МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ ТА КІБЕРНЕТИЧНОЮ БЕЗПЕКОЮ

КВАЛІФІКАЦІЙНА РОБОТА

на тему: “ МЕТОДИКА ОЦІНКИ ІНФОРМАЦІЙНИХ РИЗИКІВ В АВТОМАТИЗОВАНИХ СИСТЕМАХ УПРАВЛІННЯ”

на здобуття освітнього ступеня магістра
зі спеціальності 125 Кібербезпека
освітньо-професійної програми Управління інформаційною безпекою

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ Андрій СТУПЧЕНКО
(підпис) *Ім’я, ПРІЗВИЩЕ здобувача*

Виконав: Здобувач вищої освіти гр. УБДМ 61
Андрій СТУПЧЕНКО

Керівник:
к.т.н. Юрій ЩАВІНСЬКИЙ

Рецензент:
д.т.н., професор Галина ГАЙДУР

Київ 2024

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ
ТЕХНОЛОГІЙ

Навчально-науковий інститут захисту інформації

Кафедра Управління інформаційною та кібернетичною безпекою

Ступінь вищої освіти магістр

Спеціальність 125 Кібербезпека
Освітньо-професійна програма Управління інформаційною безпекою

ЗАТВЕРДЖУЮ
Завідувач кафедрою УІКБ
_____ Світлана ЛЕГОМІНОВА
"____"_____2023 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

студенту Ступченку Андрію Миколайовичу
(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи: "Методика оцінки інформаційних ризиків в автоматизованих системах управління"

керівник кваліфікаційної роботи Юрій ЩАВІНСЬКИЙ, к.т.н.
(Ім'я, ПРІЗВИЩЕ, науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від "19" жовтня 2023 р. №145

2. Строк подання кваліфікаційної роботи "18" грудня 2023 р

3. Вихідні дані до кваліфікаційної роботи: *управління кібербезпекою, організації кібербезпеки, інформаційні ризики, управління ризиками, аудит інформаційної безпеки, наукова та технічна література*

4. Перелік питань, які потрібно розробити:

1. Здійснити аналіз наукової літератури та публікацій, пов'язаних із управлінням ризиками інформаційної безпеки в автоматизованих системах управління, існуючими підходами до цієї проблеми.

2. Проаналізувати існуючі автоматизовані системи управління та їхні потенційні ризики та вразливості, розробити перелік параметрів та показників, які можна використовувати для оцінки інформаційних ризиків в автоматизованих системах управління.

3. Розробити методику аналізу та оцінки інформаційних ризиків на основі обраних параметрів та показників .

4. Провести експериментальне дослідження, використовуючи розроблену методику, на прикладі конкретних автоматизованих систем управління, оцінити ефективність розробленої методики та відпрацювати рекомендації щодо вдосконалення безпеки та надійності автоматизованих систем управління.

5. Перелік ілюстративного матеріалу: *презентація*

6. Дата видачі завдання "02" жовтня 2023 р.

КАЛЕНДАРНИЙ ПЛАН

№з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	10.10.2023	
2.	Збір та аналіз літератури, пов’язаної із управлінням ризиками інформаційної безпеки в автоматизованих системах управління	23.10.2023	
3.	Аналіз основних існуючих автоматизованих систем управління та їхніх потенційних ризиків та вразливостей	27.10.2023	
4.	Розроблення переліку параметрів та показників, які можна використовувати для оцінки інформаційних ризиків в автоматизованих системах управління	10.11.2023	
5.	Розроблення методики аналізу та оцінки інформаційних ризиків в АСУ	15.11.2023	
6.	Формулювання висновків за результатами проведеного дослідження.	22.11.2023	
7.	Оформлення роботи.	04.12.2023	
8.	Оформлення презентації.	14.12.2023	
9.	Отримання рецензії на роботу.	18.12.2023	
10.	Захист в ДЕК.	.01.2024	

Здобувач вищої освіти _____ Андрій СТУПЧЕНКО
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Керівник
кваліфікаційної роботи _____ Юрій ЩАВІНСЬКИЙ
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

ПОДАННЯ
ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ
на здобуття освітнього ступеня магістра

Направляється здобувач Ступченко А.М.. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 125 Кібербезпека
(код, найменування спеціальності)
Освітньо-професійної програми Управління інформаційною безпекою
(назва)
на тему: “ Методика оцінки інформаційних ризиків в автоматизованих системах управління ”
Кваліфікаційна робота і рецензія додаються.

Директор ННІЗІ _____ Віталій САВЧЕНКО
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Висновок керівника кваліфікаційної роботи

Здобувач **СТУПЧЕНКО Андрій** у кваліфікаційній роботі дослідив сучасний стан захисту інформації в автоматизованих системах управління, їх потенційні ризики та вразливості, розробив перелік параметрів та показників, які можна використовувати для оцінки інформаційних ризиків в автоматизованих системах управління, розробив методику оцінки інформаційних ризиків на основі обраних параметрів та показників, відпрацював рекомендації щодо вдосконалення безпеки та надійності автоматизованих систем управління. **СТУПЧЕНКО Андрій** показав розуміння проблеми дослідження та бачення основних теоретичних та практичних напрямів її вирішення, довів уміння самостійного застосування методів наукового дослідження, проявив себе як організований, відповідальний виконавець. Результати дослідження апробовані на одній науково-практичній конференції.
Це дозволяє оцінити виконану кваліфікаційну роботу здобувачу **СТУПЧЕНКУ Андрію** на оцінку “добре” та присвоїти йому кваліфікацію “Магістр кібербезпеки за освітньо-професійною програмою “Управління інформаційною безпекою””.

Керівник кваліфікаційної роботи _____ Юрій ЩАВІНСЬКИЙ
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

“___“_____2024 року

Висновок кафедри про кваліфікаційну роботу

Завідувач кафедрою
Управління інформаційною
та кібернетичною безпекою _____ Світлана ЛЕГОМІНОВА
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну магістерську роботу

здобувача вищої освіти Ступченка Андрія Миколайовича
на тему "МЕТОДИКА ОЦІНКИ ІНФОРМАЦІЙНИХ РИЗИКІВ В АВТОМАТИЗОВАНИХ СИСТЕМАХ УПРАВЛІННЯ"

Актуальність

Актуальність теми визначена сучасним швидким розвитком технологій, зростанням кількості кіберзагроз та залежністю стійкості автоматизованих систем управління від впливу загроз. Забезпечення безпеки цих систем стає критично важливою задачею. Збільшення вимог до надійності систем управління, особливо в критичних галузях, таких як енергетика, медицина та транспорт, вимагає глибокого розуміння та ефективного управління інформаційними ризиками. Разом з тим, достатньої уваги управлінню і оцінці інформаційних ризиків у автоматизованих системах не приділяється, що потребує детальних наукових розробок.

Позитивні сторони

У роботі послідовно і логічно розкрито основи захисту інформацій у автоматизованих системах управління, проаналізовані сучасні методи та підходи до оцінки ризиків. Визначена методика оцінки ризиків, яка включає поєднання основних вимог міжнародних нормативно-правових актів та застосування штучного інтелекту. При цьому доцільно використані інформаційні ресурси інтернету. Зроблені висновки про застосування методики, що дозволить правильно організовувати заходи інформаційної безпеки у автоматизованих системах управління.

Недоліки

Разом з тим, доцільно було б приділити більше уваги обґрунтуванню вибраних критеріїв оцінки ефективності запропонованої методики. Не повністю розкриті організаційні показники оцінювання ризиків інформаційної безпеки.

Однак, вищезгадані зауваження не впливають на загальну позитивну оцінку кваліфікаційної роботи.

Висновок: Кваліфікаційна робота виконана на належному науково-методичному рівні і заслуговує оцінки «добре» а її автор Ступченко Андрій Миколайович - присвоєння кваліфікації «Магістр з кібербезпеки за спеціалізацією Управління інформаційною безпекою».

Рецензент: завідувач кафедри
Інформаційної та кібернетичної
безпеки,
д.т.н, професор _____ Галина ГАИДУР
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня магістра: 78 стор., 15 рис., 4 табл., 56 джерел.

Метою роботи є розробка та обгрунтування методики оцінки інформаційних ризиків в автоматизованих системах управління з метою забезпечення високого рівня захисту інформації в них.

Об'єктом дослідження є захист інформацій в автоматизованих системах управління.

Предмет дослідження – способи оцінювання інформаційних ризиків в автоматизованих системах управління.

Методи дослідження. Для вирішення завдань і дослідження інформаційних процесів в автоматизованих система використовуються методи системного аналізу, теорії управління, аналіз, синтез, моделювання, узагальнення, методи статистичного аналізу.

Короткий зміст роботи. Як результат у роботі проведено аналіз наукової літератури та публікацій, пов'язаних із управлінням ризиками інформаційної безпеки в автоматизованих системах управління, існуючими підходами до цієї проблеми. Проаналізовані існуючі автоматизовані системи управління та їхні потенційні інформаційні ризики і вразливості виявили проблему оцінювання інформаційної безпеки в таких системах. Встановлено, що безпеці автоматизованих систем до недавнього часу не приділялось достатньої уваги, що становить велику проблему для їх надійного функціонування сьогодні та зумовило процес досліджень у цьому напрямку. Розроблений перелік параметрів та показників, які можна використовувати для оцінки інформаційних ризиків в автоматизованих системах управління. Розроблена методика аналізу та оцінки інформаційних ризиків з використанням штучного інтелекту на основі обраних параметрів та показників, проведено експериментальне дослідження, використовуючи розроблену методику на прикладі конкретної автоматизованої системи управління, оцінена ефективність розробленої методики та відпрацьовані рекомендації щодо вдосконалення безпеки та надійності

автоматизованих систем управління.

Галузь застосування. Розроблена методика для оцінювання ризиків та підходи можуть бути використані при плануванні та реалізації автоматизованих систем управління та створенні у них системи інформаційної та кібербезпеки.

КЛЮЧОВІ СЛОВА: УПРАВЛІННЯ РИЗИКАМИ ІНФОРМАЦІЙНА БЕЗПЕКА, АВТОМАТИЗОВАНІ СИСТЕМИ УПРАВЛІННЯ.

ABSTRACT

The text part of the qualification work for obtaining a master's degree: 78 pages, 15 figures, 4 tables, 56 sources.

The purpose of the work is development and substantiation of information risk assessment methods in automated control systems in order to ensure a high level of information protection in them..

Object of research is information protection in automated management systems..

Subject ***of research*** is methods of assessing information risks in automated management systems

Research methods Methods of system analysis, management theory, analysis, synthesis, modeling, generalization, methods of statistical analysis are used to solve tasks and research information processes in automated systems.

Brief content of research. As a result, the paper analyzes the scientific literature and publications related to the management of information security risks in automated management systems, existing approaches to this problem. The analyzed existing automated management systems and their potential information risks and vulnerabilities revealed the problem of assessing information security in such systems. It was established that the security of automated systems was not paid enough attention until recently, which is a big problem for their reliable functioning today and determined the research process in this direction. A list of parameters and indicators that can be used to assess information risks in automated management systems has been developed. A method of analyzing and assessing information risks using artificial intelligence based on selected parameters and indicators was developed, an experimental study was conducted using the developed method on the example of a specific automated control system, the effectiveness of the developed method was evaluated and recommendations were developed for improving the safety and reliability of automated control systems.

Field of research. The developed risk assessment methodology and approaches

can be used in the planning and implementation of automated management systems and the creation of information and cyber security systems in them.

KEYWORDS: RISK MANAGEMENT, INFORMATION SECURITY, AUTOMATED CONTROL SYSTEMS.

ЗМІСТ

ВСТУП 11

РОЗДІЛ 1. ТЕОРЕТИЧНІ АСПЕКТИ ІНФОРМАЦІЙНИХ РИЗИКІВ В АВТОМАТИЗОВАНИХ СИСТЕМАХ УПРАВЛІННЯ... 13

1.1 Основи захисту інформації в автоматизованих системах управління..... 13

1.2 Основні поняття теорії ризиків в автоматизованих системах управління..... 22

РОЗДІЛ 2. РОЗРОБКА МЕТОДИКИ ОЦІНКИ РИЗИКІВ В АВТОМАТИЗОВАНИХ СИСТЕМАХ УПРАВЛІННЯ..... 32

2.1 Аналіз різних методів та підходів до оцінки інформаційних ризиків 32

2.2 Методика оцінки ризиків у автоматизованих системах управління… 51

РОЗДІЛ 3. РЕКОМЕНДАЦІЇ З ПРАКТИЧНОГО ЗАСТОСУВАННЯ МЕТОДИКИ ОЦІНКИ РИЗИКІВ У АВТОМАТИОВАНИХ СИСТЕМАХ УПРАВЛІННЯ 61

3.1 Оцінка ефективності застосування методики оцінки ризиків 61

3.2 Проведення дослідження та рекомендації з практичного застосування методики 64

ВИСНОВКИ 70

ПЕРЕЛІК ПОСИЛАНЬ 72

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ..... 79

ВСТУП

Актуальність теми. Актуальність теми "Методика оцінки інформаційних ризиків в автоматизованих системах управління" визначається сучасним контекстом швидкого розвитку технологій, зростанням кількості кіберзагроз та залежністю від інформаційних технологій у різних галузях. Сучасне інформаційне середовище піддається постійним атакам хакерів, вірусам та іншим кіберзагрозам. Організації у всіх галузях все більше використовують автоматизовані системи управління для оптимізації процесів. Забезпечення безпеки цих систем стає критично важливою задачею. Застосування штучного інтелекту, Інтернету речей (IoT) та інших інноваційних технологій у системах управління робить необхідність оцінки ризиків ще більш актуальною, оскільки нові технології часто приносять із собою нові види загроз. Збільшення вимог до надійності та доступності систем управління, особливо в критичних галузях, таких як енергетика, медицина та транспорт, вимагає глибокого розуміння та ефективного управління інформаційними ризиками.

Відсутність ефективного управління інформаційними ризиками в автоматизованих системах управління може призвести до серйозних наслідків, таких як витік конфіденційної інформації, порушення бізнес-процесів та негативний вплив на репутацію компанії, а в АСУ критично важливої інфраструктури - до порушення життєво важливих функцій людини, суспільства, держави. Таким чином, розробка методики оцінки ризиків у цьому контексті є вкрай актуальною та важливою для забезпечення безпеки та стійкості сучасних автоматизованих систем управління.

Метою роботи є розробка та обгрунтування методики оцінки інформаційних ризиків в автоматизованих системах управління з метою забезпечення високого рівня захисту інформації в них.

Об'єктом дослідження є захист інформацій в автоматизованих системах управління.

Предмет дослідження – способи оцінювання інформаційних ризиків в автоматизованих системах управління.

Методи дослідження. Для вирішення завдань і дослідження інформаційних процесів в автоматизованих система використовуються методи системного аналізу, теорії управління, аналіз, синтез, моделювання, узагальнення, методи статистичного аналізу.

Короткий зміст роботи. Як результат у роботі проведено аналіз наукової літератури та публікацій, пов'язаних із управлінням ризиками інформаційної безпеки в автоматизованих системах управління, існуючими підходами до цієї проблеми. За результатами аналізу встановлено, що сама безпека АСУ не була відносно високим пріоритетом до недавнього часу. АСУ історично проектувалися як автономні системи з власною технологією. Основними цілями проектування були безперервність процесу та функціональність. Безпеці від внутрішніх і зовнішніх загроз часто не приділялося багато уваги, окрім простого контролю фізичного доступу. Сьогодні АСУ все частіше з'єднуються з іншими мережами, включаючи Інтернет, і спостерігається різке зростання кількості вразливостей безпеки та можливостей боротьби. Розроблений перелік параметрів та показників, які можна використовувати для оцінки інформаційних ризиків в автоматизованих системах управління. Розроблена методика аналізу та оцінки інформаційних ризиків на основі обраних параметрів та показників, проведено експериментальне дослідження, використовуючи розроблену методику, на прикладі конкретних автоматизованих систем управління, оцінена ефективність розробленої методики та відпрацьовані рекомендації щодо вдосконалення безпеки та надійності автоматизованих систем управління.

Галузь застосування. Розроблені підходи можуть бути використані при плануванні та реалізації автоматизованих систем управління та створенні у них системи інформаційної та кібербезпеки. Розроблена методика оцінки ризиків дозволить ефективніше виявляти та запобігати потенційним атакам.

Апробація результатів кваліфікаційної роботи. Результати дослідження було оприлюднено на науково-практичній конференції «Проблеми комп'ютерної інженерії». Збірник тез. – К.: ДУІКТ, 2023. С. 118-120 (м. Київ, 01 грудня 2023 року), яка проведена в Навчально-науковому інституті захисту інформації ДУІКТ.

РОЗДІЛ 1
ТЕОРЕТИЧНІ АСПЕКТИ ІНФОРМАЦІЙНИХ РИЗИКІВ В АВТОМАТИЗОВАНИХ СИСТЕМАХ УПРАВЛІННЯ

1.1 Основи захисту інформації в автоматизованих системах управління

За останні кілька років IT-безпека стала домінуючою темою у сфері управління процесами. Автоматизовані системи управління (АСУ) лежать в основі промислових та інфраструктурних систем і є однією з найважливіших частин критичної інфраструктури (рис. 1.1).

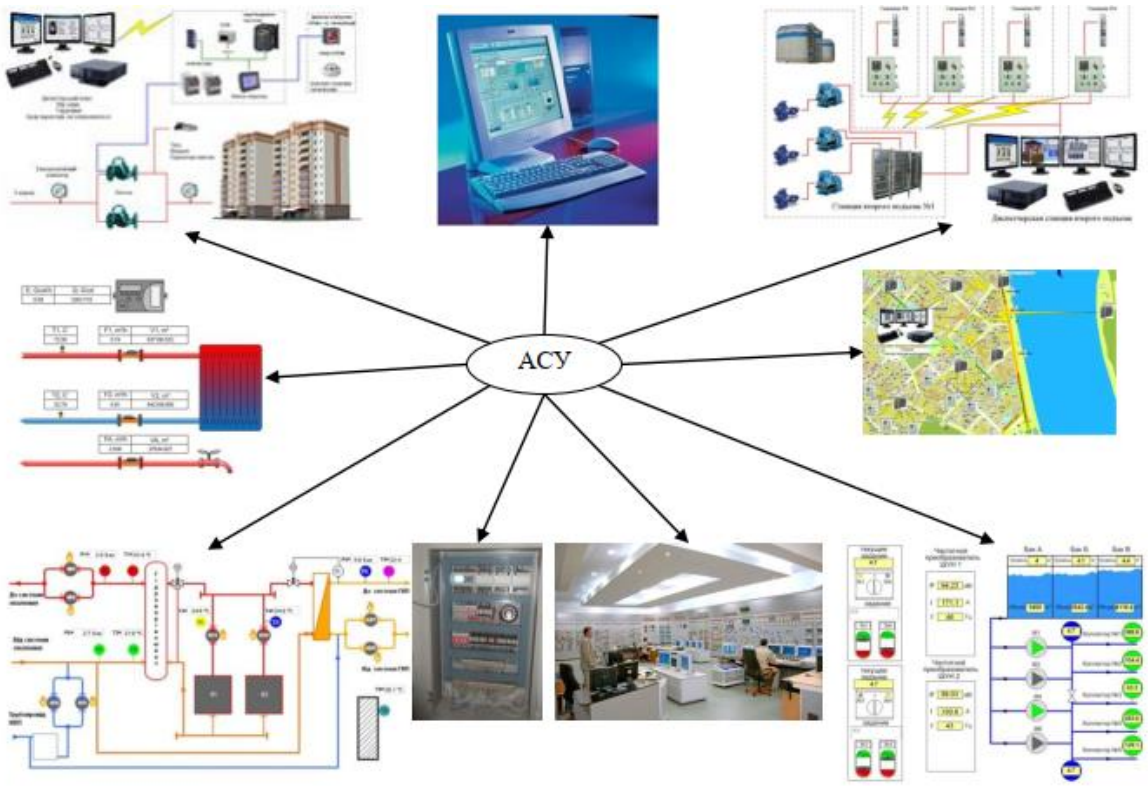

Рис.1.1. Різновиди АСУ

Проте світ інформаційної безпеки значною мірою ігнорує ці системи і більшість фахівців з інформаційної безпеки, схоже, вважають, що захисні процеси, заходи та механізми, які застосовуються до корпоративних комп'ютерів загального призначення, також застосовні до систем управління. У той же час більшість інженерів систем управління майже нічого не знають про захист

інформації і не визнають навіть потенціалу тих речей, які фахівці з інформаційної безпеки вважають стандартними. Цю невідповідність, як зазначають науковці [1-3], необхідно усунути, інакше ми будемо платити за це ціну принаймні протягом одного покоління.

