**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**
**ТЕРНОПІЛЬСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ ІМ. І. ПУЛЮЯ**

**Кафедра** *кібербезпеки*

# МАГІСТЕРСЬКА КВАЛІФІКАЦІЙНА РОБОТА

**НА ТЕМУ:**

## РОЗРОБКА МЕТОДИКИ ПІДВИЩЕННЯ РІВНЯ ЗАХИЩЕНОСТІ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНОЇ СИСТЕМИ

Студента групи *СБ-61 Левенець Олени Володимирівни*

Дипломник _____ / *О.В. Левенець* /

Керівник роботи _____ / *М.Б. Александер* /

Рецензент: _____ / /

Завідувач кафедри _____ *Н. В. Загородна*

“___” _____ *2020 р.*

2020

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**
**ТЕРНОПІЛЬСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ**
**ІМ. І. ПУЛЮЯ**

**Кафедра** *кібербезпеки*
**Спеціальність** *125 Кібербезпека*

***"З А Т В Е Р Д Ж У Ю"***
Завідувач кафедри кібербезпеки
_____ *Н. В. Загородна*
"____" _____ *2020 р.*

# ЗАВДАННЯ

**на магістерську кваліфікаційну роботу студенту групи СБ - 61**
*Левенець Олені Володимирівні*

**1. Тема роботи:** *" Розробка методики підвищення рівня захищеності інформаційно-комунікаційної системи "* затверджена наказом по університету від " " 2020 р. № .

**2. Термін здачі студентом закінченої роботи:** " 14 " грудня 2020 р.

**3. Вихідні дані для роботи:** *Уточнити зміст поняття «захищеність інформаційно-комунікаційної системи». Провести аналіз методик підвищення рівня захищеності інформаційно-комунікаційних систем. Розробити інформаційно-комунікаційну систему для ПАТ «Зборівгаз» із дотриманням вимог до рівня захищеності інформації. Запропонувати комплекс заходів посилення захисту від вразливостей опрацювання корпоративної інформації. Визначити напрямки вдосконалення та впровадження раціональної структури інформаційно-комунікаційної системи ПАТ «Зборівгаз». Провести апробацію результатів роботи. Надати рекомендації з безпеки.*

**4. Зміст розрахунково-пояснювальної записки:** *Вступ – актуальність теми магістерської кваліфікаційної роботи. Основна частина – уточнення поняття «захищеність інформаційно-комунікаційної системи». Аналіз комерційних та наукових методик підвищення захищеності інформаційно-комунікаційних систем. Розробка методики визначення профілю захищеності на базі теорії ігор. Розробка інформаційно-комунікаційної системи ПАТ «Зборівгаз» із дотриманням вимог підвищення захищеності інформації. Висновки.*

**5. Перелік графічного матеріалу:** *Графічний матеріал містить 10 слайдів презентації і висвітлює основні аспекти дипломної роботи. Роздрук слайдів подано у додатку Н.*

**6. Перелік програмних продуктів, які належить використати в процесі розроблення роботи (проекту)**: *Пакет MS Office: процесор тексту Microsoft Word., пакет Visio, процесор презентацій Microsoft Power Point.*

**7. Консультування роботи, із зазначенням розділів роботи**

| Розділ | Консультант | Завдання видав | | Завдання прийняв | |
|---|---|---|---|---|---|
| | | підпис | дата | підпис | дата |
| | | | | | |

**8. Дата, коли видано завдання :** *“ ” 2020 р.*

Керівник _____ *М.Б. Александер*

Завдання прийняв до виконання _____ *О.В. Левенець*

## КАЛЕНДАРНИЙ ПЛАН

| № з/п | Назва етапів роботи | Термін виконання етапів роботи | Примітка |
|---|---|---|---|
| *1.* | *Пошук науково-технічної літератури. Складання плану дипломної роботи.* | *.2020* | *виконано* |
| *2.* | *Написання основних розділів дипломної роботи.* | *.2020* | *виконано* |
| *3.* | *Написання додаткового розділу дипломної роботи.* | *.2020* | *виконано* |
| *4.* | *Розроблення рекомендацій.* | *.2020* | *виконано* |
| *5.* | *Написання та оформлення пояснювальної записки.* | *.2020* | *виконано* |
| *6.* | *Подання завершеної дипломної роботи на кафедру.* | *14.12.2020* | *виконано* |

Студент _____ *О.В. Левенець*

Керівник _____ *М.Б. Александер*

## АНОТАЦІЯ

Магістерська робота присвячена розробці методики підвищення рівня захищеності інформаційно-комунікаційної системи. Уточнено поняття «захищеність інформаційно-комунікаційної системи», проаналізовано комерційні та наукові методики підвищення захищеності інформаційно-комунікаційних систем, стандарти кібербезпеки. Запропоновано для вибору профіля захищеності корпоративної інформаційно-комунікаційної системи базуватись на математичному апараті теорії ігор, який надає можливість обрати засоби захисту інформації, враховуючи обмеження ресурсів підприємства. Для ПАТ «Зборівгаз» розроблено інформаційно-комунікаційну систему із дотриманням вимог до підвищення захищеності корпоративної інформації.

Ключові слова: захищеність інформаційно-комунікаційної системи, профіль захищеності, теорія ігор, ПАТ «Зборівгаз».

## ANNOTATION

The master's thesis is devoted to the improvement of the methods of development of the secure information-communication system. The concept "security of information and communication system" has been clarified, commercial and scientific methods of improvement the security of information and communication systems, cyber security standards have been analyzed. It is proposed to choose the security profile of the corporate information and communication system based on the mathematical apparatus of game theory, which gives the opportunity to choose the means of protection of information, given the limitations of the resources of the enterprise. For PJSC “Zborivgaz” has developed an information and communication system with compliance with the requirements for improvement corporate information security.

Keywords: security of information and communication system, security profile, game theory, PJSC “Zborivgaz”.

# ЗМІСТ

Вступ……6
Розділ 1. Методики підвищення рівня захищеності інформаційно-комунікаційної системи…….……...8
1.1. Аналіз і уточнення поняття захищеності інформаційно-комунікаційної системи…….…..8
1.2. Комерційні методики підвищення рівня захищеності інформаційно-комунікаційної системи…….…...9
1.3. Методики підвищення захищеності інформаційно-комунікаційної системи, затверджені стандартами з кібербезпеки…….…14
1.4. Методики підвищення рівня захищеності інформаційно-комунікаційної системи, розроблені науковцями…….17
Висновки до першого розділу……...23
Розділ 2. Застосування теорії ігор для вибору інструментів захисту інформаційно-комунікаційної системи……...24
2.1. Поняття профілів захищеності інформаційно-комунікаційної системи……24
2.2. Вибір інструментів захисту інформаційно-комунікаційної системи на базі теорії ігор……26
Висновки до другого розділу……39
Розділ 3. Реалізація інформаційно-комунікаційної системи для підвищення рівня захищеності на прикладі ПАТ «Зборівгаз»……..40
3.1. Техніко-економічне обґрунтування проекту підвищення рівня захищеності інформаційно-комунікаційної системи ПАТ «Зборівгаз»……..40
3.2. Підвищення рівня захищеності засобами Active Directory……46
Висновки до третього розділу…….…….62
Висновки…….…...63
Список використаних джерел…….….66
Додатки……...73

# ВСТУП

**Актуальність** проблеми підвищення захищеності інформаційно-комунікаційних систем зростає зі швидкістю, пропорційною збільшенню обсягів та важливості даних, що зберігаються в інформаційних системах. А на сьогодні в Україні це дані про здоров'я, освіту, господарську та фінансову діяльність, державні документи тощо. Кожні 8 років обсяг цифрових даних у світі збільшується вдесятеро. За оцінками Forbes, світовий обсяг даних до 2025 р. становитиме 175 зеттабайтів. Методи визначення захищеності інформаційної системи поділяються на кількісні, та якісні. Об'єднати всі показники і отримати числовий результат допомагає математична теорія нечіткої логіки. Показниками кількісних методів є вартість ресурсів, критичність ресурсів, захищеність від окремої загрози, імовірність реалізації загрози через експлойт, рівень втрати цінності інформації від зловмисних дій, величина залишкового ризику. Існує значна кількість українських та міжнародних методик підвищення рівня захищеності інформаційних систем, що відображає інтерес науковців і практиків до даної проблеми. Однак немає загальноприйнятого методу підвищення захищеності. Ми вважаємо причиною цього бурхливий ріст кібербезпеки як нової галузі інформаційних технологій, необхідність у якій зростає експоненційно. Наші подальші дослідження будуть спрямовані на узагальнення методик підвищення рівня захищеності інформаційно-комунікаційної системи.

**Об'єктом** дослідження є захищеність інформаційно-комунікаційних систем.

**Предметом** дослідження є методи підвищення рівня захищеності інформаційно-комунікаційних систем.

**Завдання** дослідження:

1. Вивчити стан дослідженості проблеми підвищення рівня захищеності інформаційно-комунікаційної системи в українській та зарубіжній науковій літературі.
2. Розвинути та удосконалити методики підвищення рівня захищеності інформаційно-комунікаційної системи.

3. Розробити проект інформаційно-комунікаційної системи для ПАТ «Зборівгаз» з метою підвищення рівня захищеності інформації, що в ній циркулює.

**Методи** дослідження: аналіз, синтез, порівняння – для вивчення літератури; статистичні методи та методи прогнозування – для визначення загроз безпеці інформації; математичне моделювання, теорія ігор – для визначення профілю захищеності інформаційно-комунікаційної системи.

**Наукова новизна** дослідження:

- уточнено поняття захищеності інформаційно-комунікаційної системи;
- набули подальшого розвитку методики підвищення рівня захищеності інформаційно-комунікаційної системи.

**Практичне значення** дослідження:

- методика підвищення профілю захищеності інформаційно-комунікаційної системи з використанням теорії ігор може застосовуватись на підприємствах та в організаціях;
- проект інформаційно-комунікаційної системи ПАТ «Зборівгаз» доцільно реалізувати на підприємстві для підвищення захищеності інформації та удосконалення взаємодії підрозділів підприємства.

Результати роботи апробовані на VIII науково-технічній конференції «Інформаційні моделі, системи та технології» Тернопільського національного технічного університету імені Івана Пулюя.

Пояснювальна записка обсягом 123 сторінки містить 34 таблиці, 16 рисунків, 26 формул, 10 лістингів, 11 додатків. Список використаних джерел розміщується на 7 сторінках і містить 64 джерела.

# РОЗДІЛ 1. МЕТОДИКИ ВИЗНАЧЕННЯ РІВНЯ ЗАХИЩЕНОСТІ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНОЇ СИСТЕМИ

## 1.1. Аналіз і уточнення поняття захищеності інформаційно-комунікаційної системи

У сучасному науковому дискурсі вивчається поняття захищеності інформаційно-комунікаційних систем. Згідно із дослідженнями вчених Безбогова А. А., Біячуєва Т. А., Богуша В. М., Бурячок В. Л., Сичова Ю. Н., Юдіна О. К. [5; 6; 8; 37; 47] безпекою інформаційно-комунікаційної системи вважають здатність цих систем: 1. протистояти втручанням у процеси їх функціонування та викраденню, спотворенню, знищенню інформації; 2. виявляти, запобігати, нейтралізувати сторонні впливи на їх роботу.

У більшості праць, що стосуються питань інформаційної безпеки, в українських та міжнародних стандартах кібербезпеки розглядається не проблема захищеності інформаційно-комунікаційної системи, а поняття ризику інформаційної безпеки. Вчені Голобородько М. Ю., Курченко О. А., Кирись О. С. [13] у своєму дослідженні виявляють взаємозв’язок між цими поняттями та встановлюють, що рівень захищеності і відносний ризик доповнюють один одного до одиниці та пропонують розраховувати рівень захищеності за формулою $\eta = 1 - \bar{R}$.

Огляд публікацій із захисту інформації виявив, що поняття «захищеність інформаційної системи» належить до базових. Можливо тому більшість вчених не вважають за потрібне його досліджувати та сприймають як інтуїтивно зрозуміле. Е. А. Каліберда, А. А. Рибкін у своїй публікації [19] зазначають, що захищеність – це одна із характеристик якості, що найскладніше формалізується, призначення і функції якої тісно пов’язані з особливостями функціональної придатності інформаційної системи.

У своїй роботі захищеністю інформаційно-комунікаційної системи ми вважаємо її здатність забезпечувати цілісність, конфіденційність та доступність

інформації, виявляти зловмисні втручання та не допускати їх впливу на інформацію.

## 1.2. Комерційні методики підвищення рівня захищеності інформаційно-комунікаційної системи

Захист інформаційно-комунікаційної системи на сьогодні став актуальним для більшості підприємств, оскільки документація зберігається на серверах у базах даних, інформація передається каналами зв'язку. Порушення інформаційного забезпечення може спричинити навіть зупинку роботи компанії. У відповідь на такий запит на ринку з'явились компанії з кібербезпеки, які надають послуги із забезпечення визначеного рівня захищеності активів компанії. Розглянемо методики підвищення рівня захищеності інформаційно-комунікаційної системи, які розроблені у комерційному середовищі.

Компанія Science Soft (scnsoft.com) [59] надає послуги із забезпечення захисту корпоративної інформаційної системи на трьох рівнях. Перший рівень гарантує мінімальний захист і придатний для підприємств малого бізнесу у галузях, де рівень інформаційної безпеки не регламентований. Ключові точки першого рівня кіберзахисту забезпечують захист корпоративної мережі від найпоширеніших кіберзагроз, таких як фішингова атака (надсилання працівникам компанії листів чи повідомлень у мессенджерах із гіперлінками на сайти зловмисників, з вірусами у прикріплених файлах) та шкідливе програмне забезпечення (може потрапляти в мережу компанії через інтернет, з електронних листів, надсилатись через програми-шпіони, атаки на браузер тощо). Такий рівень захисту може бути прийнятним лише для невеликих та невідомих компаній, які не становлять цінності для хакерів.

Технічно мінімальний рівень захисту реалізується конфігуруванням фаєрволу та регулярним оновленням антивірусного забезпечення. Фаєрвол сканує мережевий трафік для відстеження аномальних пакетів. Антивірус захищає від відомого шкідливого програмного забезпечення – шпіонів, хробаків тощо, перевіряючи файли, які працівники відкривають та завантажують з

інтернету. Для забезпечення першого рівня захисту організації не потрібен відділ кібербезпеки, необхідні функції може виконувати відділ інформаційних технологій.

Рівень захищеності корпоративної інформаційно-комунікаційної системи потрібно перевіряти. Для першого рівня захищеності перевірку на вразливості та тестування на проникнення в корпоративну мережу достатньо проводити раз на рік.

Другий рівень захисту інформаційно-комунікаційної системи забезпечує захист корпоративної мережі від нецілеспрямованих атак, таких як шкідливе програмне забезпечення, спам, спуфінг тощо. Імовірність зазнати впливу нецілеспрямованої атаки дуже висока. Якщо стандарти кібербезпеки у галузі не регламентовані, багатьма вимогами до захисту активів на підприємствах можуть знехтувати, тому таку інформаційно-комунікаційну систему неважко скомпрометувати.

Для забезпечення кіберзахисту на другому рівні крім антивіруса і фаєрвола потрібно забезпечити такі компоненти:

- захист електронної пошти (сканування на наявність шкідливого програмного забезпечення, відфільтровування спаму), оскільки електронна пошта часто стає точкою входу зловмисників у корпоративну мережу;
- мережева сегментація: поділ на підмережі (наприклад, за департаментами), зв’язок між підмережами через фаєрвол, що унеможливлює проникнення шкідливого програмного забезпечення з однієї підмережі до іншої;
- система виявлення та попередження проникнень використовується для ідентифікації інформації про можливі інциденти безпеки та їх блокування до того як шкідливий вплив пошириться на мережу.

Для забезпечення другого рівня захищеності підприємство потребує у своєму штаті фахівців з інформаційної безпеки, відповідальних за виявлення та управління ризиками кібербезпеки, розробку політик захисту. Для цього на підприємстві має бути організований відділ кібербезпеки або потрібно

звернутись до провайдера послуг кібербезпеки. Організація підрозділу кібербезпеки доволі витратна, оскільки вимагає закупівлі обладнання, програмного забезпечення та найму кваліфікованих фахівців. У короткотривалій перспективі дешевшим рішенням є використання послуг провайдера кібербезпеки. Тоді компанії достатньо найняти одного фахівця з кібербезпеки, який координуватиме співпрацю із провайдером послуг інформаційного захисту. Фірма-провайдер послуг кібербезпеки розробляє стратегію захисту, проводить щоквартальне сканування на предмет виявлення вразливостей та щорічне тестування на проникнення для виявлення, зниження та управління ризиками кібербезпеки.

Сучасна стратегія кібербезпеки повинна враховувати захист персональних пристроїв (ноутбуків, планшетів, смартфонів), які належать працівникам та використовуються для виконання завдань компанії (BYOD), поширюватись на хмарні обчислення та включати навчання працівників стосовно допустимої поведінки в корпоративній мережі.

Ключова задача третього рівня кіберзахисту – захист корпоративної мережі від спрямованих атак. Це спеціально розроблені атаки саме для визначеної організації. Середні та великі компанії регульованих галузей, такі як банки, організації охорони здоров’я, урядові структури нерідко стають об’єктами кібератак.

Компанії регламентованих галузей повинні будувати систему кібербезпеки відповідно до вимог стандартів (HIPAA, PCI DSS тощо). Наступні компоненти кібербезпеки мають закривати всі можливі вектори атаки:

– безпека кінцевих пристроїв. Цей метод забезпечує захищений доступ будь-якого пристрою (смартфона, ноутбука тощо) до корпоративної мережі шляхом встановлення на нього клієнтського програмного забезпечення. Серверне програмне забезпечення безпеки кінцевих пристроїв встановлюється на корпоративний сервер управління. Така комбінація засобів дає змогу моніторити активність кожного користувача, який

віддалено підключається до мережі зі смартфона, планшета чи іншого пристрою.

– DLP програмне забезпечення використовується для попередження втрати інформації. Застосування цих заходів надзвичайно важливе для організацій фінансового сектору та галузі охорони здоров'я. DLP програмне забезпечення необхідне для даних кредитних карток, медичних карт пацієнтів тощо.
– SIEM (програмне забезпечення управління інформаційною безпекою та подіями) збирає інформацію, аналізує та видає звіти про активність в IT-середовищі. Основна перевага SIEM – централізоване опрацювання log-файлів з усіх комп'ютерів корпоративної мережі, що регламентується вимогами стандартів PCI DSS, HIPAA для забезпечення здатності відповідати у реальному часі на інциденти кібербезпеки.

