Вінницький національний технічний університет
Факультет інформаційних технологій та комп'ютерної інженерії
Кафедра захисту інформації

МАГІСТЕРСЬКА КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Захищена автоматизована система контролю та управління букмекерською конторою»

Виконав: студент 2-го курсу, групи 1БС-20м
спеціальності 125 – Кібербезпека
(шифр і назва напряму підготовки, спеціальності)
_____ Лабусюк В.М.
(прізвище та ініціали)
Керівник д. т. н., проф, зав. каф. ЗІ
_____ Лужецький В.А.
(прізвище та ініціали)
Опонент: к.т.н., проф, проф. каф. ОТ
_____ Азарова А.О.
(прізвище та ініціали)

«____» _____ 2021 р.

Допущено до захисту
Завідувач кафедри ЗІ
д.т.н., проф.
_____ Лужецький В.А.
«____» _____ 2021 р.

Вінниця ВНТУ – 2021 рік

Вінницький національний технічний університет
Факультет інформаційних технологій та комп'ютерної інженерії
Кафедра захисту інформації
Освітньо-кваліфікаційний рівень магістр
Спеціальність 125 Кібербезпека
ОПП Безпека інформаційних і комунікаційних систем

ЗАТВЕРДЖУЮ
Завідувач кафедри ЗІ, д.т.н., проф.
_____ В.А. Лужецький
_____ _____ 2021 року

ЗАВДАННЯ

НА МАГІСТЕРСЬКУ КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ

Лабусюку Віталію Михайловичу

1. Тема роботи: «Захищена автоматизована система контролю та управління букмекерською конторою»,
керівник роботи: Лужецький Володимир Андрійович д. т. н., проф, зав. каф. ЗІ,
затверджена наказом ректора ВНТУ №_____ від __ 2021 р.
2. Строк подання студентом роботи _____2021 р.
3. Вихідні дані до роботи:
   - об'єкт захисту – букмекерська контора «LiveScore»;
   - структура об'єкту захисту;
   - ресурси об'єкту захисту;
   - метод моделювання – логіко-імовірнісний;
   - комплекси систем захисту.
4. Зміст розрахунково-пояснювальної записки: Вступ. Аналіз інформаційних джерел. Структура і ресурси букмекерської контори. Розробка математичної моделі оцінювання рівня захищеності. Розробка політики безпеки. Економічна частина. Висновки. Перелік використаних джерел. Додатки.
5. Перелік ілюстративного матеріалу.
Структура букмекерської контори (плакат, А4). Логіко-ймовірнісна модель оцінки рівня інформаційної безпеки (плакат, А4). Моделі загроз та порушника (плакат, А4). Комплекс засобів для системи захисту (плакат, А4). Використовувані інструменти (плакат, А4). Okta Identity and Access Management(плакат, А4). Symantec DLP (плакат, А4). McAfee Network Security Platform (плакат, А4).

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанти	Підпис, дата	
		завдання видав	завдання прийняв
1	Лужецький В.А., д. т. н., проф, зав. каф. ЗІ		
2	Лужецький В.А., д. т. н., проф, зав. каф. ЗІ		
3	Лужецький В.А., д. т. н., проф, зав. каф. ЗІ		
4	Лужецький В.А., д. т. н., проф, зав. каф. ЗІ		
5	Лесько О. Й., проф., зав. каф. ЕП і ВМ		

7. Дата видачі завдання 9 вересня 2021 року

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів бакалаврської дипломної роботи	Строк виконання етапів роботи	Примітка
1	Аналіз завдання. Вступ	01.09.2021 – 07.09.2021	
2	Розробка технічного завдання	08.09.2021 – 9.09.2021	
3	Аналіз інформаційних джерел за напрямком магістерської кваліфікаційної роботи	20.09.2021 – 26.09.2021	
4	Формулювання загальних вимог до АСКУ букмекерської контори	27.09.2021 – 4.10.2021	
5	Розробка математичної моделі оцінювання рівня захищеності	05.10.2021 – 9.10.2021	
6	Розробка політики безпеки та створення оптимальної КСЗІ	10.10.2021 – 29.10.2021	
7	Аналіз ТЗ, висновки	30.10.2021 – 5.11.2021	
8	Попередній захист та доопрацювання МКР	16.11.2021 – 0.11.2021	
9	Перевірка магістерської роботи на наявність плагіату		
10	Представлення МКР до захисту, опонування		
11	Захист МКР		

Студент _____ В.М. Лабусюк

Керівник роботи _____ В.А Лужецький

АНОТАЦІЯ

УДК 004.031.43

Лабусюк В.М. Захищена автоматизована система контролю та управління букмекерською конторою. Магістерська кваліфікаційна робота зі спеціальності 125 – кібербезпека, освітня програма – Безпека інформаційних і комунікаційних систем. Вінниця: ВНТУ, 2021. 99 с.

На укр. мові. Бібліогр.: 22 назв; рис.: 14; табл. 25.

Магістерська кваліфікаційна робота присвячена розробці захищеної автоматизованої системи контролю та управління букмекерською конторою. Проведено аналіз інформаційних джерел щодо актуальності проблеми, світових позицій щодо забезпечення безпеки в цій сфері, підвищення безпеки програмного забезпечення букмекерів. У роботі здійснено формулювання загальних вимог до автоматизованої системи управління та контролю букмекерською конторою. Проведено аналіз структури обєкту захисту, ресурсів, аналіз конкурентного середовища. Розроблено математичну модель оцінки рівня захищеності. Розроблено політику безпеки автоматизованої системи контролю та управління.

Ілюстративна частина складається з 8 плакатів, що демонструють структурну модель досліджуваного обєкта захисту, а також результат моделювання захисту.

В економічному розділі оцінено витрати на розробку.

Ключові слова: захист букмекерської контори, автоматизована система контролю та управління, загрози букмекерській діяльності, інструкцій з безпеки системному адміністратору

ABSRACT

Labusiuk V.M. Protected automated control and management system of the bookmaker. Master's thesis in specialty 125 – cybersecurity. Vinnitsa: VNTU, 2021. – 99 p.

In Ukrainian language. Bibliographer: 22 titles; fig.: 14; tabl. 25.

The master's qualification work is devoted to the development of a secure automated system of control and management of a bookmaker's office. The analysis of information sources on the urgency of the problem, world positions on security in this area, improving the security of bookmakers' software. The paper formulates the general requirements for the automated management and control system of the bookmaker. The analysis of the structure of the object of protection, resources, analysis of the competitive environment is carried out. A mathematical model for assessing the level of security has been developed. A security policy and an optimal automated control and management system have been developed.

The graphic part consists of 4 posters showing the structural model of the studied object of protection, as well as the result of modeling protection.

The economic section estimates the development costs.

Keywords: bookmaker protection, automated control and management system, threats to bookmaking, security instructions for system administrator

ЗМІСТ

ВСТУП

За останні десятиліття, особливо як наслідок сучасних реалій спричинених світовою пандемією, розвиток букмекерської діяльності набув надзвичайно широкого попиту в мережі інтернет, де люди тепер можуть робити фінансові транзакції з метою встановлення ставок у небачених раніше кількостях, що вимагає приділенню особливої уваги, так як мова йде про мільйони людей по всьому світі, і обороти мільярдів доларів, конфіденційність їх персональних даних та їх платіжних карток. Така діяльність вимагає особливого контролю як з боку законодавства країн де вони проводяться [1], так і забезпечення інформаційної безпеки відповідно до вимог нормативно-правових документів щодо обробки та забезпечення таємниці персональних даних. Важливим є забезпечення надійності їх операцій та стабільного функціонування в умовах та наслідках пандемії. Не менш важливим є забезпечення їх відмовостійкості, так як йде мова про репутацію самих букмекерських контор так і гарантій обробки фінансових операцій що вимагаються законами відповідних держав. Для забезпечення захисту, обмежененя доступу неавторизваних користувачів букмекерських контор, постає питання розробки захищеної автоматизованої системи контролю та управління такою букмекерською конторою. Така система має в собі набір інструкцій, правил, політик, стандартів, процесів, для роботи букмекерської організації, її співробітників та її ресурсів.

Букмекерські контори страждають від витоку інформації, внутрішніх та зовнішніх загроз, тому розроблювана автоматизована система контролю та управління повинна забезпечити надійну роботу усієї організації та її клієнтів.

Актуальність. Стрімкий розвиток та перенесення букмекерських кантор на простір інтернету [2] вимагає заходів забезпечення доступності їх вебсервісів, при сучасних тенденціях ринка з особливою увагою на надзвичайну кількість запитів що веде до роботи з великими об’ємами даних. Цілісності, так як мова йде про фінансові питання, де мінімальне втручання у вміст запиту може пошкодити операції. Та конфіденційності, де особисті дані гравців та персоналу

букмекерської контори повинні знаходитись в повній таємниці. Виникає необхідність захисту інформаційної безпеки букмекерських контор від загроз у вигляді різних мережевих атак, та інших обчислювальних навантажень, у вирішенні яких необхідне правильне моделювання за допомогою автоматизованої системи керування та управління.

Об'єктом дослідження є процеси захисту автоматизованої системи контролю та управління букмекерської контори.

Предметом дослідження є методи та засоби захисту автоматизованої системи контролю та управління букмекерською конторою.

Метою магістерської кваліфікаційної роботи є підвищення рівня захищеності автоматизованої системи контролю та управління букмекерської контори.

Для досягнення мети необхідно розв'язати такі задачі:

– визначити предметну область букмекерських організацій;

– проаналізувати сучасні методи та засоби захисту букмекерських контор;

– розробити захищену автоматизовану систему контролю та управління букмекерською конторою;

– розробити математичну модель оцінювання рівня захищеності;

– розробити політики безпеки.

Методи дослідження. Для виконання поставлених задач були використані методи ідентифікації загроз, методи для оцінювання рівня захищеності; методи аналізу результатів моделювання.

Наукова новизна. Вперше запропоновано математичну модель оцінювання захищеності автоматизованої системи контролю та управління букмекерською конторою, яка забезпечує обгрунтований вибір комплексу засобів для системи захисту.

Практична цінність роботи полягає у розробці автоматизованої системи контролю та управління букмекерської контори.

1 АНАЛІЗ ІНФОРМАЦІЙНИХ ДЖЕРЕЛ

1.1. Позиції урядів щодо букмекерської діяльності

У цьому підрозділі досліджуються політичні документи [3] що викладають позицію уряду щодо запропонованих змін до Закону про авторизовані букмекерські операції (Закон), вперше піднятий південноавстралійською Лігою букмекерів (SABL) у середині 2007 року. У ньому враховано відповіді, отримані на звіт про проблеми, оприлюднений у березні 2008 р. Відповіді надійшли від:

- Harness Racing SA (HRSA);
- Управління Уповноваженого з питань алкогольних напоїв та азартних ігор (OLGC);
- Незалежний орган з питань азартних ігор (IGA);
- Mr Syd McDonald;
- Управління з перегонів;
- Ліга букмекерів Південної Австралії (SABL);
- SA TAB;
- Чистокровні гонки Південної Австралії (TRSA).

Цей програмний документ містить відповіді уряду на кожне з питань, порушених у Проблемному документі. Цей документ має таку саму структуру, що й документ про проблеми, і містить відповіді в наступних розділах:

- ліцензування;
- дозволи;
- правила;
- виконання та дотримання;
- невитребувані виграші;
- інформаційна служба про ставки.

Таблиця нижче (табл. 1.1) підсумовує політичні позиції, досягнуті в цьому політичному документі.

Таблиця 1.1. Підсумок політичних позицій.

Сфера	Позиції
Ліцензування	Уряд Південної Австралії пропонує внести зміни до Закону про уповноважені букмекерські операції, щоб включити положення про кримінальну розвідку та заборонити інспекторам, уповноваженому з питань алкоголю та азартних ігор, членам і секретарю незалежного управління азартних ігор брати участь у азартних іграх з ліцензіатом. Комісар з питань алкоголю та азартних ігор погодився використовувати дискреційні повноваження для продовження терміну дії ліцензії для букмекерської контори з поточного однорічного терміну до трирічного терміну з 1 січня 2013 року. Дискреційні повноваження будуть використовуватися для проведення фінансових оцінок на основі ризиків протягом термін дії ліцензії.
Дозволи	Уряд Південної Австралії пропонує скасувати дозвіл, що міститься в розділах 54-59 Закону про уповноважені букмекерські операції 2000 року. Домовленості про поле підлягають переговорам між гоночними клубами (або їх агентами) та букмекерськими конторами. Щоб забезпечити дотримання затвердженої урядом ліцензійної угоди з SA TAB, Уповноважений встановить умови ліцензії, які обмежують, коли і де букмекери можуть приймати ставки.
Правила	Регуляторні функції, пов’язані з Правилами ліцензування букмекерських контор 2000 року, продовжуватимуть виконуватися державними установами. Незалежний орган з питань азартних ігор погодився: провести комплексну оцінку букмекерських контор

	Правилами ліцензування з метою зменшення адміністративного навантаження на букмекерські контори; а також отримати подання від букмекерських контор, гоночних клубів та інших зацікавлених сторін щодо Правил ліцензування букмекерських контор. Пропонується внести зміни до Закону про авторизовані букмекерські операції, щоб спростити дію розділу 62(1)(b) стосовно цінних паперів букмекерської контори. Розділ 62(1)(b) має стосуватися будь-якої букмекерської контори, а не лише претендента на букмекерську ліцензію.
Забезпечення виконання та дотримання	Незалежний орган з питань азартних ігор збереже дисциплінарну функцію.
Невитребувані виграші	Департамент казначейства і фінансів, а також споживчих і ділових послуг (CBS – раніше Управління з питань алкогольних напоїв та азартних ігор) розпочали обговорення з букмекерськими конторами та індустрією перегонів, щоб визначити, чи є можливими угоди про незатребувані виграші, якими керують букмекерські контори. Позови будуть розглядатися протягом одного року. Незатребувані виграші, які не були заявлені протягом одного року, потрібно буде переслати до CBS для виплати на консолідований рахунок.
Інформаційна служба ставок	Відповідальність за схвалення відповідно до розділу 61 Закону про авторизовані букмекерські операції від 2000 року не зміниться.

Управління вважає, що повинна існувати система безпеки букмекерської контори, і що основним обґрунтуванням цієї системи має бути захист клієнтів букмекерських контор. Орган надає перевагу збереженню існуючої системи

окремих цінних паперів букмекерської контори, встановленої на належному рівні. Наразі правила дозволяють Уповноваженому фіксувати рівні для ліцензіата за ліцензіатом. Як сказано в даний час, це має бути діяльністю на основі винятків, оскільки більшість букмекерських контор підпадають під фіксовані рівні зобов'язань за замовчуванням.

Ці правила дозволяють створити модель фонду довіри, оскільки вони дозволяють такому органу, як Ліга букмекерів Південної Австралії, бути схваленим як гарант або постачальник безпеки за зобов'язаннями букмекерів.

Нинішня позиція влади щодо галузевої схеми полягає в тому, що переважна більшість учасників галузі має бути задоволена тим, що пропонується. Управління робить це зауваження в контексті досвіду інших фондів довіри, де великі розкрадання призвели до того, що оператори, які відповідають вимогам, постраждали.

Ліга підтримує OLG [3] C у продовженні адміністрування розміщення облігацій, тобто системи безпеки. Ліга вважає, що належний контроль за облігаціями має замінити потребу подавати річну фінансову звітність.

Букмекери повинні мати справу з двома державними регулюючими органами щодо подання та повернення цінних паперів. У той час як уповноважений орган тримає готівку, Незалежне управління азартних ігор (IGA) утримує банківські гарантії та іпотеку. Домагаючись звільнення банківської гарантії або погашення іпотеки з боку IGA, букмекерська контора повинна спочатку отримати згоду уповноваженого, оскільки саме Комісар повинен бути впевнений, що забезпечення гарантій залишилося достатньо. Уряди інших штатів регулюють розмір необхідного забезпечення або гарантії, але не мають цього забезпечення. Управління цінними паперами здійснюється букмекерськими асоціаціями. Рівень безпеки повинен бути достатньо високим, щоб гарантувати впевненість і захист, бути справедливим для всіх букмекерів і підлягати оцінці позивачів у випадку, якщо букмекерська контора не зможе виконати свої зобов'язання щодо ставок.

Системою безпеки й надалі керуватимуть CBS та IGA. IGA розгляне деталі системи безпеки під час всебічної оцінки Правил ліцензування букмекерських контор.

Як зазначено в документі [3], пропонується внести зміни до Закону про авторизовані букмекерські операції 2000 року, щоб спростити дію розділу 62(1)(b) стосовно цінних паперів букмекерської контори.

Міністерство казначейства та фінансів і CBS розпочали обговорення з букмекерськими конторами та індустрією перегонів, щоб визначити, чи є можливими угоди про невитребувані виграші, які керують букмекерські контори. Позови будуть розглядатися протягом одного року. Невитребувані виграші, які не були заявлені протягом одного року, потрібно буде виплатити на консолідований рахунок.

Галузевий форум, що складається з найбільших британських компаній, що займаються азартними іграми в Інтернеті, протягом кількох місяців лобіював постачальників Інтернет-послуг, щоб забезпечити всім своїм клієнтам кращу безпеку.

Багато букмекерських контор почали вирішувати проблему DDoS атак, це було підтверджено технічним директором на сайті онлайн-букмекерів Blue Square, виступаючи на Конгресі e-Crime Congress у Лондоні. Один із висновків конференції було запровадити розповсюдження брандмауерів своїм клієнтам.

На конгресі e-Crime Congress також піднімалися питання щодо впровадження Закону про зловживання комп’ютерами, яке за висновками заслуговує схвалення, але часу приділеного на дослідження цього питання недостатньо для впровадження. Європейський віце-президент зі стратегії безпеки Computer Associates повідомив що така ситуація є образою для британського бізнесу, якому найбільше загрожують кібератаки.

1.2. Підвищення безпеки програмного забезпечення букмекерів

Було досліджено програмне забезпечення букмекерських контор, зокрема New Bookmaker Software. Програмне забезпечення New Bookmaker Software – це система, яка використовується в інформаційних системах спортивних ставок, і вважається досить захищеною для збереження всієї таємної інформації для учасників та власників таких букмекерських контор в режимі реального часу [4]. Програмна складова пропонує просунуте програмне забезпечення з підвищеною безпекою та масштабованістю, яке вважається захистом від шахрайства, програмне забезпечення характеризується високим рівнем архітектурної структури та непроникним брандмауером. Програмне забезпечення New Bookmaker Software використовується у великих закладах ставок, підтримує надвисоку частоту для операцій зі ставками в мережах.

Оскільки ставки – це те, що стосується грошей, безпека такого програмного забезпечення є одним з найважливіших критеріїв для зміцнення довіри та впевненості учасників до таких онлайн-операцій. Серед використовуваного програмного забезпечення великих букмекерських контор, варто відмітити також програмне забезпечення BOOKIE [5], що також ідеально підходить для невеликих контор, які працюють лише в одному відділенні або магазині. Коли ми говоримо про безпеку програмного забезпечення букмекерів, існує багато запобіжних заходів, щоб зробити його безпечним для користувачів. Система є однією з найбільш захищених від кіберзлочинності або шахрайства; є ряд заходів щодо його встановлення та інфраструктури, які ми будемо досліджувати.

1.2.1 Внутрішня безпека букмекерської контори

Програмне забезпечення розробляється таким чином, що після використання в букмекерській конторі особа або власник можуть легко контролювати всі дії з панелі керування. Панель управління використовується як точка внутрішньої безпеки в самому магазині, це означає, що всі системи, які безпосередньо пов’язані з сервером, знаходяться під повною безпекою.

Менеджер сервера може виявити будь-яку помилку або шахрайство, які можуть статися з цього магазину в режимі реального часу, будь-який сервер, підключений до терміналу керування, може бути негайно відключений при виявленні будь-якої підозрілої активності, термінали також підключені до віддалених центральних серверів, які вчасно відстежують усі деталі.