Разом з тим, важливі об’єкти, від яких залежить сталий розвиток держави, суспільства та людини, наприклад, багато електростанцій і промислових підприємств зі своїми системами автоматизації, не обладнані для боротьби із загрозами кібербезпеки. Ключовим питанням, згідно з нещодавнім звітом IEC Technology Report, є те, що безпека занадто часто розуміється лише з точки зору IT (інформаційних технологій). Ті, хто відповідає за безпеку, часто не беруть до уваги операційні обмеження в таких секторах, як енергетика, виробництво, охорона здоров'я або транспорт. Зростання кількості підключених пристроїв прискорило конвергенцію колись окремих сфер IT та операційних технологій (OT).

З точки зору кібербезпеки, проблема полягає в тому, що на відміну від бізнес-систем, системи промислової автоматизації та управління (англ. - Industrial Automation And Control Systems, IACS) фактично розроблені для полегшення доступу з різних мереж. Це пов'язано з тим, що промислове середовище має справлятися з різними видами ризиків.

IT-безпека в рівній мірі зосереджена на захисті конфіденційності, цілісності та доступності даних – так звана «тріада C-I-A» (рис. 1.2).

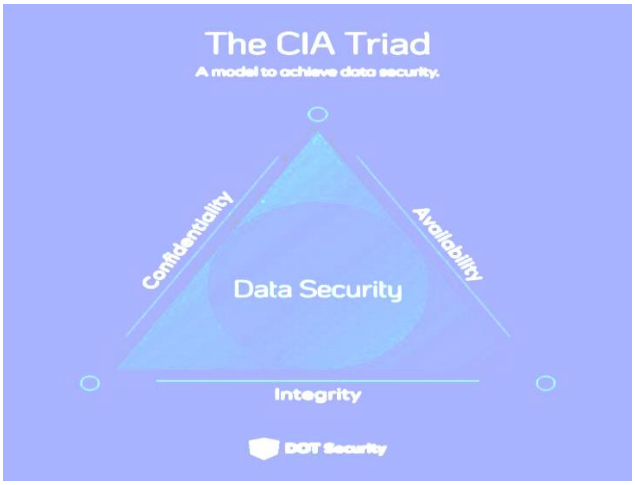

Рис. 1.2. Тріада C-I-A конфіденційності, цілісності та доступності

Однак у світі АСУ доступність має першорядне значення. Пріоритети для середовищ АСУ зосереджені на безпеці відносно зовнішнього середовища, а також на захисті навколишнього середовища. Тому у разі надзвичайної ситуації, щоб мати можливість захистити персонал або мінімізувати наслідки стихійних лих, життєво важливо, щоб оператори могли отримувати точну та своєчасну інформацію та могли швидко вжити відповідних заходів, таких як відключення електроенергії або перехід на резервне обладнання.

Останніми роками зростає інтерес до безпеки систем управління технологічними процесами та SCADA (англ. Supervisory Control and Data Acquisition). Крім того, нещодавні комп'ютерні атаки, такі як хробак Stuxnet, показали, що є сторони, які мають мотивацію та ресурси для ефективної атаки на системи управління.

У той час як попередні роботи пропонували нові механізми безпеки для систем управління, мало хто з них досліджував нові і принципово відмінні дослідницькі проблеми захисту систем управління в порівнянні з захистом традиційних інформаційних технологій (IT) систем. Зокрема, складність нових шкідливих програм, що атакують системи управління – шкідливих програм, включаючи атаки нульового дня, руткітів, створених для систем управління, і програмного забезпечення, підписаного довіреними центрами сертифікації – показала, що дуже важко запобігти та виявити ці атаки, ґрунтуючись виключно на інформації про IT-систему.

Системи SCADA, які використовуються для нагляду за електричними мережами, а також установками та машинами на промислових об'єктах, часто покладаються на «безпеку через невідомість», відображаючи вкорінену думку про те, що оскільки ніхто не знає і не піклується про свої комунікаційні системи або дані, їм не потрібно їх захищати. Однак системи SCADA тепер можуть мати широко поширені мережі зв'язку, які все частіше прямо чи опосередковано охоплюють тисячі об'єктів, при цьому зростаючі загрози (як навмисні, так і ненавмисні) потенційно можуть завдати серйозної шкоди людям та обладнанню.

Тому модернізація відповідних та ефективних заходів безпеки стала

досить складною для цих SCADA-систем. Наприклад, у світі IT системи виявлення та запобігання вторгнень IDPS (англ. - Intrusion Detection and Prevention System) (рис.1.3) знаходяться на передовій захисту від шкідливого програмного забезпечення.

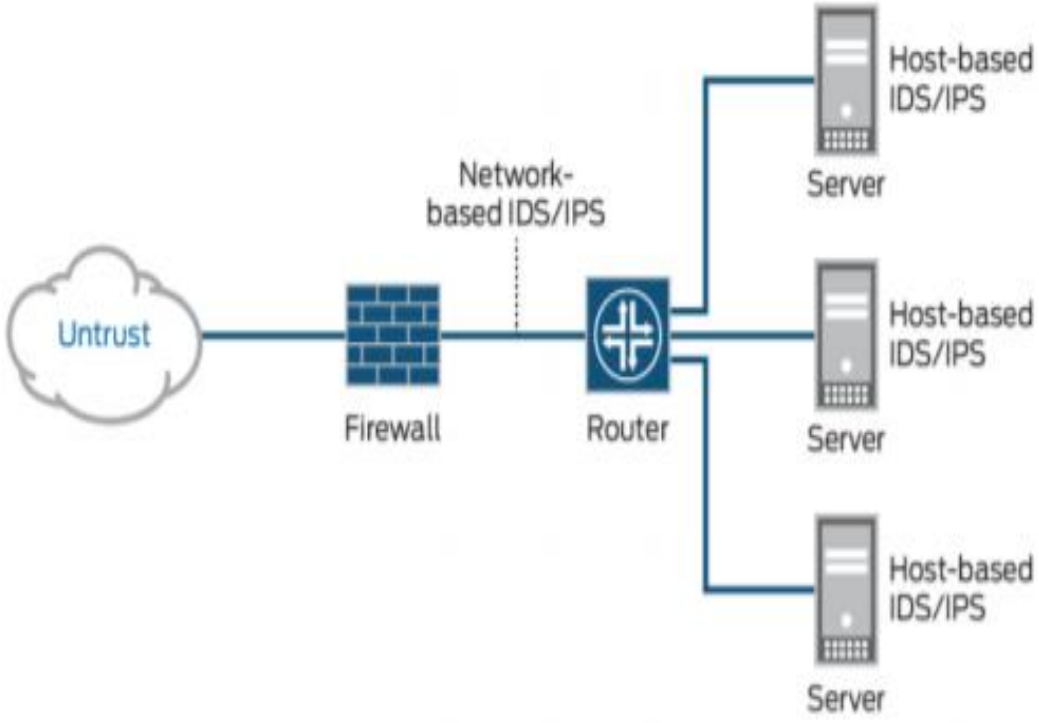

Рис.1.3. Схема системи виявлення та запобігання вторгнень IDPS

IDPS, як правило, є програмними додатками, які підслуховують мережевий трафік. Залежно від того, як вони налаштовані, засоби автоматизації можуть робити все: від повідомлення про вторгнення до вжиття заходів, спрямованих на запобігання або пом'якшення наслідків порушень. Але проблема систем SCADA полягає в тому, як відрізнити звичайні дані від потенційно нав'язливих, які можуть завдати шкоди [4].

Міжнародні стандарти забезпечують вирішення багатьох із цих проблем на основі найкращих світових практик [5-7]. Наприклад, стандарт IEC 62443 призначений для підтримки роботи систем автоматизації. Його можна застосовувати до будь-якого промислового середовища, включаючи об'єкти

критичної інфраструктури, такі як енергетичні компанії або атомні станції, а також у секторах охорони здоров'я та транспорту.

Наприклад, програма промислової кібербезпеки IECEE (англ. - IEC System for Conformity Assessment Schemes for Electrotechnical Equipment and Components) – тестує та сертифікує кібербезпеку в секторі промислової автоматизації. Схема оцінки відповідності IECEE включає програму, яка забезпечує сертифікацію за стандартами серії IEC 62443 [8].

У роботі [9] формально визначені системи виявлення, захисту, автоматизації та управління, як цілісний набір функціональних можливостей енергосистеми, які дозволяють захищати, автоматизувати та контролювати електричну мережу, що охоплює польові, технологічні та експлуатаційні зони.

Науковці у своїй роботі [10] провели дослідження еволюції захисту та управління в енергосистемах, що охоплює вплив досягнень у галузі комунікаційних, інформаційних та мережевих технологій (як представлено на рис. 1.4).

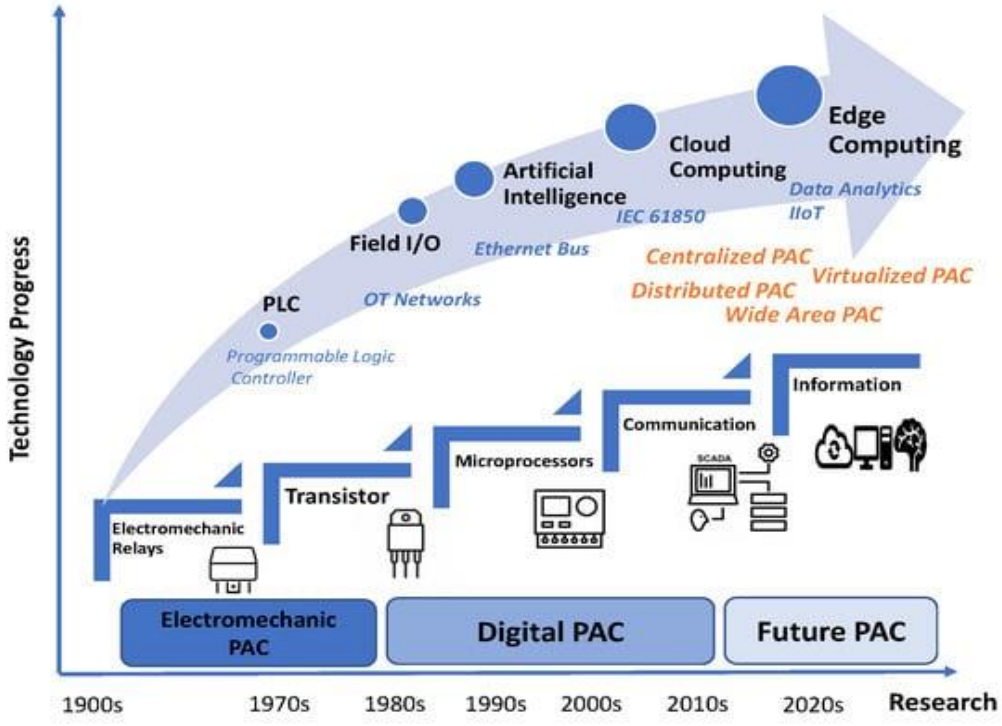

Рис.1.4. Еволюція систем захисту автоматизації та управління

У сучасних умовах великий обсяг інформації в електронному обміні призвів до підвищення актуальності завдань створення автоматизованої системи захищеного електронного обміну інформацією.

Тому захист інформації в автоматизованих системах (АС) є вкрай необхідним завданням, що забезпечує її достовірність, безпеку і конфіденційність. Науковці [11] відзначають автоматизовану систему як систему, що складається з персоналу і сукупності засобів автоматизації його діяльності, що реалізує інформаційні технології виконання встановлених функцій. Інформація в АС безпечна, якщо всі компоненти автоматизованої системи захищені від можливих загроз на необхідному рівні. Автоматизовані системи, що надають охоронну інформацію, називаються захищеними. Захист інформації спочатку формувався різними способами.

При пересиланні інформації від однієї компанії (резидента) до іншої (нерезидента), як правило, дотримуються корпоративних, галузевих та національних вимог до такого обміну. Однак ситуація між відомствами різних держав у транскордонній взаємодії ускладнюється. Вирішення цього питання було успішно досягнуто в країнах-членах Європейського Союзу. Для реалізації юридично значущої взаємодії вони враховували закони та вимоги до співпраці 28 країн Європейського Союзу. Створення такої біржі зайняло більше 10 років. Обмін документами між підрозділами «Департамент-Департамент» і «Департамент-Європейська Комісія» спочатку здійснювався на базі електронних цифрових підписів. Поряд з цим, була реалізована можливість обміну на основі третьої довіреної сторони – операторів обміну. У серпні 2014 року, після появи нового нормативно-правового акту про електронну ідентифікацію та довірчі послуги для електронних транзакцій на внутрішньому ринку, а також скасування Директиви 1999/93/ЄС з'явилася можливість здійснення обміну.

У цій статті показано, як, використовуючи знання про фізичну систему, що контролюється, можна виявляти комп'ютерні атаки, які змінюють поведінку цільової системи управління. Використовуючи знання про фізичну систему, можна зосередитися на кінцевій меті атаки, а не на конкретних механізмах того,

як використовуються вразливості та як прихована атака. Аналізуючи безпеку механізмів, досліджуючи наслідки прихованих атак можна гарантувати, що автоматичні механізми реагування на атаки не доведуть систему до небезпечного стану.

Другорядною метою є ініціювання дискусії між фахівцями з контролю та безпеки – двома сферами, які в минулому мало взаємодіяли. Науковці зауважують, що інженери з управління можуть використовувати інженерію безпеки для розробки – на основі комбінації їхніх найкращих практик – алгоритмів керування, які виходять за рамки безпеки та відмовостійкості, і включають міркування щодо виживання під час цілеспрямованих атак [12]. У даній роботі зроблено огляд основних підходів до вибору захисних заходів для автоматизованих систем управління технологічними процесами. Метою дослідження була розробка методу вибору заходів захисту інформації на кожному рівні АСУ з використанням теорії множин в рамках аналізу базових комплексів заходів захисту. У рамках дослідження розглянуто відповідні атаки на промислову інфраструктуру, побудовано алгоритм вибору захисних заходів АСУ, а також запропоновано необхідність використання захисних заходів для кожного рівня системи відповідно до індивідуальної оцінки класу захисту даних на відповідному рівні. Автори дійшли висновку, що необхідно виключити з розгляду «уточнення адаптованого базового набору» алгоритму вибору заходів захисту АСУ у разі, якщо адаптований базовий набір захисних заходів АСУ забезпечує блокування всіх загроз безпеці на системному рівні, що розглядається. Запропоновано підхід до вибору заходів захисту на основі побудови діаграм Ейлера-Венна. Результати досліджень рекомендовано використовувати при моделюванні загроз інформаційній безпеці та розробці вимог до засобів захисту інформації АСУ.

При проведенні досліджень науковці оперують термінами, які визначені в нормативно-правових документах [13-14].

Під автоматизованою системою розуміють систему, яка здійснює автоматизоване оброблення даних. До її складу входять технічні засоби обробки,

а також методи і процедури, програмне забезпечення.

Інформація в АС − це сукупність усіх даних і програм, які використовуються в АС незалежно від засобу їх фізичного та логічного представлення.

Під захистом інформації в АС розуміється сукупність організаційно-технічних заходів і правових норм для запобігання шкоди інтересам власників інформації. Закон визначає й інші терміни: “обробка інформації“, “несанкціонований доступ“, “розпорядник АС“, “персонал АС“, “користувач АС“, “витік інформації“, “підробка інформації“, “блокування інформації“ та ін.

Об’єктами захисту закону є інформація, що обробляється в АС, права власників інформації, права користувача. Суб’єктами відносин закон визнає власників інформації або їхніх уповноважених осіб, власників АС та їхніх представників, користувачів інформації, користувачів АС.

За ст. 4 [13] право власності на інформацію встановлюється з урахуванням норм авторського права на підставі угоди між власником вхідної інформації і користувачем АС. Якщо угоди немає, така інформація належить користувачу АС, який здійснив обробку. Користувач може обробляти інформацію лише за згодою власника, якщо це загальнодоступна інформація.

Відповідно до ст.7 цього закону власник АС повинен забезпечити захист інформації згідно угоди з власником інформації. Якщо інформація належить до державної таємниці, її захист здійснюється згідно з рішенням уповноваженого Кабінету Міністрів України. Власник АС не відповідає за шкоду, завдану інформації, якщо при цьому не було порушено встановлених власником інформації правила її захисту.

Розпорядником АС за даним законом вважається фізична або юридична особа, яка має право розпоряджання АС за угодою з її власником або за його дорученням.

Під персоналом АС розуміють фізичні особи, яких власник АС або уповноважена ним особа чи розпорядник АС визначили для здійснення функцій управління та обслуговування АС.

Користувач АС – це фізична або юридична особа, яка має право використання АС за угодою із розпорядником АС.

Під порушником розуміється фізична або юридична особа, яка навмисно чи ненавмисно здійснює неправомірні дії щодо АС та інформації в ній.

Витоком інформації вважається результат дій порушника, внаслідок яких інформація стає відомою (доступною) суб'єктам, що не мають права доступу до неї.

Підробка інформації - навмисні дії, що призводять до перекручення інформації, яка повинна оброблятися або зберігатися в АС; блокування інформації - дії, наслідком яких є припинення доступу до інформації; порушення роботи АС -- дії або обставини, які призводять до спотворення процесу обробки інформації.

За втрату інформації вважають дію, внаслідок якої інформація в АС перестає існувати для фізичних або юридичних осіб, які мають право власності на неї в повному чи обмеженому обсязі.

Захисту підлягає будь-яка інформація в АС, необхідність захисту якої визначається її власником або чинним законодавством.

Право власності на інформацію, створену як вторинну в процесі обробки в АС, встановлюється з урахуванням норм авторського права на підставі угоди між власником вхідної інформації і користувачем АС. Якщо такої угоди немає, то така інформація належить користувачу АС, який здійснив цю обробку. Користувач АС може проводити обробку інформації лише за наявності згоди на те її власника або уповноваженої ним особи, якщо ця інформація не віднесена до категорії загальнодоступної.