Реалізувати третій рівень захищеності корпоративної мережі має підрозділ кібербезпеки, який працює цілодобово, або зовнішній провайдер послуг кібербезпеки. Основні заходи захисту інформаційного простору: розробка та впровадження стратегії безпеки, проведення аудиту вразливостей, щоквартальне тестування на проникнення, моніторинг загроз, організація відповіді на інциденти.

Моніторинг загроз включає перманентну перевірку корпоративної мережі та кінцевих пристроїв (серверів, безпровідних пристроїв, мобільних пристроїв тощо) на предмет загроз кібербезпеці, таких як вторгнення чи спроба викрадення даних. Моніторинг загроз набуває все більшої актуальності у зв'язку з тенденціями збільшення частки віддаленої роботи, впровадження BYOD, оскільки об'єкти, що підлягають захисту, далеко за межами периметру корпоративної мережі.

Відповідь на інциденти необхідна, щоб незначні події порушення інформаційної безпеки не стали великими проблемами з масштабними наслідками. Вчасно вжиті доцільні заходи дозволяють мінімальними ресурсами відновити працездатність корпоративних активів.

Для великих і середніх компаній сьогодні актуальне питання захисту активів у хмарах. Постають питання відсутності повного контролю захищеності інформації. Залежно від моделі хмарної інфраструктури фахівці кібербезпеки застосовують різні моделі захисту.

В умовах хмарних моделей IaaS (інфраструктура як сервіс) та PaaS (платформа як сервіс) стратегія безпеки подібна до захисту корпоративної мережі. Відмінності викликані лише фактором віддаленості. Важливе завдання компанії – обрати IaaS/ PaaS провайдера, який гарантує якісні послуги, надає сервери у хмарі і дозволяє реалізувати політику захисту виділених віртуальних машин. Перевіреними практиками кібербезпеки у такому випадку є шифрування даних, які зберігаються на віддалених серверах та передаються каналами зв’язку, моніторинг мережевого трафіку на предмет зловмисної активності, резервне копіювання даних.

Деякі вендори IaaS/ PaaS надають споживачам своїх послуг вбудовані сервіси кібербезпеки, але на сьогодні це винятки, а не правило. Наприклад, Microsoft Azure надає клієнтам різноманітні можливості захисту у хмарі, захист додатків від розповсюджених вразливостей. Хмарні сервіси Amazon (AWS) пропонують вбудований фаєрвол, можливості шифрування тощо.

Модель хмарної інфраструктури SaaS (програмне забезпечення як сервіс) передбачає послуги для використання, хостингу та захисту програмного забезпечення. Однак, деякі функції забезпечення кібербезпеки залишаються за компанією. Потрібно керувати доступом працівників до додатків, формувати ролі доступу відповідно до функцій підрозділів підприємства.

Таким чином, ми розглянули методики визначення рівня захищеності корпоративної інформаційно-комунікаційної системи, якими користуються фахівці-практики з кібербезпеки. Ці методики орієнтовані на реалізацію функцій, узгоджених з менеджментом та працівниками компанії. У наступних пунктах розглянемо методики визначення захищеності інформаційно-комунікаційної системи, які оперують числовими величинами.

## 1.3. Методики підвищення захищеності інформаційно-комунікаційної системи, затверджені стандартами з кібербезпеки

З метою врахування світового ландшафту ІТ-загроз та кращих практик захисту інформаційно-комунікаційних систем при розробці заходів кібербезпеки потрібно враховувати регламенти галузевих стандартів.

Тлумачний словник Оксфорда [62] визначає стандарти як рівень якості чи досягнень. Стандарти з кібербезпеки визначають як опис стратегії та політик підприємств із забезпечення інформаційної безпеки, виражений вимірюваними критеріями. Стандарти визначають, яких показників потрібно дотримуватись, щоб забезпечити необхідний рівень захищеності корпоративної інформації. Регламентуються основні кроки управління процесами інформаційних технологій.

Багато компаній із тих галузей народного господарства, у яких рівень захищеності інформаційно-комунікаційної системи підприємства не регламентований, приймають рішення впроваджувати загальні стандарти з кібербезпеки ISO/IEC 27001. Американським інститутом стандартизації розроблене сімейство стандартів NIST [53], яке спочатку застосовувалось для федеральних установ. На сьогодні стандарти NIST набули популярності та впроваджуються підприємствами різних галузей. Альтернативою деталізованим стандартам NIST Sybersecurity Framework та ISO27001став лаконічний стандарт Cyber Essentials, розроблений для компаній, що взаємодіють з урядом Великої Британії.

Банківські установи керуються галузевими стандартами PCI DSS та SWIFT Customer Security Control Framework (CSCF). Установи охорони здоров’я – стандартом HIPAA. Зберігання персональних даних громадян Євросоюзу регламентується стандартом GDPR.

ISO/IEC 27006:2011 Information technology. Security techniques. Requirements for bodies providing audit and certification of information security management systems (Інформаційні технології. Методи забезпечення безпеки. Вимоги до органів аудиту та сертифікації СУІБ) [54]. Вимоги, що містяться в

стандарті ISO / IEC 27006: 2011, повинні бути продемонстровані з точки зору компетентності та надійності будь-яким органом, який надає сертифікат СУІБ, а інструкції, що містяться в ISO / IEC 27006: 2011, надають додаткову інтерпретацію цих вимог для будь-якого органу, який надає сертифікат СУІБ.

НД ТЗІ 1.4-001-2000 «Типове положення про службу захисту інформації в автоматизованій системі» [27]. Цей нормативний документ системи технічного захисту інформації (НД ТЗІ) встановлює вимоги до структури та змісту нормативного документу, що регламентує діяльність служби захисту інформації в автоматизованій системі - “Положення про службу захисту інформації в автоматизованій системі”. НД ТЗІ призначений для суб’єктів відносин (власників або розпорядників АС, користувачів), діяльність яких пов’язана з обробкою в автоматизованих системах інформації, що підлягає захисту згідно з нормативно-правовими актами, а також для розробників комплексних систем захисту інформації в автоматизованих системах.

Використання цього НД ТЗІ створює умови для запровадження єдиного підходу щодо визначення і формування завдань, функцій, структури, повноважень служби захисту інформації, а також організації її робіт з захисту інформації впродовж всього життєвого циклу автоматизованих систем в державних органах, на підприємствах, в установах та організаціях усіх форм власності (далі – організаціях).

НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу, затверджений наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації СБ України від 28.04.99 р. № 22 [26]. Цей нормативний документ технічного захисту інформації (НД ТЗІ) визначає методологічні основи (концепцію) вирішення завдань захисту інформації в комп'ютерних системах і створення нормативних і методологічних документів, регламентуючих питання:

– визначення вимог щодо захисту комп'ютерних систем від несанкціонованого доступу;

- створення захищених комп'ютерних систем і засобів їх захисту від несанкціонованого доступу;
- оцінки захищеності комп'ютерних систем і їх придатності для вирішення завдань споживача.

Документ призначено для постачальників (розробників), споживачів (замовників, користувачів) комп'ютерних систем, які використовуються для обробки (в тому числі збирання, зберігання, передачі і т. д.) критичної інформації (інформації, що вимагає захисту), а також для державних органів, що здійснюють функції контролю за обробкою такої інформації.

Вивчення стандартів не дало вичерпної відповіді на питання побудови інформаційно-комунікаційної системи заданого рівня захищеності, оскільки положення стандартів дають можливість оцінити ризики кібербезпеки, а не захищеність [62, 11]. Ступінь ризику найчастіше оцінюється як низький, середній, високий чи критичний.

Поняття «захищеність» інформаційно-комунікаційної системи розкривається у НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу, затверджений наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації СБ України від 28.04.99 р. № 22 [28]. Цей нормативний документ установлює критерії оцінки захищеності інформації, оброблюваної в комп'ютерних системах, від несанкціонованого доступу.

Критерії є методологічною базою для визначення вимог з захисту інформації в комп'ютерних системах від несанкціонованого доступу; створення захищених комп'ютерних систем і засобів захисту від несанкціонованого доступу; оцінки захищеності інформації в комп'ютерних системах і їх придатності для обробки критичної інформації (інформації, що вимагає захисту).

Критерії надають порівняльну шкалу для оцінки надійності механізмів захисту інформації від несанкціонованого доступу, реалізованих в комп'ютерних системах, а також базу для розробки комп'ютерних систем, в яких мають бути реалізовані функції захисту інформації.

Критерії можуть застосовуватися до всього спектра комп'ютерних систем, включаючи однорідні системи, багатопроцесорні системи, бази даних, вбудовані системи, розподілені системи, мережі, об'єктно-орієнтовані системи та ін.

Цей документ призначено для постачальників (розробників), споживачів (замовників, користувачів) комп'ютерних систем, які використовуються для обробки (в тому числі збирання, зберігання, передачі і т. ін.) критичної інформації, а також для органів, що здійснюють функції оцінювання захищеності такої інформації та контролю за її обробкою. Рівень захищеності диференціюється за сімома рівнями гарантій (Г1-Г7), які є ієрархічними. Ієрархія рівнів захищеності інформаційно-комунікаційної системи відображає поступове зростання впевненості у тому, що ІТ-послуги протистоять актуальним загрозам, технічні механізми роботи коректно реалізовані та забезпечують належний рівень захищеності інформації.

За результатами огляду положень міжнародних стандартів інформаційної безпеки та нормативних документів України, що регламентують розробку та безпечне функціонування інформаційно-комунікаційних систем констатуємо, що питанню числового вимірювання рівня захищеності увага не приділяється. У наступному пункті визначимо наукові розробки щодо розв’язання задачі визначення рівня захищеності інформаційно-комунікаційної системи.

## 1.4. Методики підвищення рівня захищеності інформаційно-комунікаційної системи, розроблені науковцями.

Як засвідчив аналіз стандартів з кібербезпеки та роботи ІТ-компаній, у практичній діяльності із захисту інформації гостро постає питання вимірювання рівня захищеності інформаційно-комунікаційної системи. Науковці проводять дослідження цієї проблеми і пропонують різні напрями її вирішення, залежно від математичної моделі методу оцінювання.

У дослідженнях Белла [51], Біба, Лападула, Руссо, Ульмана, Харрісона розроблено моделі складних інформаційно-комунікаційних систем які становлять базу для вирішення проблем інформаційної безпеки. Науковці

М. З. Згуровський, Н. Д. Панкратова [18; 34; 64] використали методологію системного аналізу і розробили теорію дослідження безпеки структурованих систем. Сучасні інформаційно-комунікаційні системи мають відкриту архітектуру та використовують багаторівневий стек протоколів, захищеність інформації, що циркулює у таких системах, досліджували О. М. Новіков та А. О Тимошенко [31].

Оскільки події інформаційної безпеки мають імовірнісний характер, О. М. Новіков, А. О. Тимошенко, А М. Хнигічева [43] запропонували модель захищеності складних інформаційно-комунікаційних систем на базі логіко-ймовірнісного методу. Основна ідея дослідження – враховуючи загрози інформаційній безпеці та механізми протидії, обчислювати інтегральний показник захищеності інформаційно-комунікаційної системи. Цей показник відображає ймовірність перебування системи у захищеному стані. Інтегральний показник захищеності агрегує часткові показники захищеності інформаційно-комунікаційної системи, які відображають імовірності реалізації загроз окремим властивостям інформації: конфіденційності, цілісності та доступності.

Ймовірність виникнення небезпечного стану інформаційно-комунікаційної системи ($Н_с$) досліджують О. С. Можаєв, І. О. Рябінін, Є. Д. Соложенцев [24; 35; 61].

$$Н_с = P\{F(X_1, \dots, X_m) = 1\},$$

де $F(X_1, \dots, X_m)$ – функція від умови небезпечних станів системи.

Формула ймовірності виникнення безпечного стану $Б_с$:

$$Б_с = P\{F'(X_1, \dots, X_m) = 1\} = 1 - Н_с$$

Модель О. М. Новікова, А. О. Тимошенко, А М. Хнигічевої базується на моделі безпеки системи з повним перекриттям. Це означає, що в інформаційно-комунікаційній системі необхідний хоч би один засіб для забезпечення безпеки для кожного способу реалізації загроз (рис. 1.4).

На рис. 1.4 використано такі позначення: $t_1, \dots, t_5 \in T$; Т – множина загроз безпеці інформаційно-комунікаційної системи; $m_1, \dots, m_4 \in M$; М – множина механізмів захисту; $o_1, \dots, o_4 \in O$; О – множина активів підприємства.

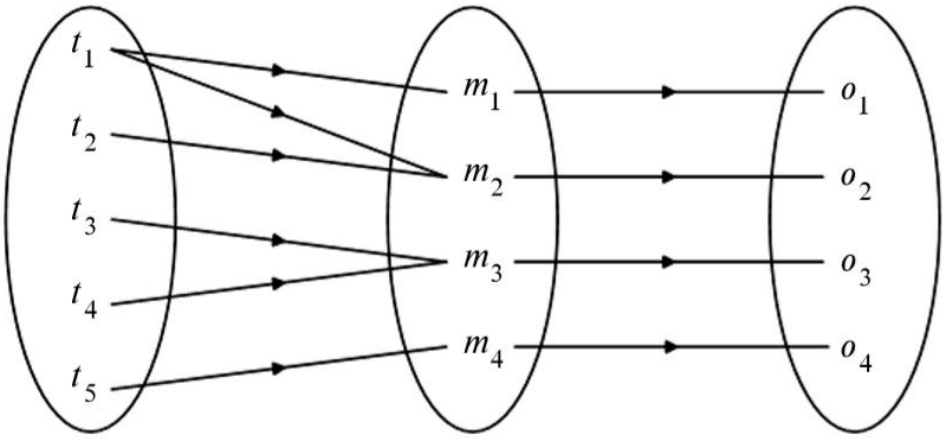


Рис. 1.4 – Модель безпеки інформаційно-комунікаційної системи з повним перекриттям

Наступним кроком визначення захищеності інформаційно-комунікаційної системи є локалізація загроз безпеки. Вплив кожної загрози оцінюється експертами у вигляді показника ефективності реалізації загрози. Формула 1.1 виражає показник ефективності реалізації $i$-ї загрози, спрямованої на порушення визначеної властивості інформації на $j$-му рівні стеку протоколів:

$$E_{ij} = Q_{ij}R_{ij}, \tag{1.1}$$

де $Q_{ij}$ – частка збитку, що привноситься $i$-ю загрозою в сумарний показник; $R_{ij}$ – ймовірність реалізації $i$-ї загрози.

У даній моделі множина загроз T представлена множиною показників ефективності їх реалізації $E = \{E_i\}, i \in \{1, \dots, L\}$, де $E_i$ – показник ефективності реалізації $i$-ї загрози; $L$ – кількість загроз у моделі.

Після ідентифікації загроз безпеки інформаційно-комунікаційної системи вибирають адекватні механізми захисту. Показником працездатності механізму захисту є ймовірність запобігання з його допомогою визначеній загрозі:

$$P_{M_i} = M_i K_i,$$

де параметр $M_i$ може набувати значень 0 або 1 і визначає наявність чи відсутність захисту від $i$-ї загрози, $K_i$ – коефіцієнт міцності механізму захисту від $i$-ї загрози.

У моделі визначення рівня захищеності інформаційно-комунікаційної системи множина механізмів захисту $M$ задається у вигляді

$$M = \{M_i\}, i \in \{1, \dots, L\}.$$

Модель оцінювання ймовірності збереження інформаційно-комунікаційною системою захищеного стану *P* визначається функцією множини загроз безпеці системи *T*, вираженими в показниках ефективності їх реалізації *E* і множини механізмів захисту *M* з коефіцієнтами надійності *K*:

$$P = f(E, M, K).$$

Захищеність інформації означає її конфіденційність, цілісність і доступність. Позначимо імовірності збереження конфіденційності, цілісності та доступності інформації в інформаційно-комунікаційній системі відповідно $P_к$, $P_ц$, $P_д$. Для визначення простору захищеності задають систему координат з координатними векторами, довжини яких дорівнюють $P_к$, $P_ц$, $P_д$ (рис. 1.3.2).