1.2.2 Хмарна безпека

Програмне забезпечення букмекерських контор підключено до хмарної безпеки, завдяки чому його робота не буде порушена, тип з'єднання обслуговується високоякісною інтернет-інфраструктурою брандмауера і належним [6] чином перевіряється на будь-які шахрайські дії в режимі реального часу.

Концепція "безпека хмари" відрізняється від терміну "безпека у хмарі". Вперше різниця була сформульована Amazon [7] для роз'яснення спільної відповідальності постачальників і клієнтів. Постачальники хмарних послуг зазвичай відповідають за фізичну та мережеву інфраструктуру хмарної служби. Клієнти, які в даному випадку є букмекерською організацією – за налаштування доступу, парольну політику та інші питання, які не залежать від сервіс-провайдера.

Ці питання регулюються договірними угодами та зобов'язаннями. Основним є договір про рівень обслуговування (SLA) з постачальником та замовником. Така угода містить кількісні та якісні характеристики наданих послуг, їх доступність, ступінь підтримки користувачів, час виправлення несправності тощо.

На мережевому шлюзі розміщуються спеціальне обладнання для моніторингу передбачуваного трафіку і пристроїв. Однак сьогодні цього вже недостатньо. Щоб усунути прогалини в безпеці, букмекерським організаціям потрібна єдина панель управління, яка забезпечує наочність і дозволяє сформувати узгоджені політики безпеки у всій інфраструктурі для ефективного управління ризиками. Рішення безпеки повинні обмінюватися і зіставляти відомості про загрози, отримувати і впроваджувати централізовано узгоджені

політики і зміни в конфігураціях і координувати всі ресурси для своєчасного реагування на виявлені загрози.

Окрім того, вони мають охоплювати всю розподілену інфраструктуру, динамічно масштабуватися при збільшенні ресурсів додатків і автоматично адаптуватися в міру пристосування інфраструктури до мінливих вимог. І, що не менш важливо, ці рішення повинні забезпечувати узгоджену функціональність і застосування політик незалежно від свого форм-фактору й місця розгортання.

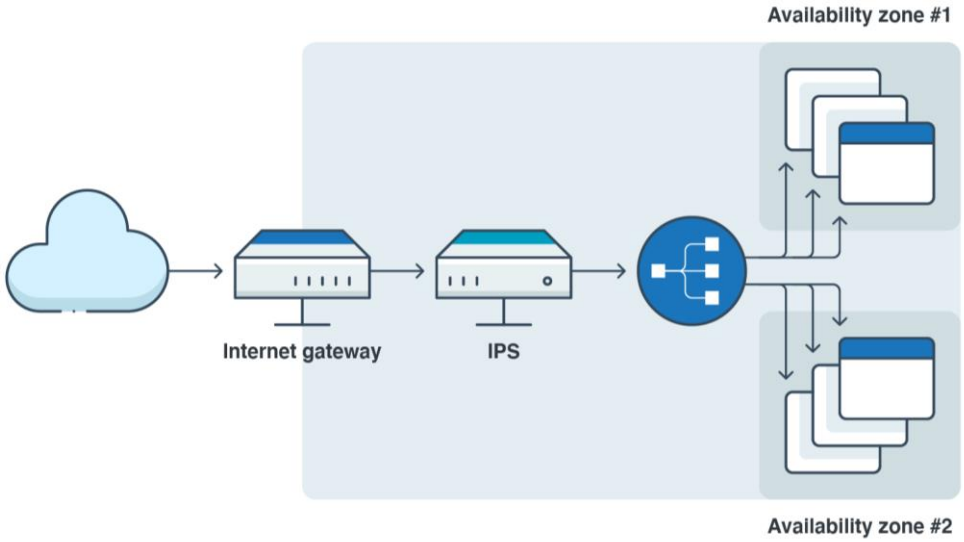


Рисунок 1.1. Структура хмарної безпеки.

Система мережевої безпеки у хмарі повинна мати можливість "бачити" весь трафік букмекінга, незалежно від джерела.

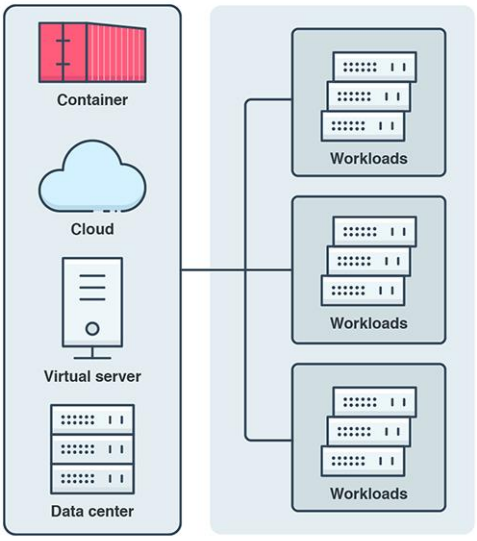


Рисунок 1.2. Структура розподілу навантаженості серверів

Робочі навантаження повинні контролюватися щодо загроз, незалежно від їх характеру та походження.

Традиційна безпека не може бути розгорнута на певних серверних або контейнерних платформах, але самі програми потрібно захищати так само надійно, як і інші частини інформаційної системи. Для багатьох компаній швидке та ефективне програмування та розгортання нових додатків є головними рушіями переходу до хмари. Але ці програми є потужними точками входу для загроз виконання веб-додатків, таких як введення коду, автоматизовані атаки та віддалені виконання команд.

1.2.3 Точний касовий інтерфейс

Програмне забезпечення забезпечує високу безпеку через касу, точність кожної системи, встановленої в касі, є свідченням того, наскільки безпечне програмне забезпечення. Весь інтерфейс, підключений до касових апаратів, також пов’язаний з основним сервером та іншими зовнішніми серверами. BOOKIE дійсно може побачити, чи потрібні їм усі деталі до копійки, що виходять із каси, це полегшує відстеження будь-якого типу транзакції, яка відбулася з інтерфейсу. Сканування та штрих-коди також можуть виявити що-небудь або підроблену картку. Усі запити, вхідні-вихідні на шлюзи сервера, а також проміжні повязані з касою мають необхідність журналюватися, та зберігатися на протязі довгого часу, аби мати гарантійність підтвердження прозорості процесу. Усі мережеві запити які виконують до внутрішнього шлюзу, а також з ним пов’язані проміжні, повинні мати унікальний ідентифікатор запиту, за допомогою якого можна бути відслідкувати порядок обробки запиту у журналах. Це дозволяє проводити тестування та перевірку якості.

1.2.4 Трансляція діяльності центрального сервера

Програмне забезпечення дозволяє передавати все, що відбувається з внутрішніх серверів, це включає всі ставки та спортивні заходи, які проводяться в Інтернеті. Воно також передає та надає інформацію про учасників, які використовували які компютери та в який час дня чи ночі, діяльність миттєво транслюється [8] на інші підключені пристрої, щоб підвищити безпеку в режимі

реального часу. Ця система миттєвої передачі захищає всі ігри в реальному часі та прибуток.

1.2.5 Зашифрований мастер-пароль

Існують також інші заходи, які вживаються для перевірки безпеки облікових записів гравців, для входу до програмного забезпечення клієнту потрібен головний пароль. Потім пароль шифрується в обліковому записі учасників та на компютері в режимі реального часу, процес продовжується на комп'ютері користувача або будь-якому іншому пристрої, який він або вона використовує. Кожна діяльність учасника відбувається з його комп'ютера без будь-якої особистої інформації чи інформації для входу на головний сервер.

Безпека програмного забезпечення букмекерських контор останнім часом була підвищена завдяки постійним удосконаленням та покращенням, але одним із важливих факторів є те, що це безпечніше, ніж коли-небудь раніше, з використанням хмарних технологій, в яких розміщена центральна система безпеки, яка працює в повній мірі.

1.2.6 Пошук "слабої ланки"

Витоки даних відбуваються в результаті того, що кіберзлочинці використовують найслабші ланки в букмекерській інформаційній системі. У багатьох букмекерських організаціях впровадження хмари призводить до розширення можливостей для атаки у геометричній прогресії. Для усунення цих слабких ланок потрібно забезпечувати єдиний рівень безпеки [9], навіть коли інфраструктура постійно змінюється. Оскільки інфраструктури розширюються і змінюються настільки швидкими темпами, важливо, щоб будь-які зміни в мережі здійснювалися в строгій відповідності із загальним планом безпеки. Вимога використовувати належні інструменти, політики і процедури безпеки до того, як будуть задіяні будь-які нові ресурси, дозволяє адаптувати рішення безпеки до змін в інфраструктурі і в додатках. Для цього необхідно вибирати інструменти безпеки, які розуміють інфраструктуру, в якій вони будуть розміщені, і які зможуть забезпечити узгоджену роботу у всіх середовищах, гарантуючи дотримання політик і високу прозорість для безпечного запуску.

1.3. Оцінка безпеки функціонування існуючих букмекерських контор

Стандарт безпеки сильно відрізняється у різних букмекерських контор, і тому варто дослідити існуючі оцінки та найкращу практику, коли справа доходить до обробки фінансових транзакцій. Хоча минуло багато часу з тих пір, як велика фірма не виплачувала клієнтам усіх залишок, надзвичайно конкурентна природа сучасних букмекерських послуг призвела до того, що менші та неефективні фірми борються або їх поглинає більші організації на напіврегулярній основі [10]. Можливо, найбільша проблема останнього часу виникла з оголошенням Betbright про припинення торгівлі та бурею через їхнє рішення не виплачувати всі свої ставки перед оплатою – щось було вирішено лише після негативної преси та особистого втручання колишнього виконавчого директора Betbright.

Варто зазначити, що Комісія з азартних ігор [11] не втрутилася, щоб вимагати, щоб ці зобов’язання були виконані в повному обсязі, це вказує на межі їх поточних повноважень, крім того Betbright запропонував лише «базовий» рівень захисту своїх клієнтів.

Реальність така, що гравці роблять регулярні ставки, дуже важливо знати про безпеку коштів, розміщених у кожній фірмі.

1.3.1. Захист коштів.

Кожна букмекерська контора зобов’язана Комісією з азартних ігор оголошувати рівень захисту коштів, внесених у них.

Сам рівень оголошується самостійно, але Комісія з азартних ігор може перевірити точність, хоча не вказано, як часто це робиться.

Справді корисним ресурсом як частина цього є Реєстр захисту коштів, створений Форумом букмекерів на конях (HBF) і опублікований у грудні 2017 року як частина їх Статуту ставок.

Цей реєстр забезпечує простий рейтинг кожної фірми на основі її власного аудиту – базовий, середній чи високий.

Нижче наведено описи для кожного рівня захисту відповідно до сайту HBF (табл. 1.2).

Таблиця 1.2. Описи захисту за статистикою HBF.

Базовий	Без додаткового захисту. Гроші на цих рахунках все одно розглядалися б як частина бізнесу, якби він згорів.
Середній	Існують заходи (наприклад, страхування), які гарантують, що гроші на окремих рахунках будуть передані клієнтам у разі банкрутства компанії.
Високий	Гроші клієнтів зберігаються на рахунку, який юридично та практично окремо від решти компанії. Цей рахунок контролюється незалежною особою або зовнішнім аудитором.

Для кожної великої букмекерської контори HBF опублікувала поточний застосовний рейтинг (вважається правильним станом на грудень 2017 року), і він є цікавим для дослідження.

Наприклад, у цій таблиці стверджується, що такі, як Betfred, William Hill, Betway, Black Type і William Hill, пропонують лише базовий рівень захисту.

Великі фірми, такі як Bet365, Ladbrokes, Bet Victor і Skybet, є середніми, тоді як лише кілька великих імен – Betfair, Coral & Paddy Power мають високий рейтинг.

З 35 компаній, які перевіряє HBF, має бути занепокоєння, що лише 5 мали високий рейтинг із 13 середніми і більшість – 17, усі оцінені як просто базові.

Варто зазначити, що це дослідження було вперше опубліковано в грудні 2017 року, і з тих пір деякі рейтинги, можливо, змінилися, так само, як кількох компаній із переліку більше немає. Це є попереджувальним знаком , як швидко все змінюється в букмекерському світі.

Відповідно до пункту 1 версії Статуту ставок за грудень 2017 року – «Розширений захист коштів гравців» – HBF створив Реєстр ступеню захисту коштів, на які претендують різні букмекерські компанії. Детальна інформація

про категоризацію Комісії з азартних ігор у цій сфері наведена на цій організації [12].

Слід зазначити, що Комісія з азартних ігор надає відповідним конторам вирішувати, до якої категорії вони належать, але вони можуть перевірити точність цієї самооцінки.

Клієнтам рекомендується ознайомитися з відповідними умовами та політик та переконатися, що компанія, про яку йдеться, надає той рівень послуг, на який вони претендують.

1.3.2. Обережність перед розміщенням та регулярні зняття коштів

Якщо кошти розміщаються на рахунку букмекерської контори лише з базовим рівнем захисту – якщо ця контора розвалиться, теоретично гравці навряд чи побачать більшість з цих грошей знову. Ймовірно, що для цих великих фірм цього не станеться, хоча це може бути, але для менших компаній це повинно викликати занепокоєння.

Цілком імовірно, що бачимо інші приклади, згідно з Betbright, коли невиплачені ставки на Antepost не оплачуються (принаймні не без великого PR-штурму, який змусить їх), особливо враховуючи прецедент їхнього закриття, створений на початку 2021 року. Інші фірми знають, що їм це вдасться уникнути в майбутньому.

Тому, необхідно проявляти інтерес до оцінок захищеності, бути дуже обережним, де гравці роблять свої ставки на Antepost – і зосереджуватися на тому, щоб розміщувати їх у тих фірм, які мають принаймні середній або високий рейтинг, і ті більш відомі «великі» букмекерські контори рідше закриваються і не виконують свої зобов’язання.

Це може означати, що з певними ставками Antepost гравцям доведеться брати дещо гірші ціни, але набагато краще гарантувати виплату, якщо та коли така ставка виграє, ніж страх, що букмекерська контора, з якою гравці роблять ставку, вирішить не платити. Враховуючи прецедент «Betbright», зовсім не дивно, якщо інші контори копіюють їх підхід і намагатимуться закрити рахунки, не розраховуючи всі невиконані ставки.

Також доцільно підтримувати баланси в тих конторах з базовим рейтингом на відносно мінімальному рівні, оскільки гроші гравців там є не захищені.

Те ж саме стосується всіх букмекерських контор – тому що якщо на букмекерському рахунку є великі суми грошей, які гравцю не потрібно мати на ньому – набагато краще, щоб вони надійно заховалися на персональному банківському рахунку, щоб заробляти відсотки. Це просто хороша загальна практика.

1.3.3. Контроль зняття коштів букмекерами

Як ми всі вже знаємо – букмекери дуже стараються, щоб профілювати гравців щодо обмежень рахунку та частоти зняття коштів, а суми, які вилучаються, це те, що вони можуть контролювати.

У іноземних відкритих джерелах вказано, що було поставлено запитання букмекерському інсайдеру щодо вмісту фінансового рахунку, і він вважає, що було б розумно спустошувати свій рахунок постійно, навіть якщо це лише невелика сума.

Проблема закриття букмекерськими конторами облікових записів або обмеження ставок, які можна зробити на будь-яку ставку, є популярною практикою, яка впливає на багатьох гравців у сучасному світі ставок. Особливо це впливає на тих, які роблять ставки на скачки та інші «нішові» види спорту та ліги, де букмекери обережно ставляться до «гострого бізнесу».

Щоб допомогти вирішити цю зростаючу проблему – як член Клубу Smart Betting Club, гравець може отримати доступ до кількох експертних звітів, присвячених тому, щоб допомогти зрозуміти, як і чому застосовуються обмеження та як уникати їх якнайшвидше.

1.4. Вплив карантиних обмежень спричиних вірусом sars-cov-2 на діяльність букмекерів

На світову індустрію азартних ігор коронавірус справив величезний вплив: він призвів до закриття казино та різних гральних закладів, залів для гри в бінго, лотерейних точок та навіть барів і пивоварень. Призупинилися спортивні заходи в усьому світі. Проте одна з галузей, в якій спостерігається різке зростання, – це індустрія онлайн-гемблінгу. Пандемія й зумовлена нею ізоляція призвели до різкого збільшення відвідуваності онлайн-казино і сайтів з азартними іграми.

Онлайн-платформи шукають більш дієві способи привабити клієнтів і зупиняються на варіантах, які в період пандемії COVID-19 дозволять ігровій індустрії ефективніше пропонувати свої послуги. До таких привабливих пропозицій належать можливість робити депозит на мінімальну суму, різноманітні бонуси, а також можливість робити ставки на ті види подій, які частково замінюють відсутність змоги поставити на звичні спортивні змагання.

Під час самоізоляції люди зазвичай мають більше вільного часу, що, як наслідок, спонукає заходити на сайти з улюбленими розвагами за будь-якої нагоди. Психоемоційний стан людей під час світової кризи, їхня фінансова нестабільність, відсутність роботи – це чинники, що також викликають бажання відволіктися.

Тому в політиках букмекерських організацій запроваджують на постійній основі практику по лімітах на певні процеси, наприклад ліміт по витрачених грошах в день\тиждень\місяць, ліміт програних ставок за такий період, і т.п.

Для любителів спорту своєрідною заміною стали ставки на віртуальний різновид змагань. Перевагою віртуального спорту є коротка тривалість матчів і доступність 24/7.

1.5. Висновок по першому розділу

У цьому розділі було проаналізовано інформаційні джерела пов’язанні з діяльністю букмекерських організацій, а саме:

- позиції урядів щодо букмекерських організацій;
- підвищення безпеки програмного забезпечення букмекерів;
- оцінка безпеки функціонування існуючих букмекерських контор;
- вплив карантиних обмежень спричиних вірусом sars-cov-2 на діяльність букмекерів.

Проведений попередній аналіз дозволив зорієнтуватися на предметній області досліджуваної теми та сфокусуватися на проблемних питаннях, а саме безпеці діяльності такої організації, та дослідити методи побудови розроблюваної автоматизованої системи контролю та управління букмекерської контори.

2 СТРУКТУРА І РЕСУРСИ БУКМЕКЕРСЬКОЇ КОНТОРИ

2.1. Аналіз структури обєкту захисту

В якості об’єкта дослідження обрано букмекерську контору “Live Score”. Структура досліджуваного об’єкта зображена на рисунку 2.1. Досліджувана контора спеціалізується на надані послуг створення ставок на спортивні події.

Підприємство складається із відділів, кожний з яких відповідає за виконання відповідних функцій. Усі відділи підприємства підпорядковуються директору. Йому безпосередньо підзвітні його заступники(керівники відділів), кожному з яких підпорядковуються відділи.

Головним управляючим букмекерської контори є його директор. Директор керує всією діяльністю довіреного йому об’єкта. До його обов’язків входить досягнення максимальної ефективності і як наслідок збільшення клієнтів контори, досягнення максимального фінансового прибутку роботи контори, зниження втрат та витрат. В свою чергу директор має помічників, які працюють на керівних посадах кожного з відділів.

Економічний відділ є найважливішим відділом, так як займається фінансовим плануванням та всіма економічними розрахунками підприємства, що зберігаються на його сервері. Безпеці цього відділу повинна приділятися особлива увага, від його функціонування залежить робота всього підприємства.

Відділ прогнозування бере на себе відповідальність за роботу фінансових компонентів в послугах які надає букмекерська контора, тобто логісти які там працюють розробляють математичні моделі якими буде обраховуватися вірогідності тієї чи іншої події.

Процеси які запроваджуються для покращення ефективності механізмів діяльності інформаційної букмекерської системи перед клієнтами розробляються у відділі розробки, менеджери цього відділу є основним вузлом комунікації між усіма іншими відділами і програмістами.

Бухгалтерія веде облік, керує та нараховує заробітні плати працівникам. В її обов’язки входить робота з налоговою.