1.2 Основні поняття теорії ризиків в автоматизованих системах управління

Теорія ризику – це дослідження ролі невизначеності в прийнятті рішень, дослідження того, як люди та організації оцінюють потенційні загрози та можливості, керують ними та розробляють стратегію щодо них. Це наріжний камінь фінансового, страхувального та бізнес-планування, керуючи тим, як ми готуємося до невідомого. Ця теорія намагається пояснити рішення, які люди приймають, коли вони стикаються з невизначеністю щодо майбутнього. Як правило, ситуація, в якій може бути застосована теорія ризику, передбачає низку можливих станів світу, низку можливих рішень і результат для кожної комбінації стану та рішення.

Управління ризиком – це процес ідентифікації, оцінки та контролю ризиків, які виникають внаслідок використання фінансових інструментів; це ключовий компонент фінансового планування. Для кількісної оцінки ризику та сприяння прийняттю рішень на основі рівня ризику часто використовуються математичні моделі [15].

Теорія ризиків інформаційної безпеки включає виявлення, оцінку та пом’якшення ризиків, які потенційно можуть завдати шкоди інформаційним активам організації. Метою управління ризиками інформаційної безпеки є мінімізація ймовірності інцидентів безпеки та їх впливу на організацію.

Теорія ризиків визначає чотири основні компоненти ризику безпеки для автоматизованих систем:

- вразливість – прояв властивих станів системи (наприклад, фізичних, технічних, організаційних, культурних), які можуть бути використані супротивником для негативного впливу (спричинення шкоди або пошкодження) цієї системи;
- намір – бажання або мотивація супротивника атакувати ціль і викликати несприятливі наслідки;
- здатність – здатність і здатність атакувати ціль і спричиняти

негативні наслідки;

- загроза – намір і можливість негативно вплинути (заподіяти шкоду чи збиток) системі шляхом негативної зміни її станів.

Таким чином, ризик є результатом використання загрозою вразливості з негативними наслідками.

Як зазначалося вище, ризик оцінюється як міра ймовірності та серйозності несприятливих ефектів або наслідків із відповідним ступенем невизначеності.

Імовірність (або ймовірність) – описує можливість настання події. Існує два підходи до оцінки ймовірності: частотний і суб'єктивний. Частотна оцінка ймовірності оцінює ймовірність того, що подія відбудеться, часто використовуючи історичні дані про частоту. Суб'єктивна оцінка ймовірності відображає віру в те, що подія відбудеться з певною ймовірністю.

Наслідки – це наслідки події. Термін «побічний ефект» означає точку зору; тому ми повинні враховувати цілі зацікавлених сторін під час аналізу наслідків. Наприклад, з точки зору нападника, руйнівні наслідки нападу є позитивними. З точки зору жертви, наслідки цього нападу, безперечно, можна вважати несприятливими.

Невизначеність – нездатність визначити справжню ситуацію, тому будь-яка оцінка повинна включати суб'єктивні (але бажано експертні) судження.

На перший погляд, серйозність невизначеності наслідків може бути легшим компонентом ризику безпеки для оцінки, оскільки активи та продуктивність організації повинні бути добре зрозумілими та виміряними, тоді як намір і можливості загрози можуть бути предметом спекуляцій. Однак існує багато видів наслідків, які пов'язані з несприятливою подією. Вони можуть включати політичні чи нормативні наслідки, вплив на навколишнє середовище та дії зацікавлених сторін. Ці типи наслідків дуже непросто охарактеризувати, і вони можуть являти собою найбільш суттєві наслідки несприятливої події.

Тому першочергова задача теорії ризиків – визначити показники інформаційної безпеки АСУ для її оцінювання. Показники інформаційної безпеки автоматизованих систем управління (АСУ) визначають ефективність

заходів та процесів забезпечення безпеки інформації в системі. Вони використовуються для вимірювання рівня безпеки та ефективності заходів протидії загрозам. Ось декілька типових показників інформаційної безпеки для АСУ:

1. Рівень кібербезпеки - кількість спроб несанкціонованого доступу або атак на систему протягом певного періоду.

2. Доступність - час відновлення після відмови: час, необхідний для відновлення роботи системи після відмови.

3. Ідентифікація та автентифікація - кількість невдалих спроб ідентифікації: Кількість спроб невдалих спроб ідентифікації користувачів.

4. Визначення та захист конфіденційної інформації: кількість випадків витоку інформації - кількість випадків, коли конфіденційна інформація може бути викрита.

5. Керування правами доступу - кількість несанкціонованих змін прав доступу: кількість випадків, коли права доступу змінюються без відповідних авторизацій.

6. Моніторинг та виявлення загроз - кількість виявлених аномалій: кількість виявлених незвичайних або аномальних подій в системі.

7. Безпека мережі - кількість виявлених вторгнень в мережу: кількість випадків виявлення спроб вторгнення в мережу системи.

8. Шифрування та захист даних - ступінь використання шифрування: відсоток даних, які передаються чи зберігаються у зашифрованому вигляді.

9. Безпека систем управління доступом - правильність налаштувань системи управління доступом: оцінка правильності налаштувань та ефективності системи управління доступом.

10. Підготовленість до інцидентів та відновлення - час реакції на інцидент: час, який потрібен для реакції на інцидент та прийняття заходів з відновлення.

11. Оцінка забезпеченості бюджетом - витрати на кібербезпеку: сума коштів, витрачених на заходи забезпечення безпеки та кіберзахисту.

12. Оцінка свідомості користувачів - рівень навчання користувачів з питань

безпеки: оцінка рівня знань користувачів щодо основ безпеки.

Ці показники допомагають визначити, наскільки ефективно заходи безпеки в системі та які аспекти потребують уваги та вдосконалення. Вони можуть служити основою для прийняття рішень з управління ризиками та вдосконаленням системи кіберзахисту.

Показники безпеки, які підтримують управління ризиками в АСУ, узгоджені з основними нормативно-правовими документами міжнародної інформаційної безпеки (ISO/IEC 27004 (BS7799-4), «Показники та вимірювання інформаційної безпеки».

Очікується, що зусилля щодо загальних вразливостей і ризиків, відкритої мови оцінки вразливостей і загальної системи оцінки вразливостей покращать узгодженість таких показників.

Існують системи виявлення вторгнень (IDS), які створюють показники на основі подій, які вони спостерігають. Показники, створені IDS, зазвичай включають незважену та зважену кількість типів подій, а також тенденції з часом. Як було зазначено на семінарі з безпеки I3P SCADA у червні 2005 року, архітектура безпеки для системи SCADA, особливо тієї, яка повністю або частково покладається на Інтернет-протокол для зв'язку, повинна включати IDS.

Однак навіть за відсутності IDS дані системного журналу можна використовувати для створення показників безпеки; Інститут SANS зауважує, що більшість підприємств могли б ефективніше використовувати дані системного журналу для отримання показників продуктивності та безпеки

Якщо припустити, що вимоги безпеки були належним чином визначені для пом’якшення очікуваних ризиків, невиконання цих вимог свідчить про довгостроковий ризик. Показники ризику. Ризик можна загалом охарактеризувати як поєднання загроз, вразливостей і впливів. Таким чином, метрики ризику оцінюють один, або комбінацію двох або всіх цих факторів, або атрибути цих факторів, які служать індикаторами або предикторами ризику.

Нижче наведено деякі з ключових показників ефективності (KPE), які можна використовувати для вимірювання ефективності інформаційної безпеки в

автоматизованих системах управління [16]:

- кількість інцидентів безпеки - цей показник вимірює кількість інцидентів безпеки, які сталися за певний період часу. Це допомагає визначити тенденції та закономірності в інцидентах безпеки та може використовуватися для оцінки ефективності засобів контролю безпеки.

- середній час виявлення - цей показник вимірює час, потрібний для виявлення інциденту безпеки з моменту його виникнення. Низький рівень означає, що інциденти безпеки виявляються швидко, що може допомогти мінімізувати вплив інциденту;

- середній час відповіді - цей показник вимірює час, необхідний для відповіді на інцидент безпеки після його виявлення. Низький рівень означає, що інциденти безпеки вирішуються швидко, що може допомогти мінімізувати вплив інциденту;

- кількість вразливостей - цей показник вимірює кількість вразливостей, які були виявлені в системі. Це допомагає визначити області системи, які потребують додаткового контролю безпеки;

- відповідність виправлень - цей показник вимірює відсоток систем, які були виправлені протягом певного періоду часу. Високий рівень відповідності виправлень вказує на те, що виправлення безпеки застосовуються своєчасно, що може допомогти зменшити ризик інцидентів безпеки.

Дуже високорівневі показники потенційного впливу використовуються як драйвери для вимог безпеки. FIPS 199 (NIST 2004) визначає три рівні потенційного впливу на організації або окремих осіб через порушення безпеки інформаційної системи [17]. FIPS 199 визначає ці рівні для кожної з трьох цілей безпеки, визначених FISMA: конфіденційність, цілісність і доступність. (Зазвичай АСУ сильно впливають на цілісність і доступність.) Таким чином, FIPS 199 дозволяє класифікувати інформаційну систему з точки зору потенційного впливу.

Подібним чином DoDD 8500.1 (DoD 2002) визначає три рівні категорії забезпечення місії (MAC), яка відображає рівень потреби в захисті цілісності та

доступності, три рівні занепокоєння щодо конфіденційності на основі конфіденційності інформації, яку обробляє IT-система, і три рівні надійності, тобто міцності та надійності в управлінні безпекою або рішенні безпеки [18] .

Підхід до ранжирування ризиків, визначений у Методології оцінки вразливості безпеки для нафтової та нафтохімічної промисловості (API 2004), визначає п’ять рівнів загрози, зацікавленість противника в атаці на актив і вразливість. Методологія також визначає структуру для ранжирування рівнів наслідків, пов’язаних із подією безпеки, але дозволяє галузевим користувачам методології визначати рівні наслідків, специфічні для їхньої бізнес-моделі. Методологія, включаючи підхід до ранжування ризиків, безпосередньо і безпосередньо застосовна в галузі.

Метод ієрархічного голографічного моделювання можна використовувати для визначення ризиків для АСУ та пов’язаних взаємозалежних і взаємопов’язаних інфраструктур.

Ієрархічне голографічне моделювання (англ. - Hierarchical holographic modeling, HHM) може ідентифікувати великий набір критично важливих компонентів і підсистем PCS, пріоритетність яких може бути надзвичайно важкою, особливо в умовах обмежень у часі та ресурсах. Метод HHM був запропонований Хеймсом в 1981 році і розглядався як систематична і всеосяжна методологія. Мета полягає в тому, щоб зафіксувати та продемонструвати внутрішні особливості та сутності з різних аспектів, точок зору, поглядів, вимірів та ієрархій однієї системи. Для великомасштабних, багатоцільових і багаторівневих ризиків метод HHM може вирішувати проблеми за допомогою багатокутних і всеспрямованих досліджень, а також аналізувати підсценарій, відокремлений від цілого в різних ракурсах. Ще у 1991 році Центром управління ризиками інженерних систем був розроблений метод ранжування та фільтрації ризиків (RFRF). На цій основі була створена модель RFRM, яка відповідає вимогам практичного застосування. Вісім етапів цієї моделі сформульовані наступним чином: розпізнавання сценаріїв, попередня фільтрація сценарію, стандарт подвійної фільтрації, мультистандартна оцінка, кількісний рейтинг,

управління ризиками, оцінка сценарію фільтрації та фактичний зворотний зв'язок за сценарієм (рис. 1.5).

Рис. 1.5. Етапи моделі RFRM

1) розпізнавання сценаріїв - різні сцени ризику описуються шляхом генерації моделі HHM для складних систем;

2) попередня фільтрація сценарію - цей етап досягається шляхом фільтрації сцен ризику на вищезгаданій стадії. Особа, яка приймає рішення, забезпечує первинну оцінку на основі прочитаної літератури та експертного досвіду;

3) стандарт подвійної фільтрації:

- по-перше, нерелевантні ризики визначаються якісно відповідно до результатів і можливостей етапу 2;

- потім нерелевантні ризики фільтруються на основі матриці фільтрації

ризиків;

- нарешті, виконується операція сортування ефективних ризиків для підвищення точності на наступному етапі;

4) мультистандартна оцінка - для кожної сцени ризику оцінка повинна одночасно враховувати результати та можливості ризику, редукційність, надійність та надмірність. Цей етап зосереджений на вимірюванні здатності факторів ризику перемогти захисну систему, де решта ризиків може бути обґрунтовано оцінена;

5) кількісний рейтинг - кількісна матриця ризику використовується для оцінки ризику, визначеного на етапі 4, а рейтинг оцінки сцен ризику додатково представлений для виявлення ключових факторів ризику.

Зауважимо, що попередні п'ять етапів можуть виконувати ідентифікацію та фільтрацію ризиків, а останні три етапи можуть забезпечувати управління ризиками, зворотний зв'язок та модифікацію.

HHM є підготовчим етапом для проведення методу фільтрації, ранжування та управління ризиками RFRM для зменшення кількості критичних компонентів. Використовуючи метрики безпеки, RFRM можна застосувати для визначення пріоритетів компонентів PCS і пов’язаних з ними режимів збоїв у керованому наборі на основі їх критичності для роботи в галузі. HHM є дієвим інструментом, який на основі статистичних методів допомагає аналітикам безпеки зрозуміти глибину проблем при оцінюванні ризиків і застосуванні потім методу RFRM [19-20] .

Автоматизовані системи включають сотні або тисячі унікальних компонентів і підсистем, які можуть бути вразливими до зловмисної атаки (наприклад, кібер-активної фізичної або фізичної кібератаки).

Автоматизовані системи управління можуть зіткнутися з різноманітними ризиками. У таблиці 1.1 наведений перелік основних ризиків, які можуть виникнути у таких системах, а також їх аналіз.

Таблиця 1.1

Перелік ризиків у АСУ та їх аналіз

Найменування ризику	Зміст ризику	Аналіз ризику
Недостатня якість даних	Помилки в даних, відсутність актуальності даних	Неправильно оброблені або застарілі дані можуть призвести до неправильних рішень та втрати ефективності управління
Кібербезпека	Атаки хакерів, віруси, атаки типу "фішинг"	Неправильна захист від кіберзагроз може призвести до несанкціонованого доступу до системи, втрати даних або порушення роботи системи управління
Відмова обладнання	Несправність апаратної частини системи	Відмова обладнання може призвести до припинення роботи системи управління та вплинути на продуктивність
Недостатня навченість персоналу	Неправильне використання системи або недостатня реакція на виникаючі проблеми	Невірне використання системи може вивести на некоректні рішення та негативно позначитися на результативності діяльності
Проблеми інтеграції	Несумісність з іншими системами або обладнанням	Несправність інтеграції може призвести до втрати даних, неправильного функціонування систем та порушення процесів управління
Ризики в роботі з штучним інтелектом	Помилки алгоритмів машинного навчання, неправильне визначення призначень	Несправності в алгоритмах штучного інтелекту можуть призвести до неправильних прогнозів та рішень
Законодавчі ризики	Невідповідність системи законодавству	Невідповідність може призвести до правових санкцій та штрафів
Недостатня масштабованість	Неспроможність системи вирішувати завдання при збільшенні обсягів роботи	Потреба в постійному розширенні може стати обтяжливою та вплинути на функціонування
Недостатня надійність	Велика ймовірність виникнення помилок або відмов	Недостатня надійність може вплинути на стабільність роботи системи та призвести до втрат даних
Ризики приватності даних	Несанкціонований доступ до особистої інформації	Витік або використання особистих даних без дозволу може призвести до порушення законодавства та втрати довіри

ВИСНОВОК до розділу 1. Показники використовуються в багатьох галузях як інструмент, який допомагає особам, які приймають рішення, приймати обґрунтовані бізнес-рішення на основі кількісно виміряних,

повторюваних параметрів, а не здогадок чи найкращих припущень. Спільнота контролерів процесів використовує метрики, щоб організувати великі набори даних у значущі представлення, з яких вони можуть отримати корисні тенденції та оцінки ефективності. Але метрики для оцінки та аналізу безпеки АСУ не є широко доступними. Частково це пов’язано з історичною недостатньою увагою до кібербезпеки АСУ і обмеженими технологіями безпеки, спеціально розробленими для АСУ.

Наступний крок – розробити вимоги до показників, які відповідають потребам автоматизованих систем управління в любій галузі.. Мета полягає в тому, щоб ці вимоги слугували достатньою довідковою інформацією для постачальників і власників/операторів АСУ для кращого розуміння показників безпеки та того, як їх можна застосовувати до їхніх продуктів, систем і політик.

РОЗДІЛ 2
РОЗДІЛ 2. РОЗРОБКА МЕТОДИКИ ОЦІНКИ РИЗИКІВ В АВТОМАТИЗОВАНИХ СИСТЕМАХ УПРАВЛІННЯ

2.1 Аналіз різних методів та підходів до оцінки інформаційних ризиків

Зростаюче впровадження організаціями легких автоматизувань, таких як роботизована автоматизація процесів (РАП), викликає занепокоєння щодо надійності та безпеки пов'язаних систем, при цьому проблеми безпеки даних стають ще більш актуальними, коли інструменти такого роду розгортаються для обробки потенційно конфіденційних даних. Однак кількість наукової літератури про розробку цих інструментів таким чином, щоб зменшити ризики, пов'язані з безпекою даних організації, залишається недостатньою.

Оцінка та управління ризиками сформувалася як наукова галузь близько 30–40 років тому. Розроблено принципи та методи концептуалізації, оцінки та управління ризиками. Ці принципи і методи в значній мірі представляють основу цієї області і сьогодні, але було досягнуто недостатньо багато практичних результатів, пов'язаних як з теоретичною платформою, так і з практичними моделями і процедурами [21-25].

На сьогоднішній день оцінки ризиків добре зарекомендували себе в ситуаціях зі значною кількістю даних і чітко визначеними межами їх використання. Були розроблені статистичні та ймовірнісні інструменти, які забезпечують корисну підтримку прийняття рішень для багатьох типів додатків. Однак рішення про ризики все частіше стосуються ситуацій, що характеризуються великою невизначеністю та виникненням. Такі ситуації вимагають різних типів підходів і методів, і основним викликом для сфери ризику є розробка відповідних рамок та інструментів для цієї мети [26-28]. Існує загальний дослідницький фокус на динамічній оцінці та управлінні ризиками, а не на статичній або традиційній оцінці ризиків.

Науковці відзначають, що необхідно продовжувати розробляти оцінки ризиків, які здатні врахувати ці проблеми, пов'язані з виміром знань і динамікою часу. Чистий імовірнісний підхід, наприклад, Байєсовий аналіз, був би нездійсненним, оскільки фонові знання – основа для моделей ймовірностей та завдань – були б поганими. Існує потреба в адаптивному балансі різних стратегій управління ризиками, включаючи стратегії застереження та увагу до сигналів і попереджень [29-34] .

