МІНІСТЕРСТВО ОСВІТИ ТА НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

Навчально-науковий інститут захисту інформації

На рецензію Завідувач кафедри УІКБ доктор економічних наук, професор _____ С.В. Легомінова «___»_____20__ р.	До захисту Завідувач кафедри УІКБ доктор економічних наук, професор _____ С.В. Легомінова «___»_____20__ р.

ДИПЛОМНА РОБОТА
на тему:

КОМПЛЕКСНЕ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПРИ ПРОВЕДЕННІ КІБЕРСПОРТИВНИХ ЗМАГАНЬ

СТУДЕНТ: Поляков Дмитро Андрійович _____
(підпис)

КЕРІВНИК: к.в.н., доцент Якименко Юрій Михайлович
_____
(підпис)

НОРМОКОНТРОЛЕР: к.держ.упр.,доцент Мужанова Тетяна Михайлівна
_____
(підпис)

Київ – 2022

МІНІСТЕРСТВО ОСВІТИ ТА НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

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

Освітньо-кваліфікаційний рівень - магістр
Галузь знань - «12 Інформаційні технології»
Спеціальність -«125 Кібербезпека»
Спеціалізація - «Управління інформаційною безпекою»

"ЗАТВЕРДЖУЮ"
Завідувач кафедри УІКБ
д.е.н., професор_____ С.В.Легомінова
(підпис)
"___"_____ 2021 р.

ЗАВДАННЯ
на магістерську атестаційну роботу

Студенту **Полякову Дмитру Андрійовичу**

1.**Тема роботи " Комплексне забезпечення інформаційної безпеки при проведенні кіберспортивних змагань"**, затверджена наказом по університету від " 11 " жовтня 2021 р. №. 170
2. **Термін здачі** студентом закінченої дипломної роботи 25 грудня 2021р.
3. **Вихідні дані до роботи**:
- дослідити вимоги нормативно-правових документів України з підготовки та проведення кіберспортивних змагань,
- проаналізувати загрози та комплексне забезпечення інформаційної безпеки при проведенні кіберспортивних змагань,
- провести дослідження програмно-технічних засобів і способи забезпечення інформаційної безпеки при проведенні кіберспортивних змагань,
- розробити методику проведення кіберспортивних змагань і оцінки ефективності забезпечення їх інформаційної безпеки (для вибраного прикладу).

4. **Склад розрахунково-пояснювальної записки** (перелік питань до розробки).
1. Аналіз вимог до проведення кіберспортивних змагань.
2. Організація забезпечення інформаційної безпеки при проведенні кіберспортивних змагань.
3. Дослідження і розробка рекомендацій по комплексному забезпеченню інформаційної безпеки кіберспортивного змагання.

5. **Перелік обов'язкових демонстраційних креслень**:

1. Типові схеми щодо комплексного забезпечення інформаційної безпеки при проведенні кіберспортивних змагань.

2. Презентація доповіді, виконана в Microsoft PowerPoint.

6. **Термін виконання дипломної роботи**:

подання закінченої роботи керівнику 22 грудня 2021 року.

подання роботи на рецензію 23 грудня 2021 року.

7. **Дата видачі завдання** 26.10.2021 року.

Керівник _____ Якименко Юрій Михайлович
(підпис) (прізвище, ім'я, по-батькові)

Завдання прийняв для виконання _____ Поляков Дмитро Андрійович
(підпис) (прізвище, ім'я, по-батькові)

Календарний графік

№ з/п	Назва етапів магістерської атестаційної роботи	Термін виконання етапів	Відмітка про виконання
1.	Підбір науково-технічної літератури.	29.10.2021 р.	
2.	Аналіз та систематизація матеріалу. Вступ	5.11.2021 р.	
3.	Аналіз вимог нормативно-правових документів України з підготовки та проведення кіберспортивних змагань.	13.11.2021 р.	
4.	Аналіз загроз та комплексне забезпечення інформаційної безпеки при проведенні кіберспортивних змагань.	1.12.2021 р.	
5.	Дослідження методики проведення кіберспортивних змагань і оцінки ефективності забезпечення їх інформаційної безпеки.	15.12.2021 р.	
6.	Оформлення та друк пояснювальної записки	25.12.2021 р.	
7.	Отримання відгука та рецензії на роботу	29.12.2021 р.	
8.	Оформлення презентацій	4.01.2022 р.	
10.	Попередній захист на кафедрі	8.01.2022 р.	
11.	Захист в ДЕК	___01.2022 р.	

РЕФЕРАТ

Магістерська дипломна робота присвячена дослідженню процесів забезпечення інформаційної безпеки при проведенні кіберспортивних змагань. Робота складається з вступу, трьох розділів, що містять 21 рисунок, 8 таблиць та 3 формули, висновки та списку використаних джерел з 60 найменувань. Загальний обсяг роботи становить 104 сторінки, серед яких 6 аркушів займає перелік умовних позначень та список використаних джерел, 15 сторінок - додатки.

Об'єктом дослідження є процес захисту інформації та впровадження комплексної системи захисту інформації проведенні кіберспортивних змагань на прикладі українського організатора «WePlay».

Предмет дослідження – засоби та методи захисту інформації та рекомендації щодо впровадження комплексної системи захисту під час проведення кіберспортивного змагання.

Метою роботи є розробка комплексу рекомендацій щодо забезпечення інформаційної безпеки при проведенні кіберспортивних змагань.

Як результат у роботі проведено: аналіз вимог до проведення кіберспортивних змагань , в тому числі світовий досвід і досвід України при проведенні кіберспортивних змагань; досліджено організація забезпечення інформаційної безпеки при проведенні кіберспортивних змагань, зокрема організаційно-технічні (режимні) заходи захисту об'єктів змагань і методи їх проведення; розглянуті програмно-технічні засоби і способи забезпечення інформаційної безпеки при проведенні кіберспортивних змагань; розроблена методика проведення кіберспортивних змагань і оцінки ефективності забезпечення їх інформаційної безпеки; розроблені рекомендації по комплексному забезпеченню інформаційної безпеки кіберспортивного змагання на прикладі.

Сфера застосування. Розроблені підходи можуть складати підґрунтя для розроблення системи для забезпечення захисту інформації під час проведення кіберспортивних змагань, що можна буде використовувати під час проведення та організацій турнірів як державного, так і міжнародного значення.

Ключові слова: Кіберспорт, кіберспортивні змагання, турнір, інформаційна безпека, забезпечення інформаційної безпеки, системи безпеки

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ІБ	Інформаційна безпека
ІС	Інформаційна система
ПЗ	Програмне забезпечення
ОС	Операційна система
НСД	Несанкціонований доступ
DOTA 2	Комп'ютерна командна гра в жанрі арени бою
CS: GO	Комп’ютерна гра від першої особи
The International	Найбільший з Dota 2 щорічний кіберспортивний турнір
Major	Найбільший з CS:GO щорічний кіберспортивний турнір
LAN (ЛАН)	Термін, означає, що гравці знаходяться в одному приміщенні та пов'язані локальною мережею
СВВ	Система виявлення вторгнень
UESF	Ukrainian Esport Federation (Федерація кіберспорту України)

ВСТУП

Актуальність дослідження. Комп'ютери, мережі, інтернет стали невід'ємною частиною нашого повсякденного життя. Наш світ, що швидко розвивається, з кожним днем все більше стає залежним від комп'ютерних технологій та мереж. Однак ця залежність виникла не раптово. З кожним роком фінансування комп'ютерних технологій значно зростало і не дивно, що ці технології проникли практично у всі сфери діяльності людини.

З появою відеоігор кіберспорт розвивався поступово, але 2011 став поворотним, коли американська компанія з виробництва ігор «Valve» вийшла на ринок кіберспорту і провела турнір «The International» з ігрової дисципліни «DOTA 2» з призовим фондом в 1 000 000 $ [6]. До того часу жодна організація не проводила турнір з таким великим призовим фондом, у зв'язку з чим на кіберспорт, як явище та нову галузь бізнесу, звернули увагу не лише звичайні гравці у комп'ютерні ігри, а й світові ЗМІ, а також держави, які стали створювати федерації комп'ютерного спорту при міністерствах спорту і визнавати законодавчо кіберспорт на рівні зі звичайним спортом.

Таким чином, зародилося «явище» кіберспорту як галузь бізнесу, що призвело до популяризації ігрових дисциплін, та проведення турнірів із них із великим призовими фондами.

Ступінь наукової розробки. З популяризацією кіберспорту питання безпекової складової у змаганнях з комп’ютерних ігор ще недостатньо розкрито в науковій літературі. Критично важливим стає питання захисту даних гравців та забезпечення кібербезпеки під час проведення турнірів і вивчення тактики кіберзлочинців. Існує практика побудови інтегрованої системи безпеки, яка включає системи: відеоспостереження, контролю і управління доступом, охорони периметра, захисту інформації, інформаційної безпеки. Питання організації забезпечення інформаційної безпеки при проведенні кіберспортивних змагань ще не знаходять адекватного і достатнього висвітлення у науково-технічній літературі. Тому одержані в роботі результати є спробою дослідження процесів

комплексного забезпечення інформаційної безпеки при проведенні кіберспортивних змагань.

Практичне значення одержаних результатів. У практичній діяльності можуть бути використані: методики проведення кіберспортивних змагань і оцінки ефективності забезпечення їх інформаційної безпеки; рекомендації по комплексному забезпеченню інформаційної безпеки кіберспортивного змагання. Застосування матеріалів роботи надасть можливість полегшити розуміння підходів до організації забезпечення інформаційної безпеки при проведенні кіберспортивних змагань.

Розділ 1
АНАЛІЗ ВИМОГ ДО ПРОВЕДЕННЯ КІБЕРСПОРТИВНИХ ЗМАГАНЬ

Кіберспорт – це змагання із комп'ютерних ігор (eSports). Вони можуть бути командними чи індивідуальними. Його відносять до спорту, оскільки тут є всі ознаки класичного спорту, аж до боротьби з допінгом.

Види спорту тут – це самі ігри. У кожному регіоні популярна своя гра. У Східній Європі - це Counter Strike: Global Offensive, Minecraft. У Японії популярніші ігри з персонажами, стилізованими під анімаційних героїв Dota 2, League of Legends. В Америці люблять Call of Duty, Valorant.

Як і в звичайному спорті, в кіберспорті є "топові" - найбільш популярні - команди та гравці. На глобальному ринку зірки кіберспорту заробляють непогані гроші. Наприклад, гравець Dota 2 з Данії Йохан Сандстейн, за даними Esports Earnings, заробив у 2019 році $6,9 млн. В Україні провідною кіберспортивною командою є NAVI. Заробіток її гравців, за словами головного менеджера, може становити від $2000 до $40000 на місяць [1].

Турніри можуть проходити онлайн (через мережу) чи на окремому майданчику. Кіберспортивні арени дозволяють зробити якісне шоу, що приваблює більше топових команд та спонсорів. За даними аналітичного сервісу Newzoo, аудиторія кіберспортивних турнірів сьогодні сягає 500 млн. глядачів у світі. Це люди віком 18-35 років [1].

В Україні кіберспорт лише починає набирати обертів. У період 2019-2021 років кіберспортивна аудиторія в Україні зросла на 23,6%. Наразі ігри дивляться 1,36 млн осіб, зазначають у WePlay з посиланням на дані Newzoo.

Порівняно з іншими країнами, це мало. Наприклад, у Німеччині в 2020 році кіберспортивна аудиторія склала 9,84 млн осіб (згідно з даними NewZoo). Ринку є куди зростати. Обсяг кіберспортивного ринку в Україні засновник WePlay оцінює у кілька мільйонів доларів, при тому що глобальний обсяг кіберспортивного ринку, за даними Newzoo, цього року становитиме $1,1 млрд [1].

1.1. Світовий досвід і досвід України у проведенні кіберспортивних змагань

Кіберспорт кінця 90-х рр. минулого століття перетворився на мейнстрімний (основний) медіапродукт, що приваблює мільйони глядачів та став популярним у всіх країнах світу. Навколо кіберспортивних змагань, як і навколо традиційних спортивних дисциплін, з'явилася ціла індустрія, що включає продаж спорядження (мишок, гарнітур, килимків, відеокарт) та одягу, атрибутики, реклами, трансляцій та ін. У 2020 р. прибуток цього ринку перевищив $1 млрд., а у 2023 р. вона, за найскромнішими прогнозами, перевищить $1,5 млрд. [7].

Нижче будуть наведені найкрупніші турніри по основним дисциплінам. Усі цифри наведено за даними сайту Esports Earnings.

DOTA2. Турніри з Dota 2 з великими грошовими призами почалися ще до того, як гра вийшла зі статусу бета-тестуваня. Власне, перша публічна демонстрація Dota 2 і була проведена на першому турнірі The International, 17-21 серпня 2011 р. на виставці Gamescom у Кельні, Німеччина. Тим самим The International, який встановив нові стандарти призових для кіберспорту, одразу взявши планку $1,6 млн. З 2013 р. призовий фонд The International почав рости як на дріжджах, з кожним роком легко перекриваючи рекорд попереднього: $2,9 млн. (2013), $10,9 млн. (2014), $18,4 млн. (2015), $20,8 млн. (2016), $24,8 млн. (2017), $25,5 млн. (2018), $34,3 млн. (2019) [7].

The International 2020 було скасовано через COVID-19, але його призовий фонд вже встигли сформувати – $40 млн. Ці гроші пішли у The International 2021, який пройшов у Стокгольмі, Швеція [7].