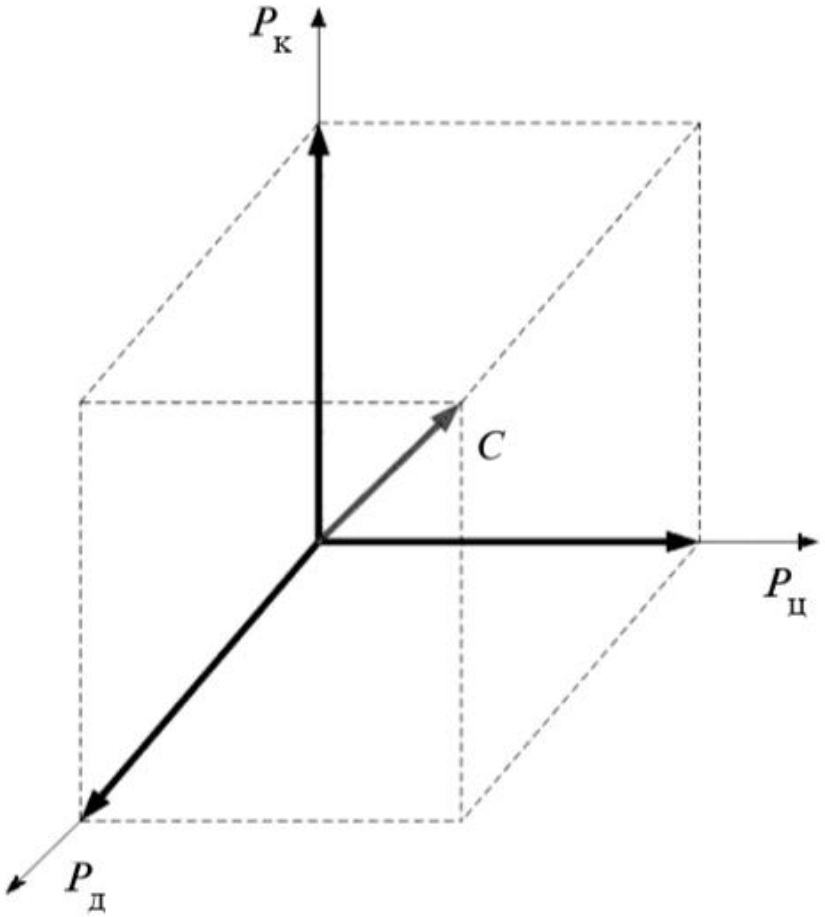


Рис. 1.5 – Простір захищеності інформаційно-комунікаційної системи

Комплексний показник захищеності інформації *C* є векторною сумою ймовірностей збереження конфіденційності, цілісності і доступності інформації:

$$|C| = \sqrt{(P_д^2 + P_ц^2 + P_к^2)}.$$

Доступність, цілісність та конфіденційність інформації виражені формулами нижче.

$$T_{i1}(M) = \sum_{j=1}^{N}\left( E_{j1}\prod_{k=1}^{j-1}(1 - E_{k1})\prod_{k=1}^{j}(1 - M_{k1}K_{k1}) \right),$$

$$T_{i2}(M) = \sum_{j=1}^{N}\left( E_{j2}\prod_{k=1}^{j-1}(1 - E_{k2})\prod_{k=1}^{j}(1 - M_{k2}K_{k2}) \right),$$

$$T_{i3}(M) = \sum_{j=1}^{N}\left( E_{j3}\prod_{k=1}^{j-1}(1 - E_{k3})\prod_{k=1}^{j}(1 - M_{k3}K_{k3}) \right).$$

Вирази для визначення захищеності за умови реалізації *j*-ї загрози на *i*-му рівні стеку протоколів для доступності, цілісності та конфіденційності інформації:

$$P_{i1}(M) = \prod_{j=1}^{N}(1 - E_{j1}) +$$

$$+\sum_{j=1}^{N}\left[ E_{j1}\prod_{k=1}^{j-1}(1 - E_{k1})\left( \sum_{k=1}^{j} M_{k1}K_{k1}\prod_{l=k+1}^{j}(1 - M_{l1}K_{l1}) \right)\right],$$

$$P_{i2}(M) = \prod_{j=1}^{N}(1 - E_{j2}) +$$

$$+\sum_{j=1}^{N}\left[ E_{j2}\prod_{k=1}^{j-1}(1 - E_{k2})\left( \sum_{k=1}^{j} M_{k2}K_{k2}\prod_{l=k+1}^{j}(1 - M_{l2}K_{l2}) \right)\right],$$

$$P_{i3}(M) = \prod_{j=1}^{N}(1 - E_{j3}) +$$

$$+\sum_{j=1}^{N}\left[ E_{j3}\prod_{k=1}^{j-1}(1 - E_{k3})\left( \sum_{k=1}^{j} M_{k3}K_{k3}\prod_{l=k+1}^{j}(1 - M_{l3}K_{l3}) \right)\right].$$

Із врахуванням усієї множини загроз попередні вирази набудуть вигляду:

$$P_1(M) = \prod_{i=1}^{L_1}\left(\prod_{j=1}^{N}(1 - E_{ij1}) + \sum_{j=1}^{N}\left[E_{ij1}\prod_{k=1}^{j-1}(1 - E_{ik1}) \times \right.\right.$$

$$\left.\left. \times \left(\sum_{k=1}^{j} M_{ik1}K_{ik1}\prod_{l=k+1}^{j}(1 - M_{il1}K_{il1})\right)\right]\right),$$

$$P_2(M) = \prod_{i=1}^{L_2}\left(\prod_{j=1}^{N}(1 - E_{ij2}) + \sum_{j=1}^{N}\left[E_{ij2}\prod_{k=1}^{j-1}(1 - E_{ik2}) \times \right.\right.$$

$$\left.\left. \times \left(\sum_{k=1}^{j} M_{ik2}K_{ik2}\prod_{l=k+1}^{j}(1 - M_{il2}K_{il2})\right)\right]\right),$$

$$P_3(M) = \prod_{i=1}^{L_3}\left(\prod_{j=1}^{N}(1 - E_{ij3}) + \sum_{j=1}^{N}\left[E_{ij3}\prod_{k=1}^{j-1}(1 - E_{ik3}) \times \right.\right.$$

$$\left.\left. \times \left(\sum_{k=1}^{j} M_{ik3}K_{ik3}\prod_{l=k+1}^{j}(1 - M_{il3}K_{il3})\right)\right]\right),$$

де $L_1$, $L_2$, $L_3$ – кількості загроз із множини $T$ для конфіденційності, доступності та цілісності інформації, $N$ – кількість рівнів стеку протоколів в інформаційно-комунікаційній системі.

Модель, запропонована у праці А. М. Хнигічевої, О. М. Новікова, А. О. Тимошенка дає змогу визначити захищеність інформаційно-комунікаційної системи з точки зору збереження цілісності, конфіденційності та доступності інформації. Також модель визначає інтегральний показник захищеності.

**Висновки до першого розділу**

Питання підвищення рівня захищеності інформаційно-комунікаційних систем актуальне як для ІТ-компаній, що забезпечують кібербезпеку, їх клієнтів, так і для наукового дискурсу.

У практиці захисту інформації користуються спрощеною шкалою оцінювання захищеності, яка за допомогою якісних характеристик визначає базовий, середній та високий рівень захищеності інформаційно-комунікаційної системи. Такий же підхід до оцінювання захищеності викладений в українських та міжнародних стандартах з кібербезпеки.

Науковці розв’язують питання підвищення рівня захищеності інформації з використанням різних математичних інструментів, зокрема логіко-імовірнісного інструментарію. У нашому дослідженні основою кількісного оцінювання та підвищення рівня захищеності є модель А. М. Хнигічевої, О. М. Новікова, А. О. Тимошенка. У наступному розділі ми удосконалимо її, враховуючи різноманітність, функціонал та вартість сучасних інструментів захисту інформації.

# РОЗДІЛ 2. ЗАСТОСУВАННЯ ТЕОРІЇ ІГОР ДЛЯ ВИБОРУ ІНСТРУМЕНТІВ ЗАХИСТУ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНОЇ СИСТЕМИ

## 2.1. Поняття профілів захищеності інформаційно-комунікаційної системи

Поняття профілів захищеності пов’язано з тим, що інформаційно-комунікаційна система постійно змінюється відповідно до появи нових задач, які повинна розв’язувати організація. Захищеність інформаційно-комунікаційної системи – у практиці величина непостійна. Можна говорити про певний рівень захищеності лише у визначений момент часу. Якщо навіть припустити, що протягом відрізку часу інформаційно-комунікаційна система залишалась незмінною, за цей час зміниться ландшафт загроз і знизить захищеність системи.

Поняття профілів захищеності інформаційно-комунікаційної системи визначається у нормативних документах для технічних систем захисту інформації [26-30] та отримало наукову інтерпретацію у роботі В. Б. Толубко, О. А. Курченко, А. В. Шевченко [39].

Профілі захищеності диференціюються за рівнями захисту інформації в інформаційно-комунікаційній системі і позначаються у [39] варіант 1 – варіант 5 від мінімального до максимального рівня захисту. Пріоритетною властивістю інформації, яка має бути захищена, авторами визначається цілісність. Стандартним профілем захищеності (варіант 1) визначається 1.Ц.1 чи 1.Ц.2 [39].

1.Ц.1 = { НР-1, НИ-1, НК-1, НО-1, НЦ-1, НТ-1 }
1.Ц.2 = { ЦА-2, ЦО-1, НР-2, НИ-2, НК-1, НО-1, НЦ-1, НТ-1 }

Варіант 2 – профіль захищеності, який убезпечує не лише від загроз цілісності інформації, але й від загроз доступності. Такий профіль визначений в 1.ЦД.1 та 1.ЦД.2-4 [39].

1.ЦД.1={ЦА-1,ЦО-1, ДР-1, ДВ-1, НР-2, НИ-2, НК-1, НО-1, НЦ-1, НТ-1 }
1.ЦД.2={ЦА-1,ЦО-1, ДР-2, ДС-1, ДЗ-1, ДВ-2, НР-2, НИ-2, НК-1, НО-1, НЦ-1, НТ-2 }
1.ЦД.3={ЦА-1,ЦО-1, ДР-2, ДС-2, ДЗ-2, ДВ-2, НР-3, НИ-2, НК-1, НО-1, НЦ-2, НТ-2 }
1.ЦД.4={ЦА-1,ЦО-1, ДР-2, ДС-3, ДЗ-3, ДВ-3, НР-4, НИ-2, НК-1, НО-1, НЦ-2, НТ-2 }

Варіант 3 – профіль захищеності, який убезпечує від загроз цілісності, доступності і конфіденційності інформації. Використовується профіль захищеності 1.КЦД.1-4 [39].

1.КЦД.1 = { КА-1, КО-1, ЦА-1, ЦО-1,
ДР-1, ДВ-1, НР-2, НИ-2, НК-1, НО-1, НЦ-1, НТ-1 }
1.КЦД.2 = { КА-1, КО-1, ЦА-1, ЦО-1,
ДР-2, ДС-1, ДЗ-1, ДВ-2, НР-2, НИ-2, НК-1, НО-1, НЦ-1, НТ-2 }
1.КЦД.3 = { КА-1, КО-1, ЦА-1, ЦО-1,
ДР-2, ДС-2, ДЗ-2, ДВ-2, НР-3, НИ-2, НК-1, НО-1, НЦ-2, НТ-2 }
1.КЦД.4 = { КА-1, КО-1, ЦА-1, ЦО-1,
ДР-2, ДС-3, ДЗ-3, ДВ-3, НР-4, НИ-2, НК-1, НО-1, НЦ-2, НТ-2 }

Варіант 4 – локально-мережевий профіль захищеності. Гарантує конфіденційність, цілісність, доступність інформації при підключенні до локальної мережі. Використовуються профілі 2.КЦД.1-5 [39].

2.КЦД.1 = { КД-2, КО-1, ЦД-1, ЦО-1, ДР-1, ДВ-1,
НР-2, НИ-2, НК-1, НО-2, НЦ-2, НТ-2 }
2.КЦД.2 = { КД-2, КА-2, КО-1, ЦД-1, ЦА-2, ЦО-1, ДР-1, ДВ-1,
НР-2, НИ-2, НК-1, НО-2, НЦ-2, НТ-2 }
2.КЦД.3 = { КД-2, КА-2, КО-1, КК-1, ЦД-1, ЦА-3, ЦО-2, ДР-2, ДС-1, ДЗ-1, ДВ-2,
НР-3, НИ-2, НК-1, НО-2, НЦ-3, НТ-2 }
2.КЦД.4 = { КД-3, КА-3, КО-1, КК-1, ЦД-1, ЦА-3, ЦО-2, ДР-3, ДС-2, ДЗ-2, ДВ-2,
НР-4, НИ-2, НК-1, НО-3, НЦ-3, НТ-2 }
2.КЦД.5 = { КД-4, КА-4, КО-1, КК-2, ЦД-4, ЦА-4, ЦО-2, ДР-3, ДС-3, ДЗ-3, ДВ-3,
НР-5, НИ-2, НК-2, НО-3, НЦ-3, НТ-2 }

Варіант 5 - глобально-мережевий профіль захищеності. Забезпечує захищеність при підключенні до інтернет та для розподілених інформаційно-комунікаційних систем. Використовуються профілі 3.КЦД.1-5 [39].

3.КЦД.1={КД-2, КО-1, КВ-1, ЦД-1, ЦО-1, ЦВ-1, ДР-1, ДВ-1,
НР-2, НИ-2, НК-1, НО-2, НЦ-2, НТ-2, НВ-1 }
3.КЦД.2={КД-2, КА-2, КО-1, КВ-2, ЦД-1, ЦА-2, ЦО-1, ЦВ-2, ДР-1, ДВ-1,
НР-2, НИ-2, НК-1, НО-2, НЦ-2, НТ-2, НВ-1 }
3.КЦД.3={КД-2,КА-2,КО-1,КК-1, КВ-3, ЦД-1,ЦА-3,ЦО-2,ЦВ-2, ДР-2,ДС-1,ДЗ-1,ДВ-2,
НР-3, НИ-2, НК-1, НО-2, НЦ-3, НТ-2, НВ-2 }
3.КЦД.4={КД-3,КА-3,КО-1,КК-1,КВ-3, ЦД-1,ЦА-3,ЦО-2,ЦВ-2, ДР-3,ДС-2,ДЗ-2,ДВ-2,
НР-4, НИ-2, НК-1, НО-3, НЦ-3, НТ-2, НВ-2, НА-1, НП-1 }
3.КЦД.5={КД-4,КА-4,КО-1,КК-2,КВ-4, ЦД-4,ЦА-4,ЦО-2,ЦВ-3, ДР-3,ДС-3,ДЗ-3,ДВ-3,
НР-5, НИ-2, НК-2, НО-3, НЦ-3, НТ-2, НВ-2, НА-1, НП-1 }

Інформаційно-комунікаційна система трансформується відповідно до розвитку підприємства, з’являються нові функції, тому повинен змінюватись і

профіль захищеності. Нарощувати арсенал функцій захисту можна поступово від профілю Варіант 1 до профілю Варіант 5.

## 2.2. Вибір інструментів захисту інформаційно-комунікаційної системи на базі теорії ігор

Розглянемо інформаційно-комунікаційну систему, захист якої можливий з використанням різноманітного програмного забезпечення та апаратного обладнання, профіль захищеності обирається адміністратором мережі з урахуванням обмеженого кошторису щодо їх придбання та експлуатації.

Корпоративна мережа має вразливості, що можуть призвести до порушення цілісності, конфіденційності та доступності інформації, внаслідок чого організації завдається матеріальна шкода зловмисником. Вважатимемо, що загрози корпоративній мережі відомі (із статистичних даних та бібліотек атак CAPEC, ISACA, OWASP Top Ten та ін.).

Визначимо завдання вибору профілю захищеності інформаційно-комунікаційної системи: при заданому векторі загроз обрати оптимальну комбінацію засобів захисту корпоративної мережі від локальних та мережних загроз за критерієм мінімізації потенційних збитків від атак при обмеженому бюджеті організації.

Враховуючи вектор загроз інформаційній безпеці та різноманіття засобів захисту корпоративної мережі, а також беручи до уваги ймовірнісно-грошові потоки, поставлену проблему можна вирішити за допомогою математичного апарату теорії ігор, який дозволяє: сформувати задачу захисту інформаційно-комунікаційної системи в математичному вигляді, щоб скористатися критеріями відшукання оптимальних стратегій захисту; оцінити витрати на забезпечення безпеки інформаційного ресурсу, збитки від реалізації атаки та з урахуванням цих даних прийняти оптимальне рішення; обрати ефективний профіль захищеності.

Дослідження базується на тому, що адміністратор безпеки інформаційно-комунікаційної системи та зловмисник є гравцями в деякій грі, де кожна сторона

робить свої кроки, вибираючи стратегію поведінки, прагнучи оптимально забезпечити свій інтерес. Метою гри є пошук оптимальної стратегії поведінки як з точки зору адміністратора інформаційної безпеки, так і з точки зору зловмисника, адже обидві сторони намагаються звести до мінімуму свої невдачі.

На першому кроці математичного моделювання для пошуку оптимальної стратегії захисту інформаційно-комунікаційної системи проведемо математичну дуельну бінарну гру двох сторін, однією з яких є система захисту інформації, а іншою – можливі атаки зловмисників. Оскільки метою є визначення адміністратором безпеки оптимальної стратегії захисту, а цілі зловмисників, що атакують, по суті, не важливі, то можна вважати, що зловмисник захоплений бажанням завдати якомога більшої шкоди системі.

Стратегії адміністратора інформаційної безпеки позначимо рядками $S_i$ (i=1,...,n) матриці гри, а стратегії зловмисника – її стовпцями $A_j$(j =1,...,m). До стратегій адміністратора належать різні засоби захисту інформації та всі можливі профілі захищеності, до стратегій зловмисника – різноманітні види локальних та мережних атак. Елементами матриці є ймовірності успішної реалізації атаки зловмисником $p_{ij}$ за умови, що використовується один з можливих профілів захищеності.

Вважаємо, що елементи профілів захищеності незалежні один від одного, тобто робота або несправність одного з них ніяк не впливає на інший. Тому, виходячи з теореми, що ймовірність поєднання кількох незалежних подій дорівнює добутку ймовірностей цих подій, ймовірність успішної реалізації атаки при використанні різних профілів захищеності має вигляд:

$$P(AB) = P(A) \cdot P(B)$$

При такому припущенні одержимо матрицю для гри двох гравців, варіант якої подано у табл. 2.2, де рядок $S_0$ виражає ймовірність успішної реалізації атаки при використанні поточних (апріорі використовуваних) засобів захисту інформації.

Вважаємо, що також відомі ймовірності проведення кожного типу атак $p_j^{(A)}$, значення яких залежить від статистичних даних, а також оцінені вартість

кожного із засобів захисту $X_i(i = 1,...,n)$ та розмір збитку від реалізації певної атаки $Y_j(j = 1,...,m)$ .

Таблиця 2.2 – Початкова матриця для гри двох гравців

| | $A_1$ | $A_2$ | … | $A_m$ |
|---|---|---|---|---|
| $S_0$ | $p_{01}$ | $p_{02}$ | … | $p_{0m}$ |
| $S_1$ | $p_{11}$ | $p_{12}$ | … | $p_{1m}$ |
| $S_2$ | $p_{21}$ | $p_{22}$ | … | $p_{2m}$ |
| ... | ... | ... | … | ... |
| $S_n$ | $p_{n1}$ | $p_{n2}$ | … | $p_{nm}$ |
| $S_{1+2}$ | $p_{11} \cdot p_{21}$ | $p_{12} \cdot p_{22}$ | | $p_{1m} \cdot p_{2m}$ |
| … | … | … | … | … |

Процесу оцінювання ймовірностей реалізації загроз і вразливостей необхідно приділяти особливу увагу. Виконання даного етапу можна доручити як групі внутрішніх співробітників, так і спеціальним експертам. Ми сформували групу експертів із кількох міжнародних IT-компаній. Також необхідно використовувати не тільки експертні дані, але й враховувати статистику загроз, яку проводять аналітичні агентства з інформаційної безпеки. Ми базуємось на звітах з кібербезпеки за останні роки [49; 64].

Для того, щоб приймати рішення про доцільність впровадження певного профілю захищеності інформаційно-комунікаційної системи, потрібно враховувати потенційні збитки за умов реалізації атаки, потенційний виграш при впровадженні системи захисту інформації, а також сукупні витрати на впровадження та підтримання працездатності системи захисту інформації.