Існує також потреба в значних дослідженнях і розробках для отримання адекватних методів моделювання та аналізу – крім «традиційних» – для «обробки» різних типів систем. Прикладами можуть служити критичні об'єкти інфраструктури (наприклад, електричні мережі, транспортні мережі і т.д.), які є складними системами і часто взаємозалежними, тобто «системами систем». Іншим прикладом є додатки типу безпеки, де якісні оцінки часто виконуються на основі суджень про наміри та можливості суб'єктів, без посилання на шкалу ймовірності. Схоже, що існує величезний потенціал для значного вдосконалення способів оцінки безпеки шляхом розробки структур, які інтегрують стандартні підходи до безпеки та способи оцінки та лікування невизначеності.

Деякі роботи [35-38] усувають цю прогалину, представляючи дослідження, в якому РАП було успішно розроблено для процесу, в якому програмний робот обробляє конфіденційні особисті дані. Ґрунтуючись на роботах про бездумність автоматизації, соціотехнічної оболонки та безпеки за задумом, це емпіричне дослідження, в якому використовувалися дослідження дизайну дій у корпорації Wärtsilä, вказувало на три принципи дизайну, пов'язані з оболонкою, правами доступу та контрольними журналами. Дотримуючись цих принципів, компанія Wärtsilä створила навколо робота конверти, які забезпечують безпечну роботу автоматизації та обробку конфіденційних даних. Це дослідження просуває теорію проектування та розгортання соціотехнічної оболонки, впроваджуючи новий підхід до безпеки шляхом огортання для розробки орієнтованого на безпеку оболонок бездумних агентів автоматизації. У статті також обговорюється практична корисність спроектованого артефакту як з точки зору

дизайну, так і з точки зору оцінки [39-40] .

Автоматизовані системи управління мають вирішальне значення для багатьох критичних інфраструктур. Щоб забезпечити безпечні та ефективні бізнес-операції та підтримати національну мету щодо захисту критичної інфраструктури, необхідно розглянути кіберзагрози таким системам. Показники безпеки підтримують управління кіберризиками та інтеграцію управління кіберризиками в загальне управління бізнес-ризиками.

В роботах [41-44] розглянуто модель автоматизованої системи безпечного транскордонного обміну інформацією. Дана автоматизована система являє собою комплекс наступних модулів, що забезпечують інформаційну безпеку: шифрування даних, електронний цифровий підпис, контроль доступу до інформації, що зберігається, на основі двофакторної автентифікації, вирішення можливих конфліктних ситуацій. У роботах описані моделі двох модулів автоматизованої системи: електронного цифрового підпису та контролю доступу до інформації на основі двофакторної автентифікації. Детально описано математичну модель формування та верифікації цифрового підпису. Описано поетапну програмну реалізацію даної моделі з аналізом отриманих результатів. Розглянуто алгоритм двофакторної автентифікації на базі програми-автентифікатора та мобільного телефону. Проведено генератор секретних кодів, заснований на методі вичерпного пошуку. Описано генератор тригонометричних функцій, який використовується для обчислення одноразового пароля. Наведено поетапну програмну реалізацію цієї моделі [45].

Таким чином, співтовариство інформаційної безпеки визначило різноманітні показники безпеки. Деякі з цих показників є безпосередньо та негайно застосовні до зацікавлених сторін в організаціях, де використовуються АСУ. Інші вказівки щодо показників безпеки можна адаптувати або пристосований до проблемного домену безпеки АСУ. Однак більшість заходів і ресурсів показників безпеки вважаються не безпосередньо актуальні для зацікавлених сторін.

У звіті [46] представлений короткий огляд існуючих систем показників,

стандартів і інструментів оцінки, які потенційно можуть бути застосовані до АСУ у нафтовій і газовій промисловості. Розгляд результатів семінару з оцінки та ранжування систем інформаційної безпеки в АСУ проведений в роботах [47-50], де розглядалась таксономія метрик для систем управління процесами на основі ISO/IEC 17799, ANSI/ISA TR99.00.01. Оскільки показники є ключовим компонентом управління ризиками, представлений огляд методів оцінки ризиків, а також показників фільтрації та ранжирування ризиків, описані проблеми та поточні зусилля щодо розробки нових інструментів метрики, спеціально розроблених для оцінки безпеки АСУ.

Доповідачі [48, 51-53] ініціювали науково-дослідницький проект диспетчерського контролю та збору даних (SCADA), який вивчає шляхи підвищення безпеки систем керування процесами АСУ, що є ключовими для багатьох критичних інфраструктур. Було вказано, що необхідно усунути кіберзагрози таким системам, щоб забезпечити безпечне та ефективне ведення бізнесу та підтримати національну мету захисту критичної інфраструктури. Показники безпеки повинні підтримувати управління кіберризиками та інтеграцію управління кіберризиками в загальне управління бізнес-ризиками.

Термін «метрики» описує широку категорію інструментів, які використовуються особами, які приймають рішення, для оцінки даних у багатьох різних сферах організації. У своїй найпростішій формі метрика – це вимірювання, яке порівнюється зі шкалою або орієнтиром для отримання значущого результату. Наприклад, у компанії може працювати 100 осіб, 98 із яких пройшли навчання з безпеки. Таким чином, 2% співробітників компанії не пройшли навчання. Це вимірювання можна використовувати для визначення метрики безпеки шляхом порівняння з контрольними показниками. Одним з орієнтирів може бути ціль щодо навчання працівників, скажімо, не більше 1% ненавчених.

Іншою може бути лінія тренду, яка показує відсоток навчених працівників з кожним місяцем (рис. 2.1).

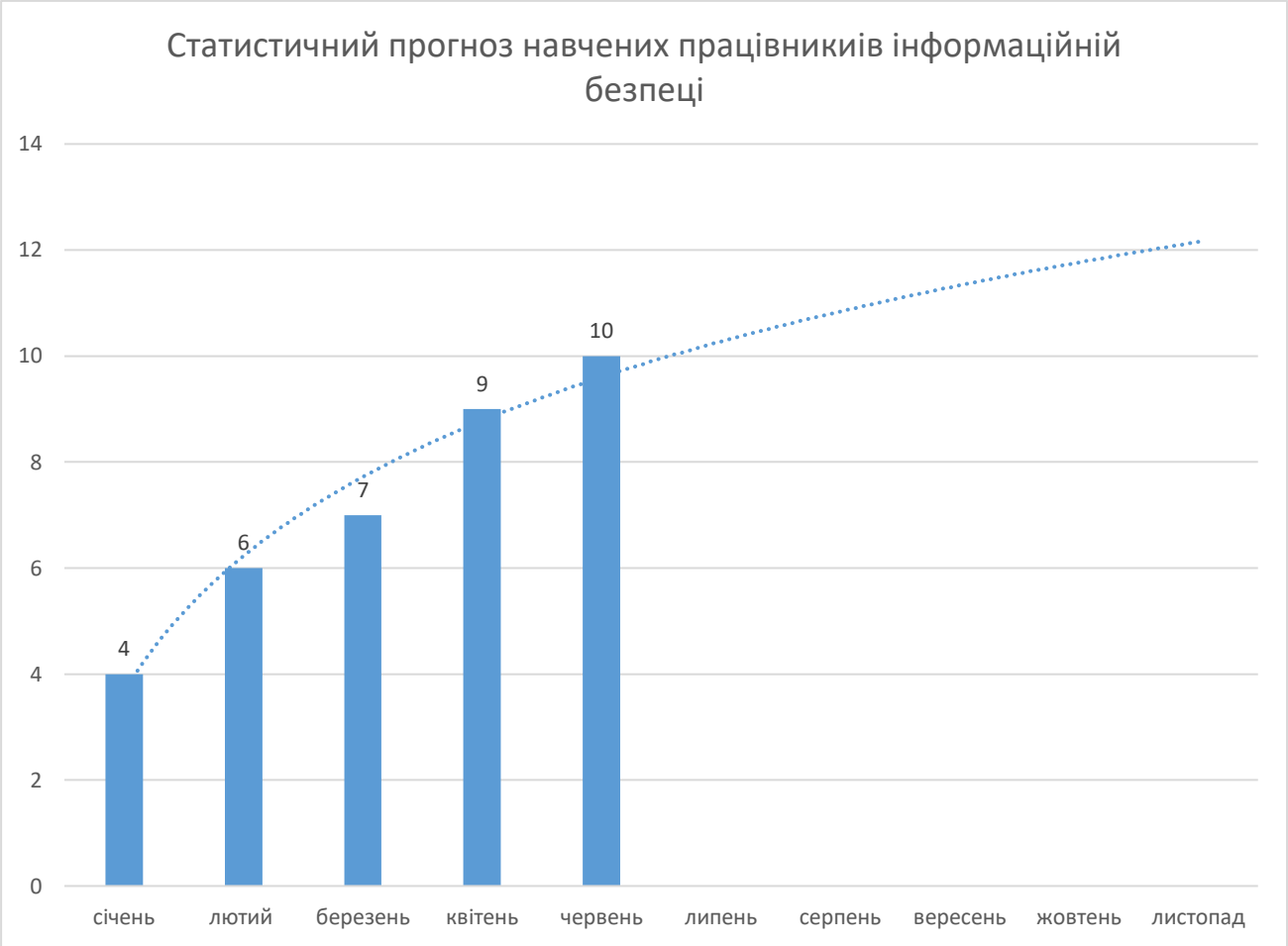

Рис.2.1. Статистичний прогноз навчених працівників інформаційній безпеці

Це забезпечує метрику, за якою компанія тепер може відповісти на такі запитання, як: «Чи кращий у нас цей місяць, ніж минулого?» або «Чи досягаємо ми нашої цілі навчання безпеки?».

Метрики широко використовуються промисловістю. Дуже часто можна побачити показники безпеки, розміщені по всьому промисловому об’єкту, які відстежують кількість інцидентів або закритих викликів порівняно з кількістю відпрацьованих людино-годин. Показники продуктивності для відстеження кількості годин простою на годину роботи також є поширеними. Одним із прикладів показника продуктивності, який використовується на виробничих потужностях, є показник загальної ефективності обладнання, що використовується для оцінки продуктивності частини обладнання, процесу чи цілого об’єкта

$$Zef = As * Per * Qua$$

де As – доступність як відсоток часу, протягом якого обладнання працювало;

Per – продуктивність, як відсоток виробленої продукції порівняно з номінальною продукцією виробника оригінального обладнання;

Qua – якість, як це відсоток придатного продукту до всього виробленого продукту.

Цей простий показник включено в інструменти автоматизації, щоб надати тенденції ефективності в реальному часі та автоматизовані звіти, як інструменти для визначення тенденцій ефективності в режимі реального часу.

Інструменти вимірювання також були розроблені для оцінки промислових АСУ. Наприклад, Honeywell Industry Solutions надає інструмент керування тривогами під назвою «Alarm Scout», який автоматично відстежує сигнали тривоги керування процесом і надсилає електронною поштою «Звіт про контроль продуктивності сигналізації» керівникам або зацікавленим сторонам. Звіт містить різноманітні показники активності тривоги, які відстежують тенденції тривоги, активність тривоги на точку та інші корисні показники, які особи, які приймають рішення, можуть використовувати для швидкого аналізу ефективності тривоги. Оператори можуть отримувати сотні сигналів тривоги щогодини, що ускладнює виявлення аномальних тенденцій, але автоматизована метрика тривоги може швидко виявити сигнали тривоги, які працюють поза очікуваним контрольним показником.

Наразі метрики для відстеження або аналізу безпеки керування процесом не є широко доступними. Однією з причин цього є те, що сама безпека АСУ не була відносно високим пріоритетом до недавнього часу. АСУ історично проектувалися як автономні системи з власною технологією. Основними цілями проектування були безперервність процесу та функціональність. Безпеці від внутрішніх і зовнішніх загроз часто не приділялося багато уваги, окрім простого контролю фізичного доступу. Сьогодні АСУ все частіше з’єднуються з іншими

мережами, включаючи Інтернет, і спостерігається різке зростання кількості вразливостей безпеки та можливостей боротьби.

Було проведено значну роботу з розробки метрик безпеки для систем інформаційних технологій (IT), і доступний багатий набір інструментів. Але цілі та проблеми безпеки IT-мереж не завжди такі ж, як для АСУ, і показники IT-безпеки не завжди можна застосувати безпосередньо до АСУ, навіть якщо базові технології можуть бути однаковими. Наприклад, в IT-системах часто доцільно використовувати надійні паролі користувачів з обмеженим терміном служби та блокувати обліковий запис у разі невдалих спроб. Однак для користувача, який керує кількома комплексами з АСУ, може виникнути значна плутанина під час критичних подій, і може знадобитися доступ до системи з невеликою затримкою або без неї, щоб запобігти перериванню процесу. У таких випадках політика доступу повинна враховувати конкретні експлуатаційні вимоги.

Показники, засновані на відповідності стандартам безпеки або найкращим практикам. Далі, для більш ясної картини щодо структури оцінювання ризиків, необхідно навести короткий та невичерпний список різних методологій ризик-менеджменту (рис. 2.2), а найпопулярніші з них необхідно розглянути більш детально.

1. Фреймворк "NIST Risk Management Framework" на базі американських урядових документів NIST (National Institute of Standards and Technology, Національного інституту стандартів і технологій США) включає набір взаємопов'язаних т. зв. «спеціальних публікацій» (англ. Special Publication (SP), будемо для простоти сприйняття називати їх стандартами):

1.1. Стандарт NIST SP 800-39 "Managing Information Security Risk" ("Управління ризиками інформаційної безпеки") пропонує трирівневий підхід до управління ризиками: організація, бізнес-процеси, інформаційні системи. Цей стандарт описує методологію процесу управління ризиками: визначення, оцінка, реагування та моніторинг ризиків.

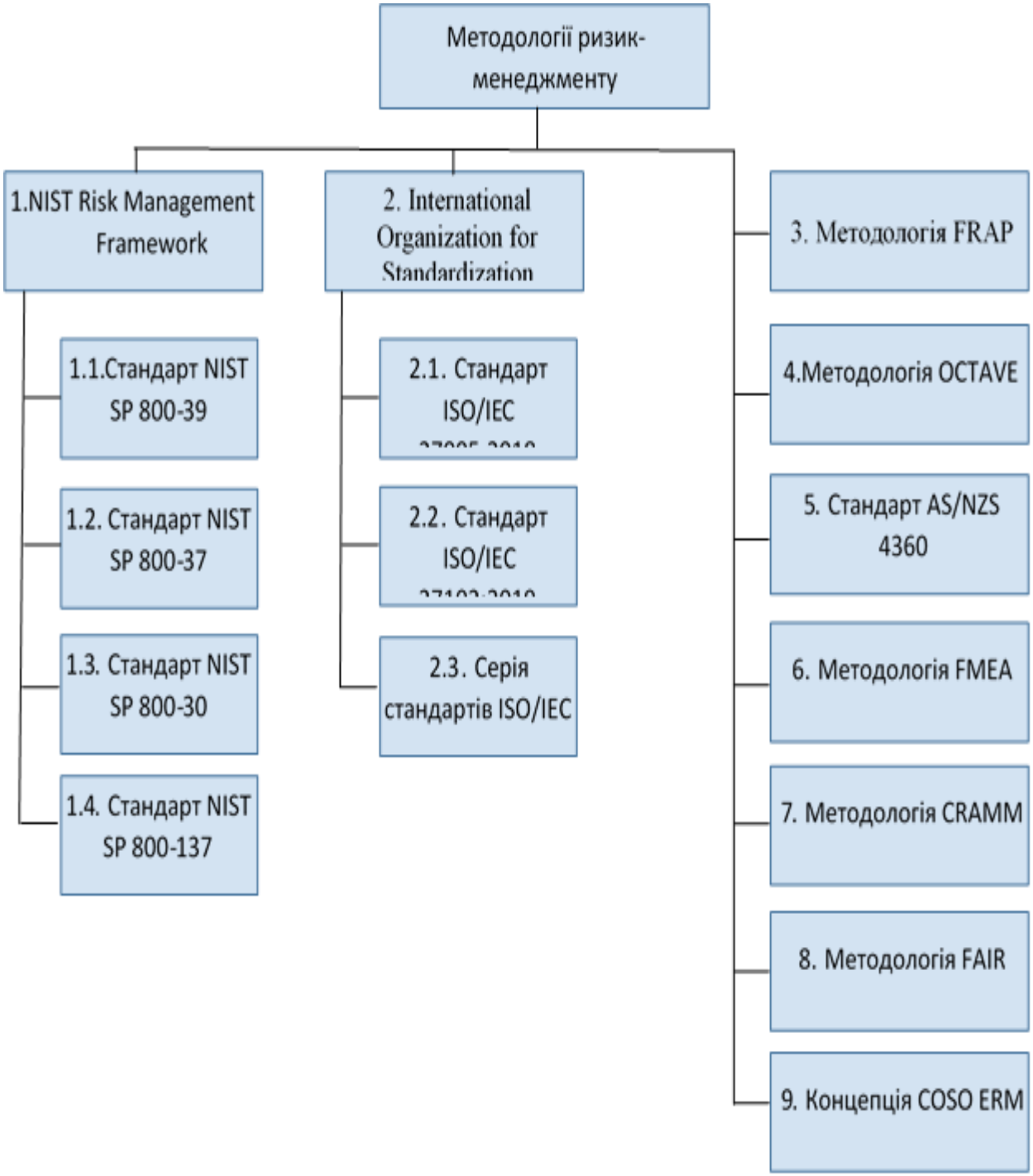

Рис. 2.2. Методології ризик-менеджменту

1.2. Стандарт NIST SP 800-37 «Risk Management Framework for Information Systems and Organizations» («Фреймворк управління ризиками для інформаційних систем та організацій») пропонує для забезпечення безпеки та конфіденційності використання підходу управління життєвим циклом систем.

1.3. Стандарт NIST SP 800-30 Guide for Conducting Risk Assessments (Посібник з проведення оцінки ризиків) сфокусований на IT, ІБ та операційних

ризиках. Він описує підхід до процесів підготовки та проведення оцінки ризиків, комунікування результатів оцінки, а також подальшої підтримки процесу оцінки.

1.4. Стандарт NIST SP 800-137 "Information Security Continuous Monitoring" ("Безперервний моніторинг інформаційної безпеки") описує підхід до процесу моніторингу інформаційних систем та IT-середовищ з метою контролю застосованих заходів обробки ризиків ІБ та необхідності їх перегляду.

2. Стандарти Міжнародної організації зі стандартизації ISO (International Organization for Standardization):

2.1. Стандарт ISO/IEC 27005:2018 "Information technology - Security techniques - Information security risk management" ("Інформаційна технологія. Методи та засоби забезпечення безпеки. Менеджмент ризику інформаційної безпеки") входить до серії стандартів ISO 27000 і є логічно взаємопов'язаним ІБ із цієї серії. Цей стандарт відрізняється фокусом на ІБ під час розгляду процесів управління ризиками.

2.2. Стандарт ISO/IEC 27102:2019 "Information security management - Guidelines for cyber-insurance" ("Управління інформаційною безпекою. Посібник з кіберстрахування") пропонує підходи до оцінки необхідності придбання кіберстрахування як заходи обробки ризиків, а також до оцінки та взаємодії зі страховиком.