Counter-Strike: Global Offensive. CS: GO – вже третя після класичного Counter-Strike 1.6 (2003) та Counter-Strike: Source (2004) ітерація оригінального Half-Life: Counter-Strike (2000). І найуспішніша, судячи з кількості турнірів. Відразу після релізу Valve критикували за обмеження розміру призового фонду великих турнірів з CS:GO у $250 тис. на тлі мільйонних призів у Dota 2, тому починаючи з MLG Major Championship: Columbus 2016 суми зросли до $1 млн. і

вище. Найбільші турніри з Counter-Strike: Global Offensive проводять World Electronic Sports Games – $1,5 млн., ELEAGUE – $1 млн. і більше, StarLadder та інші. [7].

На відміну від Dota 2, вкрай популярної у Китаї, Південній Кореї та інших країнах Східної Азії, найкращі команди, найсильніші гравці та більшість уболівальників «Контри» перебувають у Європі.

Найпопулярніші турніри кінця 2021 року. Головним івентом (подією) останнього місяця осені в кіберспорті став чемпіонат світу з League of Legends - Worlds 2021[7].

Вирішальний матч турніру показав феноменальну активність глядачів: на піку за протистоянням команд EDward Gaming і DWG KIA спостерігало понад 4 млн людей. Це рекорд не тільки League of Legends, а й усіх кіберспортивних дисциплін - з усіх турнірів більше набрав лише Free Fire World Series 2021 Singapore. На рис.1.1 показані найпопулярніші по огляду турніри з кіберспорту у кінці 2021 року.

Рис.1.1 Найпопулярніші по огляду турніри з кіберспорту у кінці 2021 року.

На другому місці опинилося кіберспортивне змагання PGL Stockholm Major за CS:GO, на яке глядачі чекали цілих два роки. За фіналом першості, де зустрілися Natus Vincere та G2 Esports, одночасно стежило понад 2,7 млн глядачів. Так багато раніше не збирав жоден турнір у цій дисципліні, попередній рекорд з піку глядачів був побитий більш ніж удвічі! У топ-5 івентів місяця також увійшли турніри з мобільних ігор. По Mobile Legends: Bang Bang пройшов турнір ONE Esports MPL Invitational 2021, в якому брали участь найкращі команди регіональних ліг. Найбільше глядачів (1,7 млн осіб) зібрало протистояння індонезійської команди RRQ Hoshi та філіппінців Blacklist International, які зустрілися у півфіналі. Завдяки фанатам гри з Індії, Індонезії та В'єтнаму вирішальний раунд фінального дня турніру на піку набрав більше мільйона людей! У вирішальному матчі зустрілися команди NAVI та Team Vitality: колектив із СНД виявився сильнішим, а на піку фінал зібрав 861 тисячу глядачів [7].

Були особливості участі у турнірах англомовних глядачів. У листопаді англомовна аудиторія в основному стежила за Worlds і PGL Major, причому пік глядачів чемпіонату світу з League of Legends виявився найвищим на 9%: змагання набрали 1,18 млн і 1,08 млн глядачів відповідно. Першу трійку замкнув ще один турнір з CS:GO - BLAST Premier Fall Finals 2021 (372 тисячі людей на піку) [8]. На рис.1.2 представлені найпопулярніші по огляду турніри з кіберспорту англомовних глядачів у кінці 2021 року.

На четвертому місці опинився стримерський івент Twitch Rivals x World Series of Warzone по однойменній "королівській битві" у серії Call of Duty. У рамках івента пройшло соло-змагання на $100 тисяч (всі гроші діставалися переможцю), в якому перемогла команда Сет Scump Абнер: ближче до кінця цей івент зібрав 203 тисячі глядачів на англомовних стримах. Першу п'ятірку замкнув ще один турнір з Call of Duty: Warzone — Last Dance in Verdansk. У ньому взяли участь топові контент-мейкери Північної Америки (DrDisRespect, TimTheTatman, Swagg, HusKerrs та інші), а на піку івент зібрав понад 184,5 тисячі англомовних глядачів [8].

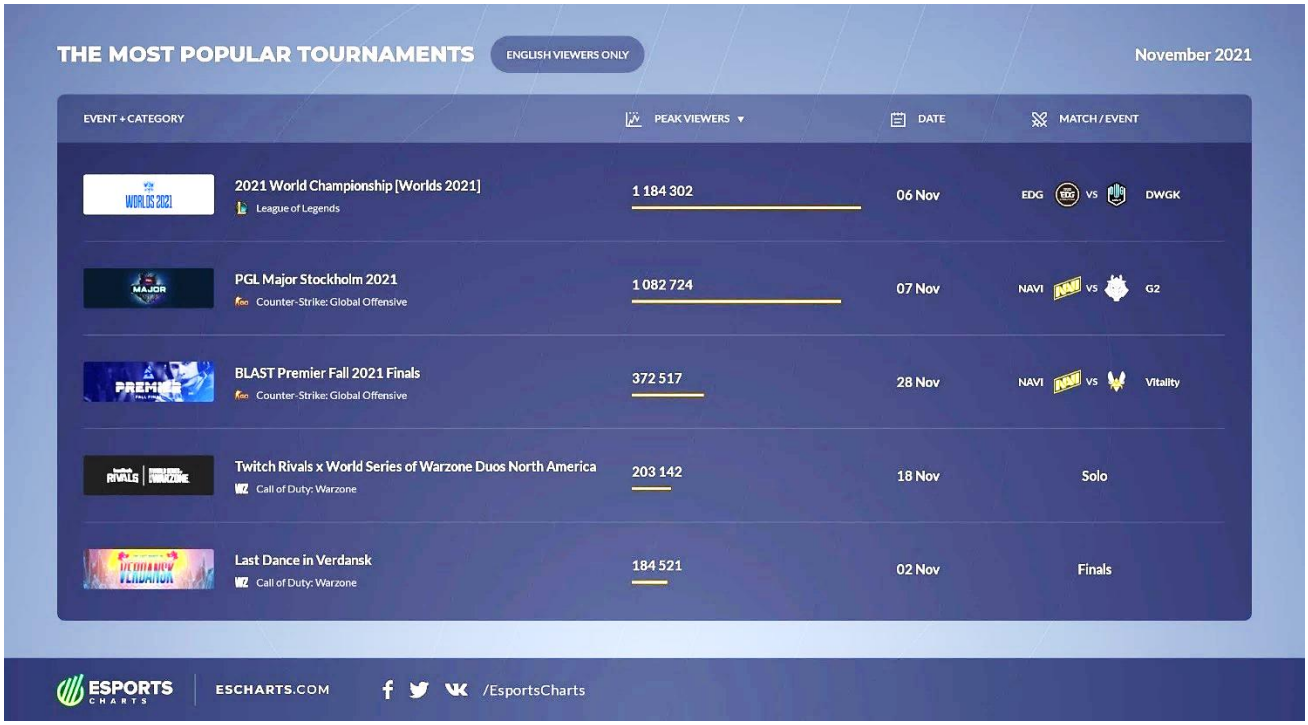

Рис 1.2 Найпопулярніші по огляду турніри з кіберспорту англомовних глядачів у кінці 2021 року

Кіберспорт в Україні. Тільки з 2010-х кіберспорт став по-справжньому розвиватися в Україні. Вихід ігор Dota 2, CS: GO (Counter Strike: Global Offensive), League of Legends викликав інтерес не лише мільйонів гравців, але й спонсорів.

Перший масштабний кіберспортивний турнір в Україні відбувся 2010 року, коли відкрилася «Київ Кіберспорт Арена». А з 2012 року регулярно проходили кіберзмагання на ігровому майданчику StarLadder. У 2018 році своя кіберарена з'явилася і в Дніпрі.

У 2010 році в Україні з'явилися і перші серйозні кіберуспіхи: українці виграли $1 млн на міжнародному турнірі з Dota 2. Розмір призового виграшу команди вразив навіть найбільших скептиків. Стало зрозуміло, що на кіберспорті можна заробляти.

У 2014 році в Україні була створена кіберспортивна організація HellRaisers. Зараз складається з двох команд у дисциплінах CS: GO та Dota 2, а також підрозділи у Fortnite. HellRaisers зібрала найкращих гравців України та країн СНД з великими виступами у кіберспорті.

Незважаючи на те, що кіберспорт був визнаний офіційним видом спорту в нашій країні лише наприкінці 2020-го, з 2017-го просуванням цієї індустрії займається Федерація кіберспорту України (UESF).

UESF є членом ключових світових кіберспортивних організацій, що гарантує вітчизняним командам участь у міжнародних змаганнях із великими призовими фондами.

Наприклад, завдяки членству у Міжнародній федерації кіберспорту (IESF) збірна команда України з Dota 2 зіграла у відбірному турнірі до IESF World Championship для команд зі Східної Європи у вересні 2020 року.

За останні чотири роки UESF провела понад 330 регіональних, національних та міжнародних турнірів, у яких взяли участь понад 40 тис. гравців [8].

Щодо «приватного» кіберспорту — нещодавно популярна українська команда NAVI увійшла до топ-3 світових кіберспортивних колективів, які заробили найбільше призових.

За перші шість місяців 2021-го українські кіберспортсмени з Natus Vincere виграли $1,22 млн. На $800 тис. більше вдалося заробити американській команді Susquehanna Soniqs, яка посіла перше місце та виграла турнір PUBG Global Invitational.S. А на другому рядку рейтингу опинилася нідерландська Team Liquid з $1,27 млн призових у своєму активі [8].

Національний спорт. Крім Наказу Міністерства молоді та спорту від сьомого вересня 2020 року, який надав кіберспорту в Україні офіційне визнання, 21 липня 2021 року Федерація кіберспорту України отримала національний статус.

Цей статус надав UESF ще більше повноважень для проведення офіційних змагань, запуску освітніх програм, формування мережі офіційних тренувальних баз збірних команд, присвоєння звань та розрядів спортсменам та інших кроків для розвитку кіберспорту в Україні.

Президент Федерації Іван Данишевський заявляв, що головна проблема кіберспорту в Україні — «менеджмент та відсутність комплексної системи розвитку та відповідної екосистеми» [8].

Надання кіберспорту національного статусу та державна підтримка Федерації мають допомогти у вирішенні цих проблем.

Щодо подальшого розвитку, Данишевський сподівається на створення нових методів та алгоритмів навчання кіберспортсменів, їхніх менеджерів, тренерів тощо.

Кіберспорт та Олімпіада. Розвиток кіберспорту в Україні має велике значення і для статусу національного спорту, адже незабаром цей вид змагань можуть визнати однією з дисциплін Олімпіади.

Нещодавно Міжнародний олімпійський комітет (МОК) офіційно визнав турнір Intel World Open — віртуальне змагання у відеоіграх Street Fighter V та Rocket League із призовим фондом у $500 тис. А перед літньою Олімпіадою 2020 року в Японії МОК провів першу в історії «Олімпійську віртуальну серію» [8].

Ця серія стала однією з перших спроб впровадження кіберспорту на Олімпіаді, і дозволила представникам різних країн визначити найкращих у кількох дисциплінах - бейсбол, велоспорт, веслування, вітрильний спорт та автоперегони, які були представлені відеоіграми eBaseball Powerful Pro Baseball 2020, Zwift, Zwift, Regatta та Gran Turismo відповідно.

Кіберспорт на Олімпіаді підтримали Міжнародна федерація футболу FIFA; Міжнародна федерація баскетболу FIBA; Міжнародна федерація тенісу ITF та Всесвітня організація теквондо WT. Однак головна проблема кіберспорту полягає в циклічності популярності відеоігор, через що представники МОК мають постійно обговорювати перелік дисциплін для змагань.

Представники Комітету також поки що відмовляються розглядати відеоігри з елементами насильства, які лежать в основі найпопулярніших турнірів IESF та інших організацій.

Вклад Parimatch Ukraine в український кіберспорт. За останні кілька років компанія Parimatch Ukraine підтримала низку ініціатив UESF, серед яких популярний соціальний онлайн-проект CyberUP: “ Вчись! Тренуйся! Перемагай!”, змагання в якому відбуваються у форматі турботи про фізичну форму, ерудицію та здоров'я молоді.

Представники Parimatch Ukraine також виступили партнерами кількох Чемпіонатів України та регіональних турнірів з Dota 2 та CS:GO, призові фонди яких сягали одного мільйона гривень.

Ці турніри проходили у 22 українських містах з огляду на Дніпро, Харків, Полтаву, Івано-Франківськ, Кривий Ріг, Львів, Житомир, Луцьк, Рівне, Чернівці, Хмельницький, Вінницю, Запоріжжя, Одесу, Херсон, Миколаїв, Київ та Суми.

Не менш важливою є й організація брендом Parimatch українських студій для трансляції міжнародних турнірів WePlay AniMajor та StarLadder RMR [8].

Разом із UESF, Parimatch Ukraine допомагає організовувати постійні онлайн-турніри для людей з інвалідністю. Нещодавно українська Федерація кіберспорту разом із Асоціацією електронного баскетболу розробила esports-кімнату у колонії для підлітків, де проходить навчання та незабаром мають розпочатися перші турніри.

Parimatch, у свою чергу, нещодавно виступив партнером масштабного фестивалю коміксів та косплей в Україні ComicCon, а також став одним із організаторів Esports Weekend у Харкові.

1.2 Вимоги нормативно-правових документів України з підготовки та проведення кіберспортивних змагань

26 січня 2021 року Міністерство молоді та спорту України затвердило загальні правила кіберспорту, розроблені Федерацією кіберспорту України за підтримки фахівців Міністерства [10]. Ця подія стала дуже важливим кроком в розвитку кіберспорту в Україні. Тепер всі охочі можуть керуватися цим нормативним документом для організації та проведення кіберспортивних змагань.

