунку ризику доцільно використовувати співвідношення:

$$R_{ij} = P_i^u P_{ij}^v A_{j,}$$

де $R_{ij} -$ ризик ***i-го*** ресурсу по відношенню до ***j-ї*** загрози, $P_i^u -$ ймовірність ***i***-ї загрози, $P_{ij}^v -$ вразливість захисту j-го ресурсу по відношеню до ***i***-ї загрози, $A_j -$ цінність j-го ресурсу.

Процес захисту інформації не завжди вдається описати формально. Це стосується, наприклад, моделей, які описують поведінку персоналу. У такому випадку можна використовувати моделі, побудовані на основі нечітких множин. Модель розрахунків ризиків на основі нечітких множин будується з використанням нечітких когнітивних карт, тобто простих зважених графів, вершини яких – елементи предметної області (наприклад, множина порушників), дуги – причинні зв'язки між ними. Методи оцінки ризиків на основі нечітких множин дозволяють побудувати адекватну модель навіть при недостатній кількості вихідних даних.

## Список використаних джерел

1. Домарев В.В. Управління інформаційною безпекою в банківських установах (Теорія і практика впровадження стандартів серії ISO 27k) / В.В. Домарев, Д.В. Домарев – Донецьк: Велстар, 2012. – 146 с.

2. Корниенко М.А. Модель оценки рисков информационной безопасности на основе теории нечетких множеств / М.А. Корниенко, Е.А. Островерхова // Материалы XVIII международного молодежного форума «Радиоэлектроника и молодежь в XXI веке». Т. 4 – Х.: ХНУРЭ, 2014. – С. 279.

3. Корченко А.Г. Построение систем защиты информации на нечетких множествах. Теория и практические решения / А.Г. Корченко — К.: «МК-Пресс», 2006 - 320с.

---

УДК 004.062

## ІНТЕЛЕКТУАЛЬНА СИСТЕМА ВІДЕОСПОСТЕРЕЖЕННЯ ЯК МЕТОД ЗАПОБІГАННЯ ВИТОКУ ІНФОРМАЦІЇ

**Батицька А. С.,** здобувачка вищої освіти Гр КБ-171
Науковий керівник: **Ткач Ю. М.,** к.т.н., професор
*Національний університет «Чернігівська Політехніка»*

На сьогоднішній день, безпека підприємств стоїть у пріоритеті, системи відеоспостереження використовують на місцях, які мають потребу постійного контролю або нагляду. Відеоспостереження – це можливість до високого рівня продуктивності підприємства, постійний контроль в реальному часі та підтримка на вищому рівні безпеки.

Постійний контроль 27/7 в ручному та автоматичному режимі працюють для безпеки. Влаштовані розширені відеоаналітичні функції з якими буде легко дізнатися про загрози безпеці, по всьому підприємстві автоматично і своєчасно.

Інноваційні технології системи відеоспостреження, безумовно включає в себе: програмні складні рішення та процеси вищого рівня інтелекту. Програмне забезпечення зі сполучанням відповідних камер можуть розпізнати номери проїжджаючих автомобілів, сканувати обличчя людини, поведінку, об’єкти різних форм і багато чого іншого.

− AHDкамери – аналогове транспортування зображення високої чіткості в HD форматі.

− Цифрові камери – максимальне розширення зображення, здатність мережі до передачі даних.

− Інтелектуальні камери – має відеоаналіз.

− Багатооб'єктивні зчитувальні камери – чітке зображення в деталях.

− Тепловізори – спеціальні рішення та технологічні процеси.

Рухомі циліндричні відеокамери– повний аналіз зовнішнього простору. Огляд на 360 градусів, має оптичний зум, швидкість достигає 6 м/с, а також підпорядковане інтуїтивним управлінням.

Автоматичні системи відеоспостереження – відстежують одночастно до 60-ти цілей для більшого рівня безпеки. Немає необхідності в обслуговуванні. Має системі відвідуваності, фіксування робочих та клієнтів, фіксує об’єкт навіть на великих швидкостях.

Щодо переваг систем інтелектуальних відеокамер:

− Поліпшує обслуговування клієнтів та продуктивність всього колективу.

− Надається денний контроль в реальному часі, з любої точки, де дб ви не знаходились.

− Надійна система проти можливих правопорушень. Підтримує високий рішень безпеки та мінімізація втрати важливої інформації підприємства.

Насамперед основними джерелами витоку інформації є суб’єкти та об’єкти :

− Співробітники підприємства;

− Сторонні люди;

− Злочинці;

− Твердим або рідким середовищем;