2.3. Серія стандартів ISO/IEC 31000:2018 описує підхід до ризик-менеджменту без прив'язки до IT/ІБ. У цій серії варто відзначити стандарт ISO/IEC 31010:2019 "Risk management - Risk assessment techniques" - на даний стандарт у його вітчизняному варіанті ГОСТ Р ИСО/МЭК 31010-2011 "Менеджмент ризику. Методи оцінки ризику» посилається 607-П ЦБ РФ «Про вимоги до порядку забезпечення безперебійності функціонування платіжної системи, показниками безперебійності функціонування платіжної системи та методикам аналізу ризиків у платіжній системі, включаючи профілі ризиків».

3. Методологія FRAP (Facilitated Risk Analysis Process) є відносно спрощеним способом оцінки ризиків, з фокусом лише на найкритичніших активах. Якісний аналіз проводиться за допомогою експертної оцінки.

4. Методологія OCTAVE (Operationally Critical Threat, Asset, Vulnerability Evaluation) сфокусована на самостійній роботі членів бізнес-підрозділів. Вона використовується для масштабної оцінки всіх інформаційних систем та бізнес-процесів компанії.

5. Стандарт AS/NZS 4360 є австралійським і новозеландським стандартом з фокусом як на IT-системах, а й у бізнес-здоров'я компанії, тобто. пропонує глобальніший підхід до управління ризиками. Зазначимо, що даний стандарт замінено на стандарт AS/NZS ISO 31000-2009.

6. Методологія FMEA (Failure Modes and Effect Analysis) пропонує проведення оцінки системи з погляду її слабких місць для пошуку ненадійних елементів.

7. Методологія CRAMM (Central Computing and Telecommunications Agency Risk Analysis and Management Method) пропонує використання автоматизованих засобів управління ризиками.

8. Методологія FAIR (Factor Analysis of Information Risk) – пропрієтарний фреймворк щодо кількісного аналізу ризиків, що пропонує модель побудови системи управління ризиками з урахуванням економічно ефективного підходу, прийняття поінформованих рішень, порівняння заходів управління ризиками, фінансових показників і точних ризик-моделей.

9. Концепція COSO ERM (Enterprise Risk Management) описує шляхи інтеграції ризик-менеджменту зі стратегією та фінансовою ефективністю діяльності компанії та наголошує на важливості їх взаємозв'язку. У документі описані такі компоненти управління ризиками, як стратегія та постановка цілей, економічна ефективність діяльності.

Науковці висловили загальне переконання, що наявні дослідження та стандарти безпеки слід використовувати, де це можливо, щоб запобігти повторному винаходу колеса та скористатися перевагами значного обсягу досліджень, які вже були проведені. Один із методів швидкого використання наявних досліджень у розробці метрик безпеки АСУ – використовувати стандарти безпеки, як джерело вимог до метрик. Однією з конкретних

рекомендацій є ISO-17799, Кодекс практики управління інформаційною безпекою (ISO 2005). Цей стандарт містить вичерпну довідку для встановлення політики безпеки та пропонується як хороше джерело показників політики.

Учасники висловили певний інтерес до показників, які надають операторам АСУ легкий для розуміння показник справності системи. Це може бути на основі комбінації вхідних даних, таких як програмне забезпечення для виявлення вторгнень, моніторинг конфігурації системи та аналіз виявлення системних аномалій. Через потребу в безперервності процесу та характер комунікацій АСУ автоматизовані дії вважалися небажаними.

Однак системні оператори зазвичай не мають часу або навичок, щоб вручну інтерпретувати мережевий трафік і шаблони доступу під час роботи системи. Таким чином, такий показник, як біт переходу/незапуску, який попереджає оператора про аномалії в системі, можна використовувати для спонукання до дії оператора. Ця дія може бути такою ж простою, як інформування системного адміністратора безпеки або ручне закриття некритичних точок доступу.

З цих та інших рекомендацій, наданих під час семінару, стає зрозуміло, що діапазон бажаних інструментів вимірювання безпеки є широким і потребує значного вдосконалення, якщо вони хочуть задовольнити всі потреби галузі. Дослідницький проект I3P SCADA працює над розробкою показників безпеки, орієнтованих на потреби нафтогазової промисловості. Хоча не очікується, що всі побажання галузі будуть розглянуті, найважливіші потреби будуть розглянуті в першу чергу. Для цього дослідники I3P почнуть із формування робочої групи з представників промисловості, постачальників і дослідників, щоб визначити набір вимог до показників на основі широкого діапазону вхідних даних від літератури, наукових кіл, промисловості та урядових організацій. Ці вимоги будуть представлені у звіті про вимоги до показників, який потім використовуватиметься для визначення набору інструментів показників безпеки. Широко поширена думка, що успіх цього дослідження значною мірою залежатиме від взаємодії та співпраці з нафтогазовою промисловістю.

Була визнана необхідність представляти ризики інформаційної безпеки – тобто ризики, пов’язані із залежністю організації від інформаційних технологій або систем за наявності кіберзагроз – як складову бізнес-ризику. Люди, які приймають бізнес-рішення, покладаються на показники для підтримки своїх процесів прийняття рішень. Співтовариство інформаційної безпеки визначило різноманітні показники безпеки, деякі з яких безпосередньо й безпосередньо застосовуються до зацікавлених сторін АСУ. Інші рекомендації щодо показників безпеки можуть бути адаптовані або пристосовані до домену проблем безпеки АСУ. Однак більшість дій і ресурсів із визначення показників безпеки не є безпосередньо актуальними для зацікавлених сторін АСУ.

Показники безпеки можна охарактеризувати тим, що вони вимірюють, як було визначено на семінарі з інформаційної безпеки – рейтинг системи: організаційні показники оцінюють ефективність організаційних програм і процесів; операційні показники описують системи, які використовуються, методи роботи та середовище загроз; і технічні показники дозволяють порівнювати продукти та реалізовані системи, а також алгоритми, специфікації, архітектури та альтернативні конструкції. Ці широкі категорії не виключають одна одну. Можна очікувати певного збігу, але ці категорії дійсно забезпечують корисну високорівневу категоризацію (рис. 2.3), з якої можна визначити та впорядкувати інструменти.

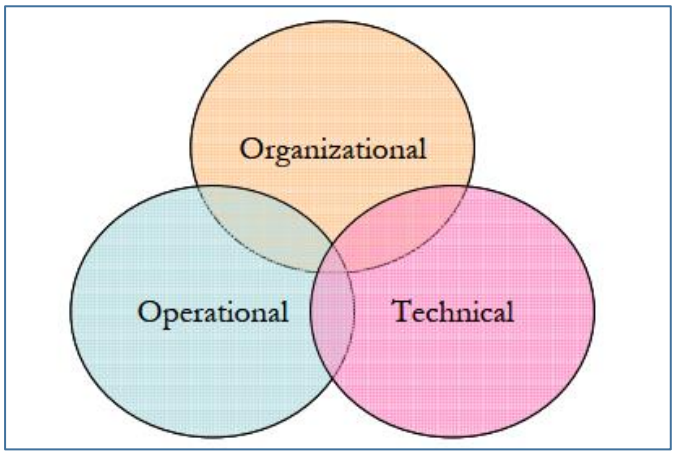

Рис. 2.3. Категоризація показників, визначена на семінарі з рейтингу та рейтингу системи інформаційної безпеки

Організаційні показники можна розглядати як оцінку адекватності стандартів, політики та процедур, прийнятих організацією для підвищення безпеки. Організаційні показники можуть включати відповіді на повний набір запитань «так»/«ні», наприклад:

- Чи прийнято організацією галузевий стандарт безпеки АСУ?
- Чи існує політика, яка вимагає щорічної перевірки кібербезпеки кожного АСУ?
- Чи існує політика, яка вимагає від операторів АСУ та обслуговуючого персоналу періодичного навчання з кібербезпеки?
- Чи існує процедура, якої необхідно виконати, перш ніж АСУ стане доступною через Інтернет? Якщо так, чи передбачає ця процедура комплексну оцінку кібербезпеки, яка перевіряється і схвалено безпосереднім керівництвом і схваленням відділу безпеки?

Операційні показники можна розглядати як оцінку того, наскільки добре офіційні політики та процедури організації впроваджуються відповідальними співробітниками. Операційні показники можуть ґрунтуватися на відповідях на такі типові запитання:

- Чи перевірки кібербезпеки АСУ проводяться персоналом, який пройшов спеціалізовану підготовку з кібербезпеки?
- Якщо так, чи був це сертифікований навчальний курс, який відповідає галузевим стандартам?
- Чи кожна перевірка проводиться персоналом, незалежним від технічної групи, яка відповідає за повсякденну роботу АСУ?
- Чи задокументовано результати кожної інспекції, а результати розміщено в базі даних інспекції?

Технічні показники можна розглядати як оцінку адекватності безпеки, що накладається для захисту конкретних компонентів АСУ. Це показники, пов’язані з повсякденною безпекою системи. Технічні показники можуть містити відповіді на такі запитання:

- Скільки спроб було зроблено цього тижня отримати доступ до АСУ через системне підключення до Інтернету? Чи означає це збільшення на 50% від звичайного рівня використання?
- Яке співвідношення між кількістю невдалих і успішних спроб доступу до АСУ? Чи перевищує це співвідношення критерії, що викликають занепокоєння?
- Чи кабель модема, який використовується для з'єднання АСУ з його постачальником, залишається від'єднаним і зберігається на відповідній відстані (тобто щонайменше шість дюймів) від модему, коли він не використовується фактично та схвалено?

Метрики організаційної безпеки будуть корисні зацікавленим сторонам АСУ насамперед у майбутньому. До засобів АСУ можна застосувати значні рекомендації та досвід роботи з програмою безпеки та показниками процесу. Однак показники програми безпеки не будуть повністю ефективними, доки галузь не визнає потенційних переваг, пов'язаних із створенням програми безпеки, і загальні стандарти належної практики безпеки не будуть встановлені для засобів АСУ. Подібним чином, деякі метрики процесу безпеки можуть бути адаптовані до засобів АСУ з різним ступенем складності. Промисловість може використовувати ці показники для визначення необхідних або бажаних рівнів знань і зрілості процесів у запитах пропозицій (RFP), а також для вибору серед постачальників продуктів і постачальників послуг. Однак, поки можливості безпеки не стануть головним фактором галузевих інвестицій у технології та послуги, метрики процесу безпеки будуть мати обмежену користь для зацікавлених сторін АСУ. Кілька існуючих метрик програми безпеки можна негайно адаптувати до засобів АСУ. Промисловість може використовувати ці показники як показники організаційного прогресу на шляху встановлення та досягнення цілей безпеки. Наприклад, вимірювання відсотка персоналу, який пройшов навчання з питань безпеки, є частиною встановлення та досягнення цілей програми безпеки, пов'язаних із належною обізнаністю та навчанням у сфері безпеки.

Експлуатаційні показники безпеки, пов’язані з продуктивністю АСУ, можуть бути негайно корисними для промисловості та можуть бути отримані з наявних даних. Промисловість може використовувати показники операційної безпеки, які оцінюють стан безпеки організації або вказують на підозрілі зміни в поведінці системи, щоб покращити управління ризиками операцій. Хоча існуючі оперативні показники безпеки не визначені настільки, щоб бути застосовними безпосередньо до АСУ, деякі з них можуть бути адаптовані досить безпосередньо. Що ще важливіше, оперативні дані, які вже зібрані АСУ, можуть бути проаналізовані або отримані для отримання оперативних метрик безпеки, а метрики безпеки, отримані таким чином, можна легко пов’язати з іншими показниками продуктивності системи, отриманими з тих самих даних.

Технічні показники безпеки будуть корисні зацікавленим сторонам АСУ насамперед у майбутньому. Технічні показники можуть допомогти промисловості вибрати продукти, які найкраще відповідають вимогам безпеки. Наприклад, галузевий RFP може використовувати метрики технічної безпеки для визначення необхідних або бажаних характеристик продукту або системи АСУ. Однак технічні показники, специфічні для АСУ, не були визначені, і релевантність більшості технічних показників для домену АСУ є низькою. Крім того, безпека має стати відносно більш важливою серед типів функціональних вимог АСУ, перш ніж технічні показники безпеки стануть корисними.

У технічному розділі розглядається, як переглянуті стандарти ISO/IEC 17799 «Інформаційні технології – Методи безпеки – Кодекс практики управління інформаційною безпекою» (ISO 2005) і ANSI/ISA-TR99.00.01-2004 «Технології безпеки для систем виробництва та керування» (ANSI 2004) Стандарти можуть бути застосовані до показників безпеки для АСУ.

ISO/IEC 17799 (ISO 2005) – це міжнародний стандарт, який має стати відправною точкою для розробки настанов і кодексів практики для управління інформаційною безпекою в організації. Хоча він застосовний до загального IT-середовища, він не спеціалізується на АСУ. Однією з сильних сторін стандарту ISO/IEC 17799 і вагомою причиною для його розгляду є те, що він надає перелік

категорій, які можуть служити для впорядкування багатьох показників, які можуть розглядатися для забезпечення безпеки АСУ. Ми можемо розглядати організацію цих показників як таксономію.

Інші також розглядали ISO/IEC 17799 як основу для організації метрик АСУ і виявили, що в стандарті відсутні такі категорії, як оцінка вразливості та реагування на загрози. Специфічні категорії АСУ, такі як доступ до польових пристроїв, не дивно, були відсутні в стандарті. Таким чином, може статися, що ISO/IEC 17799 можна розглядати як відправну точку для організації показників безпеки в області АСУ, але майже напевно його потрібно буде адаптувати для задоволення широкого діапазону вимог до показників АСУ.

У той час як ISO/IEC 17799 надає незалежну від засобів перспективу, яка головним чином зосереджена на управлінні IT-безпекою, ANSI/ISA-TR99.00.01 (ANSI 2004) (далі TR99.1) забезпечує категоризацію та обговорення показників, які в основному спрямовані на засіб АСУ. Таким чином, TR99.1 може допомогти уточнити загальну категоризацію метрик або структуру, запропоновану ISO/IEC 17799, а також розширити категорії метрик метриками, спеціально націленими на вимоги АСУ.

Щоб пов’язати діяльність із вимірювання показників, наведену на рисунку 2.4, із стандартами ISO/IEC 17799 і TR99.1, потрібна узгоджена систематика категорій показників, яка гармонізує два стандарти та детальне розуміння кожної діяльності на рисунку. Потім таксономію можна заповнювати інформацією з високим або низьким рівнем деталізації. Перша з цих двох проблем була суттєво вирішена науковцями [54-56], де була розроблена гармонізована таксономія ISO/IEC 17799 і TR99.1. Друга з цих проблем (тобто розв’язання дій на рисунку 2.4. до достатнього рівня деталізації, щоб можна було заповнити таксономію) є більш серйозною проблемою.

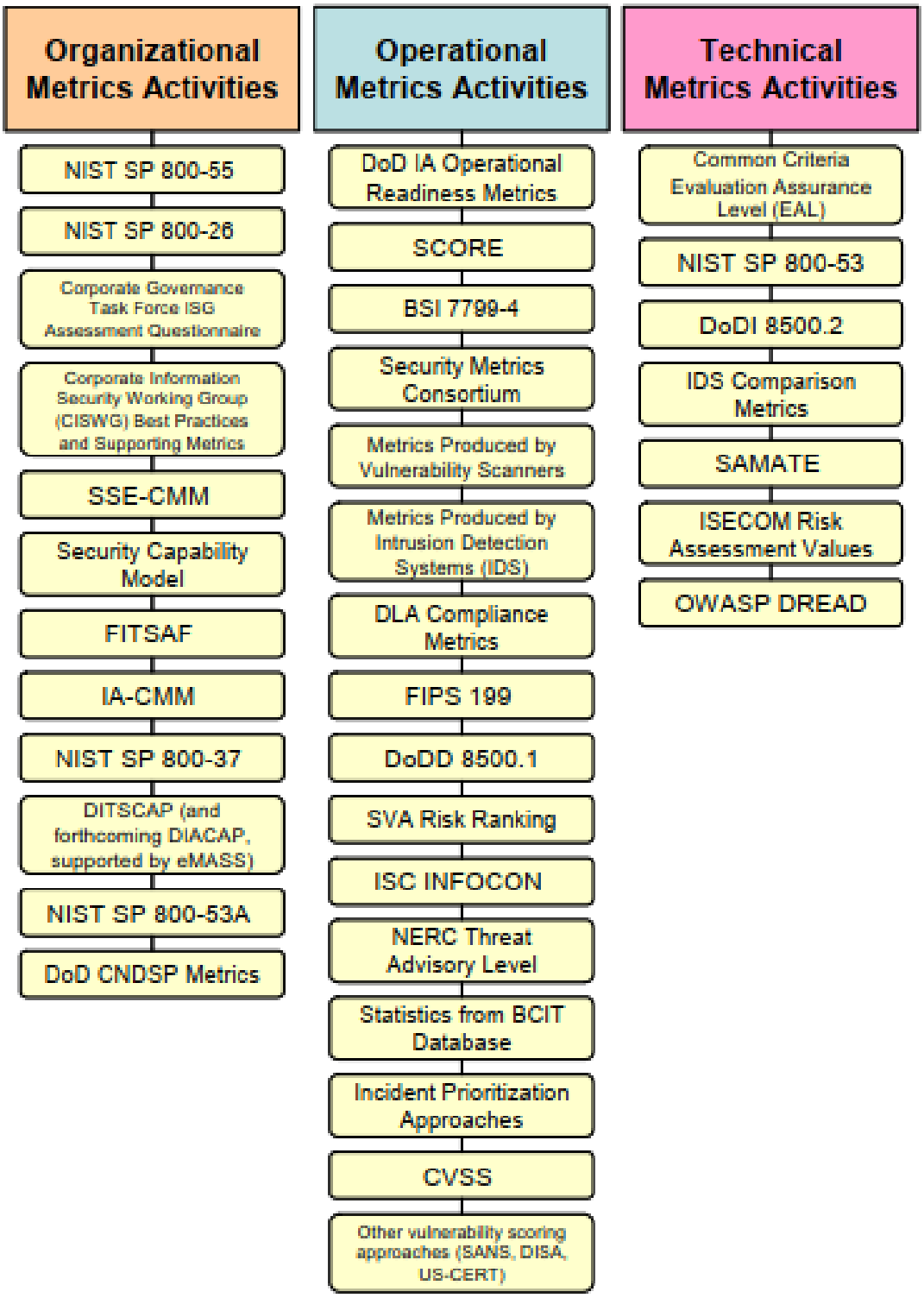

Рис.2.4. Показники діяльність за категорією ISSRR.

При цьому склад показників розглянутих методик визначений в таблиці 2.1.