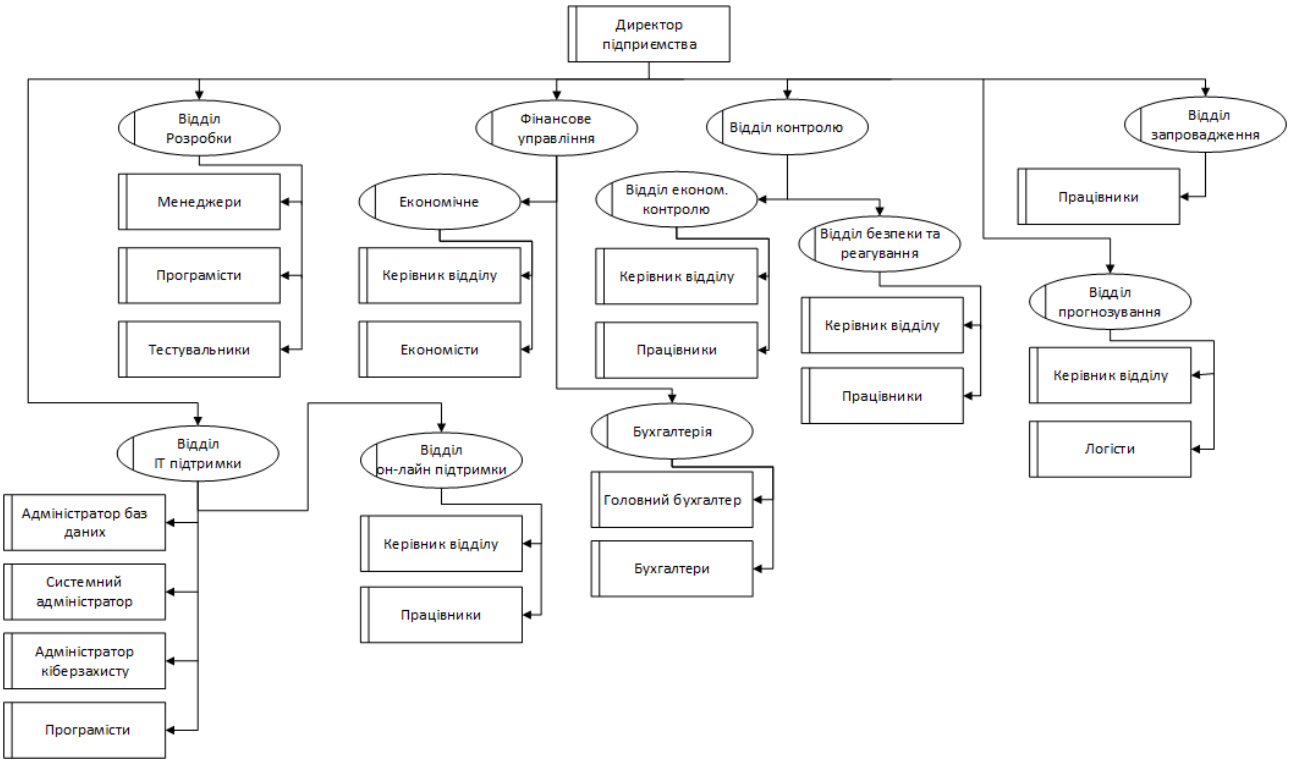


Рисунок 2.1 – Загальна структура букмекерської контори.

Відділ економічного контролю виконує перевірку розрахунків, звітів, статистики, загалом роботи виконаної економічним відділом та бухгалтерії. Це необхідно для уникнення збитків «чорної бухгалтерії» недобросовісних працівників. Іншими словами є інструментом контролю роботи економічних відділів.

Відділ контролю якості послуг виконує збір статистичних даних про стан та якість задоволення послугами від клієнтів. Формує дані для чіткого розуміння ефективності та якості послуг букмекерської контори.

Відділ безпеки та реагування – це в першу чергу звичайна охорона притаманна будь-якому підприємству. А також, спеціалісти які реагують на критичні інциденти які трапляються в реальному часі, для зменшення збитків в разі виникнення таких, персонал цього відділу працює цілодобово, так як контроль та моніторинг системи повинен виконуватися на постійній основі. Відділ розвиває системи безпеки та контролю. Відповідає за фізичну безпеку комп’ютерної мережі.

Відділ IT-Підтримки займається налаштуванням усього внутрішнього кіберпростору букмекерської контори, підтримуванням його працездатності та покращенням його ефективності.

Відділ он-лайн підтримки забезпечує допомогу клієнтам букмекерської контори або потенційним гравцям в консультуванні щодо управління їх обліковими записами, а також у вирішені проблем які могли виникнути.

2.1.1. Аналіз інформаційного середовища

Основними інформаційними ресурсами, що підлягають захисту [13] в букмекерській конторі є:

- персональні дані гравців;
- конфіденційні дані працівників;
- логістичні дані роботи грального систем;
- дані якості послуг;
- електронні розрахункові документи;
- фінансові звіти;
- контракти з партнерами;
- уся паперова документація.

Інформацію класифікують за трьома ознаками: цілісність (Ц), доступність (Д), конфіденційність (К). Саме за такими ознаками визначають рівень доступу до інформації [14], модель інформації зображена в табл. 2.1.

Таблиця 2.1 – Класифікація інформації

Цілісність	Доступність	Конфіденційність	
Ц0	Д0	К0	Критична
Ц1	Д1	К1	Дуже важлива
Ц2	Д2	К2	Важлива
Ц3	Д3	К3	Значима
Ц4	Д4	К4	Не значна

Визначивши, які ознаки мають основні інформаційні ресурси букмекерської контори, створено базу даних у якій записано декілька таблиць, що відповідають за різного роду ресурси контори. Таблиця бази даних складається з типу ресурсу, ознак інформаційної безпеки, id програмних засобів необхідних для обробки даного виду ресурсу, назва комп`ютера та його ip адреса, ролей та прав цих ролей (рис. 2.2).

№	Ресурс	Цілісніст	Доступніст	Конфіде	ПЗ id	АЗ	Ролі	Права ролей	Щелкни
1	Фінансовий звіт	0	0	1	1; 2; 5	PC4-5 (192.168.50.19-20)	Відділ економічного контролю, Економічний відділ, Відділ економічного контролю, Бугалетрія,директор	rw;rw;rw;rw;rwd	
2	Договори з гравцями	1	0	1	1; 2	PC6-9 (192.168.50.21-24)	Економічний відділ, Відділ економічного контролю, директор	rwd;rwd;rwd	
3	Персональні дані співробітників	0	0	2	1; 2; 3; 4; 5	PC10-11 (192.168.50.25-26)	Бухгалтерія, директор	rw;rwd	
4	Звіт виявлених порушень працівниками	2	1	2	1; 2	PC6-9 (192.168.50.21-24) PC2-3 (192.168.50.5-6)	Відділ економічного контролю, якості контролю, директор	rw;rwd;rdw	
5	Вихідний код роботи ігрових систем	0	0	0	3; 9	PC0-1 (192.168.50.2-3) PC20 (192.168.50.15)	Відділ розробки, адміністратор кібербезахисту, відділ IT підтримки, директор.	rwd;rdw	
6	Автентифікаційні та резервні дані	0	0	0	3; 4; 5; 12	PC13 (192.168.50.7-8)	Відділ безпеки та реагування,відділ онлайн IT-підтримки, директор.	rwd;rwd	
7	Алгоритми букмекерської системи	0	0	0	3; 4; 9; 10; 12	PC19 (192.168.50.14)	Системний адміністратор, відділ Розробки, директор	rw;rwd	
8	Персональні дані гравців	1	2	1	1; 2; 3; 4; 5	PC10-11 (192.168.50.25-26) PC13 (192.168.50.7-8)	Директор, бухгалтерія, відділ он-лайн підтримки	rwd;r;rwd	
9	Паперова документація	1	1	1	2	PC4-5 (192.168.50.19-20)	Директор, економічний відділ	rwd;rw	

Рисунок 2.2 – Витяг з бази даних, аналіз інформаційних ресурсів

Перед наведенням використовуваної моделі доступу доречно навести основні моделі управління доступом, що здебільшого використовуються організаціями та підприємствами.

Основними моделями управління доступом є:

– мандатна;

– рольова;

– дискреційна.

На досліджуваній конторі, в об`єкті захисту використовується рольова модель доступу. Ролі працівника залежать від виду діяльності та, як наслідок,

відділу до якого він належить. Загалом існує сім відділів, але у кожному з них по декілька ролей, хоча інколи різні ролі мають однакові права для одного документа. Було проведено аналіз усіх ролей та заповнено відповідну таблицю (рис. 2.3), де кожній ролі ставиться у відповідність інформація, з якою вона взаємодіє, доступ до неї, апаратне та програмне забезпечення.

id	Роль	Інформація	АЗ	Доступ	ПЗ
1	Генеральний директор	1; 3; 4; 5; 6; 7; 8; 9;	1	rwd;rwd;rwd;r	1; 2; 3; 4; 5; 6; 7
2	Заступник	2; 3; 4; 5; 6; 7; 8; 9;	1	rwd;r;rwd;rwd	1; 2; 3; 4; 5; 6; 7
3	Фінансовий директор	1; 2; 9; 10	5	rwd;r;rw;r	1; 2; 3; 5
4	Головний бухгалтер	3; 9; 10	11	rw;rw;r	1; 2; 5
5	Керівник відділу економ. Контролю	1; 2; 9; 10	7	rwd;rw;rwd;r	1; 2; 3; 4; 5; 11
7	Інженер	5; 9	2; 14; 15	rw;r	1; 2; 5
8	Економіст	2; 3; 8; 9	6; 8; 9; 10; 12	r;rw;r;rw	1; 2; 3; 4; 5; 7; 1
10	Логіст	5; 6; 7	2	rw;rw;r	1; 2; 9; 10; 11; 1
11	Програміст	6; 7	20; 21; 22; 23	rw;r	1; 2; 4; 10; 11; 1
12	Адміністратор баз даних	5; 6; 7	18	r;rw;rw	1; 4; 5; 12
13	Адміністратор кіберзахисту	5; 6; 7	19	rwd;rwd;rwd	1; 4; 5; 11; 12
15	Охорона	3	14	r:	1: 5

Рисунок 2.3 – Витяг з бази даних, ролі на підприємстві

Таблиця програмного забезпечення містить невелику кількість об’єктів, які характеризуються назвою, id АЗ, термінами дії, видом ліцензії та додатковою інформацію (рис. 2.4).

Організація займається наданням гральних послуг в мережі інтернет на фінансовій основі, для його ефективної роботи використовується ОС Windows, середа IntelJ IDEA, Docker Decktop для розробки систем, пакет MS Office для роботи з документами, photoshop в маркетинговому відділі, CentOS на серверах.

До апаратного забезпечення віднесено усі комп’ютери, комутатори, сервер та маршрутизатор (рис. 2.5).

Апаратне забезпечення характеризується видом обладнання, назвою, IP-адресою, MAC-адресою, місцем знаходження в конторі, встановленим на ньому програмним забезпеченням.

Код	Назва	Термін дії	Ліцензія	Інформація	АЗ id
1	Windows 10	17.07.2020	Купівля	ОС. Інтерфейс управління ПК.	1; 2; 3; 4; 5; 6; 7; 8; 9; 10; 11; 12; 13; 14; 15;
2	MS Office	08.03.2020	Купівля	Документація, реклама, маркетинг. Плани	3; 4; 6; 7; 8; 9; 10; 11; 12; 13; 14; 15; 16; 17;
3	MS ACCESS	08.03.2020	Купівля	БД клієнтів, розрахунків	1; 2; 5; 6; 7; 8; 9; 10; 11; 12; 14; 15; 17; 18;
4	MS SQL	08.03.2020	Купівля	Система аналізу та управління раціональними базами даних	7; 8; 9; 10; 14; 17; 18; 19; 20; 21
5	MS Excel	08.03.2020	Купівля	Дані у формі таблиць, графіків. Бухгалтерські розрах.	1; 2; 3; 4; 5; 6; 7; 8; 9; 10; 14; 15; 17; 18; 19;
6	Photoshop	13.05.2022	Купівля	Ескізи, логотипи маркетингу	14; 17; 18; 19; 20; 21
8	IntelJ IDEA		Купівля	Середа розробки грального систем	1; 2; 13; 14; 17
9	Docker Desktop		Безкоштовно	Середа моделювання контеєрезованих модулів	1; 2; 14; 17; 18; 19; 20; 21
10	Wire shark		Безкоштовно	Аналіз мережевих пакетів	14; 17; 18; 19; 20; 21
11	Skype	13.05.2022	Купівля	Онлайн підтримка клієнтів	22; 23
12	CentOS		Безкоштовно		

Рисунок 2.4 – Витяг з бази даних, програмне забезпечення

№	Вид обладнання	Назва	IP-адреса	MAC-адреса	Місце знаходження	ПЗ
1	Комп'ютер	PC0	192.168.50.2/24	00D0.FF71.B601	Відділ прогнозування	1; 3; 5; 8; 9
2	Комп'ютер	PC1	192.168.50.3/24	00D0.FF71.B602	Відділ прогнозування	1; 3; 5; 8; 9
3	Комп'ютер	PC2	192.168.50.4/24	00D0.FF71.B603	Відділ контролю якості послуг	1; 2; 5; 7
4	Комп'ютер	PC3	192.168.50.5/24	00D0.FF71.B604	Відділ контролю якості послуг	1; 2; 5; 7
5	Комп'ютер	PC4	192.168.50.19/24	00D0.FF71.B605	Економічний відділ	1; 3; 5; 7
6	Комп'ютер	PC5	192.168.50.20/24	00D0.FF71.B606	Економічний відділ	1; 3; 5; 7
7	Комп'ютер	PC6	192.168.50.21/24	00D0.FF71.B607	Відділ економічного контролю	1; 2; 3; 4; 5; 7
8	Комп'ютер	PC7	192.168.50.22/24	00D0.FF71.B608	Відділ економічного контролю	1; 2; 3; 4; 5; 7
9	Комп'ютер	PC8	192.168.50.23/24	00D0.FF71.B609	Відділ економічного контролю	1; 2; 3; 4; 5; 7
10	Комп'ютер	PC9	192.168.50.24/24	00D0.FF71.B60A	Відділ економічного контролю	1; 2; 3; 4; 5; 7
11	Комп'ютер	PC10	192.168.50.25/24	00D0.FF71.B60B	Бухгалтерія	1; 2; 3; 7
12	Комп'ютер	PC11	192.168.50.26/24	00D0.FF71.B60C	Бухгалтерія	1; 2; 3; 7
13	Комп'ютер	PC12	192.168.50.6/24	00D0.FF71.B60D	Відділ безпеки і реагування	1; 2; 7; 8
14	Комп'ютер	PC13	192.168.50.7/24	00D0.FF71.B60E	Відділ розробки	1; 2; 3; 4; 5; 6; 7; 8; 9; 10
17	Комп'ютер	PC16	192.168.50.11/24	00D0.FF71.B611	Відділ IT-підтримки	1; 2; 3; 4; 5; 6; 7; 8; 9; 10
18	Комп'ютер	PC17	192.168.50.12/24	00D0.FF71.B612	Відділ IT-підтримки	1; 2; 3; 4; 5; 6; 7; 9; 10
19	Комп'ютер	PC18	192.168.50.13/24	00D0.FF71.B613	Відділ IT-підтримки	1; 2; 3; 4; 5; 6; 7; 9; 10
20	Комп'ютер	PC19	192.168.50.14/24	00D0.FF71.B614	Відділ IT-підтримки	1; 2; 3; 4; 5; 6; 7; 9; 10
21	Комп'ютер	PC20	192.168.50.15/24	00D0.FF71.B615	Відділ IT-підтримки	1; 2; 3; 4; 5; 6; 7; 9; 10
22	Комп'ютер	PC21	192.168.50.17/24	00D0.FF71.B625	Відділ онлайн IT-підтримки	1; 7; 11
23	Комп'ютер	PC22	192.168.50.18/24	00D0.FF71.B626	Відділ онлайн IT-підтримки	1; 7; 11
24	Сервер	Server1	192.168.50.27/24	00D0.FF71.ABA2	Економічні відділи	12
25	Сервер	Server2	192.168.50.8/24	00D0.FF71.ABA3	Відділ розробки	12
26	Сервер	Server3	192.168.50.16/24	00D0.FF71.ABA4	Відділ IT-підтримки	12
27	Комутатор	Switch1	-	0001.64B5.7B27	Всі відділи окрім економічних	
28	Комутатор	Switch1	-	0001.64B5.7B28	Економічні відділи	
29	Маршрутизатор	Router1		000D.BD76.40AC		
30	Вежа стільникового					
31	Центральний офіс	Central Office	172.16.1.1	FE80::240:BFF:FE4		

Рисунок 2.5 – Витяг з бази даних, апаратне забезпечення

Комп’ютерна система підприємства підключена до мережі інтернет, а також всі комп’ютери в мережі поєднані локально. Використовується антивірус ESET NOD32 Antivirus. Для кожного з працівників, залежно від їх положення, свої правила міжмережевого екрану. На кожному комп’ютері встановлений Windows.

Інформаційне середовище охарактеризовано, перейдемо до аналізу фізичного середовища.

2.2. Аналіз ресурсів об`єкта захисту

Для більш детальної та візуально зрозумілої оцінки захищеності, побудуємо модель відношення множин ресурсів. Всі наявні ресурси можна представити у вигляді множини: І(інформація), Л(Люди), О(Обладнання), П(Програмне забезпечення).

Отже, множина ресурсів має наступний вигляд:

І={ ФЗ, ДПК, ПДС, ЗВПП, АМСІП, ПД, ЗС, ПДК, АРД }

О={ КЛ, ККЯ, КЕ, КЕК, КБ, КА, КС, КМ, КП, КД }

Л={ ГД, ФД, ГБ, ДЕК, ММ, ІІ, ЕЕ, ЛЛ, ПП,АБД, АК }

П={ WW, MO, MA, MS, ME, AP, PK, II, DD, WS, SS, COS}

Де компоненти мають наступне умовне позначення:

ФЗ – фінансовий звіт.

ДПК – договори з гравцями та партнерами

ПДС – персональні дані співробітників

ЗВПП – звіти виявлених порушень працівниками

АМСІП – архітектура мережі і схема інформаційних потоків

ПДК – персональні дані гравців

ПД – паперова документація

АРД – алгоритми роботи букмекерської системи

КЛ – комп’ютер логіста

КД – комп’ютер директора

ГД – генеральний директор

ФД – фінансовий директор

ГБ – головний бухгалтер

ДЕК – директор економічного контролю

ІІ – інженер

ЕЕ – економіст

ЛЛ – логіст

ПП – програміст

АБД – адміністратор баз-даних

АК – адміністратор кіберзахисту

WW – Windows 10

MO – MS Office

ККЯ – комп’ютер контролюючого якість
КЕ – комп’ютер економіста
КЕК – комп’ютер економічного контролю
КБ – комп’ютер бухгалтера
КА – комп’ютер розробника.
КП – комп’ютер IT-спеціаліста

МА – MS Access
MS – MS SQL
ME – MS Excel
AP – Adobe Photoshop
II – IntelJ IDEA
DD – Docker Desktop
WS –Wire Shark
SS – Skype
COS – CentOS

Відношення множини ресурсів зображено на рис. 2.6-2.9.

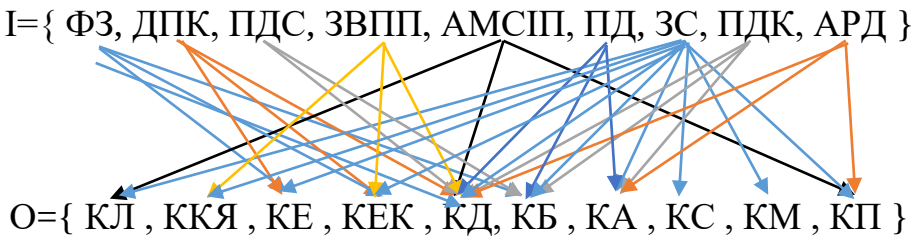


Рисунок 2.6. Відношення множин ресурсів інформації до обладнання.