Наступним кроком математичного моделювання є вирішення поставленої задачі за допомогою фінансово-економічної оцінки інвестицій, а саме показника повернення інвестицій (ROI) для кожного елемента табл. 2.2, який розраховується так:

$$ROI_{ij} = benefits_{ij} - costs_i ,$$

де $benefits_{ij}$ – оцінка тієї користі (тобто очікуваного зниження потенційних збитків), яку приносить впровадження і-го профілю захищеності інформаційно-комунікаційної системи при реалізації j-ї атаки; $costs_i$ – витрати на впровадження та підтримку працездатності і-го профілю захищеності.

Оцінка користі розраховується за такою формулою:

$$benefits_{ij} = R_0j - R_{ij},$$

де $R_{0j}$ – потенційні збитки при реалізації j-ї атаки при використанні поточних (апріорі використовуваних) засобів захисту інформації; $R_{ij}$ – потенційні збитки при реалізації j-ї атаки з впровадженням і-го профілю захищеності.

Потенційні збитки розраховуються з урахуванням ймовірності реалізації атаки зловмисником $p_{ij}$ (за умови, що атака буде проведена зі стовідсотковою ймовірністю), ймовірності проведення певного типу атак $p_j^{(A)}$, а також розміру передбачуваного збитку від реалізації певної атаки $Y_j$.

Враховуючи попередні формули і позначення, одержимо вираз:

$$R_{ij} = p_{ij} \cdot p_j^{(A)} \cdot Y_j$$

Витрати на впровадження та супровід і-го профілю захищеності інформаційно-комунікаційної системи дорівнюють $X_i$.

Отже, формула для розрахунку ROI набуде вигляду:

$$ROI_{ij} = p_{0j} \cdot p_j^{(A)} \cdot Y_j - p_{ij} \cdot p_j^{(A)} \cdot Y_j - X_i = (p_{0j} - p_{ij}) \cdot p_j^{(A)} \cdot Y_j - X_i$$

Розрахувавши ROI для кожного елемента початкової матриці, отримаємо нову матрицю гри (табл. 2.3), де елементи матриці є кількісною характеристикою вигоди впровадження обраного профілю захищеності відносно певного типу атаки.

Таблиця 2.3 – Матриця гри двох гравців після визначення ROI для кожного елемента початкової матриці

| | $A_1$ | $A_2$ | … | $A_m$ |
|---|---|---|---|---|
| $S_0$ | $ROI_{01}$ | $ROI_{02}$ | … | $ROI_{0m}$ |
| $S_1$ | $ROI_{11}$ | $ROI_{12}$ | … | $ROI_{1m}$ |
| $S_2$ | $ROI_{21}$ | $ROI_{22}$ | … | $ROI_{2m}$ |
| ... | ... | ... | … | ... |
| $S_n$ | $ROI_{n1}$ | $ROI_{n2}$ | … | $ROI_{nm}$ |

Наступним кроком є розв’язання отриманої матриці. Проведені дослідження [14] показали, що для наближеного розв’язання таких матриць може використовуватися ітеративний метод Брауна-Робінсон [4].

Враховуючи вищевикладене, для існуючої матриці розглянемо нескінченний процес повторення даної гри, при якому кожен з гравців на кожному кроці передбачає, що противник вибере змішану стратегію, яка визначається частотами появ чистих стратегій на попередніх кроках, а сам обирає чисту стратегію, що забезпечує найкращий результат при даному припущенні.

Нехай зроблено k повторень гри, в яких перший гравець вибирав чисті стратегії $i_1,...,i_k$ , а другий – $j_1,..., j_k$ . Тоді, відповідно до вищесказаного, перший гравець вибере на (k + 1) -му кроці стратегію $i_{k+1}$ з такою умовою:

$$\frac{1}{k}\sum_{v=1}^{k} a_{i_{k+1}j_v} = max_{1\le i\le n}\sum_{v=1}^{k} a_{ij_v} = v_1(k),$$

де k – номер кроку; $a_{ij}$ – елемент матриці гри; n – кількість стратегій першого гравця; v – ціна гри.

А другий гравець обере стратегію $j_{k+1}$ з умовою:

$$\frac{1}{k}\sum_{v=1}^{k} a_{i_v j_{k+1}} = max_{1\le j\le m}\sum_{v=1}^{k} a_{i_v j} = v_2(k),$$

де k – номер кроку; $a_{ij}$ – елемент матриці гри; m – кількість стратегій другого гравця; v – ціна гри.

У випадку, якщо стратегій, які відповідають визначеним умовам, декілька, гравець вибирає будьяку з них.

Таким чином, ітеративний процес збігається до істинного значення гри, тобто:

$$lim_{k\to\infty} v_1(k) = lim_{k\to\infty} v_2(k) = v$$

Це означає, що уявні платежі $v_1(k)$ та $v_2(k)$ прагнуть до справжньої ціни гри v, що для розглянутої задачі є оптимальною стратегією побудови системи захисту інформації.

Слід зазначити, що збіжність цього ітеративного методу повільна, але сам метод є достатньо простим і адекватно відображає набуття гравцями досвіду в результаті багатьох повторень конфліктної ситуації. Очікувати від методу Брауна-Робінсон оцінок, близьких до дійсних значень, можна лише при великій кількості ітерацій.

Ми провели дослідження взаємовідносин між атакувальником корпоративної інформаційно-комунікаційної системи та адміністратором безпеки підприємства ПАТ “Зборівгаз”. Предметом діяльності Товариства є: безперебійне газопостачання; виконання робіт по будівництву і проектуванню нових, розширенню діючих газових розподільчих мереж. Проблема інформаційного захисту стратегічних об’єктів інфраструктури є актуальною для України. Це засвідчила серія кібератак на електростанції у 2015 р., проведена за допомогою шкідливого програмного забезпечення BlackEnergy. В результаті ураження велика кількість населених пунктів залишилась на кілька годин без електропостачання.

Змоделюємо математичну дуельну бінарну гру двох сторін, однією з яких є система захисту інформації ПАТ “Зборівгаз”, а іншою – атаки зловмисників.

Згідно із методикою, розробленою у [14], в якості стратегій адміністратора безпеки будемо розуміти рядки $S_i$ (i=1,…, n) матриці гри, а в якості стратегій зловмисника – її стовпці $A_j$ (j=1,…,m).

Стратегіями зловмисника є види локальних та мережевих атак, що найімовірніше можуть бути реалізовані на ПАТ “Зборівгаз”. Визначимо найімовірніші з них, базуючись на висновках джерел [3; 4].

Поширеною атакою є спуфінг – підміна трафіку в мережі чи контента на сайті таким, що вигідний зловмиснику. У м. Києві викрито шахрайську офлайн-схему, у якій споживачам газу кидали у поштові скриньки рахунки на оплату, що містили реквізити банківського рахунку шахраїв. Постраждало кількасот людей. Ця та подібні схеми можуть реалізуватись і онлайн, якщо не вжити ефективних засобів захисту корпоративної інформації.

DDOS-атаки є на сьогодні однією із найрозповсюдженіших атак на корпоративні сервери. Однією із гучних DDOS-атак в Україні стало перевантаження запитами сервера Укрзалізниці, що призвело до відсутності доступу до сервісів протягом доби. Сьогодні велика кількість DDOS-атак проводиться із ботнетів, побудованих на інфраструктурі інтернету речей. Таким є ботнет Mirai, утворений скомпрометованими маршрутизаторами, відеокамерами, dvd-програвачами, смарт-телевізорами, безпровідними презентаційними системами та іншими пристроями, підключеними до мережі. Їх кількість сягає 500 000.

Фінансові дані, особиста інформація клієнтів ПАТ “Зборівгаз” зберігається у базах даних. Тому значну імовірність мають атаки ін’єкції коду, зокрема SQL-ін’єкції. Цей вид атаки надає найрізноманітніші можливості зловмиснику, які обмежуються лише засобами мови програмування та правами доступу до бажаних активів організації. Наприклад, можна переглядати усі записи бази даних, доступні для поточної сесії користувача, під іменем якого зловмиснику вдалось отримати доступ. Можна емулювати підроблені відповіді сервера на запити клієнта. Дана атака особливо небезпечна тим, що будь-хто, хто має доступ до web-сайту організації і здатний вводити дані в текстові поля, потенційно може стати джерелом атак за допомогою ін’єкцій SQL.

Атаки зловживання функціональністю не потребують додаткових засобів та спеціальних знань, тому імовірність їх здійснення висока. Суть цих атак у тому, що штатні засоби програми використовуються із зловмисною метою. Наприклад, чат чи електронна пошта можуть бути використані для надсилання усім контактам адреси веб-сайту, при переході на який завантажуватиметься шкідливий експлойт. Зловживання функціональністю більш характерне для інсайдерських атак. Атака інсайдера в сучасному виконанні – це дія злочинця він імені облікового запису користувача корпоративної інформаційно-комунікаційної системи.

Зловмисник може отримати неавторизований доступ не до аккаунта користувача, як у попередньому виді атаки, а до операційної системи. Тоді

реалізується атака “ОС-коммандінг”. Якщо такий доступ був отриманий через веб-сервер, то зловмисні команди можна виконувати прямо із браузера. Для ПАТ “Зборівгаз” існує імовірність завантаження зловмисного коду на скомпрометований сервер і його запуску, оскільки однією із найпоширеніших кіберзагроз останніх років є фішинг, від якого постраждало й багато українських підприємств.

До стратегій адміністратора ми відносимо використання засобів захисту інформації. Firewall – міжмережевий екран – пристрій, призначений для управління доступом до інтернет, шифрування даних та передачі мережевого трафіку між зонами різного рівня обмеження доступу відповідно до політик безпеки. В роботі інформаційно-комунікаційної системи ПАТ “Зборівгаз” міжмережевий екран забезпечує WAN інтерфейси для під’єднання до різних ISP, інтерфейс LAN для з’єднання з внутрішньою мережею ПАТ "Зборівгаз", DMZ інтерфейс для реалізації зони серверів загального доступу, підтримку технології NAT, управління доступом до локальної мережі та зони серверів загального доступу і захист від атак іззовні.

Хмарні сервіси захисту від DDOS (наприклад, Incapsula), гарантують захист від розподілених атак на відмову в обслуговуванні та зменшують інтенсивність атаки за лічені хвилини.

Антивірус захищає активи підприємства від шкідливого програмного забезпечення, яке може потрапити на комп’ютери ПАТ "Зборівгаз" з інтернет чи із знімних носіїв інформації.

Апаратні засоби біометричної ідентифікації користувачів дозволяють швидко та безпомилково проводити автентифікацію на робочих місцях ПАТ "Зборівгаз" за ознаками, які складно підробити.

Програмно-апаратний криптографічний комплекс захищає трафік від перегляду при перехопленні, оскільки відновити зашифроване повідомлення зловмисникові не вдасться.

Елементами матриці математичної гри, яку ми провели для розробки стратегії кіберзахисту ПАТ "Зборівгаз" є ймовірності успішної реалізації атаки зловмисником, що визначені методом експертних оцінок (табл. 2.4).

Таблиця 2.4 – Матриця дуельної бінарної гри адміністратора інформаційної безпеки ПАТ“Зборівгаз” та порушника безпеки інформації.

| | ***спуфінг*** | ***DDOS*** | ***ін'єкція коду*** | ***зловживання функціональністю*** | ***ОС-коммандінг*** |
|---|---|---|---|---|---|
| фаєрвол | 0,34 | 0,46 | 0,27 | 0,06 | 0,14 |
| антивірус | 0,43 | 0,38 | 0,27 | 0,16 | 0,17 |
| хмарний захист | 0,36 | 0,23 | 0,24 | 0,19 | 0,14 |
| біометрія | 0,63 | 0,38 | 0,38 | 0,27 | 0,21 |
| крипторгафія | 0,7 | 0,51 | 0,57 | 0,35 | 0,31 |

Оцінена вартість (грн) кожного із засобів захисту $X_i$ (i=1,…,5): (5800, 20000, 21000, 33000, 50000) та розмір передбачуваного збитку від реалізації певної атаки $Y_j$ (j=1,…,5): (80000, 100000, 90000, 150000, 170000).

Таблиця 2.5 – Матриця гри адміністратора інформаційної безпеки ПАТ “Зборівгаз” та порушника безпеки інформації після обчислення ROI

| | ***спуфінг*** | ***DDOS*** | ***ін'єкція коду*** | ***зловживання функціональніс-тю*** | ***ОС-комман-дінг*** |
|---|---|---|---|---|---|
| фаєрвол | 21400 | 40200 | 18500 | 3200 | 18000 |
| антивірус | 14400 | 18000 | 4300 | 4000 | 8900 |
| хмарний захист | 7800 | 2000 | 600 | 7500 | 2800 |
| біометрія | 17400 | 5000 | 1200 | 7500 | 2700 |
| крипторгафія | 6000 | 1000 | 1300 | 2500 | 2700 |

Для розв’язання отриманої матриці гри методом Брауна-Робінсон ми скористались онлайн-сервісом https://math.semestr.ru/games/index.php. На рис. 2.2 показане вікно внесення даних та вибору методу розв’язування.

Перевіримо, чи має платіжна матриця сідлову точку. Якщо так, то випишемо розв’язання гри в чистих стратегіях. Чистою стратегією адміністратора безпеки є вибір одного з рядків матриці виграшів, а чистою стратегією зловмисника є вибір одного із стовпців цієї матриці. Вважаємо, що адміністратор безпеки вибирає свою стратегію так, щоб отримати свій максимальний виграш, а зловмисник вибирає свою стратегію так, щоб мінімізувати виграш адміністратора.

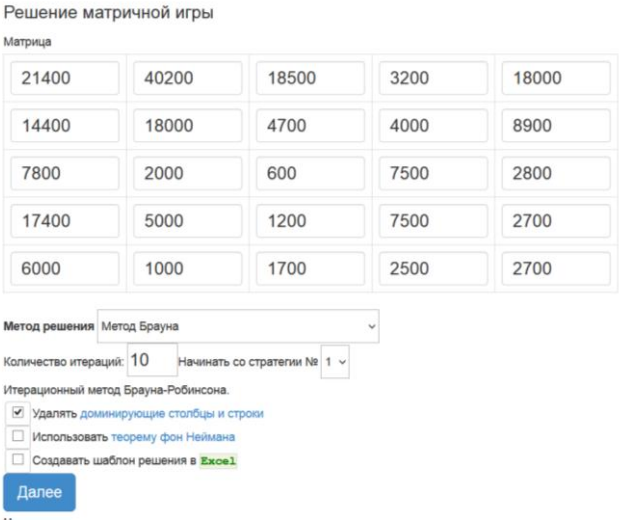


Рис. 2.2 – Вікно онлайн-сервісу розв’язування матриць гри методом Брауна-Робінсон

У табл. 2.7 визначимо мінімальні значення витрат та максимальні значення економії.

Таблиця 2.7 – Матриця гри із врахуванням мінімальних витрат на засоби захисту інформації та максимальної економії від їх використання

| | ***спуфінг*** | ***DDOS*** | ***ін'єкція коду*** | ***зловживання функціональністю*** | ***ОС-коммандінг*** | $a = \min(A_i)$ |
|---|---|---|---|---|---|---|
| фаєрвол | 21400 | 40200 | 18500 | 3200 | 18000 | 3200 |
| антивірус | 14400 | 18000 | 4700 | 4000 | 8900 | 4000 |
| хмарний захист | 7800 | 2000 | 600 | 7500 | 2800 | 600 |
| біометрія | 17400 | 5000 | 1200 | 7500 | 2700 | 1200 |
| крипторгафія | 6000 | 1000 | 1700 | 2500 | 2700 | 1000 |
| $b = \max(B_i)$ | 21400 | 40200 | 18500 | 7500 | 18000 | |

Обчислимо гарантований виграш, який визначається нижньою ціною гри $a = \max(a_i) = 4000$, що вказує на максимальну чисту стратегію використання антивіруса. Верхня ціна гри $b = \min(b_j) = 7500$. Це свідчить про відсутність сідлової точки, оскільки $a \neq b$, тоді ціна гри знаходиться у межах $4000 \leq y \leq 7500$.

Знаходимо розв’язання гри у змішаних стратегіях. Пояснюється це тим, що адміністратор безпеки та зловмисник не можуть розповісти супротивнику свої чисті стратегії, їм слід приховувати свої дії.

Перевіримо платіжну матрицю на домінуючі рядки та домінуючі стовпці. Інколи на підставі простого розгляду матриці гри можна сказати, що деякі чисті

стратегії можуть увійти в оптимальну змішану стратегію з нульовою ймовірністю.

*i-а* стратегія 1-го гравця домінує його *k-у* стратегію, якщо $a_{ij} \geq a_{kj}$ для всіх *j Э N* та принаймні для одного *j* $a_{ij} > a_{kj}$. У цьому випадку говорять також, что *i-а* стратегія (чи рядок) – домінує, *k-а* – домінована. Говорять, що *j-а* стратегія 2-го гравця домінує його *l-у* стратегію, якщо для всіх *j Э M* $a_{ij} \leq a_{il}$ і принаймні для одного і $a_{ij} < a_{il}$. У цьому випадку *j-у* стратегію (стовпець) називають домінуючою, *l-у* – домінованою.

Стратегія використання для захисту інформації фаєрвола домінує над стратегією використання криптосистеми (всі елементи рядка 1 більші чи рівні від значень 5-го рядка), отже, вилучаємо 5-й рядок матриці (табл. 2.8). Імовірність $p_5 = 0$.

Таблиця 2.8 – Матриця гри після вилучення домінованого рядка

| | ***спуфінг*** | ***DDOS*** | ***ін'єкція коду*** | ***зловживання функціональ-ністю*** | ***ОС-коммандінг*** |
|---|---|---|---|---|---|
| фаєрвол | 21400 | 40200 | 18500 | 3200 | 18000 |
| антивірус | 14400 | 18000 | 4300 | 4000 | 8900 |
| хмарний захист | 7800 | 2000 | 600 | 7500 | 2800 |
| біометрія | 17400 | 5000 | 1200 | 7500 | 2700 |

З позиції програшів зловмисника стратегія ін’єкцій коду домінує над стратегією спуфінга (всі елементи стовпця 3 менші від елементів стовпця 1), отже, вилучаємо перший стовпець матриці (табл. 2.8). Імовірність $q_1 = 0$. З позиції програшу зловмисника стратегія ін’єкцій коду домінує над стратегією DDOS-атаки (всі елементи стовпця 3 менші від елементів стовпця 2), вилучаємо другий стовпець матриці (табл. 2.8). Імовірність $q_2 = 0$.