Таблиця 2.1

Склад показників розглянутих методик

	ISO/IEC 17799	ISA TR99.1	Організаційні показники	Операційні показники	Технічні показники
Політика безпеки	+		+	+	
Оцінка вразливості та ризику		+		+	
Організаційна безпека	+		+		
Класифікація та контроль активів	+		+		+
Безпека персоналу	+	+	+		
Фізична та екологічна безпека	+	+	+	+	
Комунікації та управління операціями	+			+	
Управління доступом	+	+		+	+
Розробка та обслуговування систем	+		+	+	
Управління безперервністю бізнесу	+		+		
Відповідність	+				

Один висновок, який ми можемо зробити з таблиці 2.1, полягає в тому, що стандарти ISO/IEC 17799 і TR99.1 мало підтримують технічні показники. Це може бути наслідком суб'єктивного сприйняття того, що є технічною метрикою; однак ISO/IEC 17799 спрямований на управління IT-безпекою. Це говорить про те, що необхідно вважати заходи безпеки ISO/IEC 17799 більш орієнтованими на організаційні та операційні показники і менш застосовними до технічних показників. Потрібне глибше дослідження TR99.1, а також уточнення категорії технічних показників ISSRR, щоб вирішити, чи дійсно TR99.1 надає більше технічної підтримки метрик таксономії. Якщо ні, то для отримання повної

таксономії, яка повністю охоплює категорії показників ISSRR, необхідне розширення таксономії на основі стандартів або вказівок, які, як вважається, забезпечують більшу підтримку технічних показників, таких як Загальні критерії.

Найближча подальша робота може відбуватися за двома напрямками: по-перше, можна розробити більш повну таксономію засобів контролю, і по-друге, можна розкласти всі дії та процеси, які функціонують в АСУ, до базового рівня. які можуть заповнити таксономію. У першому випадку огляд кількох незалежних зусиль міг би посилити незалежні від засобів АСУ категорії IT, надані ISO/IEC 17799. Наприклад, звіт груп з передового досвіду та показників робочої групи корпоративної інформаційної безпеки і цілі контролю Інституту управління інформаційними та пов'язаними технологіями (COBiT) (ISACA 2005) можуть надавати додаткові деталі категоризації безпеки, ніж це зазначено в ISO/IEC 17799 і TR99.1. У другому випадку, існуючі та нові показники метрики, будуть досліджені більш детально на предмет відповідності між метрикою або мірою безпеки та елементарними елементами АСУ, щоб таксономія метрик безпеки АСУ повністю охоплювала всі засоби АСУ.

Після визначення такого відображення стане легше розробляти моделі процесів, наприклад моделі зрілості, а також визначати ключові показники ефективності.

Одним із ефективних з метод експертного опитування, який ще називають методом Дельфі. Коли створюється система індексів оцінки ризиків, спочатку вибираються різні індекси впливу ризику та перераховуються відповідно до цілей оцінки. По-друге, ці індекси складаються в анкети, а потім статистично аналізуються за коментарями експертів. Крім того, математична статистика також може бути використана для прогнозування експертних рекомендацій опитування, з метою розрахунку факторів індексу ризику, рекомендованих експертами з високим ступенем впливу.

За допомогою цього методу краще можна зробити:

- ідентифікацію та характеризування актуальних джерел загроз,

включаючи можливості, наміри та цілі навмисних загроз, а також можливі ефекти від ненавмисних загроз;

- ідентифікацію потенційних подій загроз, релевантності цих подій та джерел загроз, які можуть ініціювати події загроз;
- ідентифікацію вразливостей та попередніх умов, які впливають на ймовірність того, що актуальні події загроз призведуть до негативного впливу. Її метою є визначення того, наскільки аналізовані бізнес-процеси та інформаційні системи вразливі перед ідентифікованими раніше джерелами загроз та наскільки ідентифіковані події загроз дійсно можуть бути ініційовані цими джерелами загроз;
- визначення ймовірності того, що актуальні події загроз призведуть до негативного впливу, з урахуванням характеристик джерел загроз, уразливостей та попередніх умов, а також схильності організації до цих загроз, беручи до уваги впроваджені заходи захисту;
- визначення негативного впливу, породженого джерелами загроз, з урахуванням характеристик джерел загроз, уразливостей та попередніх умов, а також схильності організації до цих загроз, беручи до уваги впроваджені заходи захисту;
- визначення ризику від реалізації актуальних подій загроз, беручи до уваги рівень негативного впливу від цих подій та ймовірність настання цих подій.

2.2 Методика оцінки ризиків у автоматизованих системах управління

Оцінка ризиків є важливою частиною управління інформаційною безпекою в автоматизованих системах управління.

Особливі міркування стосуються показників, які підтримують аналіз ризиків безпеки для АСУ. Сьогодні у всіх галузях людської діяльності добре розуміють важливість управління ризиками, коли його застосовують до

фізичних небезпек або економічних наслідків, але воно відносно чуже, якщо розглядати безпеку АСУ. Показники безпеки на основі ризиків можна використовувати для вимірювання безпеки АСУ і порівняння цих показників із відомими тестами. Обговорення в цьому розділі далі розглядає потенційні потреби цих показників для визначення пріоритетів ризиків для АСУ і компонентів, щоб можна було реалізувати параметри управління ризиками для протидії головним проблемам у системі.

З рекомендацій учасників семінару I3P SCADA та з ряду інструментів вимірювання, стало зрозуміло, що існує широкий діапазон категорій, методів розробки та форм виведення показників безпеки керування процесом. Тому таксономія, яка є системою класифікації або категоризації, допоможе користувачам знайти предмети, які їх цікавлять, у величезному сховищі інформації. Таксономія попередньої категоризації метрик (та їх використання) була б корисною для розробки загальної картини стану метрик і прогалин у дослідженні метрик.

Кількість інструментів вимірювання інформаційних технологій для кібербезпеки зростає, і деякі з цих інструментів можна застосовувати безпосередньо до АСУ. Однак показники IT-безпеки не розроблялися з урахуванням конкретних потреб і технологій АСУ. Таким чином, необхідні додаткові дослідження та розробки, щоб застосувати ці інструменти для безпеки АСУ.

Аналіз методів, які використовуються для оцінки цих ризиків, згрупований в таблиці 2.2.

Таблиця 2.2

Аналіз методів, які використовуються для оцінки ризиків

Вид	Мета	Підхід	Ключові кроки	Результат
Якісний аналіз ризиків	Визначити ризики, які потребують детального аналізу, і визначити	Оцінка на основі сценарію	Визначати та аналізувати можливі майбутні події, які можуть негативно	якісні твердження, що пояснюють важливість і придатність засобів

Вид	Мета	Підхід	Ключові кроки	Результат
	необхідні засоби контролю на основі їх впливу на цілі		вплинути на людей, активи, процеси чи навколишнє середовище (аналіз ризиків). Зробити судження щодо управління ризиком і терпимості до нього на основі аналізу, враховуючи фактори впливу (оцінка ризику)	контролю для мінімізації зон ризику
Кількісний аналіз ризиків	призначити компонентам ризику об'єктивні чисельні або вимірювані значення	Об'єктивне та числове оцінювання	Присвоювати числові значення незалежно від компонентів ризику	кількісне пояснення впливу ризику та проблем безпеки разом із реєстром ризиків

Необхідно пам’ятати, що вибір між якісними та кількісними методами залежить від рівня знань про ризик та можливості своєчасної оцінки. Обидва підходи сприяють ефективному управлінню ризиками в автоматизованих системах управління.

Створення методики оцінки ризиків у автоматизованих системах з використанням штучного інтелекту включає в себе кілька ключових етапів. Нижче наведено загальну методику, яку можна використовувати (рис.2.5).

Також визначені пропозиції на кожному з етапів:

Етап 1: Визначення Об'єкта Оцінки

1.1. Ідентифікація автоматизованої системи: Визначте область діяльності системи. Визначте види даних, що обробляються.

1.2. Визначення цілей системи: Опишіть основні цілі та завдання системи.

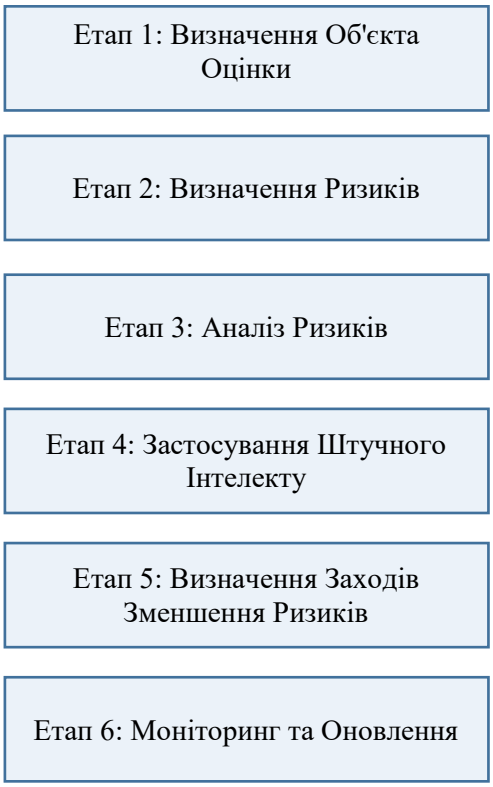

Рис. 2.5. Алгоритм методики оцінки ризиків в АСУ

Етап 2: Визначення Ризиків.

2.1. Ідентифікація потенційних загроз: Врахуйте зовнішні та внутрішні загрози. Визначте потенційні сценарії загроз.

2.2. Визначення слабких місць: Визначте вразливості системи, які можуть бути використані для атак.

Етап 3: Аналіз Ризиків.

3.1. Оцінка ймовірності та впливу: Визначте ймовірність виникнення загрози. Оцініть потенційний вплив на систему.

3.2. Матриця ризиків: Створіть матрицю ризиків, об'єднуючи ймовірність та вплив.

Етап 4: Застосування Штучного Інтелекту.

4.1. Збір та аналіз даних: Застосуйте алгоритми машинного навчання для аналізу великого обсягу даних щодо потенційних загроз та вразливостей.

4.2. Прогнозування ризиків: Використовуйте алгоритми прогнозування для передбачення можливих ризиків на основі історичних даних.

4.3. Автоматизована система моніторингу: Розробіть систему моніторингу з використанням штучного інтелекту для виявлення невідповідностей та аномалій.

Етап 5: Визначення Заходів Зменшення Ризиків.

5.1. Вибір стратегій зменшення ризиків: Виберіть стратегії для зменшення виявлених ризиків.

5.2. Визначення відповідальних за заходи: Призначте відповідальних за впровадження заходів зменшення ризиків.

Етап 6: Моніторинг та Оновлення.

6.1. Система моніторингу: Розробіть систему моніторингу для постійного виявлення та відстеження ризиків.

6.2. Оновлення стратегій: Періодично переглядайте та оновлюйте стратегії зменшення ризиків відповідно до нових загроз та вразливостей.

Застосування штучного інтелекту (ШІ) для оцінювання ризиків у автоматизованих системах управління (АСУ) може значно покращити ефективність та точність процесу оцінки. ШІ може виявляти та аналізувати складні взаємодії та залежності, а також швидко реагувати на зміни у середовищі.:

Детальний розгляд етапу 4 дозволив сформувати наступні шляхи застосування штучного інтелекту та рекомендації з їх використання в запропонованій методиці:

1. Моделювання імовірності та впливу: використовуйте алгоритми машинного навчання для розробки моделей, які можуть прогнозувати імовірність виникнення ризиків та їхній вплив на систему. Враховуйте історичні дані, а також фактори, що можуть впливати на ризик.

2. Аналіз багатовимірних даних: використовуйте ШІ для обробки та аналізу великих обсягів даних, включаючи структуровані та неструктуровані дані. Це дозволяє виявляти складні взаємозв'язки та патерни, які можуть вказувати на ризики.

3. Автоматизоване виявлення аномалій: використовуйте системи

машинного навчання для виявлення аномальних подій чи змін у поведінці системи. Це може вказувати на можливі ризики або поглиблені дослідження.

4. Прогнозування трендів: використовуйте аналітику ШІ для прогнозування та виявлення трендів у сфері кібербезпеки та ризиків. Це дозволяє підготовити систему до нових або змінюючихся загроз.

5. Експертні системи для виявлення ризиків: використовуйте експертні системи, які можуть враховувати досвід та знання експертів для аналізу ризиків та прийняття рішень.

6. Аналіз великих мережевих даних: використовуйте ШІ для аналізу великих мережевих даних для виявлення можливих атак та аномалій в мережі, що може викликати ризики безпеки.

7. Глибинне навчання для класифікації загроз: використовуйте глибинне навчання для автоматичної класифікації потенційних загроз та ризиків на основі великого обсягу даних.

8. Системи предиктивної аналітики: використовуйте системи предиктивної аналітики для попереднього прогнозування можливих ризикових сценаріїв та виявлення можливих проблем з безпекою.

9. Оцінка загроз за допомогою навчання з підкріпленням: використовуйте навчання з підкріплення для оцінки ризиків та прийняття рішень в умовах невизначеності та змінливих умов.

10. Автоматизований аналіз логів та подій: використовуйте ШІ для автоматизованого аналізу логів та подій, що дозволяє вчасно виявляти аномалії та можливі ризики.

Інтеграція ШІ у процес оцінки ризиків дозволяє не тільки збільшити точність та ефективність, але і швидше виявляти та реагувати на мінливі умови та нові види загроз у світі автоматизованих систем управління.

У Python існує низка бібліотек та фреймворків, які можна використовувати для реалізації різних аспектів оцінювання ризиків у автоматизованих системах управління за допомогою штучного інтелекту: Scikit-learn, TensorFlow та Keras, PyTorch, Pandas, NumPy, Scrapy, NLTK (Natural Language Toolkit), OpenCV, Dask.

Ці бібліотеки та фреймворки можуть бути комбіновані та використовуватися разом в залежності від конкретних завдань та потреб дослідження.

Простий приклад на основі використання бібліотеки Scikit-learn для класифікації ризиків на основі імовірностей та впливу (рис.2.6).

```
# Імпорт бібліотек
import pandas as pd
from sklearn.model_selection import train_test_split
from sklearn.ensemble import RandomForestClassifier
from sklearn.metrics import accuracy_score,
classification_report

# Завантаження даних (приклад даних, реальні дані можуть бути
складнішими)
data = pd.read_csv('your_data.csv')

# Підготовка даних
X = data.drop('Risk', axis=1)  # Ознаки (признаки)
y = data['Risk']  # Цільова змінна (риск)

# Розділення даних на навчальний та тестовий набори
X_train, X_test, y_train, y_test = train_test_split(X, y,
test_size=0.2, random_state=42)

# Створення та навчання моделі класифікації
model = RandomForestClassifier(n_estimators=100,
random_state=42)
model.fit(X_train, y_train)

# Прогнозування на тестовому наборі
y_pred = model.predict(X_test)

# Оцінка точності та вивід результатів
accuracy = accuracy_score(y_test, y_pred)
print(f'Accuracy: {accuracy:.2f}')

report = classification_report(y_test, y_pred)
          print('Classification Report:\n', report)
```

Рис.2.6. Лістинг програми для класифікації ризиків

Цей код створює та навчає просту модель класифікації (Random Forest Classifier) на основі даних про ризики (з уявленого CSV-файлу). Для роботи програми слід замінити 'your_data.csv' реальними даними та додати додаткові етапи для обробки та аналізу даних згідно з потребами класифікації.

Формат даних у файлі 'your_data.csv' буде залежати від характеру вашого дослідження та конкретного вигляду даних, які ви використовуєте для

оцінювання ризиків в автоматизованих системах управління. Приклад того, як може виглядати простий файл з даними для класифікації ризиків:

Feature1,Feature2,Feature3,Feature4,Feature5,Risk
1.2,0.8,5.6,2.3,0.7,Low
3.1,1.5,4.8,1.8,0.9,High
2.4,0.9,6.3,2.7,1.2,Low
...

У цьому прикладі:

Кожен рядок представляє один елемент даних.

Перші п'ять стовпці (Feature1, Feature2, Feature3, Feature4, Feature5) - це ознаки (признаки), які ви використовуєте для оцінювання ризиків.

Останній стовпець (Risk) - це цільова змінна, яку ви намагаєтеся передбачити чи класифікувати (наприклад, "Low" або "High").

Це приклад, і файл даних може виглядати інакше в залежності від конкретної задачі та характеру ваших даних. Важливо забезпечити правильність та репрезентативність даних для того, щоб модель могла навчатися на них та давати зрозумілі результати.

Графічне виведення результатів класифікації може допомогти легше зрозуміти ефективність вашої моделі та оцінити її працездатність. Одним із способів є використання різноманітних графіків та діаграм, таких як матриці плутанини та криві ROC-AUC. Приклад використання бібліотек matplotlib та scikit-learn для графічного представлення результатів класифікації:

```
python
Copy code
import matplotlib.pyplot as plt
from sklearn.metrics import confusion_matrix, plot_confusion_matrix, roc_curve, auc

# Вивід матриці
conf_matrix = confusion_matrix(y_test, y_pred)
plot_confusion_matrix(model, X_test, y_test, cmap='Blues', display_labels=['Low', 'High'])
plt.title('Confusion Matrix')
plt.show()

# Вивід кривої ROC-AUC
```

```
y_probs = model.predict_proba(X_test)[:, 1]  # Ймовірності класу "High"
fpr, tpr, thresholds = roc_curve(y_test, y_probs)
roc_auc = auc(fpr, tpr)

plt.figure()
plt.plot(fpr, tpr, color='darkorange', lw=2, label=f'ROC curve (area = {roc_auc:.2f})')
plt.plot([0, 1], [0, 1], color='navy', lw=2, linestyle='--')
plt.xlabel('False Positive Rate')
plt.ylabel('True Positive Rate')
plt.title('Receiver Operating Characteristic (ROC) Curve')
plt.legend(loc='lower right')
plt.show()
```

У цьому прикладі (рис. 2.7):

Матриця відображає те, які класи правильно чи неправильно класифіковані моделлю. Крива ROC-AUC демонструє залежність між чутливістю (True Positive Rate) та специфічністю (1 - False Positive Rate) для різних порогів відсічення.

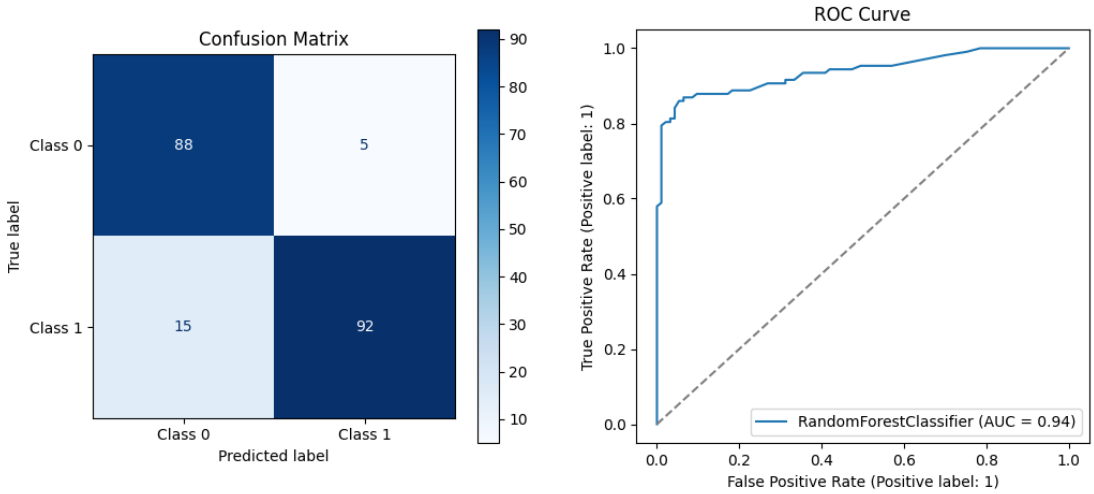

Рис.2.7. Результат класифікації за допомогою ШІ

Необхідно зазначити, що ці графіки можуть бути корисними лише у випадку бінарної класифікації (такі як "Low" та "High" у прикладі). Якщо більше ніж два класи, інші метрики та графіки можуть бути важливими для оцінки продуктивності моделі.