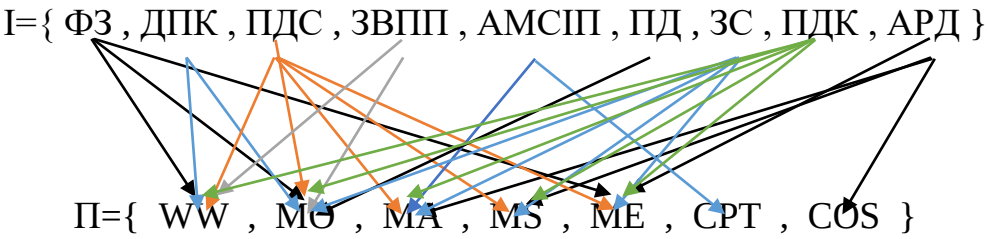


Рисунок 2.7. Відношення множин ресурсів інформації до програмного забезпечення.

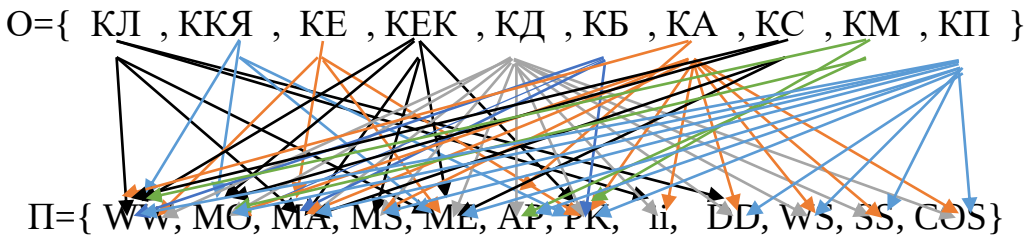


Рисунок 2.8. Відношення множин ресурсів обладнання до програмного забезпечення.

Рисунок 2.9. Відношення множин ресурсів людей до інформації.

З зображених відношень множин ресурсів можна зрозуміти залежність одних ресурсів від інших, яка інформація знаходиться на якому обладнані. Вказано які ролі персоналу мають доступу до якого обладнання, а як наслідок до програмного забезпечення та службової інформації.

2.3. Обґрунтування класу АС та його приналежність до категорії ІТС

Відповідно до класифікації автоматизованих систем (АС) представленій у НД ТЗІ 2.5-005-99, було проаналізовано і обгрунтовано клас АС, що використовується на об’єкті захисту.

Так, як на розглянутому об’єкті використовується більше однієї машини, то дана АС не може належати до класу «1».

Клас «1» — одномашинний однокористувачевий комплекс, який обробляє інформацію однієї або кількох ступенів обмеження доступу.

В досліджуваної контори існує локальна мережа, але обладнання цієї ж мережі має доступ і до зовнішньої. Тому даний комплекс не можна вважати належним класу «2»

Клас «2» — локалізований багатомашинний багатокористувачевий комплекс, який обробляє інформацію різних ступенів обмеження доступу.

Було визначено що клас «3» має в собі розподілений багатомашинний багатокористувачевий комплекс, який обробляє інформацію різних ступенів обмеження доступу. Тому у звязку з тим, що інформація, яка обробляється букмекерською конторою, має різний тип доступу, контора обробляє інформацію гравців за допомогою кількох «хмар»,було вирішено, що дана автоматизована система підпадає під клас «3»

Для визначення категорії інформаційно-телекомунікаційної системи (ІТС) необхідно звернутись до нормативного документу державної служби спеціального зв'язку та захисту інформації України [15], у якому визначається порядок категоріювання об'єктів, де циркулює ОІД, що не становить державної таємниці – НД ТЗІ 1.6-005-2013. Згідно з пунктом 5.7 даного документу ІТС об'єкту, що розглядається відповідає четвертій (IV) категорії.

2.4. Аналіз конкурентного середовища

Конкурентне середовище є досить наповненим, в області надання послуг букмекерськими конторами існують безліч конкурентних організацій що надають послуги грального бізнесу в мережі інтернет. Серед найбільших світових букмекерських контор можна виділити:

- bet365;
- betVictor;
- MrGreen;
- 888Sport;
- William Hill;
- Безліч інших неліцензійних букмеркерських контор.

Загальна кількість таких букмекерських контор може налічувати тисячі онлайн організацій, які проводять агресивну політику щодо своїх конкурентів. Така політика може визначати негативний вплив на контори-конкуренти незаконними шляхами, тобто створювати загрози діяльності досліджуваної контори. Основними чинниками впливу конкурентного середовища на об'єкт захисту є: проникнення інсайдера на територію організації, підкуп працівників, вплив за допомогою викладення дезінформації про підприємство у ЗМІ та / або безпосередньо в мережі інтернет, використання мережевих атак зі сторони конкурентів таких, як неправомірне-навмисне навантаження пропускної здатності каналів зв'язку, DDOS та інших типів атак на сайт та сервери контори з метою унеможливлення привернення уваги нових клієнтів або їх безпосереднє перехоплення. Пошкодження ліній зв'язку. Для усунення впливів на роботу

контори даних загроз, в організації присутній відділ безпеки та охорони а також адміністратор з кібербезпеки.

2.5. Модель загроз та модель порушника

2.5.1. Модель загроз

Проаналізувавши основні ресурси захисту та їх моделі, було встановлено, що найбільший вплив на безпеку контори мають такі негативні фактори, як інсайдер та хакерські атаки. Відповідно до отриманих даних у таблиці 2.2 наведено модель загроз.

Таблиця 2.2 – Модель загроз

Позначення Загрози	Джерело	Ресурси	Метод Реалізації	Вплив на властивості			Ймовірність появи загрози
				К	Ц	Д	
Інсайдер в конторі	Людина	Апаратні, інформаційні, фізичні	Проникнення, перевищення повноважень	+	–	–	Низька
Хакерські атаки	Людина	Апаратні, Інформаційні	НСД до букмекерської системи	+	+	+	Низька

З таблиці ми бачимо, що більшу шкоду для інформаційних ресурсів підприємства буде нанесено при реалізації другої загрози, але при інсайдерській атаки на ресурси зловмисник може отримати неавторизований доступ до даних та завдати досить великі фінансові збитки.

2.5.2. Модель порушника

Для побудови моделі порушників необхідно виділити по одній групі зловмисників за місцем дії, а саме для внутрішніх та зовнішніх. Згідно припущень щодо мотивів, рівня кваліфікації та інших критеріїв було побудовано модель порушника, яка відображена у табл. 2.3.

Найбільш значимим та небезпечним у букмекерській конторі є ІТ відділ та адміністратор кіберзахисту так як для забезпечення своєї роботи вони мають доступ до основної частки ресурсів. Вони становлять найбільший рівень загрози для підприємства у випадку їх неправомірних дії у системі.

Таблиця 2.3 – Модель порушника

Визначення категорії	Мотиви поруше-ння	Рівень кваліфікації та обізнаності щодо АС	Можливості використання засобів та методів подолання системи захисту	Специфікація моделі порушника за часом дії	Специфікація моделі порушника за місцем дії	Сумарний рівень загрози	Ймовірність виникнення загрози
Внутрішні порушники по відношенню до АС							
Співробітники ІТ-відділу	М3	К4	З3	Ч3	Д5	15	Висока
Зовнішні порушники по відношенню до АС							
Адміністратор з кібербезпеки	М3	К6	З5	Ч4	Д6	18	Висока

Отже, створено моделі зовнішнього та внутрішнього порушників, обраховано їх рівень загрози. Максимальний можливий рівень загрози – 20 балів, створені моделі порушників досягли максимум 18 балів, що становить 90% від максимально можливої загрози. Розроблена модель порушника повинна бути використана при формуванні політики безпеки для зниження рівня загрози. Проведено аналіз середовища функціонування ІТС підприємства. Розглянуто інформаційне, фізичне середовища та середовище користувачів підприємства. Проаналізовано конкурентне середовище та наведено основні можливі фактори їх впливу на роботу підприємства. Обґрунтовано клас АС та категорію ІТС об’єкта захисту. Наведено модель загроз та модель порушника. Згідно отриманих даних, переходимо до наступного етапу розробки АСКУ, який передбачає розробку математичної моделі для оцінки рівня захищеності.

3 РОЗРОБКА МАТЕМАТИЧНОЇ МОДЕЛІ ОЦІНЮВАННЯ РІВНЯ ЗАХИЩЕНОСТІ

3.1. Ідентифікація загроз

На першому етапі ідентифікації загроз необхідно визначити назви загроз [16]. Визначивши набір загроз притаманний для букмекерської контори, для оцінки ймовірності виникнення таких загроз, було залучено трьох експертів: адміністратор кіберзахисту, керівник відділу безпеки і реагування та керівник відділу економічного контролю. Для кожної загрози була визначена експертна оцінка ризику наведена в табл. 3.1.

Таблиця 3.1. Перелік загроз та їх експертна оцінка імовірності виникнення.

№	Назва загрози	Оцінка експерта 1	Оцінка експерта 2	Оцінка експерта 3	Середня оцінка
1	Несанкціонований доступ до букмекерських даних чи програмного забезпечення ігрових систем	0.12	0.13	0.11	0.12
2	Підглядання/підбір/перехоплення паролів	0.03	0.02	0.025	0.025
3	Впровадження в систему шкідливого програмного забезпечення	0.11	0.11	0.13	0.11
4	Перевищення повноважень облікових записів в системі	0.07	0.06	0.05	0.06
5	Помилки в роботі співробітників	0.04	0.06	0.06	0.053
6	Опублікування службових даних в соц.мережах	0.05	0.07	0.045	0.055

7	Злам міжмережевого екрана або його відмова	0.05	0.05	0.05	0.05
8	Несанкціонована автентифікація	0.02	0.02	0.04	0.026
9	DDoS-атаки	0.11	0.10	0.12	0.11
10	SQL-ін’єкції	0.03	0.03	0.02	0.026
11	Зовнішній моніторинг мережі	0.04	0.04	0.03	0.036
12	Втрата даних авторизації	0.06	0.06	0.05	0.056
13	Шантаж працівників	0.03	0.04	0.03	0.033
14	Використання шпигунських пристроїв	0.03	0.03	0.03	0.03
15	Стихійне лихо	0.005	0.004	0.004	0.004
16	Пожежа	0.005	0.005	0.006	0.005
17	Копіювання секретних даних	0.04	0.03	0.04	0.03
18	Безвідповідальне ставлення до роботи	0.03	0.04	0.03	0.033
19	Інсайдер	0.12	0.09	0.12	0.11
20	Пошкодження носіїв даних	0.01	0.01	0.01	0.01

Визначення і оцінка загроз букмекерської контори дозволяє сфокусуватися на виборі найнеобхідніших комплексних систем захисту. Було визначено що найбільшу вірогідність виникнення має:

– несанкціонований доступ до букмекерських даних чи програмного забезпечення ігрових систем;
– впровадження в систему шкідливого програмного забезпечення;
– інсайдер.

Для забезпечення надійності АСКУ від перелічених загроз пропонується комплекс систем захисту (рис. 3.1).

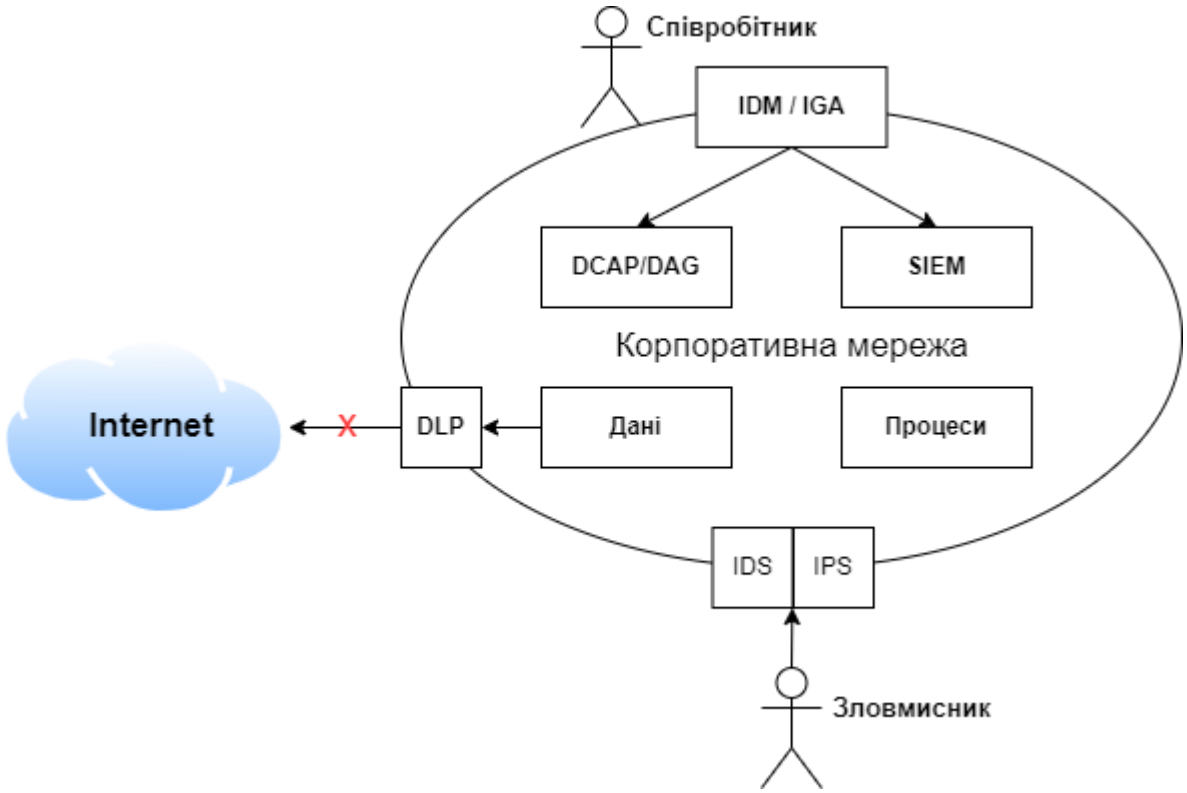


Рисунок 3.1. Комплекс систем захисту.

На рисунку представлені такі системи:

– система керування обліковими записами – IDM (IDentity Management);
– система керування та адміністрування обліковими записами – IGA (Identity Governance & Administration);
– система аудиту і захисту, орієнтовані на дані – DCAP (Data-Centric Audit and Protection);
– система керування доступом до даних – DAG (Data Access Governance);
– система керування подіями безпеки – SIEM (Security Information and Event Management);
– система запобігання витоку даних – DLP (Data Leak Prevention);
– система виявлення вторгнень – IDS (Intrusion Detection System);
– система запобігання вторгненням – IPS (Intrusion Prevention System).

Було розглянуто та порівняно актуальні IDM станом на 2021р [17], порівняння зображені в табл. 3.2.

Таблиця 3.2. Порівняння актуальних IDM

IDM	Okta identity management	VMware workspace One Access	Auth0	OneLogin	SecureAuth
Кілька політик SSO	+	+	+	+	+
Синхронізація паролів	+	-	+	-	-
Надання SaaS	+	+	+	+	+
Інтеграція кількох каталогів	+	+	+	-	+
Автентифікація для локальних програм	+	+	+	+	+
Інтеграція Mobile device management сторонніх розробників	+	+	-	-	+
Бібліотека звітів	+	-	+	+	+

Аналіз табл. 3.2 показав що найбільше функціональних можливостей має система Okta identity management. Було вирішено застосувати її як основну систему керування обліковими записами АСКУ.

Щодо систем запобігання витоку даних було розглянуто Symantec DLP, McAfee DLP, Forcepoint DLP, SecureTrust Data Loss Prevention [18]. Досліджено особливості кожної з них (табл. 3.3).

Таблиця 3.3. Порівняння актуальних DLP систем.

Назва	Особливості
Symantec DLP	– Має функції автоматизованих робочих процесів усунення інцидентів і інтелектуальні відповіді одним клацанням миші, які дозволять швидко й ефективно реагувати на критичні втрати даних. – Забезпечує гнучкість для точного налаштування політик, щоб збалансувати безпеку та продуктивність. – Може забезпечити видимість і контроль над даними в стані спокою або в хмарних програмах. – Забезпечує інформаційно-центровану аналітику. Ця функція дозволить визначити пріоритетність ризикованої поведінки та ідентифікувати зловмисних користувачів, а отже — кращий спосіб керувати інцидентами та реагувати на них.
McAfee DLP	– Забезпечує видимість завдяки технології захоплення. – Надає уявлення про те, як дані використовуються та як вони витікають. – Має більш потужну функцію класифікації даних для ідентифікації та класифікації даних. – Може шифрувати, перенаправляти, поміщати на карантин або блокувати передачу даних, які порушують політику.

Forcepoint DLP	– Для захисту даних Forcepoint надає функції Drip DLP, Native Remediation, комплексне виявлення даних і OCR. – Може забезпечувати власну поведінкову аналітику, захист, адаптований до ризику, та забезпечення виконання політики на основі ризиків. – Має функції для запобігання повільної крадіжки даних, навіть якщо пристрої користувача знаходяться поза мережею. – Має гнучкість бази даних.
SecureTrust Data Loss Prevention	– Має функції автоматичного блокування HTTP, HTTPS і FTP-трафіку, який порушує політику відповідності. – Пропонує автоматичне шифрування, блокування, карантин або самовідповідність, якщо повідомлення електронної пошти та вкладені файли будуть визначені як порушення відповідності. – Має інтелектуальний механізм керування вмістом, який допоможе командам безпеки виявляти конфіденційні дані. Це дозволить групам безпеки зосередитися на своїх задачах щодо конкретних користувачів і систем і вжити правильних заходів. – Надає функції розширеного контролю вмісту, управління розслідуваннями та відповідності ідентифікаційних даних у реальному часі.

Проаналізувавши наявні DLP системи, для забезпечення захищеності автоматизованої системи контролю та управління букмекерською конторою було обрано систему Symantec DLP, оскільки вона має найкращу гнучкість на основі налаштовуваних політ безпеки та підсистему реагування на інциденти.

Серед актуальних на ринку систем виявлення або запобігання вторгненням (IDS/IPS) [19] розглянуто Cisco NGIPS, McAfee Network Security Platform, ZScalar Cloud IPS, їх порівняння представлено в табл. 3.4.

Таблиця 3.4. Порівняння актуальних IPS систем.

Назва	Особливості
Cisco NGIPS	Система запобігання вторгненням наступного покоління (NGIPS). Має можливість візуалізувати дані безпеки через централізований центр управління вогневою потужністю, а NGIPS також може інтегруватися з іншими інструментами безпеки Cisco. Правила політики та сигнатури загроз, які NGIPS використовує для виявлення та запобігання вторгненням, оновлюються кожні дві години. NGIPS може працювати на пристрої Cisco або екземплярі VMware і може бути гнучко розміщений у вашій мережі.
McAfee Network Security Platform	Може працювати на фізичних або віртуальних пристроях у мережі, як «систему запобігання вторгненням наступного покоління». Поєднуючи механізми виявлення на основі сигнатур і без сигнатур, Network Security Platform також корелює активність загроз із використанням програми, щоб стежити за потенційною поганою поведінкою. Віртуальна версія пристрою розширює функціональність на публічні або приватні хмари. Network Security Platform також може інтегруватися з іншим програмним забезпеченням McAfee, а також отримує постійно оновлювані дані про загрози від McAfee.
ZScalar Cloud IPS	Представляє абсолютно нову парадигму захисту від вторгнень. На відміну від більшості таких сервісів, які існують як фізичні чи віртуальні пристрої, ZScalar Cloud, як зрозуміло з назви, повністю в хмарі. Це дозволяє Cloud IPS зосередитися на

	користувачах та їх мережевому трафікі, а не на окремих серверах, і вміщує сучасні мережі, де більша частина корпоративного трафіку призначена для розміщених послуг, які не знаходяться під безпосереднім контролем IT. Оскільки Cloud IPS є пропозицією SaaS, він постійно оновлюється останніми даними про загрози. Він також пропонує розшифрування SSL.

Дослідивши актуальні IPS системи на ринку було обрано McAfee Network Security Platform, оскільки має постійну підтримку сигнатурного оновлення. Для ідентифікації та оцінки загроз було використано експертний підхід. В результаті створено комплекс системи захисту букмекерської контори. Які надалі будуть використовуватись при створенні моделі оцінювання рівня захищеності організації. Після ідентифікації ризиків переходимо до наступного етапу, розробки моделі захисту.