В цьому документі [2] визначено, що Правила визначають основні засади організації та проведення спортивних змагань з кіберспорту (електронного спорту). Вони розроблені з урахуванням Правил та технічних регламентів Міжнародної федерації кіберспорту і стосуються усіх дисциплін, з яких проводяться змагання з кіберспорту, та не поширюються на

організацію та проведення міжнародних змагань з кіберспорту на території України, організатором яких є Міжнародна Федерація Кіберспорту.

Змагання з кіберспорту проводяться з метою: розвитку і популяризації кіберспорту в Україні, обміну досвідом, знаннями та інформацією та ін. Змагання з кіберспорту проводяться згідно з положенням про проведення
відповідного змагання, що визначає умови його проведення,затверджується організатором та не може суперечити Правилам. Зареєстровані для участі у змаганнях особи мають дотримуватися цих Правил, як таких, що обов'язкові для виконання кожним із учасників змагань.

Спортивні змагання з кіберспорту поділяються на:

- особисті - визначають результати кожного учасника, за які надаються відповідні місця;
- командні - в яких учасником є команда, що складається з відповідного числа учасників, змагається за місце в турнірній таблиці, місця розподіляються між командами відповідно до системи проведення змагань:
- особисто-командні - підсумкові результати кожного учасника зараховуються, як кожному учаснику, так і команді в цілому.

Спортивні змагання з кіберспорту проводяться за системами: кругова система, олімпійська з вибуванням, олімпійська з вибуванням після двох поразок, швейцарська і змішана (як система, при якій на різних етапах проведення змагань застосовуються вищевказані системи, наприклад, кругова система – з розбивкою учасників на групи, потім олімпійська система).

Всі змагання з кіберспорту проводяться в спортивних дисциплінах, що мають класифікацію.

- стратегія в реальному часі;
- бойова арена;
- технічний симулятор;
- спортивний симулятор;
- змагальні головоломки;

- файтинг;
- тактико-стратегічний симулятор.

Загальні правила проведення змагань з цих спортивних дисциплін приведені в Правилах. Конкретні ігрові дисципліни, з яких проводяться змагання, визначаються відповідним «Положенням про змагання».

В пункті 4 Правил [2] визначені напрямки протиправного впливу на результати спортивних змагань з кіберспорту та які санкції можуть застосовуватись до учасників змагань, інших офіційних осіб змагань за цей вплив. Запобігання протиправному впливу на результати спортивних змагань та боротьба з ним здійснюються відповідно до законодавства України.

Протиправним впливом на результат спортивного змагання з метою досягнення заздалегідь визначеного результату або результату цього змагання та / або матчу визнається вчинення будь-якого з таких діянь особою (учасником змагань особисто, чи у змові з іншими особами), наприклад: використання будь-якого програмного забезпечення, що впливає на внутрішньоігрову механіку відеогри, в тому числі і призначене для зміни його внутрішньоігрових параметрів з метою надання переваги йому та / або створення перешкод для нормального ходу змагань опоненту (тобто чит-коди та ін.) та інші дії, що призводять до неправомірного досягнення результату або його зміни.

В Положенні про змагання, яке є основним документом, відповідно до цих Правил ,поряд з іншими, містяться такі розділи:

- організація та керівництво проведенням заходу;
- програма проведення заходу;
- безпека та підготовка місць для проведення заходу;
- інші умови, які забезпечують якісне проведення конкретного заходу.

В Правилах визначені технічні та інші параметри місця проведення змагань: онлайн на спеціалізованих веб ресурсах або, а в разі проведення ЛАН змагань, на спеціалізованих об'єктах або майданчиках, підготовлених для проведення відповідних спортивних змагань. Такими спеціалізованими об'єктами для

проведення ЛАН змагань з кіберспорту можуть бути кіберспортивні клуби, арени та подібні спортивні об'єкти та інші об'єкти, які відповідають встановленим вимогам.

В переліку дозволених та (або) заборонених дій спортсменів під час участі в змаганнях визначено:

- Забороняється апаратне чи програмне перепризначення клавіш та інших елементів пристроїв введення, якщо воно здійснюється поза стандартних інтерфейсів ігрової дисципліни. Проте, під час проведення змагань з використанням відеоігор, файлова структура яких відкрита для диспетчерів файлів, в разі якщо конфігураційний файл не може бути збережений для учасника змагань, може бути допущено використання заздалегідь підготовлених текстових конфігураційних файлів учасників змагань. Використання макросів і перевірка конфігураційних файлів на наявність заборонених команд обумовлюється Технічними правилами дисципліни та Положенням.
- Встановлення драйверів (керуючих програм), підключення власних пристроїв введення / виведення учасника змагань, завантаження конфігураційного файлу здійснюються тільки з дозволу судді та під його контролем або під контролем технічного фахівця, що обслуговує змагання Некоректна робота драйверів власних пристроїв введення / виведення учасника змагань, некоректна робота самих цих пристроїв не може бути причи Учасники змагань заздалегідь надають організаторам змагань всі файли, необхідні для налаштування своїх пристроїв та налаштування відображення ігрового процесу.
- За систематичні навмисні порушення, що впливають або можуть вплинути на хід окремих матчів і змагання в цілому, а також при навмисному порушенні, скоєному після застосування другого попередження, учасник видаляється зі змагань. За навмисну нечесну гру учасник видаляється зі змагань та може бути дискваліфікований (в разі участі команди - повним складом) відповідно до встановлених вимог.

В пункті 15 Правил вимогою до забезпечення безпеки під час проведення змагань відзначене, що створення умов для безпеки під час проведення ЛАН змагань з кіберспорту здійснюється відповідно до законодавства України.

В пункті 17 Правил вимогою до технічних характеристик спортивного інвентарю в кіберспорті є : Склад інвентарю визначається дисципліною або видом програми змагання (ігровою дисципліною, що використовується), або, в разі можливості вибору, Положенням.

Крім операційної системи на ігрові комп'ютери має встановлюватися програмне забезпечення, необхідне для проведення змагань, а також надаватися пристрої, необхідні для спілкування учасників, пристрої введення / виводу та інші технічні засоби. В разі проведення змагань з використанням ігор на мобільних платформах учасникам дозволяється використовувати особисті мобільні пристрої або використовувати пристрої, надані організаторами змагань.

Висновки до першого розділу

У розділі розглянуто: основні вимоги до проведення кіберспортивних змагань, світовий досвід та досвід України у проведенні кіберспортивних змагань та вимоги нормативно-правових документів з підготовки та проведення кіберспортивних змагань. Визначено, що змагання з кіберспорту проводяться з метою розвитку і популяризації кіберспорту в Україні; обміну досвідом, знаннями та інформацією.

Розділ 2
ОРГАНІЗАЦІЯ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПРИ ПРОВЕДЕННІ КІБЕРСПОРТИВНИХ ЗМАГАНЬ

При проведенні спортивних заходів можуть виникати кіберзагрози, які суттєво знижують кінцеві результати ігри або зовсім приведуть до її зупинки.

Комп'ютери та технічні пристрої за параметрами продуктивності під час проведення змагань повинні відповідати вимогам, рекомендованим Міжнародною Федерацією Кіберспорту, або, в разі їх відсутності, тими, що вказуються виробниками (розповсюджувачами, правовласниками) ігрових дисциплін, що використовуються в якості рекомендованих, а також бути обладнаними усіма необхідними для проведення змагань, пристроями введення / виводу.

Для того, щоб зробити кіберспорт більш безпечним від дій кіберзлочинців, необхідно більше уваги приділяти впровадженню сучасних систем захисту інформації при підготовці гри, в процесі гри і при обробці результатів гри.

Треба здійснювати постійний контроль за працездатністю різноманіття обладнання, прикладних систем, бізнес-додатків, IT-сервісів, що використовуються на змаганнях. Автоматизація цих процесів, запобігання збоїв – повинно стати першочерговим завданням проведення проактивного моніторингу. Від розповсюдження гри до обслуговування клієнта кожен аспект ігрового досвіду також повинен бути захищеним.

Необхідно запроваджувати тестування, допомогу експертів із кібербезпеки, індивідуальні рішення та багато інших заходів безпеки[25].

2.1. Структура і завдання органів, що забезпечують проведення кіберспортивних змагань

Кіберспортивні змагання – це більше не події для ентузіастів. Кіберспорт є формою змагальної діяльності, в основі якої лежить використання комп’ютерних

ігор. Це заходи з висококласною організацією, мільйонною аудиторією, що залучають навіть автомобільні бренди та венчурний капітал.

Взагалі, в Україні та в світі немає ні одного офіційного, державного органу для проведення кіберспортивних змагань. Хоча будь-яка компанія або організація, яка має бюджет для проведення кіберспортивного змагання зможе це зробити. На рис. 2.1 наведена загальна схема структури учасників проведення кіберспортивного змагання.

Рис. 2.1 Загальна схема структури учасників проведення кіберспортивного змагання

Український турнірний оператор WePlay! Esports організував у Буковелі професійний турнір серії Dota Pro Circuit, котрий у міжнародних ЗМІ назвали золотим стандартом змагань у своїй категорії . Оригінальнй підхід та оригінальні тематичні змагання дозволили організатору стати одним із найпомітніших гравців на ринку [11].

Щоб отримати право провести турнір у Буковелі у рамках елітної серії DPC (Dota Pro Circuit – серія змагань у рамках календарного року, рейтингові бали яких враховуються перед проведенням The International), команді WePlay! Треба було податись на тендер від Valve і придумати концепцію сильніше, ніж у конкурентів. За право проведення таких турнірів у всьому світі — від Лос-Анджелеса та Стокгольма до Сінгапуру та Куала-Лумпура — змагаються найкращі турнірні оператори.

WePlay! Esports зробили наголос на цілісні та продумані тематичні івенти, в яких офлайновий досвід доповнює онлайновий. Такими були турніри Forge of

Masters з CS:GO, таким самим став і Bukovel Minor. Враховуючи дати проведення (9-12 січня), все дійство вирішили огорнути духом Різдва: коментатори, сховавшись пледами, пили какао, звучали колядки, картинка ігрового поля в сезонній зимовій стилістиці змінювалася кадрами Карпат, знятими з дрону. Неймовірна атмосфера камерності та затишку буковельського мінору викликала у пам'яті легендарні турніри від команди Beyond the Summit, коли гравці жили, спілкувалися та змагалися у великому спільному будинку в Лос-Анджелесі. Сам WePlay! Свій підхід до організації турнірів називає esportainment – поєднання esports (кіберспорту) та entertainment (розважального шоу) [11]. Концепція припала глядачам до душі, і WePlay! Bukovel Minor став найуспішнішим із переглядів турніром серії Minor в історії, а портал Dot Esports назвав турнір у Буковелі золотим стандартом для всіх майбутніх турнірів з Dota 2 [11].

Також, WePlay! Esports став першим турнірним оператором, який організовує офіційну українськомовну студійну трансляцію. У цьому висловили свою зацікавленість платформи: наприклад, MEGOGO, у якому можна було стежити за боротьбою команд. Фінальні ігри турніру можна було переглянути і в кінотеатрі: зали мережі Multiplex у семи містах України організували трансляцію, причому глядачі могли переглянути трансляцію українською мовою. Глядачам у Twitch та інших платформах виявився цікавим кіберспортивний контент українською, і компанія продовжує розвивати цей напрямок.

2.2. Аналіз загроз та комплексне забезпечення інформаційної безпеки при проведенні кіберспортивних змагань.

Головною метою будь-якої системи захисту інформації є забезпечення сталого функціонування об'єкта, запобігання загрозам його безпеки, захист законних інтересів Замовника (організатора кіберспортивного змагання) від протиправних посягань, недопущення розкрадання фінансових коштів, розголошення, втрати, витоку, перекручування та знищення інформації, забезпечення нормальної діяльності всіх підрозділів об'єкта.

В даний час багато підприємств, компаній і державних установ вирішують завдання створення комплексу системи захисту інформації, яка відповідала б стандартам інформаційної безпеки. При проведенні кіберспортивних змагань також необхідно приділяти значну увагу комплексному забезпеченню інформаційної безпеки. [21].

2.2.1. Аналіз загроз забезпечення інформаційної безпеки при проведенні кіберспортивних змагань

У зв'язку з подальшим розвитком загроз, націлених на кіберспорт та кіберспортсменів критично важливим стає питання захисту **інформації** та забезпечення інформаційної безпеки під час проведення турнірів, вивчення тактики кіберзлочинців та способів організації їм протидії.

Для того щоб, досягти захисту інформації при проведенні кіберспортивних змагань, то потрібно вирішити наступні основні завдання [12]:

- віднесення інформації до категорії обмеженого доступу;
- прогнозування і своєчасне виявлення загроз безпеки інформаційних ресурсів, причин і умов, що сприяють нанесенню фінансового, матеріального і морального збитку, порушення його нормального функціонування і розвитку;
- створення умов функціонування з найменшою вірогідністю реалізації загроз безпеки інформаційних ресурсів і нанесення різних видів шкоди;
- створення механізму і умов оперативного реагування на загрози інформаційної безпеки і прояву негативних тенденцій у функціонуванні, ефективне припинення зазіхань на ресурси на основі правових, організаційних і технічних заходів і засобів забезпечення безпеки;
- створення умов для максимально можливого відшкодування та локалізації збитку, що наноситься неправомірними діями фізичних і юридичних осіб, ослаблення негативного впливу наслідків порушення інформаційної безпеки на досягнення стратегічних цілей.