Таблиця 2.8 – Матриця гри після вилучення домінованих стовпців

| | ***ін'єкція коду*** | ***зловживання функціональністю*** | ***ОС-коммандінг*** |
|---|---|---|---|
| фаєрвол | 18500 | 3200 | 18000 |
| антивірус | 4300 | 4000 | 8900 |
| хмарний захист | 600 | 7500 | 2800 |
| біометрія | 1200 | 7500 | 2700 |

Ми звели гру 5x5 до гри 4x3. Гравці вибирають свої чисті стратегії випадковим чином, тому виграш адміністратора інформаційної безпеки величина випадкова. Адміністратор повинен обирати свої стратегії таким чином, щоб отримати максимальний середній виграш. Зловмисник повинен обирати свої стратегії таким чином, щоб мінімізувати математичне сподівання адміністратора.

Кожне розігрування гри у чистих стратегіях називається партією. Метод Брауна—Робінсон – це ітеративна процедура побудови послідовності пар змішаних стратегій гравців, що сходиться до розв’язання матричної гри.

Нехай на першому кроці вибрана стратегія використання фаєрвола. Ітерація №1: мінімальний елемент дорівнює 3200 і знаходиться під номером j=2, отже зловмисник обирає стратегію зловживання функціональністю. Максимальний елемент дорівнює 7500 і знаходиться під номером j=3, отже адміністратор обирає стратегію хмарного захисту.

Ітерація №1: мінімальний елемент дорівнює 10700 і знаходиться під номером j=2, отже зловмисник обирає стратегію зловживання функціональністю. Максимальний елемент дорівнює 15000 і знаходиться під номером j=3, отже адміністратор обирає стратегію хмарного захисту.

Результати ітерацій зведемо у табл. 2.9-2.10.

Таблиця 2.9 – Ітерації розв’язання матриці гри методом Брауна-Робінсон для елементів і

| ***k*** | ***i*** | $B_1$ | $B_2$ | $B_3$ |
|---|---|---|---|---|
| 1 | 1 | 18500 | 3200 | 18000 |
| 2 | 3 | 19100 | 10700 | 20800 |
| 3 | 3 | 19700 | 18200 | 23600 |
| 4 | 3 | 20300 | 25700 | 26400 |
| 5 | 1 | 38800 | 28900 | 44400 |
| 6 | 1 | 57300 | 32100 | 62400 |
| 7 | 4 | 58500 | 39600 | 65100 |
| 8 | 4 | 59700 | 47100 | 67800 |
| 9 | 4 | 60900 | 54600 | 70500 |
| 10 | 4 | 62100 | 62100 | 73200 |

Таблиця 2.10 – Ітерації розв’язання матриці гри методом Брауна-Робінсон для елементів j

| ***k*** | ***j*** | $A_1$ | $A_2$ | $A_3$ | $A_4$ | $V_{min}$ | $V^{max}$ | $V_{cp}$ |
|---|---|---|---|---|---|---|---|---|
| 1 | 2 | 3200 | 4000 | 7500 | 7500 | 3200 | 7500 | 5350 |
| 2 | 2 | 6400 | 8000 | 15000 | 15000 | 5350 | 7500 | 6425 |
| 3 | 2 | 9600 | 12000 | 22500 | 22500 | $^{18200}/_{3}$ | 7500 | $^{20350}/_{3}$ |
| 4 | 1 | 28100 | 16700 | 23100 | 23700 | 5075 | 7025 | 6050 |
| 5 | 2 | 31300 | 20700 | 30600 | 31200 | 5780 | 6260 | 6020 |
| 6 | 2 | 34500 | 24700 | 38100 | 38700 | 5350 | 6450 | 5900 |
| 7 | 2 | 37700 | 28700 | 45600 | 46200 | $^{39600}/_{7}$ | 6600 | $^{42900}/_{7}$ |
| 8 | 2 | 40900 | 32700 | 53100 | 53700 | $^{11775}/_{2}$ | $^{13425}/_{2}$ | 6300 |
| 9 | 2 | 44100 | 36700 | 60600 | 61200 | $^{18200}/_{3}$ | 6800 | $^{19300}/_{3}$ |
| 10 | 1 | 62600 | 41400 | 61200 | 62400 | 6210 | 6260 | 6235 |

де: k – номер партії; i – номер стратегії, яку обирає адміністратор; j - номер стратегії, яку обирає зловмисник; $B_i$ – накопичений адміністратором виграш за k партій за умови, що в даній партії зловмисник обирає стратегію $B_i$; $A_j$ – накопичений зловмисником програш за k партій за умови, що в даній партії адміністратор обирає стратегію $A_j$. $V_{min}$ - нижня оцінка гри = min (накопичений виграш)/k. $V^{max}$ - верхня оцінка гри = max (накопичений програш)/k.

Доведено, що: $W=(V_{min}+V^{max})/2$, при $k \to \infty$ та $p_i = N_i/k$ $q_j = N_j/k$, $N_i$ - скільки разів вибирається Ai стратегія. $N_j$ - скільки разів вибирається Bj стратегія.

$N_{A1} = 3$; $P(A_1) = 3/10 = {}^{3}/_{10}$

$N_{A2} = 0$; $P(A_2) = 0/10 = 0$

$N_{A3} = 3$; $P(A_3) = 3/10 = {}^{3}/_{10}$

$N_{A4} = 4$; $P(A_4) = 4/10 = {}^{2}/_{5}$

$N_{B1} = 2$; $P(B_5) = 2/10 = {}^{1}/_{5}$

$N_{B2} = 8$; $P(B_5) = 8/10 = {}^{4}/_{5}$

$N_{B3} = 0$; $P(B_5) = 0/10 = 0$

Ціна гри, W = 6235

Стратегія адміністратора інформаційної безпеки:

$p = ({}^{3}/_{10}, 0, {}^{3}/_{10}, {}^{2}/_{5})$,

тобто для захисту у визначених частках використовувати фаєрвол, хмарний захист та біометричну ідентифікацію.

Стратегія зловмисника: q = ($^1/_5$, $^4/_5$, 0), тобто у визначених частках застосовувати ін'єкції коду та зловживання функціональністю.

Таким чином, задачу розв'язано: визначено, які саме засоби захисту цілісності, конфіденційності та доступності інформації (профіль захищеності) доцільно використовувати на ПАТ "Зборівгаз" для посилення захисту від кібератак за умов обмеженого фінансового забезпечення.

## Висновки до другого розділу

Поняття профілів захищеності пов'язано з тим, що інформаційно-комунікаційна система постійно змінюється відповідно до появи нових задач, які повинна розв'язувати організація. Поняття профілів захищеності інформаційно-комунікаційної системи визначається у нормативних документах для технічних систем захисту інформації та отримало наукову інтерпретацію в українському дискурсі з проблематики захисту інформації.

Як демонструє огляд сучасних інструментів кібербезпеки, на ринку користуються попитом багатофункціональні платформи, які поєднують кілька інструментів (антивірус, міжмережевий екран, сканер вразливостей тощо). Актуальним є питання вибору інструментарію захисту інформації в інформаційно-комунікаційній системі, враховуючи необхідні функції забезпечення безпеки та наявні ресурси підприємства.

Враховуючи вектор загроз інформаційній безпеці та різноманіття засобів захисту корпоративної мережі, а також беручи до уваги ймовірнісно-грошові потоки, поставлену проблему можна вирішити за допомогою математичного апарату теорії ігор, який дозволяє: сформувати задачу захисту інформаційно-комунікаційної системи в математичному вигляді, щоб скористатися критеріями відшукання оптимальних стратегій захисту; оцінити витрати на забезпечення безпеки інформаційного ресурсу, збитки від реалізації атаки та з урахуванням цих даних прийняти оптимальне рішення; обрати ефективний профіль захищеності.

# РОЗДІЛ ІІІ. РЕАЛІЗАЦІЯ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНОЇ СИСТЕМИ ДЛЯ ПІДВИЩЕННЯ РІВНЯ ЗАХИЩЕНОСТІ НА ПРИКЛАДІ ПАТ «ЗБОРІВГАЗ»

## 3.1. Техніко-економічне обґрунтування проекту підвищення рівня захищеності інформаційно-комунікаційної системи ПАТ «Зборівгаз»

Підприємство ПАТ “Зборівгаз” засноване згідно наказу Державного Комітету України по нафті і газу за № 215 від 31.05.1994 року. Товариство знаходиться за адресою : м. Зборів , вул. Набережна, 2.

Основною діяльністю Товариства є забезпечення природним та зрідженим газом і отримання прибутків. Предметом діяльності Товариства є: безперебійне газопостачання; виконання робіт по будівництву і проектуванню нових, розширенню діючих газових розподільчих мереж; створення безпечних умов праці, економічний та соціальний розвиток підприємства; виготовлення проектно-кошторисної документації, будівництво.

У структурі ПАТ Зборівгаз є такі служби: аварійно-диспетчерська; служба природного газу: служба підземних газопроводів; внутрішньо-будинкова служба; служба зрідженого газу; облік газу; будівельно-монтажна дільниця; служба автотранспорту.

Проектування ІКС ПАТ "Зборівгаз" з використанням профілю захищеності, визначеного засобами математичного моделювання теорії ігор, надає можливість створення ієрархічної структури опрацювання інформації та забезпечить контрольований доступ до неї з визначених політиками безпеки робочих станцій. Уся інформація, що циркулює в ІКС, повинна відповідати вимогам безпеки інформації та забезпечувати рівні захисту і доступну в залежності від статусу користувача та політик безпеки.

При проектуванні системи управління обліковими записами користувачів ПАТ "Зборівгаз" насамперед необхідно розробити топологію комп’ютерної мережі (додаток Ж). Мають бути ретельно проаналізовані такі характеристики

мережі, як передбачувані обсяги інформації, що буде опрацьовуватись, кількість робочих станцій та серверів, типи з’єднань, необхідна швидкість передачі даних, поділ мережі на сегменти. Проектування системи захисту інформації в ІКС системи проводиться відповідно до плану приміщень.

Для проектування комп’ютерної мережі ПАТ "Зборівгаз" було обрано топологію “розширена зірка”. Комп’ютерна мережа Товариства включає сервери загального доступу (DNS, HTTPS, FTP) та обмеженого доступу (SQL-сервер автоматизованої бази даних Товариства, сервер управління обліковими записами користувачів), мережеве обладнання, підмережі із різними параметрами доступу. Для комп’ютерної мережі ПАТ "Зборівгаз" обрано архітектуру Ethernet (IEEE 803.3), топологію “розширена зірка” [48].

Оскільки ІКС буде багаторанговою і обробляти дані різного типу і рівня доступу найбільш відповідними є технологія FastEthernet на рівні робочих станцій в локальному сегменті та технологія GigabitEthernet – на рівні магістральних каналів зв’язку та доступу до серверів.

Для проектування системи захисту ІКС ПАТ "Зборівгаз" за обраною топологією потрібне комутуюче обладнання, таке як: концентратори, комутатори, маршрутизатори, шлюзи, безпровідні точки доступу, DSL модеми, міжмережеві екрани.

Будівлю Товариства сегментовано на 4 компоненти (підмережі). Відповідно до вимог безпеки інформації, кількості необхідних портів, підмереж, надійності та єдиного центру управління, обрано наступне обладнання:

– D-Link DES-1005A (таблиця Б.1), некерований 5-портовий комутатор;

– D-Link DES-1008D/PRO (таблиця Б.2), некерований 8-портовий комутатор;

– D-Link DES-1016D (таблиця Б.3), некерований 16-портовий настільний комутатор, присутнє кріплення на стіну;

– D-Link DES-3010G (таблиця Б.4), керований 8-портовий L2/L3 комутатор у стійку 19”. Має можливість налаштування до 255 VLAN. (Використовується в комутаційних кімнатах А_213 та А_258);

– DES-3200-18 (таблиця Б.5), керований 16-портовий L2/L3 комутатор у стійку 19”. (Використовується в комутаційній кімнаті A_135);

– DES-3810-28 (таблиця Б.6), керований 24-портовий L3 комутатор (комутатор третього рівня, розміщений в центральній комутаційній кімнаті A_244, вона ж серверна);

– D-Link DSL-2500U (таблиця Б.7), ADSL модем для резервного доступу до мережі Інтернет;

– FireWall NETGEAR - FVS336G (таблиця Б.8), мережевий екран, який фільтрує увесь вхідний Інтернет-трафік;

– TP-Link TL-WA701ND (таблиця Б.9), безпровідна точка доступу для організації безпровідного доступу до мережі Інтернет.

Основними логічними частинами комп’ютерної мережі ПАТ "Зборівгаз" є сегменти мережі: локальна підмережа підрозділів, які знаходяться на 1 поверсі; локальна підмережа підрозділів, які знаходяться на 2 поверсі; підмережа безпровідного доступу; підмережа для серверів обмеженого доступу.

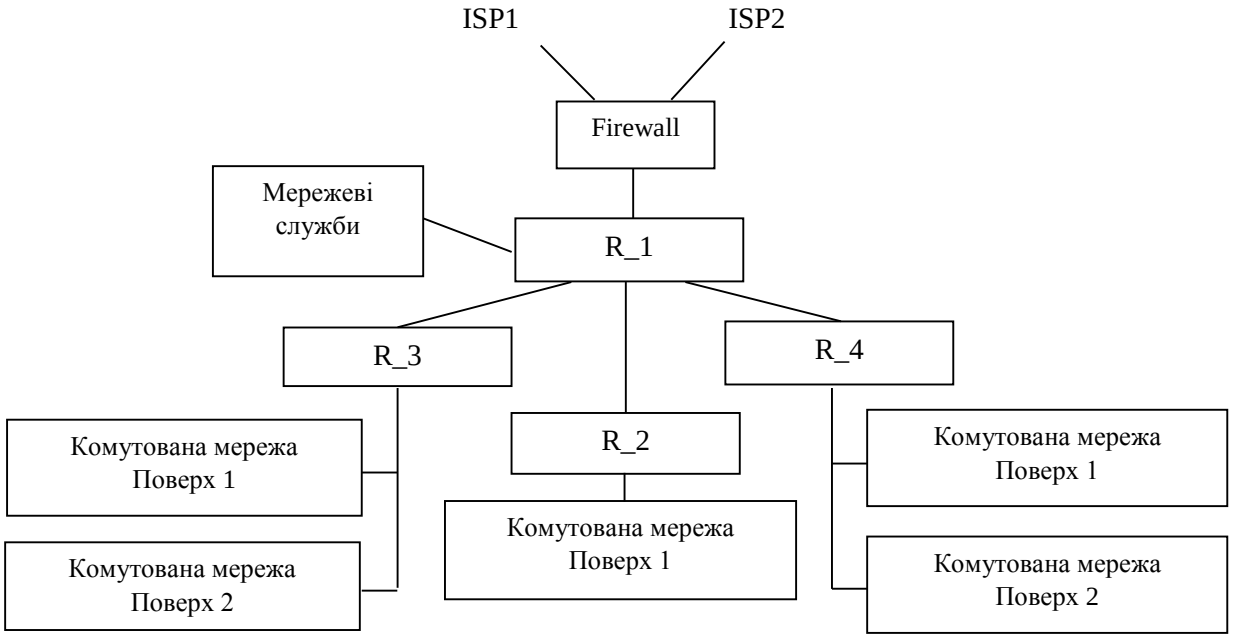


Рис. 3.1 - Структура комп’ютерної мережі ПАТ «Зборівгаз»

Виділені робочі станції ІКС ПАТ "Зборівгаз" мають доступ до мережі Інтернет, який захищений міжмережевим екраном для захисту від атак ззовні. На рис. 3.1 зображено загальну структурну схему ІКС. Наведена структура повністю відповідає вимогам технічного завдання.

При виборі активного мережевого обладнання необхідно керуватись його характеристиками та функціональними можливостями [32].

Міжмережевий екран - пристрій призначений для управління доступом до мережі Інтернет, шифрування даних та передачі мережевого трафіку між зонами різного рівня обмеження доступу відповідно до політик безпеки. В роботі ІКС міжмережевий екран повинен забезпечити: два WAN інтерфейси для під’єднання до різних ISP; мінімум один інтерфейс LAN для з’єднання з внутрішньою мережею ПАТ "Зборівгаз" (R_1); DMZ інтерфейс для реалізації зони серверів загального доступу; підтримка техології NAT; управліня доступом до локальної мережі та зони серверів загального доступу та захист від атак з зовні.

Для організації мережі було обрано міжмережевий екран FVS336G. Характеристики та функції цього пристрою наведені в додатку Б.

Комутатори 3-го рівня повинні підтримувати технологію VLAN, бути надійним та мати високу пропускну здатність. Комутатори 2-го рівня повинні також забезпечувати доступ користувачів до мережі з швидкістю 100Мбіт/с. При виборі комутатора 3 рівня було вибрано комутатори D-link DES 3200-18 та DES 3810-28. Дані пристрої відповідають вимогам технічного завдання та техніко-економічного обґрунтування. Характеристики та функції пристроїв наведені в додатку Б.

Виходячи з вимог інформаційної безпеки, кількості підключень в кожному кабінеті та на поверсі в цілому, надійності, обрано наступне обладнання:

– D-Link DES-1005A (таблиця Б.1), некерований 5-портовий комутатор.

– D-Link DES-1008D/PRO (таблиця Б.2), некерований 8-портовий комутатор.

– D-Link DES-1016D (таблиця Б.3), некерований 16-портовий настільний комутатор, присутнє кріплення на стіну.

– D-Link DES-3010G (таблиця Б.4), керований 8-портовий L2/L3 комутатор у стійку 19”. Має можливість налаштування до 255 VLAN. (Використовується в комутаційних кімнатах A_213 та A_258).

– DES-3200-18 (таблиця Б.5), керований 16-портовий L2/L3 комутатор у стійку 19”. (Використовується в комутаційній кімнаті A_135).

– DES-3810-28 (таблиця Б.6), керований 24-портовий L3 комутатор. (комутатор третього рівня, розміщений в центральній комутаційній кімнаті A_244, серверна кімната).

– D-Link DSL-2500U (таблиця Б.7), ADSL модем для резервного доступу Інтернет.

– FireWall NETGEAR - FVS336G (таблиця Б.8), мережевий екран, який фільтрує увесь вхідний Інтернет-трафік.

– TP-Link TL-WA701ND (таблиця Б.9), безпровідна точка доступу до комп’ютерної мережі.