3.2. Розробка логіко-ймовірнісної моделі букмекерської контори для оцінювання рівня захищеності

На даному етапі створюється модель оцінювання рівня захищеності організації. Моделювання дасть змогу визначити значимість реалізації кожної з попередньо ідентифікованих загроз. Що надалі дозволить отримати адекватну оцінку стану захищеності та розробити згідно отриманих даних політику безпеки на досліджуваному об’єкті захисту.

Для моделювання обрано такий математичний апарат, як логіко-ймовірнісне моделювання [20]. Для наочності модель розроблена у вигляді дерева-подій (рис. 3.2).

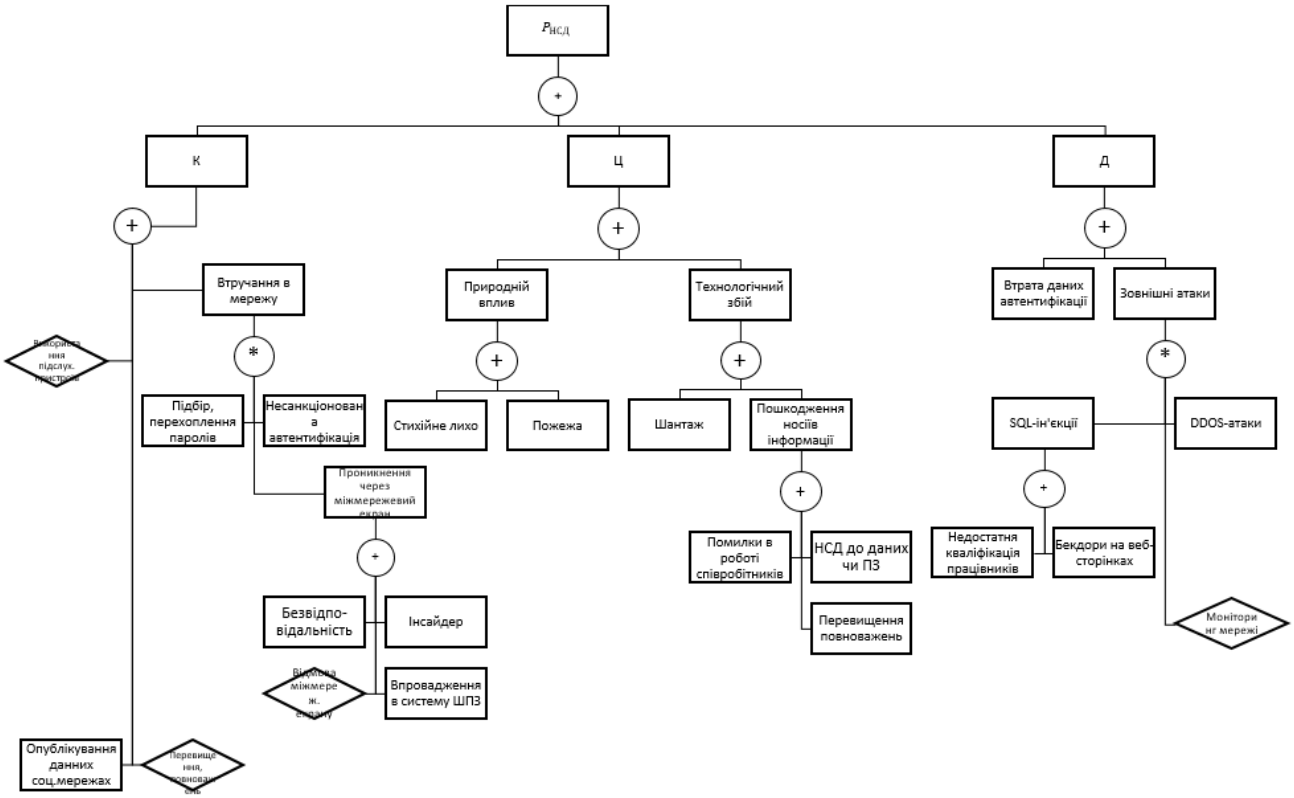


Рисунок 3.2 – Логіко-ймовірнісна модель оцінки рівня інформаційної безпеки.

Де загрози мають наступні умовні позначення:

Р1 – К;

Р2 – Ц;

Р3 – Д;

Р4 – Втручання в мережу;

Р5 – Природній вплив;

Р6 – Технологічний збій;

Р7 – Зовнішні атаки;

Р8 – Проникнення через міжмережевий екран;

Р9 – Пошкодження носіїв інформації;

РХ17 – SQL-ін'єкції;

РХ1 – Використання підслух. пристроїв в конторі;

РХ2 – Опублікування службових даних в соц. мережах;

РХ3 – Перевищення повноважень;

РХ6 – Безвідповідальність;

РХ7 – Відмова міжмережевого екрану;

РХ8 – Інсайдер;

РХ9 – Впровадження в систему ШПЗ;

РХ10 – Стихійне лихо;

РХ11 – Пожежа;

РХ12 – Шантаж;

РХ13 – Помилки в роботі співробітників;

РХ14 – НСД до букмекерських даних чи ПЗ;

РХ15 – Перевищення повноважень;

РХ16 – Пошкодження носіїв інформації;

РХ17 – SQL-ін'єкції;

РХ4 – Підглядання, підбір, перехоплення паролів;
РХ5 – Несанкціонована автентифікація;
РХ18 – DDOS-атаки;
РХ19 – Моніторинг мережі.
РХ20 – Втрата даних автентифікації.

Ця модель фактично формалізує поточний стан захисту букмекерської контори. В якості базових подій представлені початкові події, які можуть бути причинами ефективного проведення спеціальних інформаційних операцій.

Аналіз логіко-ймовірнісної моделі і проведення розрахунку дозволить отримати ймовірнісні характеристики всіх подій, що враховані у моделі, а також отримати їх ранги, що дозволить перейти до етапу підготовки рішень щодо протидії інформаційним впливам, вибору оптимального рішення і виконанню послідовного постійного контролю над рівнем інформаційної безпеки.

3.3. Аналіз результатів моделювання

Розрахунок загального впливу негативних факторів на безпеку букмекерської контори “LiveScore” зображено в таблиці 3.5:

Таблиця 3.5 – Розрахунок загального впливу негативних факторів.

Умовне позначення	Розрахункова формула	Значення
P1	1-(1-PX1)*(1-PX2)*(1-PX3)*(1-P4)	0,7904
P2	1-(1-P5)*(1-P6)	0,2338
P3	1-(1-P7)*(1-PX20)	0,0673
P4	PX4*PX5*P8	0,2192
P5	1-(1-PX10)*(1-PX11)	0,0798
P6	1-(1-PX12)*(1-P9)	0,1492
P7	PX17*PX18*PX19	0,003
P8	1-(1-PX6)*(1-PX7)*(1-PX8)*(1-PX9)	0,1322
P9	1-(1-PX13)*(1-PX14)*(1-PX15)	0,1344
P	1-(1-P1)*(1-P2)*(1-P3)	0,8016

З розрахунків видно значний вплив критичних факторів на інформаційну систему підприємства. Виконаємо ранжування негативних факторів, для виявлення найбільш небезпечних з них.

Ранжування негативних факторів, що впливають на критичні інформаційні потоки та інформаційні ресурси:

Використання різниць ймовірностей появи головної події та її ймовірності у випадку вилучення події, ранг якої розраховується:

$$Rngi = P - Pi,$$

де *P* – ймовірність появи головної події;

Pi – ймовірність появи головної події за умови вилучення *i*-тої події (ймовірність її виникнення дорівнює нулю).

На основі отриманого масиву значень різниць *Rngi* визначають найбільше значення з масиву та задають ранг для подій, яким відповідає дане значення різниці найвище значення рангу – один, після чого дані події вилучають з масиву. За аналогічним алгоритмом визначають події з наступним значенням рангу. Дана процедура повторюється доти, доки потужність масиву не буде рівною нулю (табл. 3.6).

Таблиця. 3.6 – Ранжування негативних факторів.

Подія	Rngi
РХ1	0,0012
РХ 2	0,0014
РХ 3	0,0210
РХ 4	0,0127
РХ 5	0,0171
РХ 6	0,0294
РХ 7	0,0041
РХ 8	0,0235
РХ 9	0,0357
РХ 10	0,0548
РХ 11	0,0175
РХ 12	0,0130
РХ 13	0,0260
РХ 14	0,0010

Ранг	Подія	Rngi
1	РХ 10	0,0548
2	РХ 9	0,0357
3	РХ 20	0,0335
4	РХ 6	0,0294
5	РХ 16	0,0276
6	РХ 19	0,0273
7	РХ 13	0,0260
8	РХ 8	0,0235
9	РХ 15	0,0219
10	РХ 3	0,0210
11	РХ 11	0,0175
12	РХ 5	0,0171
13	РХ 12	0,0130
14	РХ 4	0,0127

PX 15	0,0219
PX 16	0,0276
PX 17	0,0085
PX 18	0,0028
PX 19	0,0273
PX 20	0,0335

15	PX 17	0,0085
16	PX 7	0,0041
17	PX 18	0,0028
18	PX 2	0,0014
19	PX1	0,0012
20	PX 14	0,0010

Результат ранжування показує, що найбільший вплив на безпеку підприємства мають такі негативні фактори, як несанкціонований доступ до букмекерських даних чи програмного забезпечення ігрових систем та впровадження в систему шкідливого програмного забезпечення. Це підтверджує необхідність обраної комплексної системи захисту.

4 РОЗРОБКА ПОЛІТИКИ БЕЗПЕКИ

4.1. Розробка політики безпеки

Вхідні дані:

Основні загрози: несанкціонований доступ до букмекерських даних чи програмного забезпечення ігрових систем, хакерські атаки, безвідповідальність та впровадження в систему шкідливого програмного забезпечення.

Модель порушника (найбільш небезпечний): корисливий інтерес або халатність, IT-спеціаліст, що чинить атаки через мережу, використовує методи та засоби дистанційно (з використанням штатних каналів та протоколів зв'язку), час не залежить від роботи АС, порушник має доступ до контрольованої території. Ранги найбільш імовірних загроз зображені в табл. 4.1.

Таблиця 4.1. Ранжування загроз

Ранг	Загроза	Імовірність виникнення
1	Несанкціонований доступ до букмекерських даних чи програмного забезпечення ігрових систем	0.12
2	Впровадження в букмекерську систему шкідливого програмного забезпечення	0.11
3	DDoS-атаки	0.11
4	Інсайдер	0.11
5	Перевищення повноважень облікових записів в системі	0.06

Політика інформаційної безпеки

1) Загальні положення

В цьому документі надані правила для роботи букмекерської контори провайдера «Live Score», яке займається наданнями гральних послуг в мережі інтернет та обслуговуванням своїх інформаційних систем, для забезпечення цілісності, конфіденційності та доступності інформації, що створюється,

обробляється, зберігається і належить конторі. Ця політика безпеки є обов'язковою для всіх працівників підприємства, а також партнерів в області спільної діяльності.

2) Основні заходи із захисту інформації

КЗЗ від НСД в АС класу «1» та АС класу «3» створюється з використанням сервісів безпеки ОС MS Windows, які мають позитивний експертний висновок адміністрації державної служби спеціального зв'язку (ДССЗ) України.

КЗЗ від НСД в АС класу «3» забезпечується використанням програмних та апаратно-програмних засобів криптографічного захисту інформації, які мають позитивний експертний висновок адміністрації ДССЗ України.

Для забезпечення комплексного захисту інформації в букмекерській конторі використано наступні засоби захисту:

- комплексний захист мережі від DDoS CLOUD FLARE;
- IDM Okta identity management;
- система відеоспостереження;
- Symantec DLP;
- антивірусне програмне забезпечення «ESET NOD 32»;
- McAfee Network Security Platform;
- організаційні заходи;
- масив RAID-1.

Відповідність засобів захисту інформаційним загрозам описана в таблиці 4.2.

Таблиця 4.2 – Засоби захисту від негативних факторів

Найменування захисту	Загрози
Комплексний захист мережі від DDoS CLOUD FLARE	DDoS-атаки на букмекерські сервери
Okta identity management	Перевищення повноважень облікових записів в системі
Symantec DLP	Несанкціонований доступ до букмекерських даних чи

	програмного забезпечення ігрових систем
McAfee Network Security Platform	Інсайдер
Антивірусне програмне забезпечення «ESET NOD 32»;	Впровадження в букмекерську систему шкідливого програмного забезпечення
Організаційні заходи.	Всі з перерахованих
Система відеоспостереження;	Викрадення цінних паперів, несанкціоноване копіювання на носії
Масив RAID-1	Втрата букмекерських даних

3) Вибірка обладнання та приміщення, де розміщуються технічні засоби АС.

Технічні засоби АС, захист яких передбачено у цьому документі, що мають певне територіальне розташування. Усі відділи розподіленні по окремих кімнатах. Варто окремо відмітити відділ розробки, та економічного контролю, де й зберігається основна частина критичної інформації букмекерскої діяльності, що потребує захисту. До перерахованих відділів належать 5 кімнат, у кожній з яких розташоване обладнання й певна кількість робочих місць.

Детальний перелік обладнання описано у таблиці 4.3

Таблиця 4.3 – Обладнання та приміщення

Номера кімнат	Обладнання	Загальна кількість	Підключення
1-5	Комп’ютер	12	Локальна мережа
5	Сервер	2	Доступ до мережі інтернет
1-4	Сканер	3	Локальна мережа
5	Маршрутизатор	1	Доступ до мережі інтернет

4) Інформація, що підлягає захисту АС. До захисту підлягають інформаційні ресурси, що зберігаються в бухгалтерії, фінансовому відділі, фінансового контролю, а також відділі розробки. До таких ресурсів належать електронні фінансові звіти, розміщені у приміщеннях під номерами 1, 2, 3 ; посадові інструкції, що потребують захист цілісності та доступності та розміщені у всіх приміщеннях вказаних відділів у паперовому та електронному представленні; договори з гравцями та партнерами, розміщені у економічному відділі представлені в електронному вигляді; аналітичні звіти, розміщені у фінансовому відділі та на сервері у електронному вигляді; персональні дані працівників, збережені у вигляді бази даних на сервері; схема букмекерської мережі; алгоритми букмекерських гральних систем; договори з оренди, представлені у паперовому вигляді, розміщені у приміщеннях номер 1 та 2; база даних клієнтів, розміщена на сервері;

Категорії персоналу АС. Правила розмежування доступу в АС.

Персонал АС належить до трьох основних категорій: Керівник відділу, інженери, робітники. Залежно від наданих обов’язків кожен працівник входить до однієї з категорій та отримує відповідні для своєї категорії права доступу на читання та модифікацію інформації.

Працівники зобов’язані дотримуватись правил розмежування доступу. За недотримання правил розмежування доступу працівнику дається попередження або може бути накладено адміністративне покарання, в залежності від порушення, яке було здійснено відповідно до Закону України, на працівника накладається грошове стягнення і/або звільнення з посади.

Працівники категорії керівник відділу мають право на читання та модифікацію таких інформаційних ресурсів, як технологічна документація, конструкторська документація, програмна документація, інструкції по роботі з обладнанням, а для журналу інструктажів з ОП тільки право на читання.

Інженери мають доступ на читання усіх вище зазначених інформаційних ресурсів.

Особи категорії робітники мають право лише на перегляд технологічної документації, інструкції по роботі з обладнанням та журналів інструктажів з ОП.

Кожен працівник зобов’язаний дотримуватись правил та рекомендацій:

- проходження пропускного пункту є обов’язковим для кожного працівника букмекерської контори;
- дотримуватися правил роботи в локальній мережі;
- вчасно проходити курси підвищення кваліфікації;
- дотримуватись усіх правил та норм роботи в мережі;
- при виникненні певних технічних проблем звертатися до головного інженера або адміністратора кібербезпеки контори;
- кожен працівник має пам’ятати пароль від власного облікового запису, не розголошувати та не залишати його на видному місці;
- забороняється користуватись власними носіями інформації;
- забороняється користуватися власними засобами зв’язку в службових цілях;
- розголошення конфіденційної інформації, яка пов’язана з конторою, її інформацією карається матеріальним стягненням та/або звільненням.

6) Управління обліковими записами користувачів АС їх ідентифікація та автентифікація.

Для кожного користувача букмекерської контори існує власний обліковий запис користувача. Обліковий запис має права, що відповідають правам категорії, до якої належить користувач. Всі облікові записи захищені унікальними паролями. Користувачам забороняється фіксувати свої облікові дані в будь-який спосіб окрім записів у свій робочий записник. Всі паролі до облікових записів складаються відповідно до визначених норм, що забезпечує використання лише стійких паролів.

Резервна копія паролів адміністратора зберігається у сейфі адміністратора служби безпеки та реагування. У разі необхідності або при надзвичайній

ситуації адміністратор може змінити паролі користувача після узгодження із головним інженером. Планова зміна всіх паролів повинна проводитись кожних два місяці.

На обладнані використовуваного підприємством встановлений аудит входів користувачів у систему з використанням облікових записів. Адміністратор щотижнево детально перевіряє журнали аудиту на наявність спроб несанкціонованої автентифікації та авторизації.

7) Опечатування вузлів, блоків, портів введення/виведення в конторі.

Переміщення доступ до яких закривають на певний час необхідно опломбовувати. Опечатування здійснюються адміністратором кіббезпеки IT-відділу контори, який є відповідальним за безпеку. Розкриття здійснюється з дозволу адміністратора безпеки. Є спеціальний перелік вузлів, блоків, портів, які підлягають опечатуванню.

8) Блокування (демонтаж) портів та пристроїв введення/виведення на зовнішні носії інформації.

Перевірка пристроїв введення/ виведення на наявність несанкціонованих сторонніх пристроїв виконується адміністратором безпеки двічі на день. Порти, які не використовуються повинні бути фізично заблоковані. Для попередження певного виду атак через сторонні зовнішні носії на комп’ютерах підприємства встановлено спеціалізоване програмне забезпечення «Зілля», за функціонування та оновлення якого відповідає адміністратор безпеки.

9) Особливості поводження з документами в електронному вигляді.

Документи в електронному представлені, з підвищеними вимогами до цілісності повинні бути захищенні електронним цифровим підписом. Документи повинні передаватись лише внутрішньою локальною мережею та службовими носіями інформації. Забороняється передача важливих документів у відкритому вигляді. Всі документи підприємства повинні знаходитись на комп’ютерах та серверах підприємства, окрім тих, що не становлять цінності для підприємства. Детальна інформація щодо збереження документації підприємства надається в посадових інструкціях користувачів.

10) Особливості поводження з документами в паперовому вигляді.

Паперовому документація, що має вимоги до цілісності повинна знаходитися у сейфі посадових осіб.

Працюючи з документами паперового представлення працівники зобов’язані дотримуватись особливої обережності Працівники повинні обережно поводитись з паперовими документами, та не залишати їх на робочому місці без нагляду. Псування документу карається штрафом, розмір якого залежить від важливості документу

4.2.Інструкція адміністратора з безпеки

1. **Загальні положення**

1.1. Посада "Адміністратор кіберзахисту" букмекерської контори відноситься до категорії "Керівники".

1.2. Кваліфікаційні вимоги - повна вища освіта відповідного напряму підготовки (магістр, бакалавр). Стаж роботи за професіями керівників нижчого рівня відповідного професійного спрямування: для магістра - не менше 2 років, бакалавра - не менше 3 років.

1.3. Знає та застосовує у діяльності:

законодавчі та нормативно-правові акти у сфері букмекерської діяльності;

систему й організацію діловодства та ведення архівної справи;

систему організації контролю за виконанням документів;

систему роботи з персоналом в сфері інформаційної безпеки;

управлінські технології;

профіль, спеціалізацію та особливості структури підприємства;

інформаційні технології, засоби обчислювальної техніки, комунікацій та засоби для їх захисту;

правила та норми з охорони праці, виробничої санітарії та пожежної безпеки.

1.4. Адміністратор служби безпеки призначається на посаду та звільняється з посади наказом директора контори.