При аналізі забезпечення інформаційної безпеки необхідно використовувати моделі системи управління, які засновані на міжнародних стандартах. Загальна схема концептуальної моделі системи безпеки в інформаційній сфері представлена на рис.2.2.

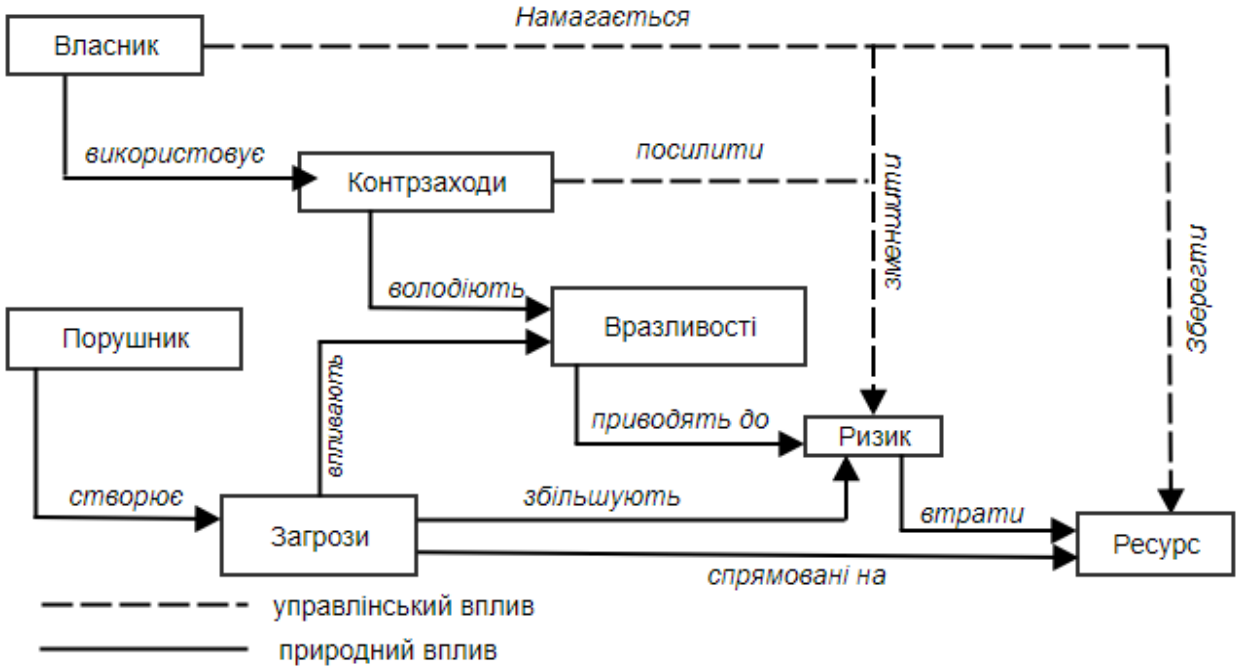

Рис. 2.2 Схема концептуальної моделі системи безпеки в інформаційній сфері [12]

Подана на рис.2.2 модель системи безпеки в інформаційній сфері відображує сукупність об’єктивних зовнішніх і внутрішніх чинників та їх вплив на стан інформаційної безпеки на об’єкті і на збереження матеріальних або інформаційних ресурсів.

Об'єктивні чинники моделі:

- загрози інформаційній безпеці, що характеризуються ймовірністю реалізації;
- вразливі місця інформаційної системи або системи контрзаходів (системи інформаційної безпеки);
- ризик – чинник, що відображує можливий збиток організації в результаті реалізації загрози інформаційної безпеки: просочування інформації та її неправомірного використання (ризик відображає вірогідні фінансові втрати – прямі або непрямі).

Для побудови збалансованої системи інформаційної безпеки потрібно спочатку провести аналіз подій інформаційної безпеки. Потім визначити оптимальний рівень ризику для організації на основі заданого критерію його оцінки. Систему інформаційної безпеки (контрзаходи) потрібно будувати так, щоб досягти заданого рівня ризику і рівня забезпечення інформаційної безпеки в цілому.

Практика використання методик проведення кіберспортивних змагань дає змогу повністю проаналізувати і документально оформити вимоги щодо гарантування рівня інформаційної безпеки під час їх проведення.

Досягти поставлених цілей можна при вирішенні таких основних завдань[13]:

- віднесення інформації до категорії обмеженого;
- прогнозування і своєчасне виявлення загроз безпеці інформаційних ресурсів причин і умов, що сприяють фінансовим, матеріальним і моральним збиткам, порушенню нормального функціонування і розвитку об'єкта;
- створення умов функціонування з найменшою вірогідністю реалізації загроз безпеці інформаційних ресурсів і зумовлення різних видів збитку;
- створення механізму і умов оперативного реагування на загрози інформаційній безпеці та прояви негативних тенденцій у функціонуванні, ефективне припинення посягань на ресурси на основі правових, організаційних і технічних заходів, засобів гарантування безпеки;
- створення умов для максимально можливого відшкодування і локалізації збитку, завданого неправомірними діями фізичних і юридичних осіб, ослаблення негативного впливу наслідків порушення інформаційної безпеки на досягнення стратегічних цілей.
- уникнути витрат на зайві заходи безпеки, що можливі у разі суб'єктивної оцінки ризиків;
- забезпечити проведення робіт в короткі терміни;
- подати обґрунтування вибору заходів протидії;
- оцінити ефективність контрзаходів, порівняти різні варіанти їх.

Загрозою інформації називають потенційно можливий вплив або вплив на автоматизовану систему з подальшим нанесенням збитку чиїмось потребам. На сьогоднішній день існує більше ста позицій і різновидів загроз інформаційній системі. Важливо проаналізувати актуальні ризики під час проведення кожного кіберспортивного заходу. [14].

Загрози інформаційної безпеки проявляються не самостійно, а через можливу взаємодію з найбільш слабкими ланками системи захисту, тобто через фактори уразливості. Загроза призводить до порушення діяльності систем на конкретному об’єкти-носії. Основні уразливості виникають унаслідок дії наступних факторів:

- недосконаліть програмного забезпечення, платформи, серверу;
- різні характеристики будови автоматизованих систем в інформаційному потоці;
- частина процесів функціонування систем є неповноцінною;
- неточність протоколів обміну інформацією та інтерфейсу;
- складні умови експлуатації і розташування інформації.

Найчастіше джерела загрози запускаються з метою отримання незаконної вигоди внаслідок заподіяння шкоди інформації. Але можливо і випадкове дію загроз через недостатній мірі захисту і масового дії загрозливого фактора. Існує поділ вразливостей за класами, вони можуть бути: об’єктивними, випадковими і суб’єктивними. Якщо усунути або як мінімум послабити вплив вразливостей, можна уникнути повноцінної загрози, спрямованої на систему зберігання інформації. [22].

Випадкові види вразливостей залежать від непередбачених обставин і особливостей оточення інформаційного середовища. Їх практично неможливо передбачити в інформаційному просторі, але важливо бути готовим до їх швидкого усунення. Усунути такі неполадки можна за допомогою проведення інженерно-технічного розгляду та відповідного удару, завданого загрозою інформаційній безпеці.

На рис. 2.3 та 2.4 зображені випадкові види вразливостей.

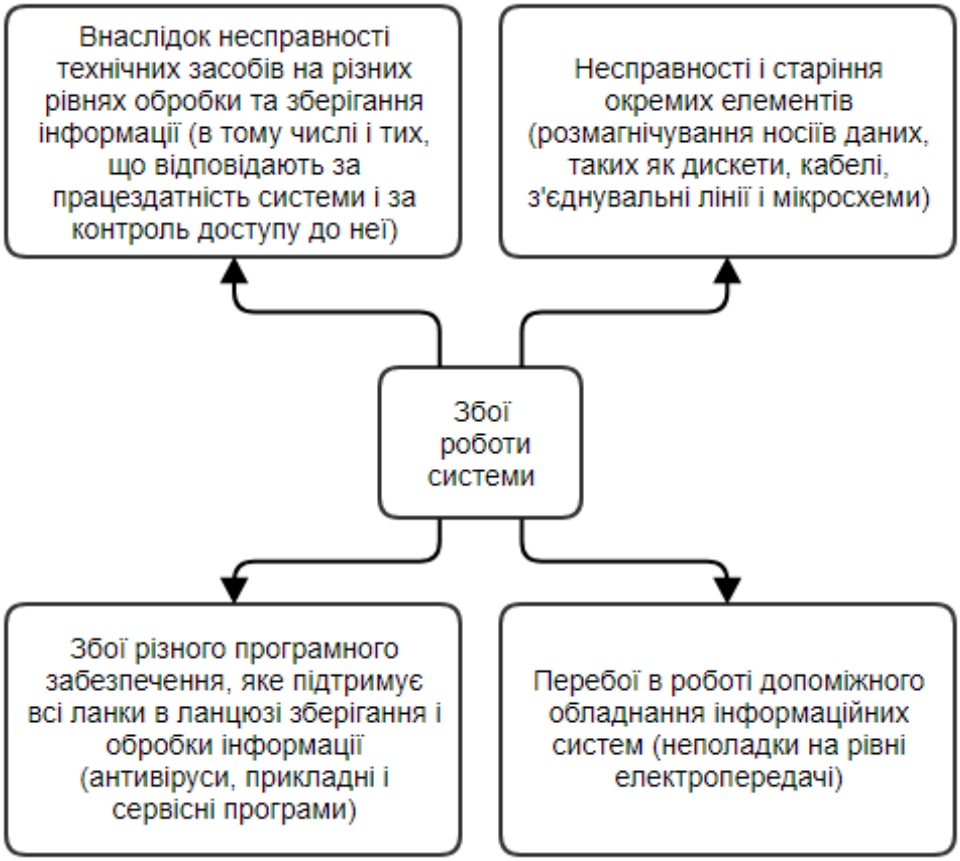

Рис. 2.3 Збої роботи системи

Фактори які послабляють інформаційну безпеку	
Пошкодження комунікацій на зразок водопостачання або електропостачання, а також вентиляції, каналізації	Несправності в роботі захисних пристроїв (паркани, перекриття в будинку, корпусу обладнання, де зберігається інформація)

Рис. 2.4 Фактори які послабляють інформаційну безпеку

Об’єктивні різновиди вразливостей безпосередньо залежать від технічної побудови обладнання на об’єкті, що вимагає захисту, і його характеристик. Повноцінне позбавлення від цих чинників неможливо, але їх часткове усунення досягається за допомогою інженерно-технічних прийомів, наступними способами:

Зміни, пов’язані з технічними засобами випромінювання:

- електромагнітні методики (побічні варіанти випромінювання і сигналів від кабельних ліній, елементів технічних засобів);
- звукові варіанти (акустичні або з додаванням вібросигналів);

- електричні (прослизання сигналів в ланцюжки електричної мережі, за наведенням на лінії і провідники, по нерівномірного розподілу струму).

Однією з найнебезпечніших на сьогоднішній день загроз інформаційної безпеки є комп'ютерні віруси. Це підтверджується багатомільйонним збитком, який несуть компанії в результаті вірусних атак[17]. В останні роки істотно збільшилася їх частота і рівень шкоди. На першому місці як і раніше залишається пошта, але, віруси здатні проникати і через програми обміну повідомленнями, такі як twitter, whatsapp та інші. Збільшилася і кількість об'єктів для можливих вірусних атак[18]. Сьогодні віруси здатні впливати і на міжмережеві екрани, комутатори, мобільні пристрої, маршрутизатори. Останнім часом особливо активні стали так звані віруси-шифрувальники. Навесні і влітку цього року мільйони користувачів постраждали від атак вірусів WannaCry, Petya, Misha. Епідемії показали, що жертвою вірусної атаки можна стати, навіть якщо не відкривати підозрілі листи. За інформацією Intel вірусом WannaCry заразилися 530 тисяч комп'ютерів, а загальний збиток компаній склав більше 1 млрд доларів[15].

Наряду з комп'ютерними вірусами, велику загрозу становлять DdoS атаки. Distributed-Denial-of-Service - «розподілена відмова від обслуговування» - це потік помилкових запитів від сотень тисяч географічно розподілених хостів, які блокують обраний ресурс одним з двох шляхів. Перший шлях – це пряма атака на канал зв'язку, який повністю блокується величезною кількістю непотрібних даних. Другий – атака безпосередньо на сервер ресурсу. Недоступність або погіршення якості роботи публічних веб-сервісів в результаті атак може тривати досить тривалий час, від декількох годин до декількох днів. Зазвичай подібні атаки використовуються в ході конкурентної боротьби. Коли гравець або команда-учасник кіберспортивного змагання є нездоланною перешкодою під час змагання для іншої команди то можуть бути зроблені DdoS атаки на адреси гравців іншої команди. Іноді менеджери організацій змагань намагаються заощадити на покупці ліцензійного ПЗ. Але слід знати, що неліцензійні програми не дають захисту від шахраїв, зацікавлених в крадіжці інформації за допомогою вірусів. Володар неліцензійного ПЗ не отримує технічної підтримки, своєчасних оновлень, що

надаються компаніями-розробниками. Разом з ним він купує і віруси, здатні завдати шкоди системі комп'ютерної безпеки. [23].

Об'єктивні уразливості:

- технологічні виходи з програм, що об'єднується терміном «програмні закладки»;
- закладки апаратури – фактори, які впроваджуються безпосередньо в телефонні лінії, в електричні мережі або просто в приміщення.