Це лише початок і може бути вдосконалено відповідно до конкретних потреб та характеристик глибшого дослідження

Ця методика дозволить створити комплексний підхід до оцінки та управління ризиками в автоматизованих системах з використанням штучного

інтелекту.

Висновок до розділу 2. Проаналізовані стандарти інформаційної безпеки дозволили зробити висновок, що їх потрібно застосовувати в комплексі, тому що не кожен стандарт визначає організаційні, операційні та технічні вимоги. Якісний аналіз ризиків швидкий, але суб'єктивний. З іншого боку, кількісний аналіз ризиків є необов'язковим і об'єктивним і має більше деталей, резервів на випадок непередбачених обставин і рішень «так/ні», але він займає більше часу і є більш складним. Кількісні дані важко зібрати, а якісні дані коштують непомірно дорого. Незважаючи на те, що вплив математичних операцій на кількісні дані є надійним, точність даних не гарантується через те, що вони є лише числовими. Дані, які важко зібрати або точність яких є сумнівною, можуть призвести до неточних результатів з точки зору цінності. У цьому випадку бізнес-одиниці не можуть забезпечити успішний захист або можуть приймати помилкові рішення щодо поводження з ризиками та витрачати ресурси без визначення дій щодо зменшення або усунення ризику. У якісному підході суб'єктивізм розглядається як частина процесу і може забезпечити більшу гнучкість в інтерпретації, ніж оцінка, заснована на кількісних даних.

Для швидкої та легкої оцінки ризиків 99 відсотків організацій використовують якісну оцінку. Однак для критичних питань безпеки є сенс інвестувати час і гроші в кількісну оцінку ризиків. Застосовуючи комбінований підхід, враховуючи необхідну інформацію та час, з наявними даними та знаннями, можна підвищити ефективність та результативність процесу оцінки ризиків та відповідати вимогам організації.

За результатами аналізу існуючих методик встановлено, що показники IT-безпеки не розроблялися з урахуванням конкретних потреб і технологій АСУ і необхідні додаткові дослідження та розробки, щоб застосувати ці інструменти для безпеки АСУ. Розроблена методика оцінювання дозволяє врахувати комплексність вимог до оцінювання ризиків інформаційної безпеки в АСУ.

РОЗДІЛ 3
РЕКОМЕНДАЦІЇ З ПРАКТИЧНОГО ЗАСТОСУВАННЯ МЕТОДИКИ ОЦІНКИ РИЗИКІВ У АВТОМАТИОВАНИХ СИСТЕМАХ УПРАВЛІННЯ

3.1 Оцінка ефективності застосування методики оцінки ризиків

Ефективність методології оцінки ризику можна оцінити за допомогою різних методик. Згідно зі статтею ISACA, оцінка ризику є невід'ємною частиною ширшої стратегії управління ризиками для впровадження заходів контролю для усунення або зменшення будь-яких потенційних наслідків, пов'язаних з ризиком. Основна мета оцінки ризику - уникнути негативних наслідків, пов'язаних з ризиком, або оцінити можливі можливості. Це об'єднані зусилля з виявлення та аналізу можливих майбутніх подій, які можуть негативно вплинути на людей, активи, процеси та/або навколишнє середовище (тобто аналіз ризику), і прийняття суджень щодо управління та допустимості ризику на основі аналізу ризику, враховуючи фактори впливу (тобто оцінка ризику).

У підході до оцінки ризиків аналізуються взаємозв'язки між активами, процесами, загрозами, вразливостями та іншими факторами. Існує багато доступних методів, але кількісний і якісний аналіз є найбільш широко відомими і використовуваними класифікаціями. Загалом, методологія, обрана на початку процесу прийняття рішень, повинна бути здатною дати кількісне пояснення впливу ризику та питань безпеки поряд з ідентифікацією ризику та формуванням реєстру ризиків. Також повинні бути якісні заяви, які пояснюють важливість і придатність засобів контролю та заходів безпеки для мінімізації цих зон ризику/

Оцінювання ефективності застосування розробленої методики оцінки ризиків у автоматизованих системах управління може включати кілька кроків.

Загальний алгоритм оцінювання ефективності показаний на рис.3.1.

Рекомендації застосування визначеного алгоритму оцінювання ефективності методик наступні:

1. Визначення ключових показників ефективності (KPE): визначте KPE, які

відображають цілі та завдання методики. Наявність надійних показників або ключових показників ефективності (KPE) у сфері інформаційної безпеки є необхідною умовою для створення успішної програми безпеки.

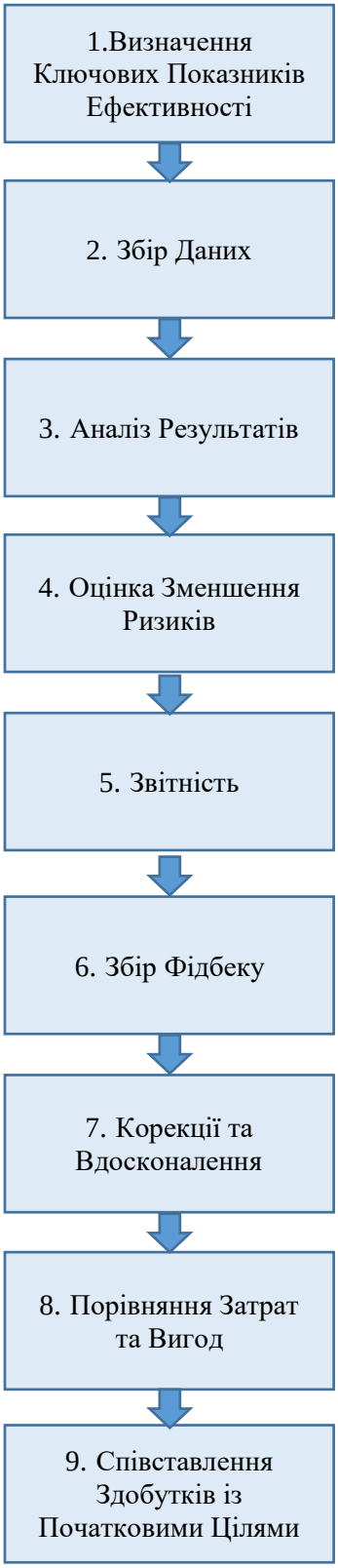

Рис.3.1. Алгоритм оцінювання ефективності методики оцінки ризиків

Вимірювання операційної ефективності, витрат і вигод завжди хвилювало менеджерів, і інформаційна безпека не є винятком. Існує кілька принципів, які допоможуть керівникам інформаційної безпеки (CISO) розробити показники, призначені для органів управління та осіб, які приймають рішення. Ці досить загальні принципи можуть бути адаптовані офіцерам безпеки, щоб створити каталог показників у рамках своїх організацій. Спеціальні показники також вимагаються різними нормативними документами.

Приклади KPE можуть включати зменшення випадків кібератак, покращення якості прийняття рішень, зниження частоти відмов обладнання тощо.

2. Збір даних: збирайте дані перед та після впровадження методики. Враховуйте кількісні та якісні показники, такі як кількість інцидентів, час відновлення після відмов, рівень задоволеності користувачів тощо.

3. Аналіз результатів: порівнюйте дані до та після впровадження методики. Аналізуйте зміни в рівні ризиків, ефективності системи та інших важливих показниках.

4. Оцінка зменшення ризиків: оцініть, чи методика дозволила зменшити імовірність виникнення ризиків та їхній вплив. Порівняйте результати оцінки ризиків до та після впровадження.

5. Звітність: підготуйте звіт, який включає в себе аналіз KPE та зроблені висновки. Презентуйте звіт у вигляді презентацій або письмової документації.

6. Збір фідбеку від користувачів та фахівців: організуйте опитування користувачів та фахівців щодо досвіду використання методики. Враховуйте їхні погляди та рекомендації для подальшого вдосконалення.

7. Корекції та вдосконалення: при необхідності вносите зміни до методики на основі отриманих результатів. Покращуйте та адаптуйте методику з урахуванням нових викликів та змін в середовищі.

8. Порівняння затрат та вигод: порівняйте витрати на розробку та впровадження методики з отриманими вигодами та зменшенням ризиків.

9. Співставлення здобутків із початковими цілями: перевірте, чи були

досягнуті початкові цілі та завдання, які ви визначили для методики.

Оцінка ефективності повинна бути систематичною та періодичною. Результати можуть слугувати основою для вдосконалення методики та подальшого управління ризиками в автоматизованій системі управління.

3.2 Проведення дослідження та рекомендації з практичного застосування методики

Для початку необхідно визначити фактори ризику на основі методу Дельфі із залучення експертів.

При виборі факторів ризику необхідно враховувати безліч складних факторів. Однак при виборі цих факторів немає відносно чітких критеріїв або стандартів. Вибір факторів ризику в основному визначається на основі досвіду дослідника відповідно до його фактичної ситуації та вимог. Зазвичай необхідно підбирати точні, здійсненні та зіставні фактори ризику, які здатні максимально максимізувати вплив цих факторів. Надалі максимальний імпакт-фактор розглядається як основний показник для оцінки загальних рівнів ризику.

Крім того, обрані фактори ризику повинні мати практичне референтне значення, і можуть бути зіставлені з факторами, відібраними іншими методами дослідження, що може проілюструвати раціональність і доцільність запропонованого методу. Загалом у цьому дослідженні для відбору факторів ризику було використано два види методу:

- огляд літератури
- та експертне опитування.

Як вже говорилося вище, метод експертного опитування ще називають методом Дельфі. Коли створюється система індексів оцінки ризиків, спочатку вибираються різні індекси впливу ризику та перераховуються відповідно до цілей оцінки. По-друге, ці індекси складаються в анкети, а потім статистично аналізуються за коментарями експертів. Крім того, математична статистика

також може бути використана для прогнозування експертних рекомендацій опитування, з метою розрахунку факторів індексу ризику, рекомендованих експертами з високим ступенем впливу.

Алгоритм дослідження позначений на рис.3.2.

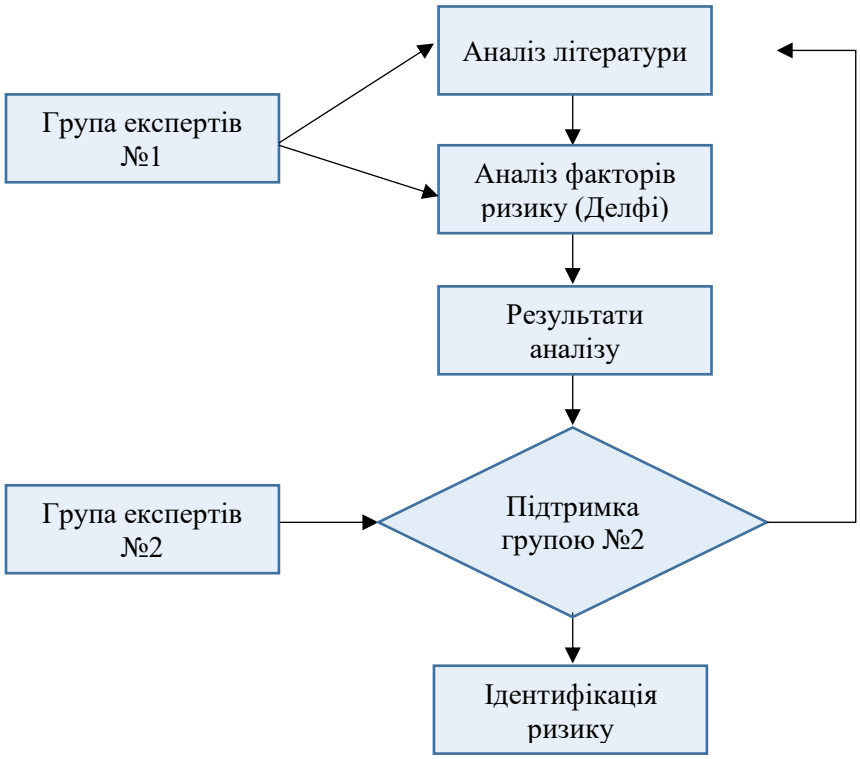

Рис. 3.2. Алгоритм дослідження

До складу експертної групи No1 фахівці АСУ як науковці так і практики. Оскільки ці експерти мали більш ніж десятирічний досвід роботи та управління, а також мали глибоке розуміння управління ризиками для засобів АСУ, спочатку було проведено анкетне опитування щодо них. Анкета складалася з двох частин. У першій частині перелічені фактори ризику, які були відсіяні після ознайомлення з літературою на початковому етапі. Друга частина була розроблена з відкритими питаннями, перераховуючи фактори ризику АСУ на основі власного досвіду експертів. Потім структура джерел ризику була збагачена і вдосконалена. Нарешті, були проаналізовані фактори ризику інтелектуальної АСУ, а попередні результати аналізу були укладені за допомогою методу Дельфі шляхом організації групи експертів. До 2-ї експертної

групи увійшли практики АСУ військової частини. Ця група експертів провела аудит результатів попереднього аналізу попереднього етапу та перевірила його комплексність, доцільність та раціональність. Якби результати були підтримані експертною групою 2, на основі результатів аналізу можна було б розробити модель ННМ. В іншому випадку будуть надані покращені пропозиції та повторені вищеописані процедури.

Відповідно до принципу ітеративного аналізу, проілюстрованого на рисунку 3.2, у цьому дослідженні було виконано три ітерації, отримані відносно обґрунтовані результати, засновані на аналізі факторів ризику. Ці фактори ризику були розділені на чотири перспективи, відповідно до фактичного стану АСУ, включаючи людський фактор, фактори навколишнього середовища та фактори управління.

На першому етапі, відповідно до встановленої вище моделі ННМ, було визначено чотири основні сценарії ризику для АСУ включаючи сценарії аналізу операторів, сценарії аналізу засобів, сценарії аналізу навколишнього середовища та сценарії управлінського аналізу.

Другим кроком була фільтрація основних сценаріїв ризику, визначених на першому етапі. Джерела ризику, визначені на першому етапі, були відносно всеосяжними, і багато підсистем ризику були успішно побудовані. Однак, якщо кожна підсистема була доопрацьована, можуть бути створені сотні джерел ризику. Насправді, не всі джерела ризику мають прямий вплив на АСУ. Таким чином, фільтрація ризиків проводилася відповідно до сценаріїв ризику, які необхідно було вивчити, і ці сценарії були об'єднані з фактичними результатами розслідування, щоб зменшити кількість ризиків для наступного кроку. У цьому дослідженні, на основі опитування 10 експертів, було відсіяно 8 неважливих сценаріїв ризику: фізіологічний статус; вік АСУ; рівень технічного обслуговування і період технічного обслуговування. В результаті залишилося 16 ризикових сценаріїв.

Серйозність ризику визначається поєднанням можливості виникнення і впливового наслідку для ризику. За ступенем тяжкості ризику його можна

розділити на чотири рівні: високий ризик, відносно високий ризик, загальний ризик і низький ризик. З точки зору осіб, які приймають рішення, немає необхідності витрачати занадто багато часу та ресурсів на усунення низьких ризиків, тому спочатку необхідно розглянути події з високим ризиком та відносно високим ризиком. При проведенні ризик-менеджменту рівні ризику, як правило, відфільтровуються і створюється матриця ранжування.

На другому етапі експерти оцінили сценарії ризику, можливості виникнення ризику та впливові наслідки ризику. Для наслідків ризиків були розроблені такі правила: якщо наслідки ризику були визнані серйозними більш ніж 6 з 10 експертів, то наслідки ризику були надзвичайно серйозними; якщо наслідки оцінювалися 6 експертами для отримання більшого рівня, але не досягали рівня тяжкості, який розцінювався як більший наслідок, ризик не був таким серйозним; Оціночні індекси для середнього та нижчого рівнів були схожими, а інші умови можна було ігнорувати. Такі ж правила застосовувалися і до можливостей ризиків. Враховуючи пропозиції 10 експертів щодо наслідків та можливостей ризиків, можна отримати рейтинг за можливостями виникнення ризику та впливовими наслідками ризику.

Після фільтрації низьких і загальних ризиків, в цілому 7 факторів ризику були збережені як важливі фактори, включаючи професійні навички, технічну підтримку, вплив середовища, надійність зв'язку, своєчасність технічного обслуговування, можливості розпізнавання цілей, оцінка ситуації (табл. 3.1) (рис.3.3).

Таблиця 3.1

Результати оцінювання ризиків експертами

№ з/п	Ризик	Оцінка експертами
1	професійні навички	0,5
2	технічна підтримка	0,6
3	вплив середовища	0,9
4	надійність зв'язку	0,8
5	своєчасність технічного обслуговування	0,3
6	можливості розпізнавання цілей	0,8
7	оцінка ситуації	0,6

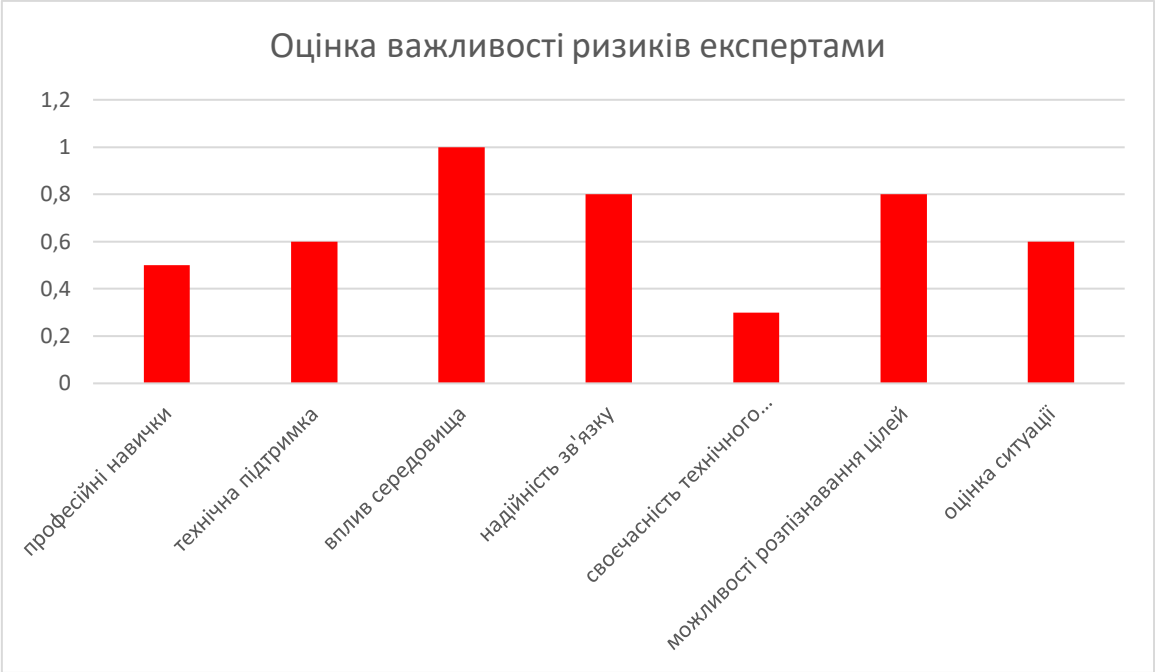

Рис.3.3. Результат оцінювання ризиків експертами

Однак інші 18 факторів ризику, які не були збережені в цьому дослідженні, також були розглянуті. Оскільки вплив був не таким високим у порівнянні з рештою 18 факторами ризику, він розглядався як другорядний фактор і міг бути відсіяний.