1.5. Адміністратор служби безпеки підпорядковується безпосередньо директору контори.

1.6. Адміністратор служби безпеки керує роботою служби безпеки.

1.7. Адміністратор служби безпеки під час відсутності, заміщається особою, призначеною в установленому порядку, яка набуває відповідних прав і несе відповідальність за належне виконання покладених на неї обов'язків.

2. **Характеристика робіт, завдання та посадові обов'язки**

2.1. Забезпечує діяльність адміністративної служби підприємства та несе персональну відповідальність перед керівництвом за виконання покладених на нього обов'язків.

2.2. Очолює та організовує роботу щодо забезпечення інформаційних зв'язків та внутрішнього адміністративного координування діяльності підприємства.

2.3. Формує інформаційно-комунікативну інфраструктуру підприємства та структуру її захисту.

2.4. Розподіляє обов'язки між співробітниками служби безпеки та керівниками всіх відділів підприємства, спрямовує, координує та контролює їх роботу.

2.5. Подає пропозиції керівництву щодо структури адміністративної служби та її модернізації.

2.6. Вживає заходи щодо вдосконалення форм і методів роботи персоналу.

2.7. Вживає заходи щодо вдосконалення КСЗІ на конторі, кожна нова стратегія захисту узгоджується з керівництвом.

2.8. Бере участь у формуванні заходів щодо захисту контори від внутрішніх та зовнішніх загроз, та в межах наданих йому повноважень контролює їх виконання.

2.9. Контролює у межах своїх повноважень стан інформаційно безпеки на підприємстві в цілому та в окремих структурних підрозділах.

2.10. Бере участь у формуванні кадрової політики контори та контролює дієздатність персоналу.

2.11. Разом з керівниками структурних підрозділів бере участь у розробленні посадових інструкцій і правил внутрішнього трудового розпорядку, вживає заходів щодо забезпечення відповідних умов праці на робочих місцях.

2.12. Очолює та організовує роботу з підготовки й проведення заходів підвищення кваліфікації у сфері безпеки за участю керівництва, організації правил пропуску сторонніх відвідувачів на територію контори.

2.13. Дотримується конфіденційності в роботі з ІзОД відповідно до вимог чинного законодавства.

2.14. Знає, розуміє і застосовує діючі нормативні документи, що стосуються його діяльності.

2.15. Знає і виконує вимоги нормативних актів про захист інформації в ІТС.

2.16. Зобов’язаний регулярно (не менше 1 разу в рік) підвищувати свою професійну кваліфікацію, шляхом проходження курсів підвищення кваліфікації в сфері інформаційної безпеки.

2.17. Здійснює перевірку роботи служби безпеки та контори.

2.18. Визначає необхідні права доступу до компонентів АС для користувачів системи.

2.19. Перевіряє не менше 2 разів на день цілісність системи, наявність її пошкоджень, у разі виявлення пошкоджень або несправностей, виконати необхідні заходи щодо їх усунення та повідомити керівництво.

2.20. Здійснює перевірку налаштувань правил безпеки у системі.

2.21. Аналізує роботу функціонуючої КСЗІ на конторі та її відповідність визначеним критеріям.

2.22. Організовує регулярні заходи, які спрямовані на підвищення рівня обізнаності працівників контори, у сфері безпеки інформації.

3. **Права**

3.1. Адміністратор кібербезпеки має право вживати дії для запобігання та усунення випадків будь-яких порушень або невідповідностей.

3.2. Адміністратор кібербезпеки має право отримувати всі передбачені законодавством соціальні гарантії.

3.3. Адміністратор кібербезпеки має право вимагати сприяння у виконанні своїх посадових обов'язків і здійсненні прав.

3.4. Адміністратор кібербезпеки має право вимагати створення організаційно-технічних умов та заходів по захисту інформації, необхідних для виконання посадових обов'язків та надання необхідного обладнання та інвентарю.

3.5. Адміністратор кібербезпеки має право знайомитися з проектами документів, деталями букмекерських ігрових систем, тощо.

3.6. Адміністратор кібербезпеки має право запитувати і отримувати документи, матеріали та інформацію, необхідні для виконання своїх посадових обов'язків і розпоряджень керівництва.

3.7. Адміністратор кібербезпеки зобов’язаний повідомляти про виявлені в процесі своєї діяльності порушення і невідповідності і вносити пропозиції щодо їх усунення.

3.8. Адміністратор кібербезпеки має право ознайомлюватися з документами, що визначають права та обов'язки за займаною посадою, критерії оцінки якості виконання посадових обов'язків.

4. **Відповідальність**

4.1. Адміністратор кібербезпеки несе відповідальність за невиконання або несвоєчасне виконання покладених цією посадовою інструкцією обов`язків та (або) невикористання наданих прав.

4.2. Адміністратор кібербезпеки несе відповідальність за недотримання правил внутрішнього трудового розпорядку, охорони праці, техніки безпеки, виробничої санітарії та протипожежного захисту у відділі безпеки.

4.3. Адміністратор кібербезпеки несе відповідальність за розголошення інформації про контору, що відноситься до ІзОД.

4.4. Адміністратор кібербезпеки несе відповідальність за невиконання або неналежне виконання вимог внутрішніх нормативних документів контори та законних розпоряджень керівництва.

4.5. Адміністратор кібербезпеки несе відповідальність за правопорушення, скоєні в процесі своєї діяльності, в межах, встановлених чинним адміністративним, кримінальним та цивільним законодавством.

4.6. Адміністратор кібербезпеки несе відповідальність за завдання матеріального збитку підприємству в межах, встановлених чинним адміністративним, кримінальним та цивільним законодавством.

4.7. Адміністратор кібербезпеки несе відповідальність за неправомірне використання наданих службових повноважень, а також використання їх в особистих цілях.

5 ЕКОНОМІЧНА ЧАСТИНА

Метою економічної частини магістерської кваліфікаційної роботи є обґрунтування економічної доцільності розробки автоматизованої системи контролю та управління букмекерською конторою. Для цього необхідно виконати такі етапи робіт:

- оцінити комерційний потенціал розробки;
- спрогнозувати витрати на виконання наукової роботи та впровадження її результатів;
- спрогнозувати комерційний ефект від реалізації результатів розробки;
- розрахувати ефективність вкладених інвестицій та період їх окупності.

5.1. Оцінювання комерційного потенціалу розробки (технологічний аудит розробки)

Об’єктом дослідження магістерської кваліфікаційної роботи є захищена автоматизована система контролю та управління букмекерською конторою.

Для проведення технологічного аудиту було залучено трьох незалежних експертів: Войтович О.П., Каплун В.А., Куперштейн Л.М. Кожен з експертів повинен ознайомитися з запропонованою розробкою та заповнити таблицю, яка визначає рекомендовані критерії оцінювання комерційного потенціалу розробки та їх можливу оцінку в балах. Після виконання цього, підраховується середньоарифметична сума балів та визначається який рівень комерційного потенціалу має нова розробка.

Здійснюємо оцінювання комерційного потенціалу розробки за 12-ю критеріями, наведеними в таблиці 5.1.

Таблиця 5.1 – Рекомендовані критерії оцінювання комерційного потенціалу розробки та їх можлива бальна оцінка

Критерії оцінювання та бали (за 5-ти бальною шкалою)					
Критерій	0	1	2	3	4
Технічна здійсненність концепції:					
1	Достовірність концепції не підтверджена	Концепція підтверджена експертними висновками	Концепція підтверджена розрахунками	Концепція перевірена на практиці	Перевірено роботоздатність продукту в реальних умовах
Ринкові переваги (недоліки):					
2	Багато аналогів на малому ринку	Мало аналогів на малому ринку	Кілька аналогів на великому ринку	Один аналог на великому ринку	Продукт не має аналогів на великому ринку
3	Ціна продукту значно вища за ціни аналогів	Ціна продукту дещо вища за ціни аналогів	Ціна продукту приблизно дорівнює цінам аналогів	Ціна продукту дещо нижче за ціни аналогів	Ціна продукту значно нижче за ціни аналогів
4	Технічні та споживчі властивості продукту значно гірші, ніж в аналогів	Технічні та споживчі властивості продукту трохи гірші, ніж в аналогів	Технічні та споживчі властивості продукту на рівні аналогів	Технічні та споживчі властивості продукту трохи кращі, ніж в аналогів	Технічні та споживчі властивості продукту значно кращі, ніж в аналогів
5	Експлуатаційні витрати значно вищі, ніж в аналогів	Експлуатаційні витрати дещо вищі, ніж в аналогів	Експлуатаційні витрати на рівні експлуатаційних витрат аналогів	Експлуатаційні витрати трохи нижчі, ніж в аналогів	Експлуатаційні витрати значно нижчі, ніж в аналогів
Ринкові перспективи					
6	Ринок малий і не має позитивної динаміки	Ринок малий, але має позитивну динаміку	Середній ринок з позитивною динамікою	Великий стабільний ринок	Великий ринок з позитивною динамікою

Критерії оцінювання та бали (за 5-ти бальною шкалою)					
Критерій	0	1	2	3	4
7	Активна конкуренція великих компаній на ринку	Активна конкуренція	Помірна конкуренція	Незначна конкуренція	Конкурентів немає
8	Відсутні фахівці як з технічної, так і з комерційної реалізації ідеї	Необхідно наймати фахівців або витрачати значні кошти та час на навчання наявних фахівців	Необхідне незначне навчання фахівців та збільшення їх штату	Необхідне незначне навчання фахівців	Є фахівці з питань як з технічної, так і з комерційної реалізації ідеї
9	Потрібні значні фінансові ресурси, які відсутні. Джерела фінансування ідеї відсутні	Потрібні незначні фінансові ресурси. Джерела фінансування відсутні	Потрібні значні фінансові ресурси. Джерела фінансування є	Потрібні незначні фінансові ресурси. Джерела фінансування є	Не потребує додаткового фінансування
10	Необхідна розробка нових матеріалів	Потрібні матеріали, що використовуються у військово-промисловому комплексі	Потрібні дорогі матеріали	Потрібні досяжні та дешеві матеріали	Всі матеріали для реалізації ідеї відомі та давно використовуються у виробництві
11	Термін реалізації ідеї більший за 10 років	Термін реалізації ідеї більший за 5 років. Термін окупності інвестицій більше 10-ти років	Термін реалізації ідеї від 3-х до 5-ти років. Термін окупності інвестицій	Термін реалізації ідеї менше 3-х років. Термін окупності інвестицій від 3-х до 5-ти років	Термін реалізації ідеї менше 3-х років. Термін окупності інвестицій менше 3-х років

Критерії оцінювання та бали (за 5-ти бальною шкалою)					
Критерій	0	1	2	3	4
			більше 5-ти років		
12	Необхідна розробка регламентних документів та отримання великої кількості дозвільних документів на виробництво та реалізацію продукту	Необхідно отримання великої кількості дозвільних документів на виробництво та реалізацію продукту, що вимагає значних коштів та часу	Процедура отримання дозвільних документів для виробництва та реалізації продукту вимагає незначних коштів та часу	Необхідно тільки повідомлення відповідним органам про виробництво та реалізацію продукту	Відсутні будь-які регламентні обмеження на виробництво та реалізацію продукту

Результати оцінювання комерційного потенціалу розробки наведено в таблиці 5.2.

Таблиця 5.2 – Результати оцінювання комерційного потенціалу розробки

Критерії	Прізвище, ініціали експерта		
	Войтович О.П.	Каплун В.А.	Куперштейн Л.М.
	Бали, виставлені експертами:		
1	2	1	2
2	2	3	2
3	4	3	3
4	3	3	4
5	3	3	4
6	3	3	3
7	0	0	0
8	4	3	4
9	2	2	3
10	3	3	3
11	4	4	4
12	2	0	1
Сума балів	$СБ_1$=32	$СБ_2$=28	$СБ_3$=33

Середньоарифметична сума балів $\overline{СБ}$	$\overline{СБ} = \frac{\sum_{1}^{i} СБ_i}{i} = \frac{x1 + x2 + x3}{3} = \frac{32 + 28 + 33}{3} = \frac{93}{3} = 31$

За даними таблиці 5.2 робимо висновок щодо рівня комерційного потенціалу розробки захищеної автоматизованої системи контролю та управління букмекерською конторою. При цьому використано рекомендації, що наведено у таблиці 5.3.

Таблиця 5.3 – Рівні комерційного потенціалу розробки

Середньоарифметична сума балів	Рівень комерційного потенціалу
0-10	Низький
11-20	Нижче середнього
21-30	Середній
31-40	Вище середнього
41-50	Високий

Отже, з отриманих даних таблиці 5.2 видно, що середньоарифметична сума балів дорівнює 31, тобто нова розробка має рівень комерційного потенціалу вище середнього.

Оцінювання рівня якості розробки захищеної автоматизованої системи контролю та управління букмекерською конторою здійснюється з метою порівняльного аналізу та визначення найбільш ефективного, з технічної точки зору, варіанта інженерного рішення.

Рівень якості – кількісна характеристика міри придатності певного виду продукції для задоволення конкретного попиту на неї при порівнянні з відповідними базовими показниками за фіксованих умов споживання.

Абсолютний рівень якості розробки захищеної автоматизованої системи контролю та управління букмекерською конторою знаходимо обчисленням

обраних для вимірювання показників, не порівнюючи їх із відповідними показниками аналогічних засобів.

Для визначення рівня якості розробки обрано систему параметрів: ймовірність обходу комплексної системи захисту, складність апаратної реалізації, швидкість реагування.

Визначаємо величину параметрів якості в балах та встановлюємо граничні значення (кращі, гірші, середні). Дані для кожного параметра представлено у таблиці 5.4.

Таблиця 5.4 – Основні параметри захищеної автоматизованої системи контролю та управління букмекерською конторою

Параметри	Абсолютне значення параметра			Коефіцієнт вагомості параметра
	Краще +5…+4	Середнє +3	Гірше +1..+2	
ймовірність обходу комплексної системи захисту			2	0.3
складність апаратної реалізації		3		0.3
відсоток покриття функцій букмекерської системи системою захисту	5			0.4

Із врахуванням коефіцієнтів вагомості відповідних параметрів можна визначити абсолютний рівень якості інноваційного рішення за формулою

$$K_{я.а.} = \sum_{i=1}^{n} Рн_i * a_i \,, \qquad (5.1)$$

де $Рн_i$ – числове значення i-го параметра інноваційного рішення, n – кількість параметрів інноваційного рішення, що прийняті для оцінювання, a_i – коефіцієнт вагомості відповідного параметра (сума коефіцієнтів вагомості всіх параметрів повинна дорівнювати 1).

Отже, абсолютний рівень якості захищеної автоматизованої системи складає 3,5 бали.

Одночасно визначаємо відносний рівень якості захищеної автоматизованої системи контролю та управління букмекерської контори, шляхом порівнюючи показники з абсолютними показниками якості найліпших аналогів, що представлено у таблиці 5.4.

Таблиця 5.4 – Порівняння основних параметрів захищеної автоматизованої системи контролю та управління букмекерської контори та товару-конкурента

Параметри	Варіанти		Відносний показник якості	Коефіцієнт вагомості параметра
	Базовий (конкурент)	Новий		
ймовірність обходу комплексної системи захисту	0,15	0,09	2	0,3
складність апаратної реалізації	2600	2812	1,7	0,3
відсоток покриття функцій букмекерської системи системою захисту	0,6	0,95	0,98	0,4

Відносний рівень якості захищеної автоматизованої системи контролю та управління букмекерської контори визначаємо за формулою 5.2:

$$К_{я.в.} = \sum_{i=1}^{n} q_i * a_i \qquad (5.2)$$

За розрахунками відносний рівень якості захищеної автоматизованої системи контролю та управління букмекерської контори 1,9. Це означає, що нова розробка якісніша на 68% відносно товару-аналога.

У найширшому розумінні конкурентоспроможність товару – це можливість його успішного продажу на певному ринку і в певний проміжок часу. Водночас конкурентоспроможною можна вважати лише однорідну продукцію з технічними параметрами і техніко-економічними показниками, що ідентичні аналогічним показникам уже проданого товару. Для того, щоб високоякісний товар був одночасно і конкурентоспроможним, він має відповідати критеріям оцінювання споживачів конкретного ринку в конкретний період часу.

Дані для розрахунку загального показника конкурентоспроможності розробки необхідно занести до таблиці 5.5.

Таблиця 5.5 – Нормативні, технічні та економічні параметри захищеної автоматизованої системи контролю та управління букмекерської контори та товару-конкурента

Параметри	Варіанти		Відносний показник якості	Коефіцієнт вагомості параметра
	Базовий (конкурент)	Новий		
ймовірність обходу комплексної системи захисту	0,15	0,09	2	0,3
складність апаратної реалізації	2600	2812	1,7	0,3
відсоток покриття функцій букмекерської системи системою захисту	0,6	0,95	0,98	0,4
Ціна за продукт, грн	17500	16000	0,68	-

Загальний показник конкурентоспроможності розробки (K) з урахуванням вищезазначених груп показників визначаємо за формулою 5.3:

$$K = \frac{I_{\text{т.п}}}{I_{\text{е.п.}}} = \frac{1{,}9}{0{,}91} = 2{,}08 \qquad (5.3)$$

де $I_{Т.П.}$ – індекс технічних параметрів (відносний рівень якості інноваційного рішення); $I_{Е.П.}$ – індекс економічних параметрів розрахований нижче за формулою 5.4:

$$I_{\text{Е.П.}} = \frac{\text{РН}_{\text{EI}}}{\text{РБ}_{\text{EI}}} = \frac{16000}{17500} = 0{,}91 \quad (5.4)$$

де $РН_{EI}$, $РБ_{EI}$ – економічні параметри (ціна придбання та споживання товару) відповідно нового та базового товарів.

Згідно розрахунків загальний показник конкурентоспроможності 0,91, що свідчить про більшу конкурентну спроможність методів та засобів криптографічного перетворення на основі латинських квадратів у порівнянні з товаром-аналогом на 104%.

5.2. Прогнозування витрат на виконання науково-дослідної та конструкторсько-технологічної роботи

5.2.1. Розрахунок витрат, що стосуються виконавців розробки захищеної автоматизованої системи контролю та управління

Команда розробки захищеної автоматизованої системи захисту та управління букмекерської контори складається з керівника та інженера.

Основна заробітна плата для розробників (дослідників) *Зо*, якщо вони працюють в наукових установах бюджетної сфери визначається за формулою:

$$З_О = \frac{M}{T_p} t \quad (5.5)$$

де M – місячний посадовий оклад розробника;

T_p – кількість робочих днів у місяці, T_p = 22 дні; t – число днів роботи.

Розрахунки заробітної плати для розробників наведені в таблиці 5.6

Таблиця 5.6 – Розрахунки основної заробітної плати розробників

Працівник	Оклад М, грн.	Оплата за робочий день, грн.	Число днів роботи, t	Витрати на оплату праці, грн.
Керівник	25000	1136,36	11	12499,96
Інженер	20000	909,09	15	13636,35
Всього:				26136,31

Основна заробітна плата робітників *Зр*, якщо вони беруть участь у виконанні даного етапу роботи і виконують роботи за робочими професіями у випадку, коли вони працюють в наукових установах бюджетної сфери, розраховується за формулою:

$$З_Р = \sum_{i=1}^{n} t_i \cdot C_i \,, \tag{5.6}$$

де t_i – норма часу (трудомісткість) на виконання конкретної роботи, годин; n – число робіт по видах та розрядах; C_i – погодинна тарифна ставка робітника відповідного розряду, який виконує дану роботу. C_i визначається за формулою:

$$C_i = \frac{M_M * K_i}{T_p * T_{зм}}, \tag{5.7}$$

де M_M – розмір мінімальної заробітної плати за місяць, грн.; в 2021 році мінімальна заробітна плата становить – 6500 грн., K_i – тарифний коефіцієнт робітника відповідного розряду, T_p = 22 дні; $T_{зм}$ – тривалість зміни, $T_{зм}$ =8 годин.