В таблиці Б.10, додаток Б представлена порівняльна характеристика 5-портових некерованих комутаторів D-link DES-1005A та TL-SF1005D.

В таблиці Б.11, додаток Б представлена порівняльна характеристика 8-портових некерованих комутаторів D-Link DES-1008D/PRO та TP-Link TL-SF1008D. Як видно із таблиці, D-Link DES-1008D/PRO підтримує більше стандартів і тому в мережі буде використовуватись D-Link DES-1008D/PRO.

В таблиці Б.12, додаток Б представлена порівняльна характеристика 16-портових некерованих комутаторів D-Link DES-1016D та TP-SF1016D. Із таблиці видно, що TP-Link не підтримує протоколу CSMA/CD. Отже, у мережі буде використовуватись комутатор D-Link DES-1016D.

Для організації доступу до мережі Інтернет організовано дві лінії зв’язку: основний канал зв’язку, локальна мережа місцевого інтернет-провайдера; резервний канал зв’язку ADSL-лінія.

В таблиці Б.13, додаток Б представлена порівняльна характеристика ADSL модемів: D-Link DSL-2500U та TP-Link TD-8610. Відповідно до таблиці Б.13, модем D-Link підтримує більше стандартів ADSL, також на інтерфейсі LAN

налаштовано автоматичний визначник полярності. Параметри швидкості передачі даних співпадають у обох типів модемів. Отже, обираємо D-Link DSL-2500U.

В кабінеті A_123 та A_125 потрібно організувати безпровідну мережу. Для порівняння були обрані дві безпровідні точки доступу: D-Link DAP-1150 та TP-Link TL-WA701ND однієї цінової категорії. В таблиці Б.14, додаток Б приведена порівняльна характеристика безпровідних точок доступу D-Link DAP-1150 та TP-Link TL-WA701ND. Порівнявши технічні характеристики можна зробити висновок, що у TP-Link доступно більше можливостей для налаштування на відміну від D-Link. TP-Link підтримує стандарти IEEE 802.11n light IEEE 802.11b, також надає більше варіантів  підключення WAN, потужність сигналу вдвічі більша, підтримує роботу у режимі моста.

Одна із точок безпровідного доступу буде використовуватись в якості повторювача (repeater). Це дасть можливість охопити більший радіус дії пристрою.

Для управління доступом до мережі Інтернет та протидії несанкціоновану доступу до інформаційних ресурсів ПАТ "Зборівгаз", використовується мережевий екран NETGEAR - FVS336G. В таблиці Б.8 представлена специфікація мережевого екрана.

Мережевий екран NETGEAR ProSafe Dual WAN Gigabit Firewall з SSL та IPsec VPN. Тунелі SSL VPN забезпечують віддалений доступ до інформативних ресурсів ПАТ "Зборівгаз". Тунелі IPsec VPN забезпечують захищені тунелі між ПАТ "Зборівгаз" в місті Зборів та ПАТ "Нафтогаз України", місто Київ (site-to-site) та здійснюють технічну підтримку технологій віддаленого доступу за допомогою клієнтських програм.

Для управління доступу в ІКС організовано виділені групи користувачів: працівники підрозділів, керівники підпрозділів, адміністрація. Кожна група має власлні привілеї та обмеження доступу.

Оскільки ІКС ПАТ "Зборівгаз" містить служби загального (HTTP та FTP) та обмеженого доступу (сервер баз даних, сервер Active Directory), слід обрати

апаратне забезпечення для них. Для організації політик розмежування доступу та управління обліковими записами користувачів використовується сервер HP ProLiant ML110 G6 SP7317GO.

На базі даного сервера організовано служби обмеженого та загально доступу. До пасивного мережевого обладнання відносяться: настінні шафи, кабелі, інформаційні розетки, конектори і кросове обладнання.

Для організації мережевих комунікацій ПАТ "Зборівгаз" обрано мережеву адресу класу С 192.168.0.0/16 (маска адреси 255.255.0.0) – додаток М.

## 3.2. Підвищення рівня захищеності засобами Active Directory

### 3.2.1 Моделі керування безпекою інформації

Завдання управління обліковими записами користувачів ПАТ "Зборівгаз" будемо вирішувати розробкою служби каталогів Active Directory. Служби каталогу надають можливості управління ресурсами і сервісами з будь-якого місця ІКС. Інформація про користувача, заноситься один раз в службу каталогу, і після цього стає доступною в межах всієї ІКС. Адреси електронної пошти, приналежність до груп, необхідні права доступу і облікові записи для роботи з різними операційними системами - все це створюється і підтримується в актуальному вигляді автоматично. Будь-які зміни, занесені в службу каталогу адміністратором, відразу оновлюються по всій ІКС. Служба каталогів Active Directory є основою логічної структури ІКС ПАТ "Зборівгаз", що базується на системі Windows і реалізує засоби захисту на яких базується система захисту інформації ІКС ПАТ "Зборівгаз" – облікові записи користувачів, груп і комп'ютерів. Облікові записи організовані в логічні структури: домен, дерево, ліс, організаційні підрозділи.

Моделі управління інформаційною безпекою - модель "Робоча група" і модель централізована доменна система. Управління обліковими записами користувачів проводиться на основі моделі централізована доменна система.

У доменній моделі існує єдина база даних служб каталогів, доступна всім комп'ютерам Товариства. Для цього в комутаційній кімнаті А_244 встановлено

спеціалізований сервер - контролер домену. На рисунку 3.2 наведено схему доменної моделі. Контролер домену зберігає доменну базу даних облікових записів, що визначає порядок розмежування прав доступу між різними групами користувачів.

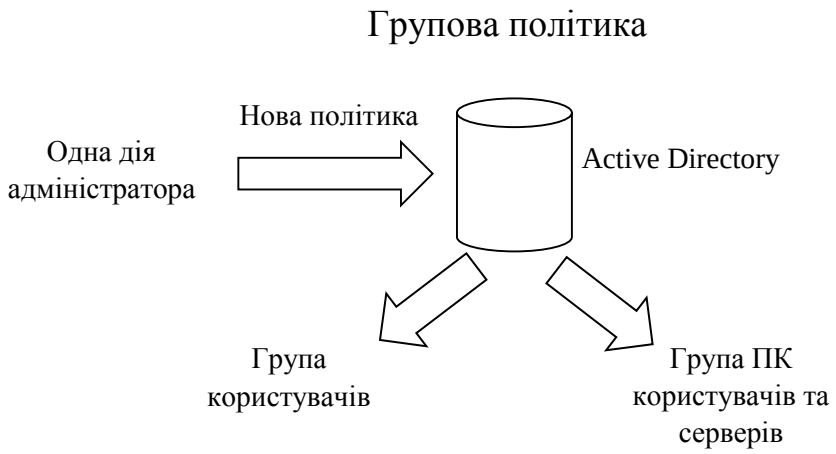


Рис. 3.2 – Групові політики доменної моделі управління

У доменній моделі управління інформаційною безпекою користувач реєструється на комп'ютері ("входить в систему") зі своїм доменним обліковим записом і, незалежно від комп'ютера, на якому була виконана реєстрація, отримує доступ до необхідних інформаційних ресурсів. Немає необхідності на кожному комп'ютері створювати велику кількість локальних облікових записів, всі записи створені одноразово в доменній БД. За допомогою доменної бази даних здійснюється централізоване управління доступом до інформаційних ресурсів відповідно до політик безпеки.

3.2.2. Призначення служби каталогів Active Directory

Каталог Active Directory зберігає інформацію, що відноситься до користувачів, груп, комп'ютерів, мережевих принтерів, спільних файлових ресурсів ІКС ПАТ "Зборівгаз". Каталог зберігає атрибутами про сам об'єкт і його властивості. Атрибутами користувача є ім'я, номер телефону, адреса, ім'я для входу в систему, пароль, групи, до яких він належить.

Служба каталогів Active Directory (AD) забезпечує ефективну роботу ІКС, в тому числі здійснює управління обліковими записами користувачів, надаючи

такі можливості: єдина реєстрація в ІКС, інформаційна безпека, централізоване управління, адміністрування з використанням групових політик, інтеграція з DNS.

3.2.3. Планування простору доменних імен

Механізм іменування об'єктів Active Directory дає змогу однозначно ідентифікувати будь-який об'єкт каталогу. У каталогах на базі протоколу LDAP для ідентифікації об'єкта в масштабі всього лісу використовуємо механізм виділених імен (Distinguished Name, DN). У Active Directory обліковий запис користувача з ім'ям користувача домену zborivgaz.te.ua, який розміщено в стандартному контейнері Users, буде мати наступне виділене ім'я: "`DC = ua`, `DC = te`, `OU = zborivgaz`, `CN = Users`":

– DC (Domain Component) - вказівник доменного імені.
– OU (Organizational Unit) - вказівник підрозділу (ОП).
– CN (Common Name) - вказівник на загальне ім'я.

Відносне виділене ім'я (Relative Distinguished Name, RDN) для користувачів Товариства RDN-ім'я має вигляд "`CN = User`".

Крім імен DN і RDN, використовується основне ім'я об'єкта (User Principal Name, UPN). Воно має формат <ім'я суб'єкта> @ <суфікс домену>. Для користувача ІКС основне ім'я, в загальному має вигляд `User@ zborivgaz.te.ua`.

Імена DN, RDN можуть змінюватись, якщо об'єкт переміщується з одного контейнера в інший AD. Для того щоб не втрачати посилання на об'єкти при їх переміщенні у лісі, всім об'єктам призначається глобально унікальний ідентифікатор (глобальний унікальний ідентифікатор, GUID), що представляє собою 128-бітове число.

Схема організації простору імен ПАТ "Зборівгаз" з розділенням простору імен DNS - два різні домени DNS, локальних і глобальних імен наведена на рисунку 3.3.

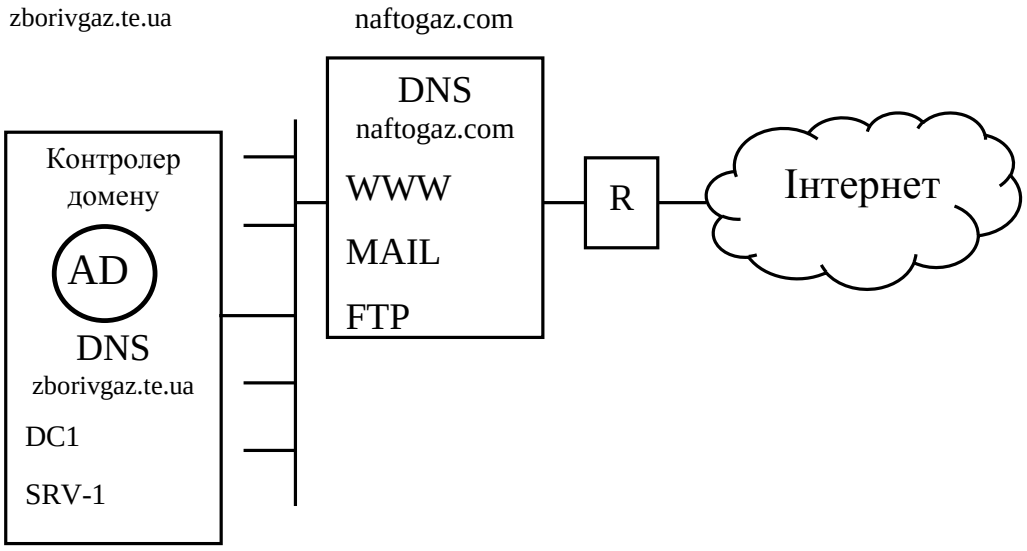


Рис. 3.3 – Організація простору імен в Active Directory

На рисунку, в лівій частині - внутрішня мережа "Зборівгаз", праворуч - мережа Інтернет, дві мережі розділені маршрутизатором "R" (крім маршрутизатора, на кордоні встановлено мережевий екран).

У цьому сценарії ІКС ПАТ "Зборівгаз" має можливість зареєструвати два доменних імені, одне для публікації зовнішніх ресурсів, інше - для розгортання Active Directory. На різних серверах DNS створюються різні зони. На внутрішньому DNS-сервері функціонує зона `zborivgaz.te.ua` для Active Directory, на зовнішньому DNS-сервері - зона для посилань на зовнішні ресурси. Важливий момент - дані зони ніяк між собою не пов'язані - ні механізмами реплікації, ні ручною синхронізацією. У зовнішній зоні зберігаються посилання на зовнішні ресурси, а у внутрішній на внутрішні ресурси Товариства, використовувані для роботи Active Directory.

Даний сценарій планування простору імен оптимальний. По-перше, ім'я зовнішнього домену ніяк не пов'язане з ім'ям внутрішнього домену, і не виникає жодних проблем з можливістю публікувати в Інтернет внутрішню структуру. По-друге, реєстрація внутрішнього імені гарантує відсутність потенційних конфліктів, викликаних тим, що політика реєстрації доменного імені може визначатись Нафтогаз України.

3.2.4 Встановлення контролера домену

Встановлення першого контролера першого внутрішнього домену першого лісу в структурі Active Directory починається з запуску з командного рядка майстра інсталяції Active Directory - Dcpromo. Наступний крок - вибір імені домену (для Active Directory це буде кореневий домен). У нашому випадку виберемо ім'я `zbrivgaz.te.ua.` Задамо NetBIOS-ім'я домену – `zbrivgaz.`

Далі майстер запропонує вибрати місце на жорстких дисках для розміщення бази даних Active Directory, журналу транзакцій і папки системного тому SYSVOL. Системний том обов'язково повинен бути розміщений на розділі з файловою системою NTFS.

Після цього майстер установки на основі параметрів мережевої конфігурації сервера шукає в мережі DNS-сервер, на якому є зона з вказаним ім'ям домену, причому в даній зоні повинні бути дозволені динамічні оновлення. Якщо такий сервер DNS в мережі не знайдений, то майстер запропонує встановити службу DNS на цьому сервері і створити відповідну зону.

Задаємо пароль адміністратора при запуску системи в режимі відновлення служб каталогів даний режим використовується для відновлення БД Active Directory з резервної копії. Потім слідує екран із зведеною інформацією про створюваний домен і параметри контролера домену. На цьому кроці в разі виявленої помилки в конфігурації можна повернутися назад і виправити помилку. Останній крок - натиснути кнопку "Готово" і перезавантажити сервер.

Враховуючи підвищені вимоги до надійності роботи та інформаційної безпеки ІКС ПАТ "Зборівгаз" важливо становити додатковий контролер домену, який спочатку бажано включити в домен в якості учасника домену.

Вказуємо ім'я домену – `zborivgaz.te.ua` і облікові дані адміністратора домену. Починається процес імпорту БД Active Directory на створюваний контролер.

3.2.5. Визначення функціональних рівнів доменів

Для розгортання Schema Master Active Directory ІКС Товариства використаємо рівень функціонування – Windows 2008 змішаний [36]. Змінювати

рівень функціонування домену можна тільки в бік його підвищення. Зробити це можна за допомогою адміністративних консолей "Active Directory - домени і довіра" або "Active Directory - користувачі й комп'ютери", як показано на рисунку 3.8.

Для підвищення рівня треба вибрати необхідний рівень і натиснути кнопку "Змінити". Після реплікації, зміни на всі контролери в домені `zborivgaz.te.ua` стануть доступні специфічні для даного рівня можливості.

Визначення функціональних рівнів для всього лісу робимо за допомогою консолі "Active Directory - домени і довіра". Тільки правою кнопкою миші треба клацнути не на імені домену, а на написі "Active Directory - домени та довіра" і задаємо рівень функціонування лісу - Windows 2008.

Глобальний каталог (global catalog) - це перелік усіх об'єктів лісу Active Directory. За замовчуванням, контролери домену містять тільки інформацію про об'єкти свого домену. Сервер глобального каталогу є контролером домену, в якому міститься інформація про кожен об'єкт (хоча і не про всіх атрибутах цих об'єктів), що знаходиться в даному лісі. Сервер глобального каталогу виконує дві функції:

– пошук об'єктів в масштабах усього лісу, клієнти можуть звертатися до глобального каталогу із запитами на пошук об'єктів по певним значенням атрибутів;

– автентифікація користувачів (сервер глобального каталогу надає інформацію про приналежність користувача у універсальних групах, universal groups.

За замовчуванням самий перший контролер домену в лісі є сервером глобального каталогу. Однак адміністратор мережі може призначити інший контролер домену сервером глобального каталогу. Це робиться за допомогою адміністративної консолі "Active Directory - сайти і служби", у властивостях вузла "NTDS Settings" обраного контролера.

3.2.6. Управління користувачами та групами

Облікові записи (accounts) користувачів, комп'ютерів і груп - один з головних елементів управління доступом до інформаційних ресурсів, а значить, і всієї системи інформаційної безпеки ІКС ПАТ "Зборівгаз". У середовищі Windows Active Directory використано три головні типи користувальницьких облікових записів.

Перший тип облікового запису - локальні облікові записи користувачів. Дані облікові записи існують в локальній базі даних SAM (Security Accounts Manager) на кожній системі, що працює під управлінням Windows 2003. Вони створюються з використанням інструменту Local Users and Groups (Локальні користувачі та групи) консолі Computer Management (Управління комп'ютером). Для входу в систему з використанням локального облікового запису такий обліковий запис обов'язково має бути створеним в базі даних SAM. Такий метод робить локальні облікові записи непрактичними для використання в ІКС Товариства.

Другий тип облікового запису - користувачі домену. Дані облікові записи зберігаються в Active Directory і можуть використовуватися для входу в систему і доступу до ресурсів по всьому лісу. Облікові записи цього типу створюються централізовано за допомогою консолі "Active Directory Users and Computers" ("Active Directory - користувачі й комп'ютери").

Третім типом облікового запису є вбудовані облікові записи. Дані облікові записи створюються системою і не можуть бути видалені.

Доменні облікові записи користувачів (а також комп'ютерів і груп) зберігаються в спеціальних контейнерах AD. Це можуть бути або стандартні контейнери Users для користувачів і Computers для комп'ютерів, або створене адміністратором Організаційний підрозділ (ОП). Виняток становлять облікові записи контролерів домену, вони завжди зберігаються в ОП з назвою Domain Controllers [36].

Процес створення облікових записів користувачів ПАТ "Зборівгаз" та облікових записів комп’ютерів проходить з використанням БД Active Directory `dc1.zborivgaz.te.ua`.