Суб'єктивні уразливості в більшості випадків являють собою результат неправильних дій співробітників при проведенні кіберспортивних змагань на рівні розробки систем зберігання і захисту інформації. Тому усунення таких факторів можливо за допомогою розробки спеціальних методик з використанням апаратури і ПЗ. На рис. 2.5 представлені помилки співробітників, що порушують інформаційну безпеку при проведенні кіберспортивних змагань (див. рис. 2.5а), а також - порушення роботи систем в інформаційному просторі змагань (див. рис. 2.5б).

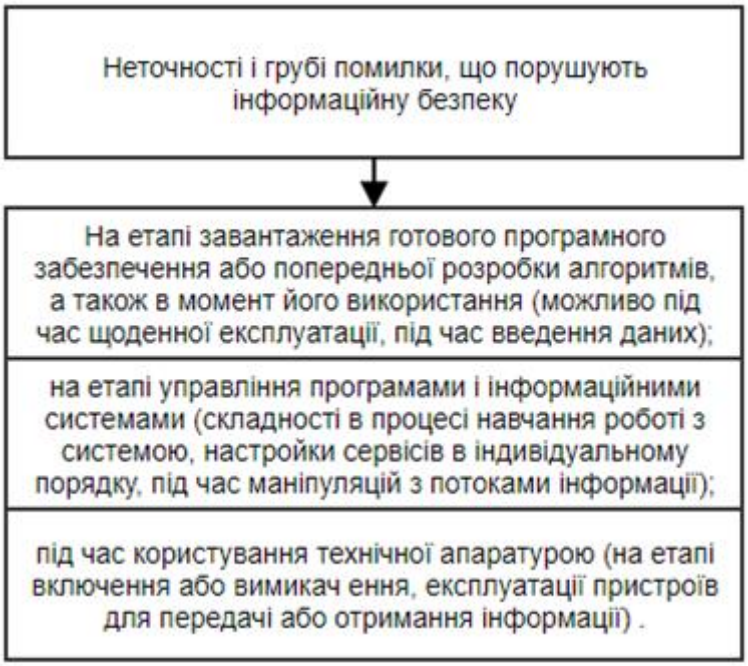

Рис. 2.5а Результати неправильних дій співробітників при проведенні кіберспортивних змагань

Рис. 2.5б Результати неправильних дій співробітників при проведенні кіберспортивних змагань

Кожна вразливість повинна бути врахована і оцінена фахівцями. Тому важливо визначити критерії оцінки небезпеки виникнення загрози і ймовірності поломки або обходу захисту інформації[16]. Показники підраховуються за допомогою застосування ранжування. Серед всіх критеріїв виділяють три основних:

Доступність – це показник, який враховує, наскільки зручно джерела загроз використовувати до певного виду уразливості, щоб порушити інформаційну безпеку. У показник повинно входити технічні дані носія інформації (на кшталт габаритів апаратури, її складності і вартості, а також можливості використання для злому інформаційних систем неспеціалізованих систем і пристроїв).

Фатальність – характеристика, яка оцінює глибину впливу уразливості на можливості програмістів впоратися з наслідками створеної загрози для інформаційних систем. Якщо оцінювати тільки об’єктивні уразливості, то

визначається їх інформативність – здатність передати в інше місце корисний сигнал з конфіденційними даними без його деформації.

Кількість – характеристика підрахунку деталей системи зберігання та реалізації інформації, яким притаманний будь-який вид уразливості в системі. Результати всіх аналізів зводяться в одну таблицю, ступінь впливу розбивається по класах для зручності підрахунку коефіцієнта уразливості системи. [24].

Якщо описувати класифікацію загроз, які обходять захист інформаційної безпеки, то можна виділити декілька з них (рис. 2.6). Поняття класів обов'язково, адже воно спрощує і систематизує всі фактори без винятку.

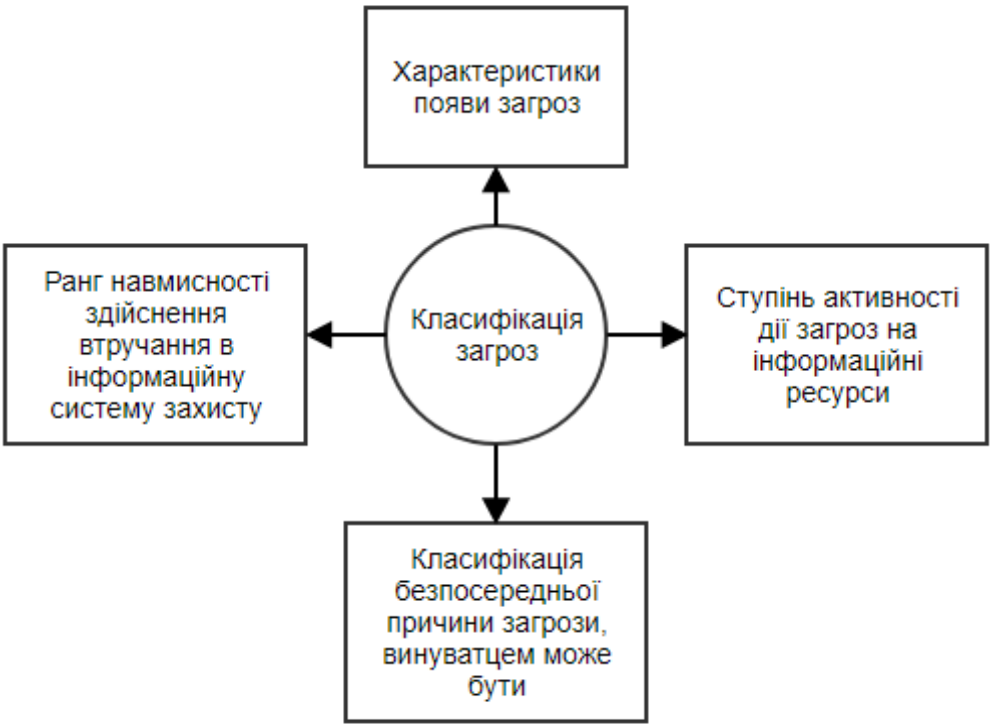

Рис. 2.6 Класифікація загроз, які обходять захист інформаційної безпеки

Ранг навмисності здійснення втручання в інформаційну систему захисту відображає рівень:

- загрози, яку викликає недбалість персоналу в інформаційному вимірі;
- загрози, ініціатором якої є шахраї, і роблять вони це з метою особистої вигоди.

Характеристики появи загроз, це:

- загрози інформаційній безпеці, які провокується руками людини і є штучними;
- природні загрозливі фактори, непідконтрольні інформаційними системами захисту і викликаються стихійними лихами.

Класифікація безпосередньої причини загрози, в яких винуватцем може бути:

- людина, яка розголошує конфіденційну інформацію, орудуючи за допомогою підкупу співробітників компанії;
- природний фактор, що приходить у вигляді катастрофи або локального лиха;
- програмне забезпечення із застосуванням спеціалізованих апаратів або впровадження шкідливого коду в технічні засоби, що порушує функціонування системи;
- випадкове видалення даних, санкціоновані програмно-апаратні фонди, відмова в роботі операційної системи.

Ступінь активності дії загроз на інформаційні ресурси визначається:

- в момент оброблення даних в інформаційному просторі (дія розсилок від вірусних утиліт);
- в момент отримання нової інформації;
- як незалежно від активності роботи системи зберігання інформації (в разі розкриття шифрів або криптографічного захисту інформаційних даних) [25].

Ще одна класифікація джерел загроз інформаційній безпеці, заснована на інших параметрах і також враховується під час аналізу несправності системи або її злому. До уваги береться наступне:

Стан джерела загрози:

- в самій системі, що призводить до помилок в роботі і збоїв при реалізації ресурсів АС;
- в межах видимості АС, наприклад, застосування підслуховуючої апаратури, викрадення інформації в роздрукованому вигляді або крадіжка записів з носіїв даних;
- шахрайство поза зоною дії АС.

Можливість доступу співробітників до системи програм або ресурсів може реалізуватися на кроці доступу до системи (несанкціонованого), а шкода (загроза інформаційним даним) може бути здійснена після згоди їх доступу до ресурсів системи.

Під час доступу до основних ресурсів системи виділяють наступні способи загрози:

- застосування нестандартного каналу шляху до ресурсів, що включає в себе несанкціоноване використання можливостей операційної системи;
- використання стандартного каналу для відкриття доступу до ресурсів, наприклад, незаконне отримання паролів і інших параметрів з подальшим маскуванням під зареєстрованого в системі користувача [27].

Розміщення інформації, яка зберігається в системі: вид загроз доступу до інформації, яка розташовується на зовнішніх пристроях пам'яті, начебто несанкціонованого копіювання інформації з жорсткого диска, отримання доступу до інформації, яка показується терміналу, наприклад, запис з відеокамер терміналів; незаконне проникнення в канали зв'язку і підключення до них з метою отримання конфіденційної інформації або для підміни реально існуючих фактів під виглядом зареєстрованого співробітника.

При цьому не варто забувати про такі загрози, як випадкові і навмисні. В системах дані регулярно піддаються різним реакціям на всіх стадіях циклу обробки і зберігання інформації, а також під час функціонування системи. Як джерело випадкових реакцій виступають такі фактори, як:

- збої в роботі апаратури;
- періодичні шуми і фони в каналах зв'язку через вплив зовнішніх факторів (враховується пропускна здатність каналу, смуга пропускання);
- неточності в програмному забезпеченні;
- помилки в роботі співробітників або інших службовців в системі;
- специфіку функціонування середовищ и Ethernet;
- форс-мажори під час стихійних лих або частих відключень електропостачання.

Похибки і в функціонуванні програмного забезпечення зустрічаються найчастіше, а в результаті з’являється загроза. Всі програми розробляються людьми, тому не можна усунути людський фактор і помилки. Робочі станції, маршрутизатори, сервери побудовані на роботі людей. Чим вище складність програми, тим більше можливість розкриття в ній помилок і виявлення вразливостей, які призводять до погроз інформаційної безпеки. Частина цих помилок не призводить до небажаних результатів, наприклад, до відключення роботи сервера, несанкціонованого використання ресурсів, непрацездатності системи. Такі платформи, на яких була викрадена інформація, можуть стати майданчиком для подальших атак і становлять загрозу інформаційній безпеці. Щоб забезпечити безпеку інформації в такому випадку, потрібно скористатися оновленнями. Встановити їх можна за допомогою пакетів, що випускаються розробниками[28].

Встановлення несанкціонованих або неліцензійних програм може тільки погіршити ситуацію. Також можливі проблеми не тільки на рівні ПЗ, але і в цілому пов’язані з захистом безпеки інформації в сеті. Навмисна загроза безпеці інформації асоціюється з неправомірними діями злочинця. В якості інформаційного злочинця може виступати співробітник компанії, відвідувач інформаційного ресурсу, конкуренти або наймані особи. Причин для вчинення злочину може бути кілька: грошові мотиви, невдоволення роботою системи і її безпекою, бажання самоствердитися. Є можливість змоделювати дії зловмисника заздалегідь, особливо якщо знати його мета і мотиви вчинків: людина володіє інформацією про функціонування системи, її даних і параметрах.

Майстерність і знання шахрая дозволяють йому діяти на рівні розробника. Зловмисник здатний вибрати найвразливіше місце в системі і вільно проникнути до інформації, стати загрозою для неї. Заінтересованою особою може бути будь-яка людина, як свій співробітник, так і сторонній зловмисник[29].

Несанкціонований доступ – один з методів комп’ютерних правопорушень. Тобто особистість, яка здійснює несанкціонований доступ до інформації людини, порушує правила, які зафіксовані політикою безпеки. При такому доступі відкрито

користуються похибками в системі захисту і проникають до ядра інформації. Некоректні настройки і установки методів захисту також збільшують можливість несанкціонованого доступу. Доступ і загроза інформаційній безпеці відбуваються як локальними методами, так і спеціальними апаратними установками. За допомогою доступу шахрай може не тільки проникнути до інформації і скопіювати її, а й внести зміни, видалити дані. Робиться це за допомогою:

- перехоплення непрямих електромагнітних вилікуваних від апаратури або її елементів, від каналів зв'язку, електроживлення або сіток заземлення;
- технологічних панелей регулювання;
- локальних ліній доступу до даних (термінали адміністраторів системи або співробітників);
- міжмережевих екранів;
- методів виявлення помилок.

Зі всіх методів доступу і загроз інформації можна умовно виділити основні (рис. 2.7):

Рис. 2.7 Різновиди методів доступу і загроз інформації

Перехоплення паролів – поширена методика доступу, з якої стикалося більшість співробітників і тих, хто займається забезпеченням інформаційної безпеки. Це шахрайство можливо за участю спеціальних програм, які імітують на екрані монітора віконце для введення імені і пароля. Введені дані потрапляють до

рук зловмисника, і далі на дисплеї з'являється повідомлення про неправильну роботу системи. Потім можливе повторне спливання віконця авторизації, після чого дані знову потрапляють в руки перехоплювача інформації, і так забезпечується повноцінний доступ до системи, можливе внесення власних змін. Є й інші методики перехоплення пароля, тому варто користуватися шифруванням паролів під час передачі, а зробити це можна за допомогою спеціальних програм або RSA[31].

Спосіб загрози інформації «Маскарад» багато в чому є продовженням попередньої методики. Суть полягає в діях в інформаційній системі від імені іншої людини в мережі компанії. Існують такі можливості реалізації планів зловмисників в системі:

- передача помилкових даних в системі від імені іншої людини;
- авторизація в інформаційну систему під даними іншого співробітника і подальше вчинення дій (з попередніми перехопленням пароля).