Таблиця 5.7 – Заробітна плата робітників

Найменування робіт	Трудомісткість, н-год.	Розряд роботи	Погодинна тарифна ставка	Тариф. коеф.	Величина, грн.
Розробка	8	5	55,767	1,51	446,14
Тестування	8	4	50,596	1,37	404,77
Впровадження	2	2	40,25	1,04	80,96
Всього					931,87

Додаткова заробітна плата $З_Д$ всіх розробників та робітників, які брали участь у виконанні даного етапу роботи, розраховується як (10…12)% від суми основної заробітної плати всіх розробників та робітників, тобто:

$$З_д = 0{,}1 * (З_О + З_Р) = 0{,}1 * (26136{,}31 + 931{,}87) = 2706{,}81 \text{ (грн.)} \tag{5.8}$$

Нарахування на заробітну плату $H_{ЗП}$ розраховується як 22% від суми основної та додаткової заробітної плати:

$$Н_{ЗП} = (З_О + З_Р + З_Д) * \frac{\beta}{100} = (26136{,}31 + 931{,}87 + 2706{,}81) * 0{,}22 = 6550{,}5 \text{ (грн.)} \quad (5.9)$$

де $З_О$ – основна заробітна плата розробників, грн.;

$З_р$ – основна заробітна плата робітників, грн.;

$З_Д$ – додаткова заробітна плата розробників, грн.;

β – ставка єдиного внеску на загальнообов'язкове державне страхування.

Розрахунок амортизаційних відрахувань виконується за такою формулою:

$$A = \frac{Ц}{t_В} \times \frac{T}{12} \quad (5.10)$$

де $Ц$ – балансова вартість обладнання, грн;

T – термін використання (T=22 дні= 0,73 місяців);

$t_В$ – корисний час використання ($t_В$ для комп'ютера становить 4 роки).

Під час виконання розробки використовувався ноутбук вартістю 14000 грн. Амортизаційні відрахування для ноутбуку представлені у таблиці 5.8.

Таблиця 5.8 - Амортизаційні відрахування

Найменування	Ціна, грн.	Корисний час використання, роки	Термін використання, міс.	Сума амортизації, грн.
Ноутбук	14000	4	0,73	212,91
Всього	212,91			

Витрати на силову електроенергію розраховуються за формулою:

$$B_Е = В \times П \times Ф \times К_П \quad (5.11)$$

де $В$ – вартість 1кВт-години електроенергії (В=4,62 грн/кВт);

$П$ – установлена потужність комп'ютеру ($П$=0,74 кВт);

$Ф$ – фактична кількість годин роботи комп'ютеру ($Ф$=22*8=176 год);

$К_П$ – коефіцієнт використання потужності ($К_П$ <1, $К_П$ = 0,8).

Відповідно до формули 5.11 витрати на силову електроенергію:

$B_E = 4{,}62 \times 0{,}74 \times 176 \times 0{,}8 = 481{,}36$ (грн.)

Інші витрати $B_{ін}$ можна прийняти як (100-300)% від суми основної заробітної плати розробників, які виконували роботу, тобто:

$$B_{\text{ін}} = 1 * (26136{,}31 + 931{,}87) = 27067{,}31 \text{ (грн.)} \quad (5.11)$$

Сума усіх попередніх витрат дає загальні витрати на виконання роботи. Усі витрати складають:

$$B = 26136{,}31 + 931{,}87 + 27067{,}31 + 481{,}36 + 6550{,}5 + 25931{,}82 + 212{,}91 = 60243{,}9 \text{ (грн.)}$$

Розрахунок загальної вартості наукової розробки $В_{заг}$ за формулою:

$$B_{заг} = \frac{B}{\alpha}, \quad (5.12)$$

де α – частка витрат, які безпосередньо здійснює виконавець даного етапу роботи, у відносних одиницях.

$В_{заг} = \frac{60243{,}9}{1} = 60243{,}9$ (грн.)

Прогнозування загальних витрат *ЗВ* на виконання та впровадження результатів виконаної наукової роботи здійснюється за формулою:

$$ЗВ = \frac{B_{заг}}{\beta} \quad (5.13)$$

Розрахунок прогнозованих загальних витрат:

$ЗВ = \frac{60243{,}9}{0{,}7} = 42170{,}73$ (грн.)

5.2.2. Розрахунок собівартості розробки захищеної автоматизованої системи контролю та управління букмекерською конторою

Витрати на силову електроенергію розраховуються за формулою:

$$B_E = B \times П \times Ф \times K_П \quad (5.14)$$

де B – вартість 1кВт-години електроенергії (В=4,62 грн/кВт);

$П$ – установлена потужність комп'ютеру ($П$=0,74 кВт);

$Ф$ – фактична кількість годин роботи комп'ютеру ($Ф$=22*8=176 год);

$K_П$ – коефіцієнт використання потужності ($K_П$ <1, $K_П$ = 0,8).

Відповідно до формули 5.14 витрати на силову електроенергію:

$B_E = 4{,}62 \times 0{,}74 \times 176 \times 0{,}8 = 481{,}36$ (грн.)

Основна заробітна плата робітників $Зр$, якщо вони беруть участь у виконанні даного етапу роботи і виконують роботи за робочими професіями у випадку, коли вони працюють в наукових установах бюджетної сфери, розраховується за формулою:

$$З_P = \sum_{i=1}^{n} t_i \cdot C_i \,, \quad (5.15)$$

де t_i – норма часу (трудомісткість) на виконання конкретної роботи, годин; n – число робіт по видах та розрядах; C_i – погодинна тарифна ставка робітника відповідного розряду, який виконує дану роботу. C_i визначається за формулою:

$$C_i = \frac{M_M * K_i}{T_p * T_{зм}}, \quad (5.16)$$

де M_M – розмір мінімальної заробітної плати за місяць, грн.; в 2021 році мінімальна заробітна плата становить – 6500 грн., K_i – тарифний коефіцієнт робітника відповідного розряду, T_p = 22 дні; $T_{зм}$ – тривалість зміни, $T_{зм}$ =8 годин.

Таблиця 5.9 – Заробітна плата робітників

Найменування робіт	Трудомісткість, н-год.	Розряд роботи	Погодинна тарифна ставка	Тариф. коеф.	Величина, грн.
Розробка	8	5	55,767	1,51	446,14
Тестування	8	4	50,596	1,37	404,77

Впровадження	2	2	40,25	1,04	80,96
Всього					931,87

Додаткова заробітна плата $З_Д$ всіх робітників, які брали участь у виконанні даного етапу роботи, розраховується як (10…12)% від суми основної заробітної плати всіх розробників та робітників, тобто:

$$З_д = 0{,}1 * (З_р) = 0{,}1 * 931{,}87 = 93{,}187 \text{ (грн.)} \quad (5.17)$$

Нарахування на заробітну плату $Н_{ЗП}$ розраховується як 22% від суми основної та додаткової заробітної плати:

$$Н_{зп} = (З_р + З_д) * \frac{\beta}{100} = (931{,}87 + 93{,}187) * 0{,}22 = 225{,}51 \text{ (грн.)} \quad (5.18)$$

де $З_р$ – основна заробітна плата робітників, грн.;

$З_Д$ – додаткова заробітна плата робітників, грн.;

β – ставка єдиного внеску на загальнообов'язкове державне страхування.

Загальновиробничі витрати з рахунку на одиницю продукції можна розрахувати за нормативами відносно до основної заробітної плати основних робітників, які виготовляють продукцію :

$$ЗВВ = Н_В * З_О, \quad (5.19)$$

Норматив загальновиробничих витрат для програмних продуктів становить 230-270%.

$ЗВВ = 2{,}7 * 931{,}87 = 2516{,}05$ (грн.)

Сума попередніх витрат утворює виробничу собівартість розробки.

$$S_В = 481{,}36 + 931{,}87 + 93{,}187 + 225{,}27 + 2516{,}05 = 4247{,}74 \text{ (грн.)} \quad (5.20)$$

5.3 Розрахунок мінімальної ціни та чистого прибутку від реалізації розробки захищеної автоматизованої системи контролю та управління букмекерською конторою

Ціна – це грошовий вираз вартості товару (продукції, послуги). Вона завжди коливається навколо ціни виробництва (перетвореної форми вартості одиниці товару, що дорівнює сумі витрат виробництва й середнього прибутку) та відображає рівень суспільне необхідних витрат праці.

Виходячи з того, що розробки, як правило, приймаються та впроваджуються за завданням замовника, або коли результатом розробки є продукція, що підлягає державному регулюванню, то нижню межу ціни реалізації розробки можна розрахувати за формулою 5.21:

$$Ц = S_B \cdot (1+\frac{P}{100}) \cdot (1+\frac{\omega}{100}), \qquad (5.21)$$

де S_B – виробнича собівартість інноваційного рішення, грн.;

P – норматив рентабельності узгоджений із замовником або встановлений державою, (Р=30…60%);

ω – ставка податку на додану вартість, % (з осені 2021 року $\omega = 20\%$).

$$Ц = 4247{,}74 * \left(1+\frac{60}{100}\right) * \left(1+\frac{20}{100}\right) = 8155{,}66 \text{ (грн.)} \qquad (5.21)$$

Із врахуванням коефіцієнта якості ціна розробки становить 8155,66 грн.

Чистий прибуток від реалізації розробки можна розрахувати за формулою:

$$П = (Ц - \frac{(Ц - МР)\cdot f}{100} - S_B - \frac{q \cdot S_B}{100}) \cdot (1-\frac{h}{100}) \cdot РП, \qquad (5.22)$$

де $Ц$ – ціна розробки, грн.; $МР$ – вартість матеріальних та інших ресурсів, що були придбані виробником для виготовлення розробки ($МР$=(0,1…0,2) $Ц$), грн.; f – зустрічна ставка податку на додану вартість, %; S_B – виробнича собівартість розробки, грн.; q – норматив, який визначає величину адміністративних витрат,

витрат на збут та інші операційні витрати, % (рекомендовано q=5…10%); h – ставка податку на прибуток, %, $РП$ – прогнозований попит продажів.

$$П = \left(8155{,}66 \ - \frac{(8155{,}66 - 8155{,}66 * 0{,}2) * 14}{100} - 4247{,}74 - \frac{5 * 4247{,}74}{100}\right) * \left(1 - \frac{18}{100}\right) * 2 = 21036{,}8$$

(грн.), (5.23)

Прогнозований чистий прибуток від реалізації розробки складає 21036,8 грн.

5.4 Розрахунок терміну окупності коштів вкладених у наукову розробку захищеної автоматизованої системи контролю та управління букмекерської контори

Термін окупності вкладених у реалізацію наукового проекту інвестицій розраховано за формулою 5.24:

$$Т_{ок} = \frac{ЗВ}{П} = \frac{42170{,}73}{21036{,}8} = 2 \text{ (роки)} \quad (5.24)$$

Оскільки $T_{ОК} < 3$ років, то фінансування наукової розробки захищеної автоматизованої системи контролю та управління букмекерської контори є доцільним.

5.5 Висновки до розділу

Отже, у цьому розділі виконано обґрунтування економічної доцільності проведення наукового дослідження та розробки захищеної автоматизованої системи контролю та управління букмекерської контори.

Рівень комерційного потенціалу розробки захищеної автоматизованої системи контролю та управління букмекерської контори вище середнього.

На основі параметрів комплексів систем захисту визначено абсолютний рівень якості захищеної автоматизованої системи контролю та управління букмекерської контори який складає 3,5 бали.

Відносний рівень якості розробки, що складає 1,9. Це означає, що нова розробка якісніша на 68% відносно товару-аналога. Загальний показник конкурентоспроможності становить 2,08, що свідчить про більшу конкурентну спроможність захищеної автоматизованої системи контролю та управління букмекерської контори у порівнянні з товаром-аналогом на 104%.

Загальні витрати, що стосуються виконавців розробки склали 88056,45 грн, а собівартість розробки – 4247,74 грн.

Розраховано мінімальну ціну та прогнозований чистий річний прибуток від реалізації розробки, які склали 8155,66 грн. та 21036,8 грн. відповідно. Термін окупності продукції вкладених інвестицій складає 2 роки, що свідчить про доцільність фінансування розробки.

ВИСНОВКИ

У ході виконання магістерської кваліфікаційної роботи розроблено захищену автоматизовану систему контролю та управління букмекерською конторою. Проаналізовано інформаційні джерела, серед них методи підвищення безпеки програмного забезпечення букмекерів, виконано оцінку безпеки функціонування існуючих букмекерських контор. В результаті аналізу було досліджено актуальність теми та досліджено методи захисту букмекерської контори. У звязку з дослідженням теми букмекерської контори було також досліджено позиції урядів щодо букмекерської діяльності.

Для досягнення поставленої мети було виконано аналіз структури букмекерської контори «Live Score» та її ресурсів. Виконано аналіз конкурентного середовища, побудовано модель загроз та модель порушника. Це дозволило виконати ідентифікацію загроз та виходячи з цього перейти до розробки захищеної автоматизованої системи контролю та управління букмекерською конторою.

Досліджено та порівняно існуючі і актуальні на ринку комплекси систем захисту, на основі попереднього аналізу було обгрунтовано та застосовано систему керування обліковими записами Okta identity management, систему запобігання витоку даних Symantec DLP, систему запобігання вторгненням McAfee Network Security Platform. Для забезпечення захисту автоматизованої системи контролю та управління букмекерською конторою було також розроблено політику безпеки на основі ідентифікованих і проаналізованих загроз.

При розрахунку витрат на розробку захищеної автоматизованої системи контролю та управління букмекерської контори, витрат експлуатації, обсягу робіт при використанні комплексів систем захисту визначено, що розробка і впровадження продукту є економічно доцільним і виправданим

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Котенко, С. В. Правове регулювання букмекерської діяльності україни та значення договору парі для її здійснення. механізм функціонування громадянського суспільства, 177.
2. Орлова, О. М. (2020). Тенденції розвитку та особливості тіньової онлайн діяльності.
3. Regulation of Bookmakers Policy Paper. Goverment of South Australia. [Електронний ресурс]. URL: https://www.treasury.sa.gov.au/__data/assets/pdf_file/0020/36830/TF12D05320-Regulation-of-Bookmakers-Policy-Paper.pdf
4. The Enhancement Of Bookmakers Software Security. [Електронний ресурс]. URL: http://www.newbookmakersoftware.com/software-security
5. Safe and Secure Online Betting Transactions With Real Bookies. [Електронний ресурс]. URL: https://www.realbookies.com/safe-and-secure-online-betting-transactions-with-real-bookies-2460/
6. Хмарна безпека. [Електронний ресурс]. URL: https://sgs4business.com/news/khmarna-bezpeka-kliuchovi-poniattia-zahrozy-ta-rishennia.html
7. Network and Application Protection on AWS. [Електронний ресурс]. URL: https://aws.amazon.com/ru/products/security/network-application-protection/
8. Bardram, J. E., & Christensen, H. B. (2004, June). Real-time collaboration in activity-based architectures. In Proceedings. Fourth Working IEEE/IFIP Conference on Software Architecture (WICSA 2004) (pp. 325-328). IEEE.
9. Web bookies demand higher security standards. [Електронний ресурс]. URL: https://www.zdnet.com/article/web-bookies-demand-higher-security-standards/
10. How secure are the funds inside bookmaker accounts? [Електронний ресурс]. URL: https://smartbettingclub.com/blog/bookmaker-accounts-security-advice/
11. HBF Register of Protection of Funds. [Електронний ресурс]. URL: https://ukhbf.org/betting-charter/hbf-register-of-protection-of-funds/
12. Protections of Bookmakers customers. [Електронний ресурс]. URL: http://www.gamblingcommission.gov.uk/for-the-public/Your-rights/Protection-of-customer-funds.aspx
13. Яремчук Ю. Є., Павловський П. В., Катаєв В. С., Сінюгін В. В. Комплексні системи захисту інформації : навчальний посібник – Вінниця : ВНТУ, 2017. – 120 с.
14. ЗАКОН УКРАЇНИ. Про внесення змін до Закону України "Про захист інформації в автоматизованих системах". м. Київ. 31 травня 2005 року. N 2594-IV.

15. НД ТЗІ 1.6-005-2013. Захист інформації на об’єктах інформаційної діяльності. Положення про категоріювання об’єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці. [Електронний ресурс]. URL: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?showHidden=1&art_id=107993&cat_id=89734&ctime=1366373635138.
16. Загрози інформаційній безпеці. Статистика. [Електронний ресурс]. URL: http://ekmair.ukma.edu.ua/handle/123456789/116415
17. The Best Identity Management Solutions for 2021. [Електронний ресурс]. URL: https://www.pcmag.com/picks/the-best-identity-management-solutions
18. BEST Data Loss Prevention Software DLP Solutions In 2021. [Електронний ресурс]. URL: https://www.softwaretestinghelp.com/data-loss-prevention-software/
19. Top 12 IDS/IPS tools. [Електронний ресурс]. URL: https://www.csoonline.com/article/3532249/12-top-idsips-tools.html
20. Дудатьєв А.В. Моделі для організації протидії інформаційним атакам. Захист інформації, 2015, 17,№ 2: 157-162.
21. Comprehensive DDoS Network Protection. [Електронний ресурс]. URL: https://www.cloudflare.com/
22. Методика оцінки комплексної системи захисту інформації на об’єкті інформаційної діяльності / С.В. Толюпа, І.В. Борисов // Науково-технічний журнал “Сучасний захист інформації”. – 2013. - №2. – С. 43-49.

ДОДАТКИ

Додаток А. Технічне завдання

Міністерство освіти і науки України
Вінницький національний технічний університет
Факультет інформаційних технологій та комп'ютерної інженерії
Кафедра захисту інформації

Затверджую
Зав. кафедри ЗІ, д. т.н., проф.

_____ В. А. Лужецький

«_____» _____ 2021 р.

ТЕХНІЧНЕ ЗАВДАННЯ
на виконання магістерської кваліфікційної роботи

на тему: «Захищена автоматизована система контролю та управління букмекерською конторою»
08-20.МКР.006.00.000 ТЗ

Керівник магістерської кваліфікаційної роботи
д. т. н., проф, зав. каф. ЗІ
_____ В. А. Лужецький

Розробив студент групи 1БС-20м
_____ В. М. Лабусюк

Вінниця 2021

1 Підстави для проведення робіт

Робота проводиться на підставі наказу ректора ВНТУ від 1 вересня 2021 року № 207.
Дата початку роботи 01.09.21 р.
Дата закінчення роботи 23.11.21 р.

2 Мета та призначення МКР

Мета – підвищення рівня захищеності автоматизованої системи контролю та управління букмекерської контори.
Об'єктом дослідження є процеси захисту автоматизованої системи контролю та управління букмекерської контори.
Предметом є методи та засоби захисту автоматизованої системи контролю та управління букмекерською конторою.

3 Вихідні дані для проведення МКР

МКР проводиться вперше і вихідними даними для проведення МКР є:

3.1 The Enhancement Of Bookmakers Software Security. [Електронний ресурс]. URL: http://www.newbookmakersoftware.com/software-security

3.2 The Best Identity Management Solutions for 2021. [Електронний ресурс]. URL: https://www.pcmag.com/picks/the-best-identity-management-solutions

3.3 BEST Data Loss Prevention Software DLP Solutions In 2021. [Електронний ресурс]. URL: https://www.softwaretestinghelp.com/data-loss-prevention-software/

3.4 Top 12 IDS/IPS tools. [Електронний ресурс]. URL: https://www.csoonline.com/article/3532249/12-top-idsips-tools.htmlhttp://www.sciencedirect.com/science/article/pii/S0957417418302070 (дата звернення 07.09.2021)

3.5 Методика оцінки комплексної системи захисту інформації на об'єкті інформаційної діяльності / С.В. Толюпа, І.В. Борисов // Науково-технічний журнал "Сучасний захист інформації". – 2013. - №2. – С. 43-49.

4 Виконавці МКР

Студент групи 1 БС-20м Лабусюк Віталій Михайлович

5 Вимоги до виконання МКР

Для покращення безпеки та ефективності контролю та управління букмекерської контори необхідно розв'язати такі задачі:

– визначити предметну область букмекерських організацій;
– проаналізувати сучасні методи та засоби захисту букмекерських контор;

– розробити захищену автоматизовану систему контролю та управління букмекерською конторою;

– розробити математичну модель оцінювання рівня захищеності;

– розробити політики безпеки.