Правила вибору символів для створення пароля користувачів ПАТ "Зборівгаз":

– довжина пароля - не менше 8 символів;

– пароль не повинен співпадати з ім'ям користувача для входу в систему, а також з його звичайним ім'ям, прізвищем, іменами його родичів, друзів, тощо;

– пароль не повинен складатися з будь-якого слова з словника;

– пароль не повинен співпадати з номером телефону користувача, номером його автомобіля, паспорта, посвідчення водія або іншого документа;

– пароль повинен бути комбінацією букв у верхньому та нижньому регістрах, цифр і спецсимволів типу @ # $% ^ * & () _ +.

Відповідно до політик безпеки та захисту інформації в ПАТ "Зборівгаз" необхідно періодично проводити зміну паролів користувачів.

Параметр "Сценарій входу" визначає виконуваний файл, який при вході користувача в систему завантажується на комп'ютер і виконується. Виконуваним файлом може бути пакетний файл (`.bat`, `.cmd`), виконується програма (`.exe`, `.com`), файл сценарію (`.vbs`, `.js`).

Закладка "Учасник груп" - дозволяє управляти списком груп до яких належить користувач.

Закладка "Вхідні дзвінки". Управління доступом користувача в корпоративну систему через засоби віддаленого доступу системи Windows Server використовуючи модем або VPN-з'єднання).

Закладки "Профіль служб терміналів", "Середовище", "Сеанси", "Віддалене управління" - дані закладки управляють параметрами роботи користувача на сервері терміналів:

– управління дозволом користувача працювати на сервері терміналів;

– розміщення профілю при роботі в термінальній сесії;

– налаштування середовища користувача в термінальній сесії;

– управління сеансом користувача на сервері терміналів;

– дозвіл адміністратору підключатися до термінальної сесії користувача.

Локальні групи сервера учасника домену або робочої станції включають в себе локальні облікові записи даного комп'ютера, і глобальні облікові записи будь-якого користувача або комп'ютера всього лісу, а також доменні локальні групи "свого" домену і глобальні й універсальні групи всього лісу.

У Active Directory групи розрізняються за типом (групи безпеки і групи поширення) і по області дії (локальні в домені, глобальні й універсальні) [36].

Типи груп:

– Групи безпеки - кожна група даного типу, так само як і кожен обліковий запис користувача, має ідентифікатор безпеки (SID), тому групи безпеки використовуються для призначення дозволів при визначенні прав доступу до різних мережевих ресурсів.

– Групи поширення - групи цього типу не мають ідентифікатора безпеки, тому не можуть використовуватися для призначення прав доступу.

Область дії груп:

– Локальні в домені zborivgaz.te.ua, які можуть містити - глобальні групи з будь-якого домену, універсальні групи, глобальні облікові записи користувачів з будь-якого домену лісу, використовуються - при призначенні прав доступу тільки до ресурсів домену `zborivgaz.te.ua`.

– Глобальні, які можуть містити тільки глобальні облікові записи користувачів домену zborivgaz.te.ua, використовуються - при призначенні прав доступу до ресурсів будь-якого домену в лісі.

– Універсальні, які можуть містити інші універсальні групи всього лісу, глобальні групи всього лісу, глобальні облікові записи користувачів з будь-якого домену лісу, використовуються - при призначенні прав доступу до ресурсів будь-якого домену.

При реєстрації в домені користувачеві передається в його сесію на комп'ютері маркер доступу (Access Token). Маркер доступу складається з набору ідентифікаторів безпеки - ідентифікатора безпеки (SID) самого користувача і

ідентифікаторів безпеки тих груп, учасником яких він є. Маркер доступу використовується при перевірці дозволів користувача на доступ до різних ресурсів домену `zborivgaz.te.ua`.

При створенні та використанні груп слід дотримуватися наступних правил:

– Включати глобальні облікові записи користувачів (Accounts) в глобальні групи (Global groups). Глобальні групи формуються функціональними обов'язками співробітників ПАТ "Зборівгаз".

– Включати глобальні групи в доменні локальні або локальні на простому сервері або робочої станції (Local groups). Локальні групи формуються на основі дозволів для доступу до конкретних ресурсів.

– Давати дозвіл (Permissions) на доступ до ресурсів локальним групам.

Крім тих груп, які створює адміністратор, на комп'ютерах локально або у всьому домені існують вбудовані групи, створені під час установки системи або створення домену, які наведено в таблиці 3.19.

Таблиця 3.1 – Групи користувачів ІКС ПАТ «Зборівгаз»

| Назва групи | Опис групи |
|---|---|
| Адміністратори | Можуть виконувати всі адміністративні завдання на даному комп'ютері. Вбудований обліковий запис, який створюється при установці системи. |
| Оператори резервного копіювання | Учасники групи можуть виконувати вхід на цей комп'ютер, виконувати резервне копіювання і відновлення даних на цьому комп'ютері, а також завершувати роботу цього комп'ютера. |
| Адміністратори DHCP (створюється при установці служби DHCP Server) | Учасники групи можуть адмініструвати службу DHCP Server. |
| Оператори мережевої конфігурації | Учасники групи можуть змінювати налаштування TCP/IP. |
| Користувачі монітора продуктивності | Учасники групи можуть стежити за лічильниками продуктивності на конкретному сервері локально або віддаленим чином. |
| Користувачі журналу продуктивності | Учасники групи можуть адмініструвати журнали продуктивності, лічильники та оповіщення на конкретному сервері локально або віддаленим чином. |

| | |
|---|---|
| Досвідчені користувачі | Учасники групи можуть створювати і модифікувати облікові записи користувачів, а також встановлювати програми на локальному комп'ютері, але не можуть переглядати файли інших користувачів. |
| Оператори друку | Учасники групи можуть управляти принтерами та чергами друку на конкретному сервері. |
| Користувачі віддаленого робочого столу | Учасники групи можуть виконувати підключення до віддаленого робочого столу комп'ютера. |
| Користувачі | Учасники групи можуть локально входити в систему на даному комп'ютері, працювати з програмами, зберігати документи та завершувати роботу ПК. |
| Вбудовані доменні локальні групи | |
| Адміністратори | Адміністратори |
| Оператори облікових записів | Оператори облікових записів |
| Оператори резервного копіювання | Оператори резервного копіювання |
| Адміністратори DNS (створюється при установці служби DNS) | Адміністратори DNS (створюється при установці служби DNS) |
| Назва групи | Опис групи |
| Оператори мережевої конфігурації | Оператори мережевої конфігурації |
| Користувачі монітора продуктивності | Користувачі монітора продуктивності |
| Користувачі журналу продуктивності | Учасники групи можуть управляти журналами продуктивності, лічильниками та оповіщеннями на контроллерах домена. |
| Оператори сервера | Учасники групи можуть виконувати більшість адміністративних задач на контролерах домену, за винятком зміни параметрів безпеки. |
| Користувачі | Учасники цієї групи локально можуть входити в систему на даному комп'ютері, працювати з програмами, зберігати документи та завершувати роботу даного комп'ютера. |
| Вбудовані глобальні групи | |
| Адміністратори домену | Ця група автоматично включається в локальну в домені групу Адміністратори, тому учасники групи Адміністратори домену можуть виконувати адміністративні завдання на будь-якому комп'ютері даного домену. Обліковий запис Адміністратор включається в цю групу за умовчанням. |
| Комп'ютери домену | Усі контролери, сервери і робочі станції домену є членами цієї групи. |

| | |
|---|---|
| Контролери домену | Усі контролери домену є учасниками цієї групи. |
| Користувачі домена | Всі глобальні облікові записи домену і входять в цю групу. Ця група автоматично включається в локальну доменну групу Користувачі. |
| Адміністратори підприємства (створюється тільки в кореневому домені лісу) | Група призначена для користувачів, які повинні мати права адміністратора в масштабах усього лісу. Адміністратори підприємства автоматично включається до групи Адміністратори на всіх контролерах домену в даному лісі. |
| Адміністратори схеми (створюється тільки в кореневому домені лісу) | Учасники цієї групи можуть змінювати схему Active Directory. |

Механізм Групових політик (Group Policy) дозволяє налаштовувати правила розмежування доступу комп'ютерів і користувачів в межах домену ПАТ "Зборівгаз". Налаштування проводиться за такими параметрами, як сценарії входу в систему і завершення сеансу роботи в системі, параметри "Робочого столу" і "Панелі управління", розміщення особистих папок користувача, налаштування безпеки системи (політики паролів, управління обліковими записами, аудиту доступу до інформаційних ресурсів, управління сертифікатами і т.д.), розгортання додатків і управління їх життєвим циклом.

Кожен об'єкт групових політик (Group Policy Object, GPO) складається з двох частин: контейнера групових політик (Group Policy Container, GPC) зберігається в БД Active Directory, і шаблону групових політик (Group Policy Template, GPT), що зберігається у файловій системі контролера домену , в структурі папки `SYSVOL`. Місце, в якому зберігаються шаблони політик `%systemroot%\SYSVOL \sysvol\Zborivgaz.te.ua\policies`, ім'я папки шаблону збігається з глобальним унікальним ідентифікатором (GUID) об'єкта Групова політика.

Кожен об'єкт політик містить два розділи: конфігурація комп'ютера і конфігурація користувача. Параметри цих розділів застосовуються відповідно або до налаштувань комп'ютера, або до налаштувань середовища користувача.

Задання параметрів групових політик проводиться "Редактором групових політик", який можна відкрити в консолі управління відповідним об'єктом AD

("Active Directory - сайти і служби", "Active Directory - користувачі й комп'ютери", локальна політика комп'ютера редагується консоллю gpedit.msc, що запускається з командного рядка ). На рисунку 3.8.1 показана закладка "Групові політики" властивостей домену `zborivgaz.te.ua` [36].

При завантаженні комп'ютера і автентифікації в домені до нього застосовуються комп'ютерні розділи всіх прив'язаних політик. При вході користувача в систему до користувача застосовується користувальницький розділ всіх групових політик.

Політики, прив'язані до деякого рівня ієрархії об'єктів AD (сайту, домену, підрозділи) успадковуються всіма об'єктами AD, що знаходяться на нижчих рівнях.

Для управління груповими політиками в ІКС ПАТ "Зборівгаз" застосовуємо такі методи: блокування спадкування політик на всіх рівнях ієрархії AD; заборона блокування конкретного об'єкта групових політик; управління пріоритетом застосування політик на конкретному рівні AD; дозвіл на застосування політик.

Крім застосування політик в момент завантаження комп'ютера або входу користувача в систему, кожен комп'ютер постійно звертається за оновленнями політики на контролер домену `dc1.Zborivgaz.te.ua`, завантажує їх і застосовує оновлені параметри.

Групові політики використовуються також для управління прикладними програм в масштабах всього домену або окремого організаційного підрозділу.

В організації управління обліковими записами користувачів використовуються такі способи управління встановленням прикладних програм [36]:

– призначення програм комп'ютерам (при даному способі програма автоматично встановлюється при завантаженні комп'ютера);

– призначення програм користувачам (програма встановлюється при першому виклику - відкриття ярлика програми або файлу, відповідного даній програмі);

– публікація програм користувачам (назва програми додається до списку доступних для встановлення програм у вікні "Установка й видалення програм" в "Панелі управління").

Дані політики використовуються для керувати встановленням програм, які встановлюються за допомогою компоненти Windows Installer, тобто для них інсталяційний пакет повинен бути створений у форматі файлу з розширенням ".msi". Якщо програму можна встановити тільки за допомогою установочної програми типу setup.exe або install.exe, то такі програми можуть бути опубліковані (але не призначені) після створення файлу типу ". zap", в якому задані відповідні параметри, необхідні для публікації.

3.8.4. Налаштування параметрів безпеки.

Відкрити консоль mmc. Кнопка "Пуск" - "Виконати" - mmc - кнопка "ОК".

Додати в нову консоль оснастки "Шаблони безпеки" та "Аналіз та налаштування безпеки". Меню "Консоль" - "Додати або видалити оснастку" - кнопка "Додати" - вибрати оснастку "Аналіз та налаштування безпеки" - кнопка "Додати" - вибрати оснастку "Шаблони безпеки" - кнопка "Додати" - кнопка "Закрити" - кнопка " ОК ".

В отриманій консолі виконуємо налаштування параметрів безпеки:

– вивчити параметри стандартних шаблонів безпеки (оснащення "Шаблони безпеки") та створити власні шаблони на основі стандартних;

– провести аналіз поточних параметрів безпеки сервера (оснащення "Аналіз та налаштування безпеки").

Характеристики стандартних шаблонів безпеки, що використовуються в управлінні обліковими записами користувачів [36]:

– DC security - використовувані за замовчуванням параметри безпеки контролера домену;

– securedc - захищений контролер домену;

– hisecdc - контролер домену з високим рівнем захисту;

– compatws - сумісна робоча станція або сумісний сервер;

– securews - захищена робоча станція або захищений сервер;

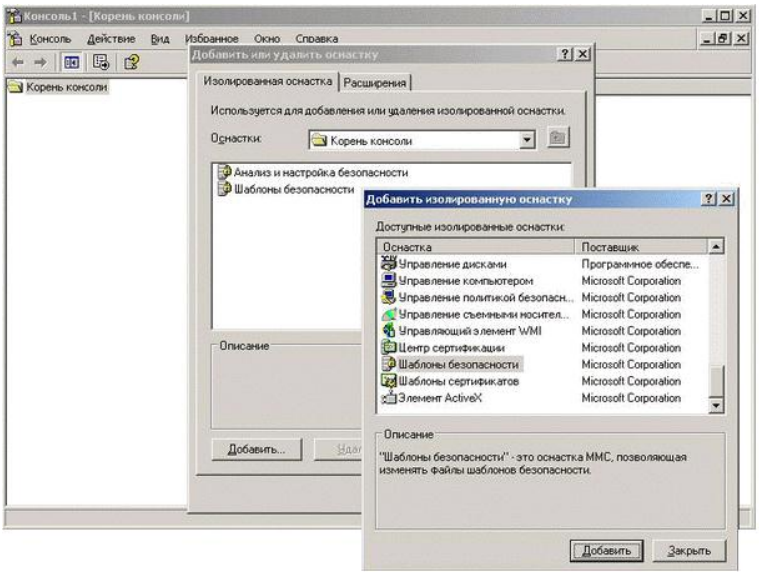


Рис. 3.4 – Налаштування правил безпеки

– hisecws - захищений сервер з високим рівнем захисту;

– setup security - початкові налаштування за замовчуванням;

– rootsec - установка стандартних NTFS-дозволів для папки, в яку встановлена операційна система.

Розглянемо аналіз налаштувань безпеки (див. рисунок 3.5). Вибрати правою кнопкою миші на значку оснастки "Аналіз та налаштування безпеки", вибрати "Відкрити базу даних", вказати шлях і назву БД (за замовчуванням БД створюється в папках профілю того адміністратора, який проводить аналіз), натиснути кнопку "Відкрити", вибрати потрібний шаблон hisecdc - "ОК".

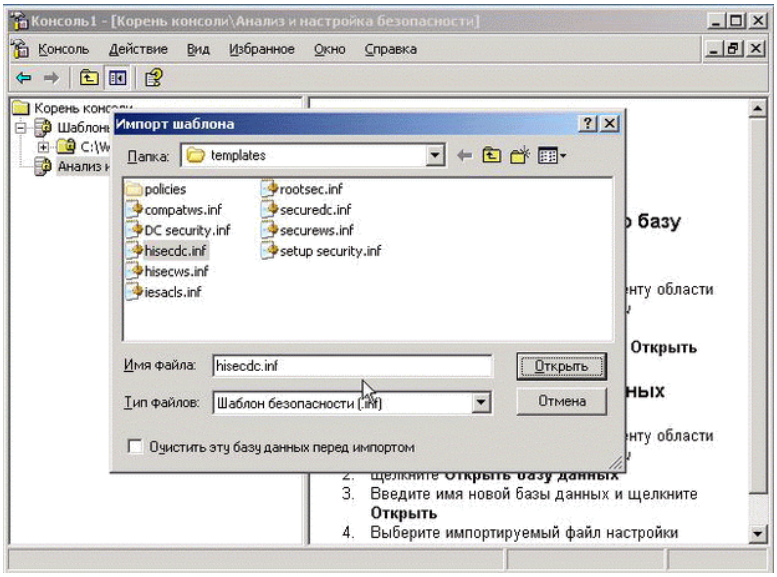


Рис. 3.5 – Аналіз налаштувань параметрів безпеки

Перш ніж приймати рішення про встановлення більш високих параметрів захисту інформації в ІКС ПАТ "Зборівгаз", необхідно ретельно вивчити її склад, вимоги до серверів і робочих станцій згідно шаблонів безпеки, попередньо встановити потрібні оновлення та налаштувати параметри на всіх системах і тільки після цього застосовувати до серверів і робочих станцій шаблони з високими рівнями безпеки інформації відповідно до рисунку 3.6.

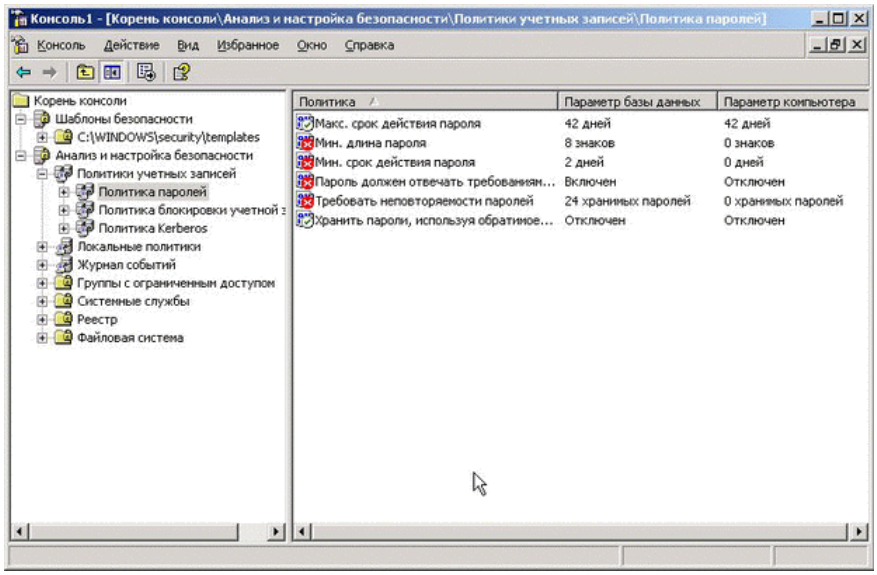


Рис. 3.6 – Налаштування політики управління паролями

Таким чином продемонстрована побудова захищеної інформаційно-комунікаційної системи ПАТ «Зборівгаз» - від рівня апаратного забезпечення до рівня додатків.