Висновок до розділу 3. Оцінка ризиків та управління ризиками є науковою галуззю та забезпечує важливий внесок у підтримку прийняття рішень на практиці.

Визначена методика оцінювання ризиків у автоматизованих системах управління дозволяє правильно оцінити фактори ризику на основі створеного алгоритму. Застосування методу Дельфі при оцінюванні дозволяє залучити до оцінювання фахівців та персонал автоматизованих систем управління, які володіють навичками визначення причин відмов та несправностей. Такий підхід дає можливість всебічно оцінити інформаційні ризики, включаючи і технічні критерії оцінки.

Проведений експеримент визначив ефективність запропонованої методики

а запропоновані рекомендації дозволяють не тільки визначити ризики у автоматизованих система, але й спланувати заходи щодо їх попередження та створити ефективну систему інформаційного захисту.

ВИСНОВКИ

Розглянуті теоретичні аспекти інформаційних ризиків у автоматизованих системах управління виявили актуальність визначеної теми дослідження.

Аналіз різних методів та підходів до оцінки інформаційних ризиків, переліку наукових досліджень дозволив зробити висновок про те, що захисту інформації у автоматизованих системах управління при їх розробці та під час експлуатації приділяється недостатньо. За результатами аналізу встановлено, що сама безпека АСУ не була відносно високим пріоритетом до недавнього часу. АСУ історично проектувалися як автономні системи з власною технологією. Основними цілями проектування були безперервність процесу та функціональність. Безпеці від внутрішніх і зовнішніх загроз часто не приділялося багато уваги, окрім простого контролю фізичного доступу.

Забезпечення безпеки цих систем стає критично важливою задачею. Збільшення вимог до надійності систем управління, особливо в критичних галузях, таких як енергетика, медицина та транспорт, військова справа, вимагає глибокого розуміння та ефективного управління інформаційними ризиками. Наукова основа оцінки ризиків та управління ризиками все ще дещо хитка з деяких питань, у тому сенсі, що як теоретична робота, так і практика спираються на перспективи та принципи, які можуть серйозно ввести в оману осіб, які приймають рішення.

У роботі розроблений перелік параметрів та показників, які можна використовувати для оцінки інформаційних ризиків в автоматизованих системах управління, який відрізняється від відомих комплексним врахуванням організаційних, операційних та технічних показників, які впливають на інформаційну безпеку автоматизованих систем управління.

Розроблена нова удосконалена методика аналізу та оцінки інформаційних ризиків на основі обраних параметрів та показників включає інструменти штучного інтелекту для автоматизації процесу аналізу та оцінювання ризиків.

Проведено експериментальне дослідження, використовуючи розроблену методику, на прикладі конкретної автоматизованої системи управління, оцінена

ефективність розробленої методики та відпрацьовані рекомендації щодо вдосконалення безпеки та надійності автоматизованих систем управління. Дослідження підтвердило ефективність методики при визначенні пріоритетів ризиків інформаційній безпеці в автоматизованій системі управління для планування першочергових заходів безпеки.

Розроблені підходи можуть бути використані при плануванні та реалізації автоматизованих систем управління та створенні у них системи інформаційної та кібербезпеки. Розроблена методика оцінки ризиків дозволить ефективніше виявляти та запобігати потенційним атакам.

Дослідження показало необхідність подальшого застосування штучного інтелекту при створенні сильнішої платформи для оцінки та управління ризиками, вирішення поточних та майбутніх викликів, зокрема пов'язаних із ситуаціями глибокої невизначеності та ризиками, що в автоматизованих системах управління.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Fred Cohen. Automated Control System Security. IEEE Security and Privacy. Vol. 8, Issue 5. September 2010. pp 62–63. URL: https://doi.org/10.1109/MSP.2010.146

2. Lee W. Lerner, Mohammed M. Farag, and Cameron D. Patterson. Run-time prediction and preemption of configuration attacks on embedded process controllers. In Proceedings of the First International Conference on Security of Internet of Things (SecurIT '12). Association for Computing Machinery, New York, NY, USA, 2012. pp. 135–144. URL: https://doi.org/10.1145/2490428.2490447

3. M. Brundle, M. Naedele. Security for process control systems: An overview. Security Privacy, IEEE, 6(6): 24--29, Nov--Dec 2008. URL: https://doi.org/10.1109/MSP.2008.150

4. Makarenko, O. & Yanko, Alina. Концепція системи виявлення та запобігання вторгнень до мережі. Системи управління, навігації та зв'язку. Збірник наукових праць. 2022. 2. 59-67. URL: https://doi.org/10.26906/SUNZ.2022.2.059.

5. Stephen Northcutt, Judy Novak. Network Intrusion Detection: An Analysts Handbook Third Edition, 2001. – 384 p.

6. Michael Collins. Network Security Through Data Analysis: From Data to Action 2nd Edition, 2017. – 428 p.

7. Yuri Diogenes, Erdal Ozkaya. Cybersecurity – Attack and Defense Strategies, 2020. – 326 p.

8. Піхота К. В., Горицький В. М. Сертифікація кібербезпеки іот: система та схеми оцінки відповідності. Збірник матеріалів Міжнародної науково-технічної конференції «ПЕРСПЕКТИВИ ТЕЛЕКОМУНІКАЦІЙ» (2021): с. 359-362.

9. Scarfone Karen. Guide to Intrusion Detection and Prevention Systems (IDPS) — 2007. — 127 p.

10. Z. Q. Bo, X. N. Lin, Q. P. Wang, Y. H. Yi, F. Q. Zhou. Developments of

Power System Protection and Control, in Protection and Control of Modern Power Systems, vol. 1, no. 1, pp. 1-8, July 2016, URL: https://doi.org/10.1186/s41601-016-0012-2.

11. Begimbayeva Y., Ussatova O., Biyashev R., Nyssanbayeva S. Duc Pham. Development of an automated system model of information protection in the cross-border exchange, Cogent Engineering, 7:1. 2020. URL: https://doi.org/10.1080/23311916.2020.1724597

12. Cárdenas A. A., Amin S., Lin Z.-S., Huang Y.-L., Huang C.-Y., Sastry S. Attacks against process control systems: risk assessment, detection, and response. In Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security, ASIACCS'11, pages 355--366, 2011. URL: https://doi.org/10.1145/1966913.1966959

13. Про захист інформації в автоматизованих системах: Закон України. Відомості Верхов. Ради України. - 1994. - № 31. - Ст. 286 URL: https://zakon.rada.gov.ua/laws/card/81/94-вр (дата звернення 20.10.2023 р.)

14. НД ТЗІ 1.4-001-2000. Типове положення про службу захисту інформації в автоматизованій системі. Наказ Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від “ 04 ” грудня 2000 р. № 53.

15. Roeser S., Hillerbrand R., Sandin P., Peterson M. Introduction to Risk Theory. In: Roeser, S., Hillerbrand, R., Sandin, P., Peterson, M. (eds) Handbook of Risk Theory. Springer, Dordrecht. 2012. URL: https://doi.org/10.1007/978-94-007-1433-5_1

16. Cadena A., Gualoto F., Fuertes W., Tello L., Tapia L., Torres J.. Metrics and Indicators of Information Security Incident Management: A Systematic Mapping Study. 2020. pp. 507-519. URL: https://doi.org/10.1007/978-981-13-9155-2_40.

17. Стандарт FIPS 140-2 технологія самошифрування. (2018). [Електронний ресурс]. – Режим доступу: URL: https://www.seagate.com/files/www-content/solutions-content/security-and-encryption/id/docs/faq-fips-sed-lr- mb-605-2-1302-ru.pdf/

18. DoD 5200.28-STD Supersedes CSC-STD-00l-83, dtd l5 Aug 83 Library No. S225,7ll. URL: https://www.dau.edu/cop/stm/documents/dodi-850001-cybersecurity

19. Haimes Y. Y., Lambert J., Duan Li, Schooff R., V. Tulsiani, Hierarchical holographic modeling for risk identification in complex systems. 1995 IEEE International Conference on Systems, Man and Cybernetics. Intelligent Systems for the 21st Century, Vancouver, BC, Canada, 1995, pp. 1027-1032 vol.2, URL: https://doi.org/10.1109/ICSMC.1995.537904.

20. Grabowski M., Merrick W., Harrold J. R., Massuchi T. A., van Dorp J. D. Risk modeling in distributed, large-scale systems, in IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans, vol. 30, no. 6, pp. 651-660, Nov. 2000, URL: https://doi.org/10.1109/3468.895888.

21. Terje Aven. Risk assessment and risk management: Review of recent advances on their foundation. European Journal of Operational Research. Volume 253, Issue 1. 2016. Pages 1-13. URL: https://doi.org/10.1016/j.ejor.2015.12.023.

22. Ibsen Chivata Cardenas, Terje Aven, Roger Flage. Addressing challenges in uncertainty quantification: the case of geohazard assessments. Geoscientific Model Development. Volume 16. Issue 6. Pages 1601-1615. 2023. URL: https://doi.org/10.5194/gmd-16-1601-2023.

23. Shkarlat O., & Shtonda R., Chernish Y., Sulimovska M. Захист інформації в автоматизованих системах суб'єктів охоронної діяльності. Сучасні інформаційні технології у сфері безпеки та оборони. 32. 17-22. 2018. URL: https://doi.org/10.33099/2311-7249/2018-32-2-17-22.

24. Miller A. Trends in Process Control Systems Security. IEEE Security & Privacy, vol. 3, no. 5, pp. 57-60, 2005. URL: https://doi.org/10.1109/MSP.2005.136.

25. Ізотов В.Б., Молдовян А.А., Молдовян Н.А. Керовані швидкі методи захисту даних в автоматизованих системах управління. Автоматизація та дистанційне керування 62, 1007–1021 (2001). URL: https://doi.org/10.1023/A:1010262023165.

26. Apostolakis G. E. How useful is quantitative risk assessment? //Risk Analysis: An International Journal. – 2004. – Vol.. 24. Issue . 3. – pp. 515-520. URL: https://doi.org/10.1111/j.0272-4332.2004.00455.x

27. Mark Lee, Jones D., Estimating P (event): concepts, approaches and issue. Landslide Risk Assessment. pp. 125-138. 2023. URL: https://doi.org/10.1680/lra.66236.125

28. Song J., Zhang Y., Cui Y., Yue T., Dang. Bayesian active learning approach for estimation of empirical copula-based moment-independent sensitivity indices. Engineering with Computers. 2023. URL: https://doi.org/10.1007/s00366-023-01865-0.

29. Cruz I., Troffaes M., Sahlin Ul. A suggestion for the quantification of precise and bounded probability to quantify epistemic uncertainty in scientific assessments. Risk Analysis. Vol. 42, Issue 2. pp. 39-253, 2022. URL: https://doi.org/10.1111/risa.13871.

30. Yazdi M., Zarei E., Adumene S., Abbassi R., Rahnamayiezekavat P. Uncertainty modeling in risk assessment of digitalized process systems. Methods to Assess and Manage Process Safety in Digitalized Process System, pp. 389-416. 2022. URL: https://doi.org/10.1016/bs.mcps.2022.04.005.

31. Borgonovo E., Li G., Barr J., Plischke E., Rabitz H., Global Sensitivity Analysis with Mixtures: A Generalized Functional ANOVA Approach. Risk Analysis. Vol. 42, Issue 2. Pp. 304-333. 2021. URL: https://doi.org/10.1111/risa.13763.

32. Ghods B., Fayaz R. Rofooei. Addressing the epistemic uncertainty in seismic hazard analysis as a basis for seismic design by emphasizing the knowledge aspects and utilizing imprecise probabilities. Bulletin of Earthquake Engineering. Vol. 20. Issue 2. pp. 741-764. 2021. URL: https://doi.org/10.1007/s10518-021-01252-4.

33. Kim H., Lundteigen M., Hafver A., Pedersen F. Utilization of risk priority number to systems-theoretic process analysis: A practical solution to manage a large number of unsafe control actions and loss scenarios. Proceedings of the Institution of Mechanical Engineers, Part: Journal of Risk and Reliability, Vol. 235, Issue 1, pp. 92-107, 2020. URL: https://doi.org/10.1177/1748006X20939717.

34. Parviainen T., Goerlandt F., Helle I., Haapasaari P., Kuikka S. Implementing Bayesian networks for ISO 31000:2018-based maritime oil spill risk management: State-of-art, implementation benefits and challenges, and future research directions. Journal of Environmental Management. Volume 278, Part 1. 2021. 111520. URL: https://doi.org/10.1016/j.jenvman.2020.111520.

35. Cadena J., Andres F. Osorio, Jose L. Torero, Genserik Reniers, David Lange. Uncertainty-based decision-making in fire safety: Analyzing the alternatives. Journal of Loss Prevention in the Process Industries. Vol. 68, 104288, 2020. URL: https://doi.org/10.1016/j.jlp.2020.104288.

36. Yu X., Liang W., Zhang L., Reniers G., Lu L. Risk assessment of the maintenance process for onshore oil and gas transmission pipelines under uncertainty. Reliability Engineering & System Safety. Vol. 177, pp. 50-67, 2018. URL: https://doi.org/10.1016/j.ress.2018.05.001.

37. Zhu T., Haugen S., Liu Y. Risk information in decision-making: definitions, requirements and various functions. Journal of Loss Prevention in the Process Industries. Volume 72, 2021, 104572, URL: https://doi.org/10.1016/j.jlp.2021.104572.

38. Aven T. The reliability science: Its foundation and link to risk science and other sciences. Reliability Engineering & System Safety. Volume 215. 2021. 107863. URL: https://doi.org/10.1016/j.ress.2021.107863.

39. Asatiani A., Hakkarainen T., Paaso K., Penttinen E. Security by envelopment – a novel approach to data-security-oriented configuration of lightweight-automation systems. European Journal of Information Systems. Published online: 25 May 2023. Pp. 1-23. URL: https://doi.org/10.1080/0960085X.2023.2217362

40. Челухін, В.А., Аксютіна, М.С., Аунг, П.З. Захист інформації автоматизованих систем методами штучного інтелекту. В: Шакірова О.Г., Башков О.В., Хусаїнов А.А. (ред.) Актуальні проблеми та шляхи розвитку промисловості: обладнання та технології. Конспект лекцій з Мережі та системи, том 200. Шпрінгер, Чам. 2021. URL: https://doi.org/10.1007/978-3-030-69421-0_74

41. Miani R.S., Zarpelao B.B., Sobesto B., Cukier M. A practical experience on evaluatingintrusion prevention system event data as indicators of security issues. In:

2015 IEEE 34thSymposium on Reliable Distributed Systems (SRDS), 2015. pp. 296–305

42. Ussatova, O., Nyssanbayeva, S. Generators of one-time two-factor authentication passwords.Informatyka, Automatyka, Pomiary w Gospodarcei Ochronie Środowiska, Poland, 2019. Vol. 2, R. 72, P. 60–64. URL: https://doi.org/10.5604/01.3001.0013.2550.

43. Biyashev R. G., Nyssanbayeva S. E. Algorithm for creation a digital signature with error detection and correction. Cybernetics and Systems Analysis. 2012. Vol. 4, pp. 489–497. URL: https://doi.org/10.1007/s10559-012-9428-5

44. Biyashev, R. G., Nyssanbayeva, S. E., & Begimbayeva, Y. Y. (). Development of the model of protected cross-border information interaction. Open Engineering. 2016. Vol. 6, 199–20. URL: https://doi.org/10.1515/eng-2016-0025.

45. Cohen F. Automated Control System Security. IEEE Security and Privacy. Vol. 8. Issue 5. September 2010. pp. 62-63. URL: https://doi.org/10.1109/MSP.2010.146.

46. Ying Z., Li Q., Meng S., Ni Z., Sun Z. A Survey of Information Intelligent System Security Risk Assessment Models, Standards and Methods. In: Zhang, X., Liu, G., Qiu, M., Xiang, W., Huang, T. (eds) Cloud Computing, Smart Grid and Innovative Frontiers in Telecommunications. CloudComp SmartGift 2019 2019. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering. 2020. Vol. 322. Springer, Cham. URL: https://doi.org/10.1007/978-3-030-48513-9_48.

47. Liang J., Zhu H., Zhang B., Liu L, Liu X., Lin H., Tian J., Chen Q. Research and Prospect of Cyber-Attacks Prediction Technology for New Power Systems. 2023 IEEE 6th Information Technology, Networking, Electronic and Automation Control Conference (ITNEC), vol.6, pp.638-647, 2023. URL: https://doi.org/10.1109/ITNEC56291.2023.10081983.

48. Hua Liu, Implementation of Electronic Commerce Taxation Management System based on Computer and Abnormal Data Retrieval Algorithm. 2022 International Conference on Edge Computing and Applications (ICECAA). pp.1006-

1009. 2022. URL: https://doi.org/10.1109/ICECAA55415.2022.9936147.

49. Bolbot V., Theotokatos G., Boulougouris E., Vassalos D. A novel cyber-risk assessment method for ship systems. Saf. Sci. 2020. 131. 104908. URL: https://doi.org/10.1016/j.ssci.2020.104908.

50. Kaplan S.; Haimes Y.Y.; Garrick B.J. Fitting Hierarchical Holographic Modeling into the Theory of Scenario Structuring and a Resulting Refinement to the Quantitative Definition of Risk. Risk Anal. 2001. 21. 807. URL: https://doi.org/10.1111/0272-4332.215153.

51. Naedele M.. Standardizing Industrial IT Security– A First Look at the IEC Approach. Proc. 10th IEEE Int'l Conf. Emerging Technologies and Factory Automation (ETFA 05), pp. 857-863, 2005. URL: https://doi.org/10.1109/ETFA.2005.1612763.

52. Naedele M.. An Access Control Protocol for Embedded Devices. Proc. 4th Int'l IEEE Conf. Industrial Informatics (INDIN 06). pp. 565-569. 2006. URL: https://doi.org/10.1109/INDIN.2006.275623.

53. Naedele M.. Addressing IT Security for Critical Control Systems. Proc. 40th Hawaii Int'l Conf. System Sciences (HICSS-40), pp. 115. 2007. [online] Available: URL: http://www2.computer.org/portal/web/csdl/doi/10.1109/HICSS.2007.48.

54. Haimes Y.Y. Kaplan S. Lambert J.H. Risk filtering, ranking, and management framework using hierarchical holographic modeling. Risk Anal. 2002, 22. pp. 383–397. URL: https://doi.org/10.1111/0272-4332.00020.

55. Byres E., Lowe J. The Myths, Facts Behind. Cyber Security Risks for Industrial Control Systems. Proc. VDE Convention, pp. 213-217, 2004.

56. Eisenhauer J. Roadmap to Secure Control Systems in the Energy Sector. US DoE and DHS, Jan. 2006, [online] Available: URL: https://www.controlsystemsroadmap.net/.