6 Вимоги до супровідної документації

Текстова документація повинна відповідати діючим стандартам України – ДСТУ 3008:2015.

7 Етапи МКР

Робота з теми виконується у 8 етапів.

Зміст етапу	Початок - закінчення	Очікувані результати	Звітна документація
Аналіз завдання. Вступ	01.09.2021 – 04.09.2021	Вступ	Чернетка вступу
Розробка технічного завдання	05.09.2021 – 15.09.2021	Технічне завдання	Проект технічного завдання
Аналіз літературних джерел за напрямком магістерської кваліфікаційної роботи	16.09.2021 – 01.10.2021	Аналіз існуючих аналогів. Вибір напрямку дослідження Аналіз відомих методів. Постановка завдання	Чернетка першого розділу
Удосконалення методів захисту АСКУ букмекерськоъ контори	02.10.2021 – 27.10.2021	Удосконалений рівень захищеності контори на основі комплексів систем захисту. Розроблено політку безпеки функціонування контори	Чернетка другого розділу
Експериментальні дослідження	28.10.2021 – 20.11.2021	Комплекс систем захисту, який реалізує розроблювані методи	Чернетка третього розділу
Розробка економічного розділу	21.11.2021 – 9.12.2021	Економічні показники дослідження	Чернетка з економічного розділу
Оформлення пояснювальної записки	10.12.2021 – 15.12.2021	Пояснювальна записка	Пояснювальна записка

8 Очікувані результати та порядок реалізації МКР

Передбачається розробка нових (удосконалення існуючих) методів які спрямовані на покращення захищеності автоматизованої системи контролю та управління букмекерською конторою. Заплановане створення політики безпеки, яка забезпечить додаткові міри безпеки.

9 Матеріали які подаються після закінчення МКР

По завершенню роботи подається пояснювальна записка та ілюстративна частина.

10 Порядок приймання МКР та її етапів

Апробація на науково-технічних конференціях та семінарах. Результати роботи будуть розглядатися на засіданні ДЕК із захисту магістерських кваліфікаційних робіт.
Попередній захист та доопрацювання МКР – 3 грудня 2021 р.
Представлення МКР до захисту – 18 грудня 2021 р.
Захист МКР – 21.12.21.

11 Вимоги до розроблення документації

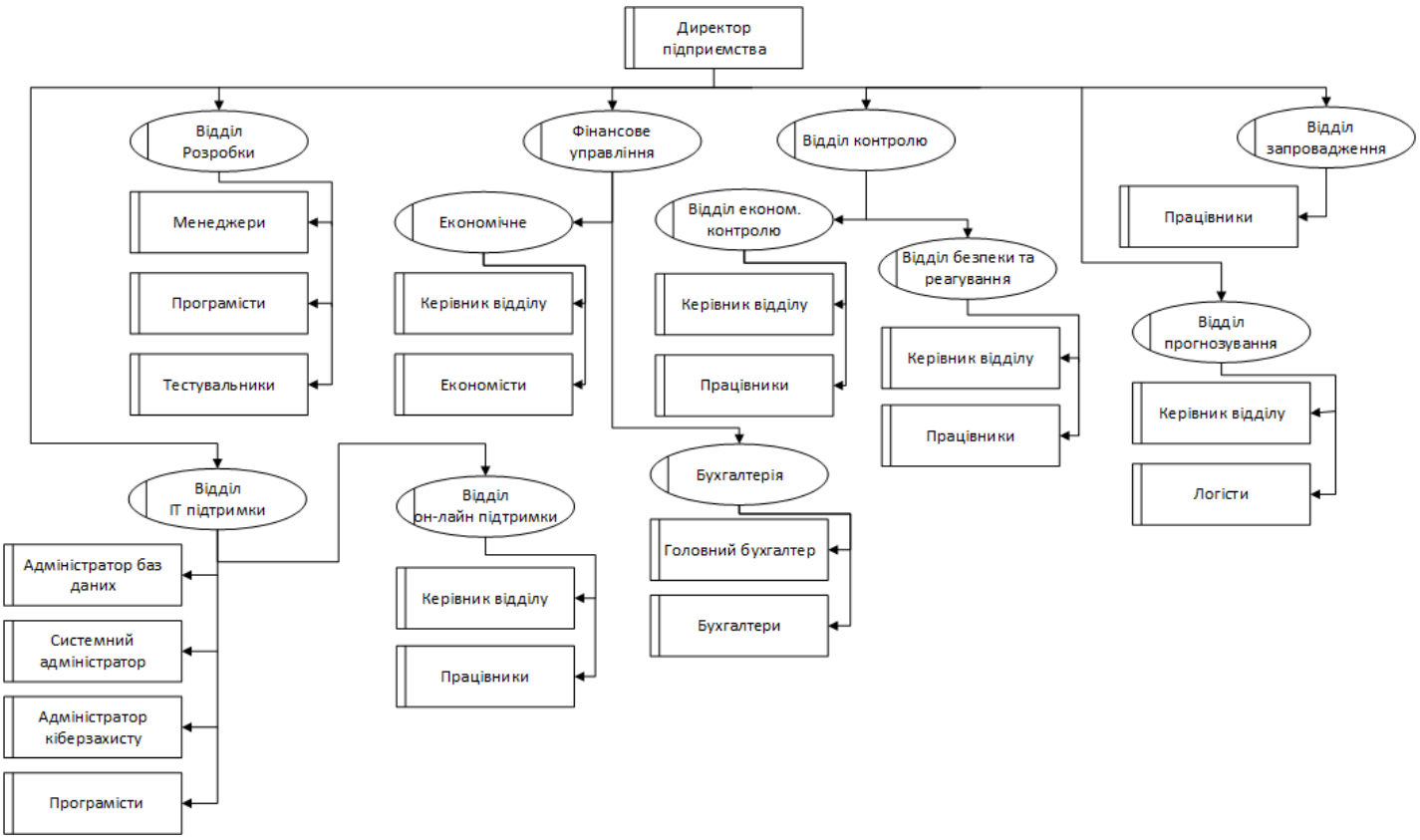
Документація буде виконуватись за допомогою комп’ютерного набору у відповідності вимог ДСТУ 3008:2015 «Інформація та документація. Звіти у сфері науки і техніки. Структура та правила оформлювання».

12 Вимоги щодо технічного захисту інформації з обмеженим доступом

У зв’язку з тим, що дана робота не містить інформації, що потребує захисту у відповідності до законів України, заходи з її технічного захисту не передбачаються.

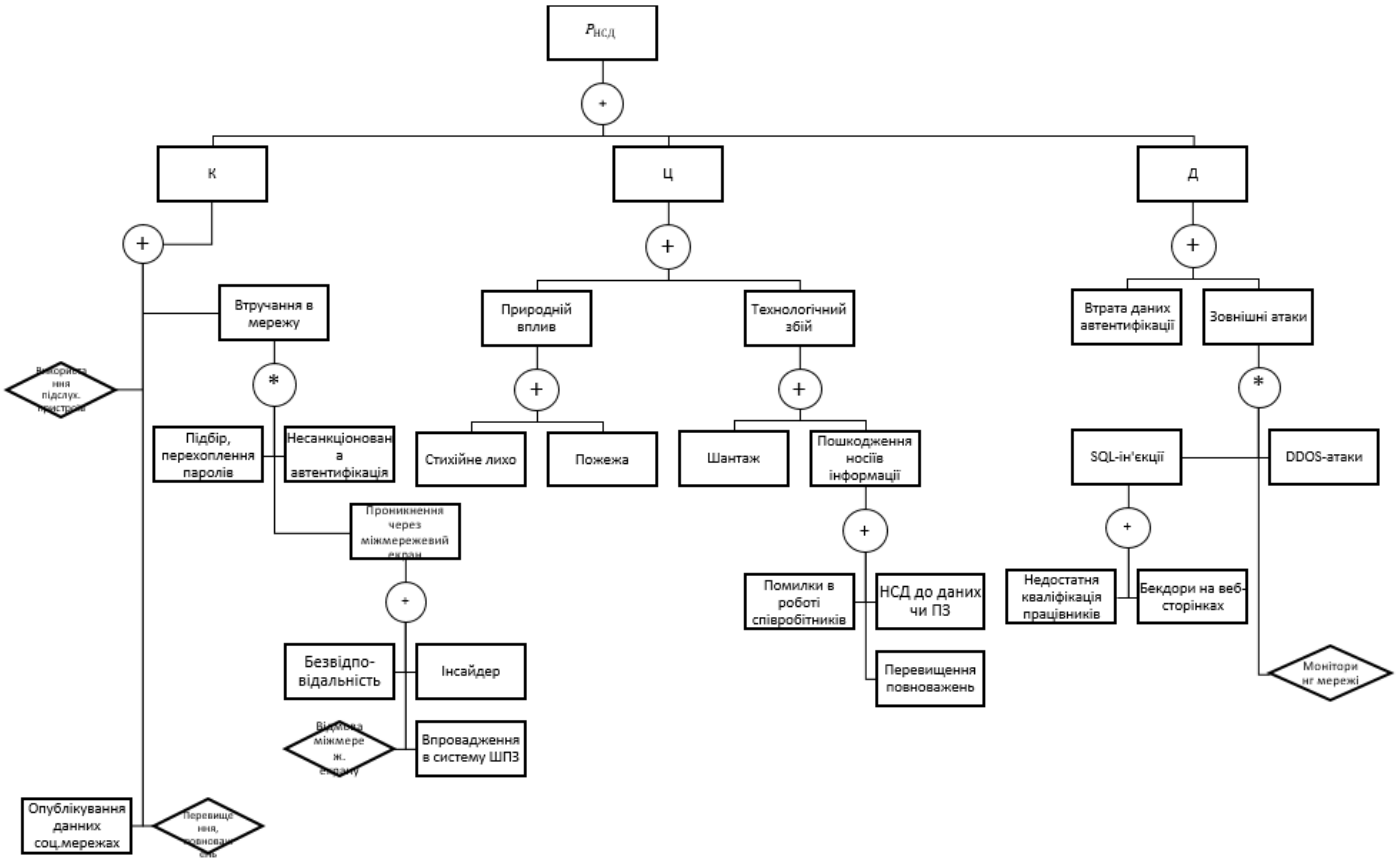
ІЛЮСТРАТИВНА ЧАСТИНА

СТРУКТУРА БУКМЕКЕРСЬКОЇ КОНТОРИ



					08-20.МКР.006.00.000 І41			
Змн.	Арк.	№ докум.	Підпис	Дата				
Розроб.		Лабусюк В.М.			Структура букмекерської контори	Літ.	Арк.	Аркушів
Перевір.		Лужецький В.А.					1	8
Рецензент		Азарова А. О.				ВНТУ гр. 1 БС-20 м		
Н. Контр.		Лужецький В.А.						
Затверд.		Лужецький В.А.						

ЛОГІКО-ЙМОВІРНІСНА МОДЕЛЬ ОЦІНКИ РІВНЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ



					08-20.МКР.006.00.000 ПЗ			
Змн.	Арк.	№ докум.	Підпис	Дата				
Розроб.		Лабусюк В.М.			Логіко-ймовірнісна модель оцінки рівня інформаційної безпеки	Літ.	Арк.	Аркушів
Перевір.		Лужецький В.А.					2	8
Рецензент		Азарова А. О.				ВНТУ гр. 1 БС-20 м		
Н. Контр.		Лужецький В.А.						
Затверд.		Лужецький В.А.						

МОДЕЛІ ЗАГРОЗ ТА ПОРУШНИКА

Модель загроз

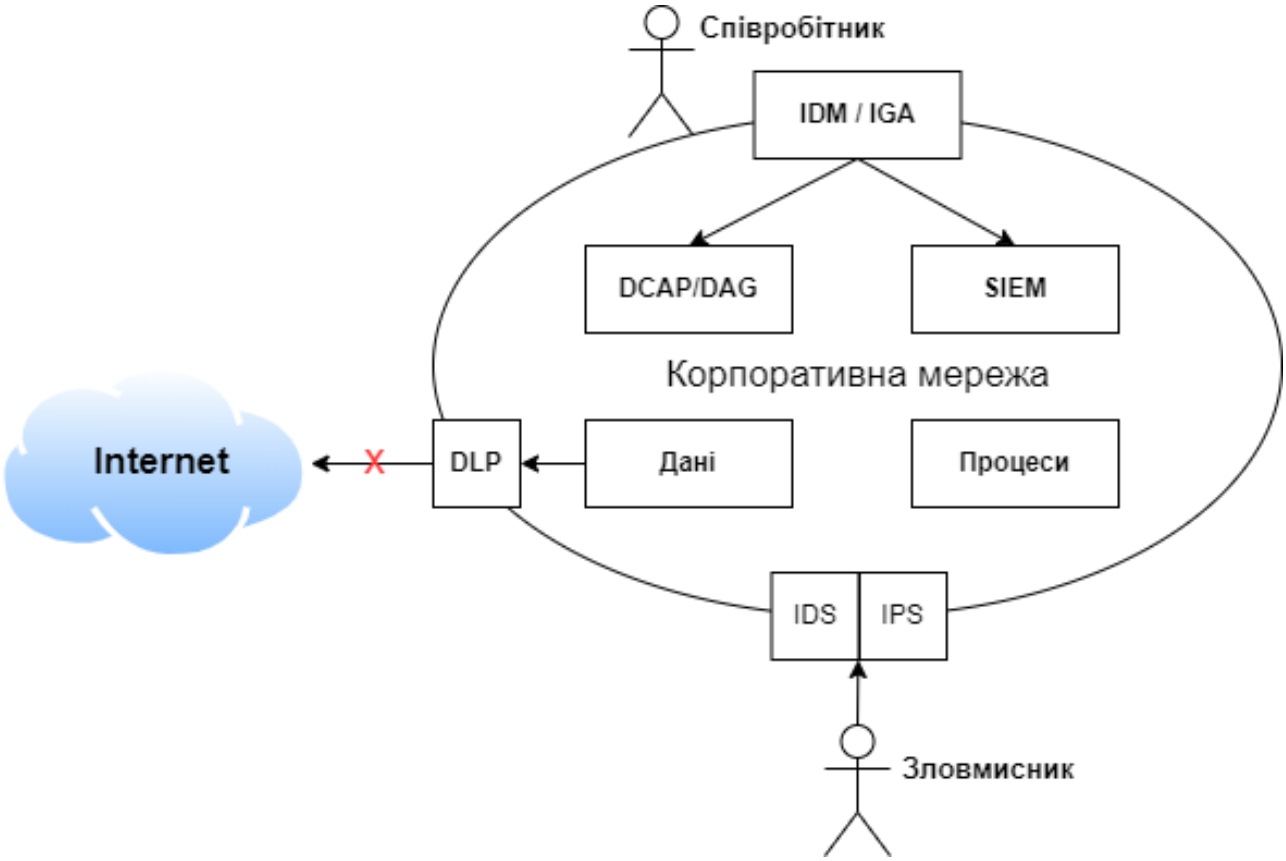
Позначення Загрози	Джерело	Ресурси	Метод Реалізації	Вплив на властивості			Ймовірність появи загрози
				К	Ц	Д	
Інсайдер в конторі	Людина	Апаратні, інформаційні, фізичні	Проникнення, перевищення повноважень	+	–	–	Низька
Хакерські атаки	Людина	Апаратні, Інформаційні	НСД до букмекерської системи	+	+	+	Низька

Модель порушника

Визначення категорії	Мотиви поруше-ння	Рівень кваліфікації та обізнаності щодо АС	Можливості використання засобів та методів подолання системи захисту	Специфікація моделі порушника за часом дії	Специфікація моделі порушника за місцем дії	Сумарний рівень загрози	Ймовірність виникнення загрози
Внутрішні порушники по відношенню до АС							
Співробітники IT-відділу	М3	К4	З3	Ч3	Д5	15	Висока
Зовнішні порушники по відношенню до АС							
Адміністратор з кібербезпеки	М3	К6	З5	Ч4	Д6	18	Висока

					08-20.МКР.006.00.000 ПЗ			
Змн.	Арк.	№ докум.	Підпис	Дата				
Розроб.		Лабусюк В.М.			Моделі загроз та порушника	Літ.	Арк.	Аркушів
Перевір.		Лужецький В.А.					3	8
Рецензент		Азарова А. О.				ВНТУ гр. 1 БС-20 м		
Н. Контр.		Лужецький В.А.						
Затверд.		Лужецький В.А.						

КОМПЛЕКС ЗАСОБІВ ДЛЯ СИСТЕМИ ЗАХИСТУ



					08-20.МКР.006.00.000 І44			
Змн.	Арк.	№ докум.	Підпис	Дата				
Розроб.		Лабусюк В.М.			Комплекс засобів для системи захисту	Літ.	Арк.	Аркушів
Перевір.		Лужецький В.А.					4	8
Рецензент		Азарова А. О.				ВНТУ гр. 1 БС-20 м		
Н. Контр.		Лужецький В.А.						
Затверд.		Лужецький В.А.						

ВИКОРИСТОВУВАНІ ІНСТРУМЕНТИ

Symantec™

McAfee
Together is power.

Betronic Software

BOOKIE
SOFTWARE

SoftGamings
BUILD YOUR OWN CASINO

					08-20.МКР.006.00.000 І45			
Змн.	Арк.	№ докум.	Підпис	Дата				
Розроб.		Лабусюк В.М.			Використовувані інструменти	Літ.	Арк.	Аркушів
Перевір.		Лужецький В.А.					5	8
Рецензент		Азарова А. О.				ВНТУ гр. 1 БС-20 м		
Н. Контр.		Лужецький В.А.						
Затверд.		Лужецький В.А.						

OKTA IDENTITY AND ACCESS MANAGEMENT

- Дозволяє аналітикам служби безпеки отримувати доступ до додаткової інформації стосовно окремих користувачів;
- дозволяє спеціалістам з безпеки автоматично скидувати паролі, міняти права доступу та завершувати підозрілі користувацькі сесії. Подібні заходи зменшують час, яке компанія залишається вразливою до кібератак.
- дозволяє користувачам синхронізувати дані облікових записів, щоб не вводити їх кожен раз при підключенні до корпоративної мережі

SYMANTEC DLP

- має функції автоматизованих робочих процесів усунення інцидентів і інтелектуальні відповіді одним клацанням миші, які дозволять швидко й ефективно реагувати на критичні втрати даних;
- забезпечує гнучкість для точного налаштування політик, щоб збалансувати безпеку та продуктивність;
- забезпечує видимість і контроль над даними в стані спокою або в хмарних програмах;
- забезпечує інформаційно-центровану аналітику. Ця функція дозволить визначити пріоритетність ризикованої поведінки та ідентифікувати зловмисних користувачів, а отже — кращий спосіб керувати інцидентами та реагувати на них.

					08-20.МКР.006.00.000 І47			
Змн.	Арк.	№ докум.	Підпис	Дата				
Розроб.		Лабусюк В.М.			Symantec dlp	Літ.	Арк.	Аркушів
Перевір.		Лужецький В.А.					7	8
Рецензент		Азарова А. О.				ВНТУ гр. 1 БС-20 м		
Н. Контр.		Лужецький В.А.						
Затверд.		Лужецький В.А.						

MCAFEE NETWORK SECURITY PLATFORM

- працює на фізичних або віртуальних пристроях у мережі
- корелює активність загроз із використанням програми, щоб стежити за потенційно небезпечною поведінкою.
- інтегрується з іншим програмним забезпеченням McAfee, а також отримує постійно оновлювані дані про загрози від McAfee.

					08-20.МКР.006.00.000 148		
Змн.	Арк.	№ докум.	Підпис	Дата			
Розроб.		Лабусюк В.М.			Mcafee network security platform	Літ.	Арк. 8 / Аркушів 8
Перевір.		Лужецький В.А.					
Рецензент		Азарова А. О.				ВНТУ гр. 1 БС-20 м	
Н. Контр.		Лужецький В.А.					
Затверд.		Лужецький В.А.					