## Висновки до третього розділу

Спроектовано інформаційно-комунікаційну систему для ПАТ «Зборівгаз», де реалізовано рівень захищеності інформації відповідно до законодавчо-нормативного регулювання діяльності підприємства та його корпоративної культури. Враховано вимоги стандартів з кібербезпеки та проведена оптимізація вибору засобів захисту інформації згідно із обмеженим бюджетом проекту.

Проектування інформаційно-комунікаційної системи ПАТ "Зборівгаз" проведене з використанням профілю захищеності, визначеного засобами математичного моделювання теорії ігор, надає можливість створення ієрархічної структури опрацювання інформації та забезпечить контрольований доступ до неї з визначених політиками безпеки робочих станцій. Уся інформація, що циркулює в ІКС відповідає вимогам безпеки інформації та забезпечує рівні захисту і доступну в залежності від статусу користувача та політик безпеки.

# ВИСНОВКИ

У роботі захищеністю інформаційно-комунікаційної системи ми вважаємо її здатність забезпечувати цілісність, конфіденційність та доступність інформації, виявляти зловмисні втручання та не допускати їх впливу на інформацію.

Комерційні методики підвищення рівня захищеності інформаційно-комунікаційної системи орієнтовані на реалізацію функцій, узгоджених з менеджментом та працівниками компанії. Позитивним аспектом такого підходу є його зрозумілість для споживачів послуг кібербезпеки та швидкість у розробці політики інформаційної безпеки. Недоліком таких методик є відсутність можливості точно виміряти рівень захищеності.

Вивчення стандартів не дало вичерпної відповіді на питання побудови інформаційно-комунікаційної системи заданого рівня захищеності, оскільки положення стандартів дають можливість оцінити ризики кібербезпеки, а не захищеність. Ступінь ризику найчастіше оцінюється як низький, середній, високий чи критичний. За результатами огляду положень міжнародних стандартів інформаційної безпеки та нормативних документів України, що регламентують розробку та безпечне функціонування інформаційно-комунікаційних систем констатуємо, що питанню числового вимірювання рівня захищеності увага не приділяється.

Науковці проводять дослідження цієї проблеми і пропонують різні напрями її вирішення, залежно від математичної моделі методу оцінювання. Базуючись на методології системного аналізу, розробили теорію дослідження безпеки структурованих систем. Сучасні інформаційно-комунікаційні системи мають відкриту архітектуру та використовують багаторівневий стек протоколів. Захищеність інформації, що циркулює у таких системах, розраховують на базі логіко-ймовірнісного методу.

Поняття профілів захищеності пов’язано з тим, що інформаційно-комунікаційна система постійно змінюється відповідно до появи нових задач, які повинна розв’язувати організація. Поняття профілів захищеності інформаційно-

комунікаційної системи визначається у нормативних документах для технічних систем захисту інформації та отримало наукову інтерпретацію в українському дискурсі з проблематики захисту інформації.

Як демонструє огляд сучасних інструментів кібербезпеки, на ринку користуються попитом багатофункціональні платформи, які поєднують кілька інструментів (антивірус, міжмережевий екран, сканер вразливостей тощо). Актуальним є питання вибору інструментарію захисту інформації в інформаційно-комунікаційній системі, враховуючи необхідні функції забезпечення безпеки та наявні ресурси підприємства.

Враховуючи вектор загроз інформаційній безпеці та різноманіття засобів захисту корпоративної мережі, а також беручи до уваги ймовірнісно-грошові потоки, поставлену проблему ми вирішили за допомогою математичного апарату теорії ігор, який дозволив: сформувати задачу захисту інформаційно-комунікаційної системи в математичному вигляді, щоб скористатися критеріями відшукання оптимальних стратегій захисту; оцінити витрати на забезпечення безпеки інформаційного ресурсу, збитки від реалізації атаки та з урахуванням цих даних прийняти оптимальне рішення; обрати ефективний профіль захищеності.

Проектування ІКС ПАТ "Зборівгаз" з використанням профілю захищеності, визначеного засобами математичного моделювання теорії ігор, надало можливість створення ієрархічної структури опрацювання інформації та забезпечило контрольований доступ до неї з визначених політиками безпеки робочих станцій. Уся інформація, що циркулює в ІКС, відповідає вимогам безпеки інформації та забезпечує рівні захисту і доступну в залежності від статусу користувача та політик безпеки.

Одним із основних завдань, вирішених при проектуванні системи управління обліковими записами користувачів ПАТ "Зборівгаз" є забезпечення інформаційної безпеки:

– технології захисту інформації запобігають крадіжці даних і зловживанню конфіденційною інформацією, а також захищають від атак вірусів

та шкідливого програмного забезпечення з мережі Інтернет. Не маючи стабільної системи мережевої безпеки, ПАТ "Зборівгаз" ризикує зазнати вторгнень, простоїв мережі, збоїв у роботі, недотримання норм регулятивного законодавства та навіть судових позовів;

– робота системи управління обліковими записами користувачів Товариства використовує комплекс засобів захисту. Навіть якщо частина обладнання виходить з ладу, решта продовжує захищати дані від можливих атак.

Встановлення рівнів мережевої безпеки надало можливість доступу до службової інформації, а також захистило їх від загроз безпеки. Система мережевої безпеки включає такі аспекти:

– захист від внутрішніх та зовнішніх мережевих атак;

– забезпечення конфіденційності обміну інформацією;

– контроль доступу до інформації, ідентифікація користувачів та їхніх дій у системі.

Адміністратор безпеки має можливість встановлювати правила доступу до даних. Доступ може надаватися залежно від ідентифікатора користувача, робочих функцій, а також за іншими важливими критеріями, що забезпечує надійність створення, зберігання та опрацювання інформації. Система захисту надає безпечний доступ до мережі працівникам, запобігаючи таким загрозам, як проникнення вірусів та несанкціонований доступ.

Напрями подальших досліджень теми:

- уніфікація критеріїв захищеності інформаційно-комунікаційної системи;
- стандартизація методики визначення рівня захищеності інформаційно-комунікаційної системи.

# СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ


1. Александер М. Б., Яциковська У. Б. Збільшення продуктивності використання обчислювального ресурсу комп’ютерної мереж // Матеріали Міжнародної науково-технічної конференції молодих учених та студентів. Актуальні задачі сучасних технологій – Тернопіль 19-20 грудня 2012. – С. 204-205.
2. Андрухів А. І. Порівняння методів оцінки захищеності корпоративних інформаційних систем / А. І. Андрухів, Д. О. Тарасов // Вісник Національного університету «Львівська політехніка». – 2006. – № 573 : Комп'ютерні системи та мережі. – С. 3–9.
3. Бартіш М. Я., Дудзяний І. М. Дослідження операцій. Ч. 3. Ухвалення рішень і теорія ігор. — Львів: Видавничий центр Львівського національного університету ім. І.Франка, 2009 . — 277 с.
4. Бартіш М. Я., Роман Л. Л. Теорія ігор. — Львів: Видавничий центр ЛНУ, 2005. — 1 А20 с.
5. Безбогов А. А. Методы и средства защиты компьютерной информации: учебное пособие / А. А. Безбогов, А. В. Яковлев, В. Н. Шамкин. – Тамбов: Изд-во Тамбовского государственного технического университета, 2006. – 196 с.
6. Биячуев Т. А., Безопасность корпоративных сетей. / под ред. Л. Г. Осовецкого. – СПб: СПб ГУ ИТМО, 2004. – 161 с.
7. Брэгг Р., Родс-Оусли М., Страссберг К. Безопасность сетей. Полное руководство. – М.: Эком, 2006. - 912 с.
8. Бурячок В. Л. Алгоритм оцінювання ступеня захищеності спеціальних інформаційно-телекомунікаційних систем // Захист інформації, Північна Америка, 13, вер. 2011. Доступно за адресою: <http://jrnl.nau.edu.ua/index.php/ZI/article/view/2028/2019>. Дата доступу: 01.10.2020.
9. Бьяфоре Б. Microsoft Visio 2007. Библия пользователя. – М.: Диалектика-Вильямс, 2009. – 800 с.

10. Васильев В.А. Модели экономического обмена и кооперативные игры. - Новосибирск: Изд-во НГУ, 1984. – 96 с.
11. Голотенко О.С. Архітектура комп’ютерних систем: конспект лекцій для студентів усіх форм навчання з курсу «Архітектура комп’ютерних систем» – Тернопіль : Вид-во ТНТУ імені Івана Пулюя, 2016 – 120 с.
12. Глушак В. В., Новіков О. М. Синтез структури системи захисту інформації з використанням позиційної гри захисника та зловмисника, ч. II, Системні дослідження та інформаційні технології, 2013, С. 89–100.
13. Голобородько М. Ю., Курченко О. А., Кирись О. С. Методи числової оцінки рівня захищеності інформації у сегменті корпоративної інформаційної системи / Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського, №2(51), 2014. – С. 137-139.
14. Добринін І. С., Борова М. П., Оптимізація вибору варіанту побудови системи захисту інформації від атак при антагоністичній грі, вип. II, Системи озброєння і військова техніка, 2018, С. 89–93.
15. Жуков І. А., Гуменюк В. О., Альтман І. Є. Комп'ютерні мережі та технології (навчальний посібник). Видавництво Національного авіаційного університету "НАУ-друк", 2004. – 276 с.
16. Захист інформації в автоматизованих системах управління: навчальний посібник / Уклад. І. А. Пількевич, Н. М. Лобанчикова, К. В. Молодецька. – Житомир: Вид-во ЖДУ ім. І. Франка, 2015. – 226 с.
17. Згуровский М. З., Панкратова Н. Д. Системный анализ (проблемы, методология, приложения). — К.: Наук. думка, 2005. — 744 с.
18. Калиберда Е. А., Рыбкин А. А. Анализ уязвимостей по степени их влияния на защищённость и качество структурно-сложных информационных систем / Вестник Омского университета, 2014, №2, С. 130-135.
19. Карпінський М. Технічні засоби захисту як основа безпеки мереж / М. Карпінський, Н. Мороз, А. Яворський // Збірник тез доповідей XVIIнаукової конференції ТНТУ ім. Івана Пулюя, 20-21 листопада 2013 року. — Т. :

ТНТУ, 2013. — Том I : Природничі науки та інформаційні технології. — С. 22.

20. Лабскер Л. Г., Ященко Н. А. Теория игр в экономике (практикум с решениями задач). - М.: Проспект, 2013. - 284 с.
21. Льюс Р., Райфа Х. Игры и решения. - М.: Изд-во иностранной литературы, 1961. - 642 с.
22. Мак-Кинси Дж. Введение в теорию игр. — М. : ГИФМЛ, 1960. — 420 с.
23. Митник О. Архітектура програмно-конфігурованих мереж / О. Митник // Матеріали VI науково-технічної конференції „Інформаційні моделі, системи та технології“, 12-13 грудня 2018 року. — Т. : ТНТУ, 2018. — С. 80.
24. Можаев А. С. Общий логико-вероятностный метод анализа надежности сложных систем: Учеб. пособ. — Л.: ВМА, 1988. — 68 с.
25. Мулен Э. Теория игр с примерами из математической экономики. — М.: Мир, 1985. — 200 с.
26. Назаревич О. Комбінована система миттєвого реагування в задачах захисту / Назаревич О., Коріненко О. // Вісник Тернопільського державного технічного університету. — том 14. — с.144-150
27. НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу. URL: https://tzi.com.ua/downloads/1.1-002-99.pdf (дата звернення: 23.09.20).
28. НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. URL: https://tzi.ua/assets/files/%D0%9D%D0%94-%D0%A2%D0%97%D0%86-2.5-004-99.pdf (дата звернення: 23.09.20).
29. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу. Затверджено нак. Департаменту спеціальних телекомунікаційних систем та захисту інформації СБ України від “ 28 ” квітня 1999 р. № 22 із змінами згідно наказу Адміністрації Держспецзв'язку від 28.12.2012 № 806. - 61 с.

30. НД ТЗІ 2.5-005 -99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу. Затверджено наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації СБ України від 28 квітня 1999 р. № 22. Зі Зміною №1, затвердженою наказом Адміністрації Держспецзв'язку від 15.10.2008, № 172. - 20с.
31. Новіков О. М., Тимошенко А. О. Побудова логіко-ймовірнісної моделі захищеної комп'ютерної системи // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. — 2001. — Вип. 3. — С. 101—105.
32. Олифер В., Олифер Н. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 5-е изд. - СПб: Питер, 2016. - 992 с.
33. Оуэн Г. Теория игр. — М. : Мир, 1971. — 232 с.
34. Панкратова Н. Д. Системний аналіз в динаміці діагностування складних технічних систем // Системні дослідження та інформаційні технології. — 2008. — № 1. — С. 33—49.
35. Рябинин И. А. Научная школа логико-вероятностных методов и концепция логико-вероятностной теории безопасности сложных систем / Под ред. И.А. Рябинина // Теория и информационная технология моделирования безопасности сложных систем / Препринт 101. — СПб.: ИПМАШ РАН, 1994. — Вып. 1. — С. 3—22.
36. Сетевой доступ в Windows Server 2008 на основе политик URL: http://www.oszone.net/6690/Windows_Server_2008 (дата звернення: 25.04.20).
37. Сычев Ю. Н. Основы информационной безопасности. Учебно-практическое пособие. – М.: Изд. Центр ЕАОИ, 2007. – 300 с.
38. Таненбаум Э., Уэзеролл Д. Компьютерные сети. Изд-во: Питер, 2013. – 960 с.
39. Толубко В. Б., Курченко О. А., Шевченко А. В. Стабілізація функціональної стійкості інформаційної системи шляхом управління

динамікою розвитку профілів захищеності // Сучасний захист інформації №3(35), 2018. – С. 51-57.

40. Уокенбах Д., Александер М., Куслейка Р. Excel 2019. Библия пользоваленя. – М.:Диалектика, 2020. – 1136 с.
41. Фон Нейман Дж., Моргенштерн О. Теория игр и экономическое поведение. - М.: Наука, 1970. – 708 с.
42. Фон Нейман Дж., Моргенштерн Э. Теория игр и экономическое поведение. — М. : Наука, 1970. — 708 с.
43. Хнигічева А. М., О.М. Новіков, А.О. Тимошенко моделювання захищеності складних інформаційно-комунікаційних систем із використанням логікоймовірнісного методу // Наукові вісті НТУУ "КПІ". – 2010. – Вип. 6. – С. 70-77.
44. Челноков А. Ю. Теория игр: Учебник и практикум для бакалавриата и магистратуры. – М.: Юрайт, 2016. – 120 с.
45. Шагин В. Л. Теория игр: учебник и практикум. - М: Юрайт, 2019. - 223 с.
46. Шиян А. А. Теорія ігор: основи та застосування в економіці та менеджменті. Навчальний посібник. – Вінниця: ВНТУ, 2009. – 164 с.
47. Юдін О. К., Богуш В. М. Інформаційна безпека держави: Навчальний посібник. – Харків: Консул, 2005. – 576 с.
48. Якубайтис Э. А. Архитектура вычислительных сетей. – М.: Статистика, 1980. – 279 с.
49. 2019 Cyberthreets Defense Report, Group CyberEdge, 2019 URL: https://go.illusivenetworks.com/2019-cyberthreat-defense-report (Last accessed 19.04.20).
50. AdRem SNMP Manager. URL: http://www.softsoft.ru/network-internet/network-monitoring/3318.htm (дата звернення: 25.04.20).
51. Bell D. E., La Padula L. J. Security Computer System: Mathematical Foumdation // Mitre Techical Report 2547. — 1973. — 2. — 35 p.

52. Do C. T., Tran N. H., Hong C., Camhoua C. A., Kwiat K. A., Blasch E., Ren S., Pissinou N., Iyengar S. S. Game Theory for Cyber Security and Privacy, ACM Computing Surveys (CSUR), 2017, Article No.: 30.
53. Framework for Improving Critical Infrastructure Cybersecurity. National Institute of Standards and Technology, 2018. – 48 p.
54. ISO/IEC 27006:2011 Information technology. Security techniques. Requirements for bodies providing audit and certification of information security management systems. URL: https://www.iso.org/standard/59144.html (Last accessed: 23.03.20).
55. Johnson A., Dempsey K., Ross R., Gupta S., Bailey D. Guide for Security-Focused Configuration Management of Information Systems. - NIST Special Publication 800-128, 2011. – 99 p.
56. Kaspersky Security Bulletin 2019. Статистика. – 18 с. URL: https://go.kaspersky.com/rs/802-IJN-240/images/KSB_2019_Statistics_RU.pdf (дата звернення: 23.03.20).
57. Kaur R., Hils A., D'Hoinne J., Watts J. Magic Quadrant for Network Firewalls. Published 17 September 2019. URL: https://www.gartner.com/doc/reprints?id=1-1OEPTVC9&ct=190820&st=sb (Last accessed 19.04.20).
58. Kissel R., Stine K., Scholl M., Rossman H., Fahlsing J., Gulick J. Security Considerations in the System Development Life Cycle. - NIST Special Publication 800-64 Revision 2, 2008. – 68 p.
59. Murashka U. 3 Levels of Corporate Network Security. URL:https://www.scnsoft.com/blog/3-levels-corporate-network-security (Last accessed: 21.02.20).
60. Shiva S., Roy S., Dasgupta D. “Game theory for cyber security”, CSIIRW '10: Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research, 2010, Article No.: 34, Pages 1–4.

61. Solojentsev E. D. Peculiarities of Logic and Probabilistic Theory with groups of Incompatible Events // Automa Бtion and Remote Control. — 2003. — N 7. — P. 187—204.
62. Understanding Cybersecurity Standards URL: https://www.cgi.com/sites/default/files/2019-08/cgi-understanding-cybersecurity-standards-white-paper.pdf (Last accessed: 21.03.20).
63. WASC Threet Classification v. 2.0, 2010. URL: http://projects.webappsec.org/f/WASC-TC-v2_0.pdf (Last accessed 19.04.20).
64. Zgurovsky M. Z. Sustainable development global simulation: Opportunities and treats to the planet // Russ. J. Earth Sci. — 2007. — 9, N 2. — http://www.agu.org/ WPS/rjes/abstract/v09/2007ES000273-abs.html;

# ДОДАТКИ