Особливо небезпечний «Маскарад» в банківських системах, де маніпуляції з платежами призводять компанію в збиток, а вина і відповідальність накладаються на іншу людину. Крім того, страждають клієнти банка[35].

Незаконне використання привілеїв – назва різновиду розкрадання інформації і підриву безпеки інформаційної системи говорить сама за себе. Саме адміністратори наділені максимальним списком дій, ці люди і стають жертвами зловмисників. При використанні цієї тактики відбувається продовження «маскараду», коли співробітник або третя особа отримує доступ до системи від імені адміністратора і чинить незаконні маніпуляції в обхід системи захисту інформації. Але є нюанс: в цьому варіанті злочину потрібно перехопити список привілеїв з системи попередньо. Це може статися і з вини самого адміністратора. Для цього потрібно знайти похибку в системі захисту і проникнути в неї несанкціоніовано. Загроза інформаційної безпеки може здійснюватися на навмисному рівні під час транспортування даних. Це актуально для систем телекомунікацій і інформаційних сіток. Умисне порушення не варто плутати з санкціонованими модифікаціями інформації. Останній варіант виконується

особами, які мають повноваження і обґрунтовані завдання, що вимагають внесення змін. Порушення призводять до розриву системи або повного видалення даних. Існує також загроза інформаційній безпеці, яка порушує конфіденційність даних і їх секретність. Всі відомості отримує третя особа, тобто стороння людина без права доступу. Порушення конфіденційності інформації має місце завжди при отриманні несанкціонованого доступу до системи. Загроза захисту безпеки інформації може порушити працездатність компанії або окремого співробітника. Це ситуації, в яких блокується доступ до інформації або ресурсів її отримання. Один співробітник створює навмисно або випадково блокує ситуацію, а другий в цей час натикається на блокування і отримує відмову в обслуговуванні. Наприклад, збій можливий під час комутації каналів або пакетів, а також загроза виникає в момент передачі інформації по супутникових систем. Їх відносять до первинних або безпосередніх варіантів, оскільки створення веде до прямого впливу на дані, що знаходяться під захистом.

Комп'ютерні віруси, що порушують інформаційну безпеку. Вони впливають на інформаційну систему одного комп'ютера або мережі ПК після попадання в програму і самостійного розмноження. Віруси здатні зупинити дію системи, але в основному вони діють локально[38].

«Черв'яки» - модифікація вірусних програм, що призводить інформаційну систему в стан блокування і перевантаження. ПЗ активується і розмножується самостійно, під час кожного завантаження комп'ютера. Відбувається перевантаження каналів пам'яті і зв'язку.

«Троянські коні» - програми, які впроваджуються на комп'ютер під виглядом корисного забезпечення. Але насправді вони копіюють персональні файли, передають їх зловмисникові, руйнують корисну інформацію. Навість захисна система комп'ютера являє собою ряд загроз захисту безпеки. Тому програмістам необхідно враховувати загрозу огляду параметрів системи захисту.

Іноді загрозою можуть стати і нешкідливі *мережеві адаптери*. Важливо визначити конфігурацію системи захисту, її характеристики і передбачити можливі шляхи обходу. Після ретельного аналізу можна зрозуміти, які системи вимагають

найбільшою мірою захищеності (акцент на вразливості). Розкриття параметрів системи захисту відносять до непрямих загроз безпеки. Справа в тому, що розкриття параметрів не дасть реалізувати шахраєві свій план і скопіювати інформацію, внести в неї зміни. Зловмисник тільки зрозуміє, за яким принципом потрібно діяти і як реалізувати пряму загрозу захисту безпеки інформації[34].

На великих кіберспортивних змаганнях методами, що захищають інформаційну безпеку, повинна займатися спеціальна служба безпеки від компанії або керівництва, які відповідають за проведення змагання . Їх співробітники повинні шукати способи впливу на інформацію і усувати всілякі прориви зловмисників. За локальним актам може розроблятися політика безпеки, яку важливо строго дотримуватися[44].

Варто звернути увагу і на виключення впливу людського фактору, а також підтримувати в справності всі технічні засоби, пов’язані з безпекою інформації. Збитки, які наносяться загрозами і ступені прояви шкоди можуть бути різними (рис. 2.8).

Збитки	
Моральний і матеріальний збиток, нанесений фізичним особам, чия інформація була викрадена	Фінансовий збиток, нанесений шахраєм в зв'язку з витратами на відновлення систем інформації
Матеріальні витрати, пов'язані з неможливістю виконання роботи через зміни в системі захисту інформації	Моральний збиток, пов'язаний з діловою репутацією компанії або спричинив порушення взаємин на світовому рівні
Можливість заподіяння шкоди є у особи, яка вчинила правопорушення (отримало несанкціонований доступ до інформації, або стався злам систем захисту)	Також збиток може бути завдано незалежно від суб'єкта, який володіє інформацією, а внаслідок зовнішніх факторів і впливів (техногенних катастроф, стихійних лих).

Рис. 2.8 Збитки, які наносяться загрозами і ступені прояви шкоди

У першому випадку вина лягає на суб’єкта, який заподіяв шкоду, а також визначається склад злочину і виноситься покарання за допомогою судового розгляду. Можливо вчинення діяння: зі злочинним умислом (прямим або

непрямим); по необережності (без умисного заподіяння шкоди). Відповідальність за правопорушення по відношенню до інформаційних систем вибирається згідно з чинним законодавством країни, зокрема, за кримінальним кодексом у першому випадку. Якщо злочин скоєно з необережності, а збиток нанесений в малих розмірах, то ситуацію розглядає громадянське, адміністративне або арбітражне право. Збитком інформаційного простору вважаються невигідні для власника (в даному випадку інформації) наслідки, пов'язані з втратою матеріального майна (викрадення комп'ютерних пристроїв). Наслідки проявляються в результаті правопорушення. Висловити збиток інформаційних систем можна в вигляді зменшення прибутку або її недоотримання, що розцінюється як упущена вигода. Головне, вчасно звернутися до суду і з'ясувати склад злочину[38].

Збиток потрібно класифікувати згідно з правовими актам і довести його в судовому процесі, а ще важливо виявити розмір діяння особистостей, розмір їх покарання на основі законодавства. Такими злочинами і безпекою найчастіше займається кіберполіція або служба безпеки країни в залежності від обсягу і значимості втручання в інформацію.

Етап захисту інформації сьогодні вважається актуальним і потрібно будь-якому спортивному змаганню. Захищати треба не тільки ПК, але і всі технічні пристрої, що контактують з інформацією. Всі дані можуть стати зброєю в руках зловмисників, тому конфіденційність сучасних IT-систем повинна знаходитися на вищому рівні. Ще не придуманий універсальний спосіб, який підходить кожному і дає стовідсотковий захист інформаційній безпеці підприємства. Важливо зупинити проникнення зловмисників на ранньому рівні і не допустити нанесення шкоди під час підготовки і проведення кіберспортивних змагань.

Як показує практика [4], проведення спортивних змагань основними видами загроз є: блокування профілів за допомогою шифрувальників-здирників з вимогою викупу, крадіжка та перепродаж ігрових облікових записів на кіберзлочиних форумах. В результаті фішингових дій можуть бути майже захоплені сервери, викрадені облікові записи елітних гравців, а сама гра — скомпрометована або використана для нелегальних угод. Ігрові турніри та власники ігрових сервісів

залишаються також мішенню для DdoS-атак, створюючи проблеми організаторам в інфраструктурі кібертурніру. DdoS-атаки можуть викликати серйозні проблеми із запізненням передачі даних, що є критичною проблемою у змаганнях, де за мілісекунди можна визначити виграші та програші. DdoS-атака може завдати репутаційної шкоди проведенню самого турніру. Вона також може бути використана для здирства, коли злочинці вимагають грошей з турнірів, щоб зупинити їх проведення[42].

На більшості великих кіберспортивних заходів також має місце така загроза, як крадіжка особистих даних гравців, тренерів, суддів. Якщо зловмисник використовує мережеві вразливості комп'ютерної системи для досягнення своїх цілей і коли на заході є тільки одна точка доступу до комп'ютерної мережі, то це ставить під удар проведення кіберспортивного змагання в цілому та його безпеку. Тому важливим аспектом цих замагань є захист від проникнення в систему і забезпечення цілосності інформації, як при підготовці до змагання, так і під час його проведення.

Для комплексного забезпечення інформаційної безпеки при проведенні кіберспортивних змагань пропонується створювати інтегровану систему безпеки, яка включає системи: відеоспостереження, контролю і управління доступом, охорони периметра, захисту інформації, інформаційної безпеки. Склад кожної конкретної системи може змінюватися – доповнюватися новими підсистемами. Це залежить від конкретних завдань, визначених на етапі проектування системи [5].

2.2.2. Організаційно-технічні (режимні) заходи захисту об'єктів змагань і методи їх проведення

Для опису технології захисту інформації конкретної інформаційної системи, в тому числі і при організації проведення кіберспортивних змагань, зазвичай розробляється Політика інформаційної безпеки у вигляді документів, яких прописані організаційні і технічні заходи забезпечення безпеки інформаційних ресурсів [36].

Політика безпеки (під час проведення кіберспортивних змагань) (англ. Organizational security policy) – сукупність документованих правил, процедур, практичних прийомів або керівних принципів у галузі безпеки інформації, якими керується організатор турніру у своїй діяльності.

Для побудови Політики інформаційної безпеки рекомендується окремо розглядати такі напрями захисту інформаційної системи:

- захист об'єктів інформаційної системи;
- захист процесів, процедур і програм обробки інформації;
- захист каналів зв'язку (акустичні, інфрачервоні, провідні оптичні, радіоканали та ін.);
- придушення побічних електромагнітних випромінювань і наведень;
- управління системою захисту та ін.

При цьому по кожному з перерахованих вище напрямків Політика інформаційної безпеки повинна описувати наступні етапи створення засобів захисту інформації:

- визначення інформаційних і технічних ресурсів, що підлягають захисту;
- виявлення повної безлічі потенційно можливих загроз і каналів витоку інформації;
- проведення оцінки вразливості і ризиків інформації за наявної безлічі загроз і каналів витоку;
- визначення вимог до системи захисту;
- здійснення вибору засобів захисту інформації та їх характеристик;
- впровадження та організація використання обраних заходів, способів та засобів захисту;
- здійснення контролю цілісності і керування системою захисту.

Політика інформаційної безпеки оформляється у вигляді задокументованих вимог на інформаційну систему. Документи зазвичай поділяють за рівнями опису (деталізації) процесу захисту.

Документи верхнього рівня Політики інформаційної безпеки відображають позицію організації до діяльності в галузі захисту інформації, її прагнення відповідати державним, міжнародним вимогам і стандартам у цій галузі. Подібні документи можуть називатися «Концепція ІБ», «Регламент управління ІБ», «Політика ІБ», «Технічний стандарт ІБ» і т.п.

Область поширення документів верхнього рівня зазвичай не обмежується, проте дані документи можуть випускатися і в двох редакціях – для зовнішнього і внутрішнього використання[46].

На верхньому рівні Політики інформаційної безпеки при проведені кіберспортивних змагань повинні бути оформлені наступні документи: «Концепція забезпечення ІБ», «Правила допустимого використання ресурсів інформаційної системи», «План забезпечення безперервності бізнесу » [39].

До середнього рівня відносять документи, що стосуються окремих аспектів інформаційної безпеки. Це вимоги на створення та експлуатацію засобів захисту інформації, організацію інформаційних та бізнес-процесів організатора турніру по конкретному напрямку захисту інформації. Наприклад: Безпека даних, Безпека комунікацій, Використання засобів криптографічного захисту, Контентна фільтрація і т.п. Подібні документи зазвичай видаються у вигляді внутрішніх технічних і організаційних політик (стандартів). Всі документи середнього рівня політики інформаційної безпеки конфіденційні.

У політику інформаційної безпеки нижнього рівня входять регламенти робіт, керівництва по адмініструванню, інструкції з експлуатації окремих сервісів інформаційної безпеки.

В організаційних заходах забезпечення безпеки інформаційних ресурсів при проведенні кіберспортивних змагань також значну роль відіграє саме організаційний захист інформації, під чим розуміється регламентація діяльності і взаємин виконавців на нормативно-правовій основі, що виключає або суттєво ускладнює неправомірне заволодіння конфіденційною інформацією і прояв внутрішніх і зовнішніх загроз.

Організаційний захист інформації на змаганнях забезпечує:

- організація охорони, режиму, роботи з кадрами, з документами;
- організація використання технічних засобів безпеки;
- інформаційно-аналітична діяльність з виявлення внутрішніх і зовнішніх загроз на процеси підготовки та проведення кіберспортивних змагань.

До основних організаційних заходів при змаганнях належать:

- організація виключення можливості таємного проникнення на територію і в приміщення сторонніх осіб;
- організація роботи зі співробітниками передбачає підбір і розстановку персоналу, включаючи ознайомлення зі співробітниками, їх вивчення, навчання правилам роботи з конфіденційною інформацією, ознайомлення з заходами відповідальності за порушення правил захисту інформації та ін.;
- організація роботи з документами та документованою інформацією, включаючи організацію розробки і використання документів та носіїв конфіденційної інформації, їх облік, виконання, повернення, зберігання і знищення;
- організація використання технічних засобів збору, обробки, накопичення і зберігання конфіденційної інформації;
- організація роботи з аналізу внутрішніх і зовнішніх загроз конфіденційної інформації та вироблення заходів щодо забезпечення її захисту;
- організація роботи з проведення систематичного контролю за роботою персоналу з конфіденційною інформацією, порядком обліку, зберігання та знищення документів і технічних носіїв.

У кожному конкретному випадку організаційні заходи носять специфічну для даної організації форму і зміст, спрямовані на забезпечення безпеки інформації в конкретних умовах проведення кіберспортивних змагань [51].

2.2.3. Програмно-технічні засоби і способи забезпечення інформаційної безпеки при проведенні кіберспортивних змагань

До складу заходів щодо забезпечення безпеки при проведенні кіберспортивних змагань входять:

- ідентифікація та аутентифікація суб’єктів доступу та об’єктів доступу;
- керування доступом суб'єктів доступу до об'єктів доступу;
- обмеження програмного середовища;
- захист машинних носіїв інформації, на яких зберігаються та (або) обробляються персональні дані;
- реєстрація подій безпеки;
- антивірусний захист;
- виявлення (запобігання) вторгнень;
- контроль (аналіз) безпеки персональних даних;
- забезпечення цілісності інформаційної системи та персональних даних;
- забезпечення доступності персональних даних;
- захист середовища віртуалізації;
- захист технічних засобів;
- захист інформаційної системи, її засобів, систем зв'язку та передачі даних;
- виявлення інцидентів (однієї події або групи подій), які можуть призвести до збоїв або порушення функціонування інформаційної системи та (або) до виникнення загроз безпеки персональних даних та реагування на них;
- управління конфігурацією інформаційної системи та системи захисту персональних даних.

В якості заходів щодо забезпечення безпеки при проведенні кіберспортивних змагань використовують програмно-технічні засоби, серед яких: мережева система виявлення вторгнень (з використанням спеціальних протоколів), брандмауер (зі сецифікою фільтрації даних), віртуальна приватна мережа (створена в основному на базі загальнодоступної мережі Інтернет з технологією VPN)

Мережева система виявлення вторгнень – система виявлення вторгнень (СВВ), яка відстежує такі види шкідливої діяльності, як DoS атаки, сканування портів або навіть спроби проникнення в мережу (див.рис. 2.9)

Мережева СВВ переглядає всі вхідні пакети на наявність в них підозрілих ознак. Якщо, наприклад, виявлена велика кількість запитів на TCP з'єднання з широким діапазоном різних портів, то, скоріш за все, проводиться сканування портів під час кіберспортивного змагання. Також подібна система найчастіше відстежує вхідні запити. Прикладом мережевої СВВ є Snort. [58]

Мережева СВВ не обмежується відстеженням тільки тим, що входить до мережевого трафіку. Часто важливу інформацію про те, що відбувається вторгнення можна отримати також з вихідного або локального трафіку. Дія деяких атак може розгортатися всередині спостережуваної мережі або сегмента мережі, і ніяк не відбиватися на вхідному трафіку.

Рис. 2.9 Узагальнена класифікація систем виявлення вторгнень

Найчастіше, мережева СВВ добре взаємодіє з іншими захисними системами. СВВ можуть на основі результатів своєї роботи оновлювати чорні списки міжмережевих екранів, заносячи туди IP адреси машин, запідозрених у здійсненні атаки зловмисників.

Заснована на протоколі СВВ (Protocol-based IDS, PIDS) являє собою систему (або агента), яка відстежує і аналізує комунікаційні протоколи зі зв'язаними системами або користувачами. Для веб – сервера подібна СВВ зазвичай веде спостереження за HTTP і HTTPS протоколами. При використанні HTTPS СВВ повинна розташовуватися на такому інтерфейсі, щоб переглядати HTTPS пакети ще до їх шифрування та надсилання у мережу.

Заснована на прикладних протоколах СВВ (Application Protocol-based IDS, APIDS) – це система (або агент), яка веде спостереження і аналіз даних, що передаються з використанням специфічних для певних програм протоколів. Наприклад, на веб-сервері з SQL базою даних СВВ буде відстежувати вміст SQL команд, що передаються на сервер.

Хостова СВВ (Host-based IDS, HIDS) – система (або агент), розташована на хості, що відслідковує вторгнення, використовуючи аналіз системних викликів, логів додатків, модифікацій файлів (виконуваних, файлів паролів, системних баз даних), стану хоста і інших джерел . Прикладом є OSSEC.

Гібридна СВВ поєднує два і більше підходів до розробки СВВ. Дані від агентів на хостах комбінуються з мережевою інформацією для створення найбільш повного уявлення про безпеку мережі. Як приклад гібридної СВВ можна привести Prelude [3].

Виходячи з того, що в неоднорідній мережі під час кіберспортивного турніру з високою ймовірністю можуть бути присутні клієнти з різними ОС, помітним мінусом мережевої IDS стає потенційна вразливість до атак, що враховує особливості реалізації різних TCP / IP-стеків, наприклад, при обробці фрагментированого мережевого трафіку. Аналізуючи механізм способу моніторингу системи виявлення вторгнень, розглянуто методи реагування (див. рис. 2.10): ***блокування з'єднання, блокування хоста комп'ютерної мережі, виявлення атак за допомогою мережевих датчиків.***

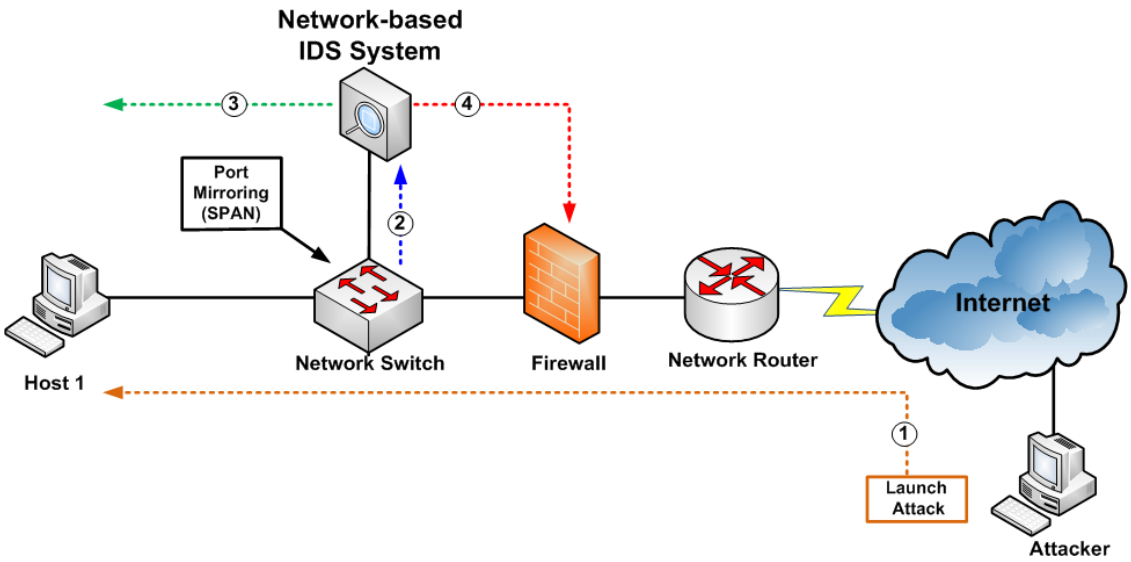

Рис. 2.10 Механізм виявлення та блокування вторгнень

Блокування з'єднання. Якщо для атаки під час змагання використовується TCP-з'єднання, то реалізується його закриття за допомогою посилки кожному або одному з учасників TCP-пакета з встановленим прапором RST. У результаті зловмисник позбавляється можливості продовжувати атаку, використовуючи мережеве з'єднання. Даний метод найчастіше реалізується з допомогою наявних мережевих датчиків.

Блокування хоста комп'ютерної мережі. Якщо з одного з хостів була зафіксована атака, то може бути проведене його блокування хостовими датчиками або блокування мережевих інтерфейсів або на нього, або на маршрутизаторі або комутаторі, за допомогою яких хост підключений до мережі. Розблокування може відбуватися через заданий проміжок часу або за допомогою активації адміністратором безпеки.

Блокування атаки за допомогою мережевого екрану (МЕ). IPS формує і надсилає нові конфігурації в МЕ за якими екран буде фільтрувати трафік від порушника.

Виявлення атак за допомогою мережевих датчиків. Мережеві датчики встановлюються в розрив каналу зв'язку так, щоб аналізувати всі пакети які проходять. Для цього вони оснащуються двома мережевими адаптерами, які функціонують у «змішаному режимі», на прийом і на передачу, записуючи всі

пакети в буферну пам’ять, звідки вони зчитуються модулем виявлення атак IPS. У разі виявлення атаки ці пакети можуть бути видалені.

Брандмауер (англ. Firewall) – є основним програмно-технічним компонентом захисту інформаційної безпеки. Брандмауер – програмний продукт або програмно-апаратний комплекс, який контролює мережеві пакети або встановлені програми. Потрібен для захисту системи кіберспортивного змагання від комп’ютерних атак. Брандмауером також можуть називати міжмережевий екран, мережевий екран або firewall.

На комп’ютерах з сучасними операційними системами йде як вбудоване програмне забезпечення. Також брандмауер може входити до складу платних антивірусних систем.

Програмні реалізації для Windows – вбудований брандмауер (можна відкрити в панелі управління або з центру управління мережами і загальним доступом), окремі програми, антивірусні системи з включеним до складу мережевим екраном. На Linux представлений, найчастіше, вбудованим в ядро Netfilter, управління якого здійснюється із застосуванням різних утиліт, наприклад, iptables або firewalld. Для BSD – ipfirewall, для управління яким використовується ipfw.

Чи потрібен брандмауер? На сервері, який підключений до мережі Інтернет безпосередньо – обов’язково. На звичайному домашньому комп’ютері, який використовується для розваг і отримання інформації можна сміливо відключити. Всі брандмауери за функціонуванням можна поділити на три категорії: *традиційні пакети фільтрів, фільтри, що враховують стан з’єднання та шлюзи додатків.*

Традиційні фільтри пакетів. Весь вхідний та вихідний трафік внутрішньокорпоративної мережі проходить через маршрутизатор, на якому відбувається фільтрація пакетів. Фільтр пакетів перевіряє кожну дейтаграмму, визначаючи як і що з нею зробити згідно з правилами, встановленими адміністратором мережі. Адміністратор турнірної мережі конфігурує брандмауер, спираючись на політику, що діє в організації (див. рис.2.11).

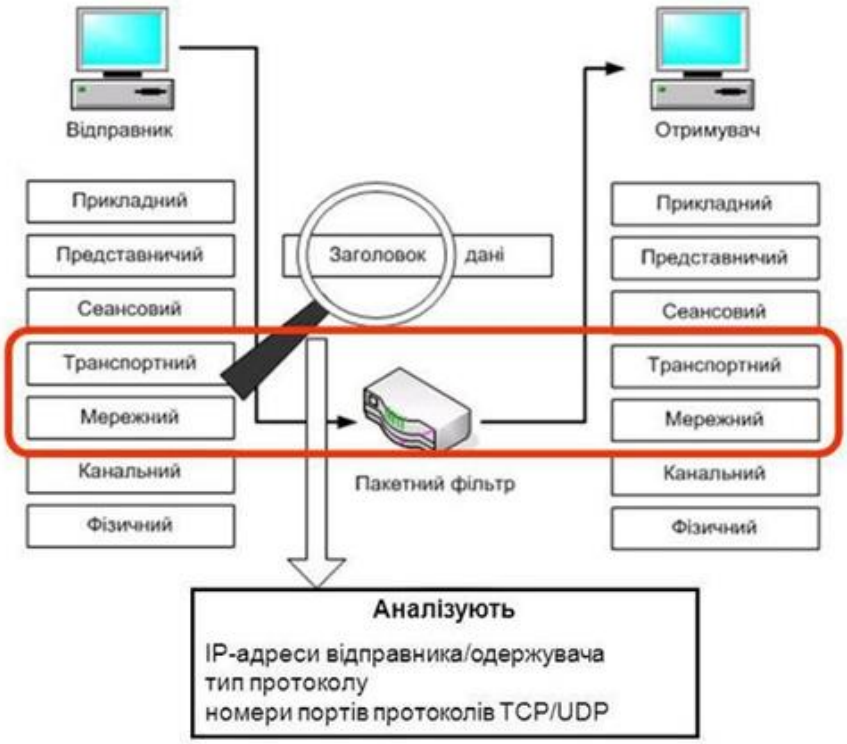

Рис. 2.11 Принцип роботи фільтрації пакетів

Рішення, пов’язані з фільтрацією, зазвичай засновані на наступних факторах: вихідна чи кінцева IP-адреса, тип протоколу в відповідному полі дейтаграми, флагові біти, тип повідомлення, різні правила, що характеризують вхідні і вихідні дейтаграми даної мережі та правила, що стосуються інтерфейсів. Правила брандмауера реалізуються в маршрутизаторах за допомогою списків контролю доступу. Ці правила застосовуються для кожної дейтаграми, яка проходить через даний інтерфейс.

Фільтри, які враховують стан з’єднання відстежують TCP-з’єднання і виконують фільтрацію на основі цієї інформації. Всі поточні TCP-з’єднання відстежуються в спеціальній таблиці з’єднань. Якщо ж вхідний пакет не буде відноситись до поточних з’єднань, то він буде відкинутий брандмауером (рис. 2.12).

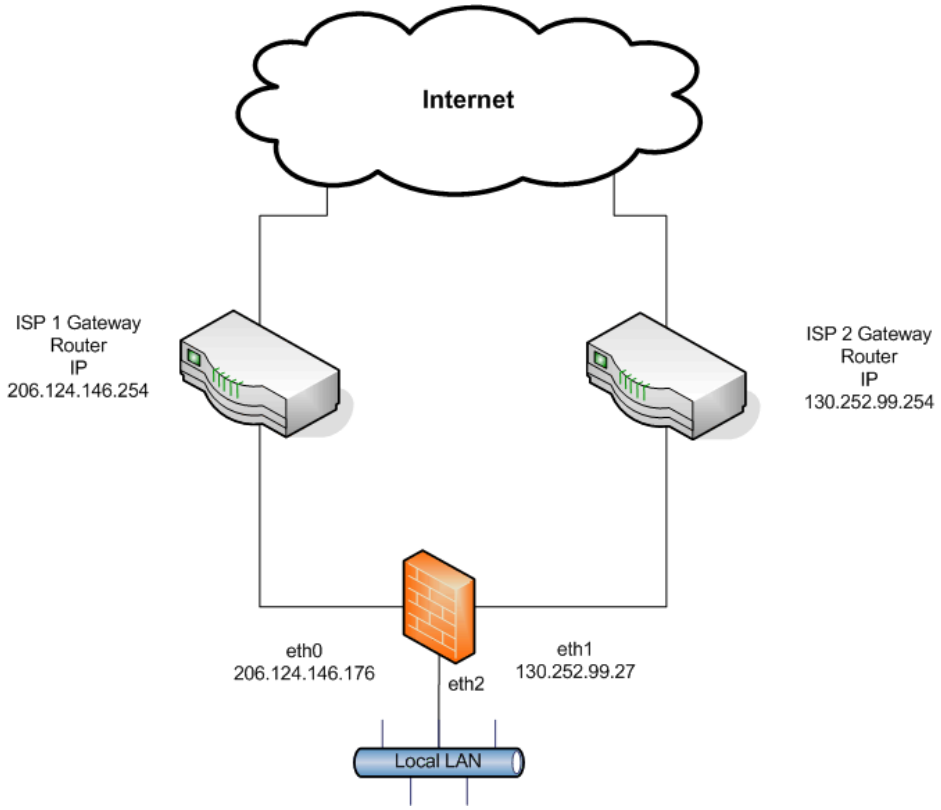

Рис. 2.12 Принцип фільтрацій які враховують стан з’єднання

Шлюзи додатків – замість аналізу IP-пакетів шлюзи цього типу вивчають дані на рівні додатків. Часто шлюзи додатків використовують додатки які відповідають за створення окремого сеансу. На відміну від фільтр-пакетів цей сеанс не допускає прямого з’єднання між двома мережами, іншими словами цей шлюз не може виступати в якості посередника для трафіку пакетів (див. рис. 2.13).

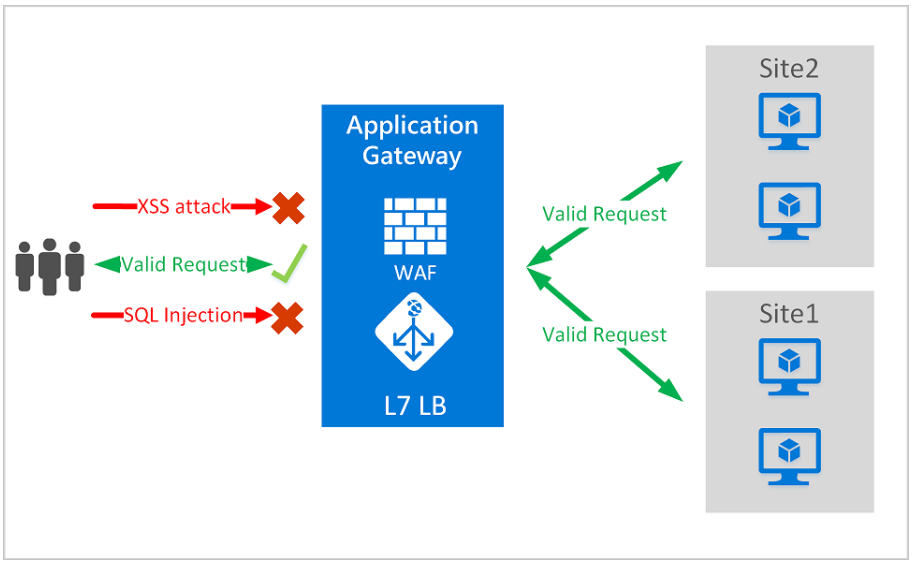

Рис. 2.13 Принцип роботи брандмауера через шлюз додатків

Якщо раціонально підібраний та правильно встановлений брандмауер функціонує під час кіберспортивного змагання то він може слугувати не поганою системою захисту від можливих злочинних нападів.

Враховуючи те, що будь-яка система, яка встановлена для запобігання можливих вторгнень, має свої певні недоліки, слід більш детальніше вивчити їх та врахувати при побудові системи захисту.
Взагалі, структура сучасних СВВ, включає в себе такі підсистеми:

- підсистема збору інформації про систему, яка підлягає захисту;
- підсистема аналізу для пошуку атак та вторгнень в систему;
- підсистема представлення даних для контролю системи в режимі реального часу (див. рис. 2.14).

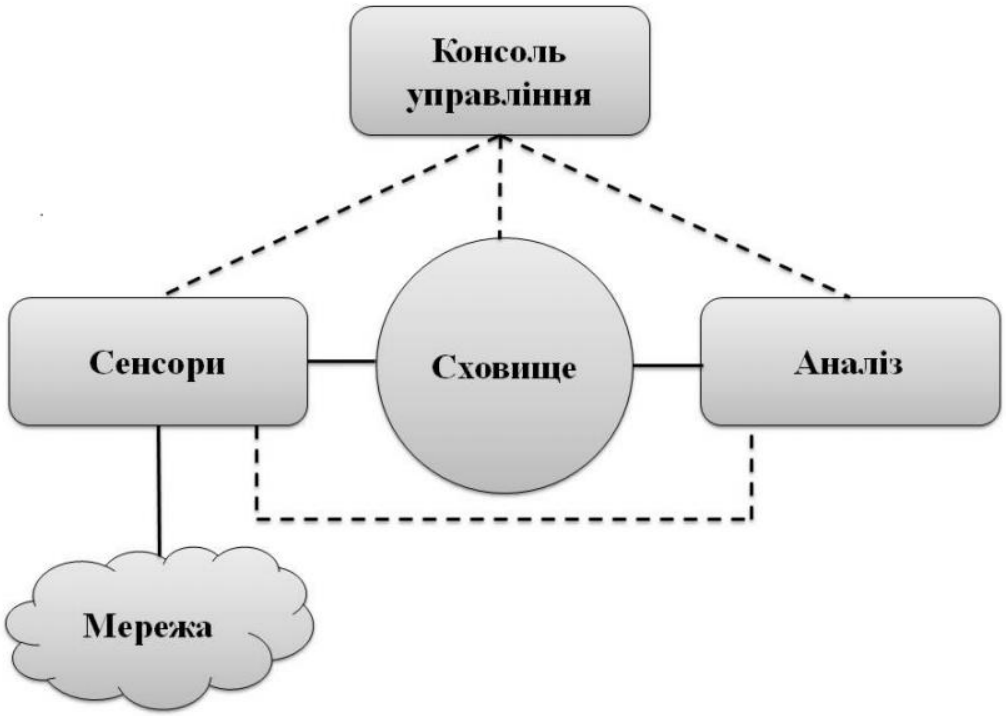

Рис. 2.14 Схема загальної структури СВВ

Підсистема збору інформації під час кіберспортивного змагання отримує дані від автономних модулів, датчиків програмного забезпечення (ПЗ) системи, датчиків хосту, міжмережевих та мережевих датчиків, скомпонованих у залежності від задач структури мережі та типу інформації, яка підлягає аналізу.

Ієрархічно підсистема аналізу як вхідні дані використовує інформацію із попередньої підсистеми і містить у собі набір аналізаторів, скомпонованих за задачами виявлення вторгнень заданого типу. Ефективність виявлення вторгнень залежить від параметрів аналізаторів та їх кількості.

Підсистема представлення даних орієнтована на різні групи користувачів, які контролюють певні підсистеми мережі. Тому в таких СВВ використовують розмежування доступу, групові політики, повноваження та ін.

У залежності від наборів параметрів оцінки стану системи сучасні СВВ використовують дві групи методів. У випадку фіксованого набору параметрів оцінки і фіксованого часу навчання використовуються методи контрольованого навчання («навчання з учителем»).

У випадку, коли множина параметрів оцінки може змінюватися протягом заданого часу дослідження, а процес навчання відбувається весь час, використовуються методи не контрольованого навчання («навчання без учителя»).

Основною ідеєю виявлення нестандартної поведінки мережі, яка підлягає захисту, є формування профілю чи образу мережі. Тому основними методами, на яких базується реалізація СВВ, є методи розпізнавання образів. При цьому образ нормальної поведінки формується на основі аналізу параметрів оцінки мережі.

Висновки про аномальну поведінку під час кіберспортивного турніру формуються на основі відхилень значень оцінок параметрів від профілю мережі. Величина та характер відхилень, як правило, в режимі реального часу, дають змогу проводити ідентифікацію аномалії – технічний збій, допустиме відхилення пов’язане із дією зовнішнього середовища, атака на мережу [37].

Формування профілю чи образу в СВВ проводиться за допомогою таких методів:

- статистичні методи аналізу параметрів оцінки;
- методи множинного опису подій та формальної логіки;
- методи нечіткої логіки та нейронні мережі.

Виходячи із способів формування профілю мережі та методів виявлення аномалій, можна визначити два класи задач:

- вибір оптимальної множини параметрів оцінки;
- визначення загального показника аномальності.

Питання визначення інтегральної оцінки аномальності поведінки мережі на сьогодні є практично не вирішеним завдяки неоднозначності розв'язку задачі формування множини оцінок параметрів мережі, яка підлягає захисту.

Розв'язок задач формування множини оцінок параметрів та їх динаміки можливий при використанні методу групового врахування аргументів, еволюційних та генетичних алгоритмів. Тоді визначення інтегральної оцінки може бути проведене за допомогою аналізу коваріацій (мірою спільної мінливості) параметрів оцінок, методів кореляційного аналізу, автокореляційних моделей. [29]

VPN –(Virtual Private Network)

Рис.2.15 Схема VPN підключення

Віртуальна приватна мережа створюється на базі загальнодоступної мережі Інтернет. І якщо зв'язок через Інтернет має свої недоліки, головним з яких є те, що вона схильна потенційним порушень захисту та конфіденційності, то VPN можуть гарантувати, що направляється через Інтернет трафік так само захищений, як і передача всередині локальної мережі. У теж час віртуальні мережі забезпечують істотну економію витрат у порівнянні з вмістом власної мережі глобального масштабу.

VPN – це логічна мережа, створена поверх інших мереж, на базі загальнодоступних або віртуальних каналів інших мереж (Інтернет). Безпека передавання пакетів через загальнодоступні мережі може реалізуватися за допомогою шифрування, внаслідок чого створюється закритий для сторонніх канал обміну інформацією. VPN дозволяє об'єднати, наприклад, декілька географічно віддалених мереж організації в єдину мережу з використанням для зв'язку між ними непідконтрольних каналів.

Технологія VPN створює віртуальні канали зв'язку через загальнодоступні мережі, так звані «VPN—тунелі». Трафік, що проходить через тунелі, що зв'язують віддалені офіси організаторів турніру, шифрується. Зловмисник, що перехопив шифровану інформацію, не зможе переглянути її, так як не має ключа для розшифровки.

Найчастіше для створення віртуальної мережі використовується інкапсуляція протоколу PPP в який—небудь інший протокол – IP (такий спосіб використовує реалізація PPTP – Point—to—Point Tunneling Protocol) або Ethernet (PPPoE). Технологія VPN останнім часом використовується не тільки для створення власне приватних мереж, але і деякими провайдерами для надання виходу в Інтернет.состоіт з двох частин: «внутрішня» (підконтрольна) мережа, яких може бути кілька, і «зовнішня» мережа, по якій проходить інкапсульоване з'єднання (зазвичай використовується Інтернет). Можливо також підключення до віртуальної мережі окремого комп'ютера. Підключення віддаленого користувача до VPN проводиться за допомогою сервера доступу, який підключений як до внутрішньої, так і до зовнішньої (загальнодоступної) мережі. При підключенні віддаленого користувача (або при установці з'єднання з іншою захищеною мережею) сервер доступу вимагає проходження процесу ідентифікації, а потім процесу аутентифікації. Після успішного проходження обох процесів, віддалений користувач (дистанційна мережа) наділяється повноваженнями для роботи в мережі, тобто відбувається процес авторизації. Класифікувати VPN рішення можна за кількома основними параметрами: *за типом використовуваного середовища і за способом реалізації.*

За типом використовуваного середовища: *Захищені* . Найбільш поширений варіант приватних приватних мереж. С його допомогою можливо створити надійну і захищену підмережа на основі ненадійної мережі, як правило, Інтернету. Прикладом захищених VPN є: IPSec, OpenVPN і PPTP. *Довірчі*. Використовуються у випадках, коли передавальну середу можна вважати надійною і необхідно вирішити лише завдання створення віртуальної підмережі в рамках більшої мережі. Питання забезпечення безпеки стають неактуальними. Прикладами подібних VPN—рішень є: Multi—protocol label switching (MPLS) і L2TP (Layer 2 Tunneling Protocol). (Коректніше сказати, що ці протоколи перекладають завдання забезпечення безпеки на інші, наприклад L2TP, як правило, використовується в парі з IPSec) [49].

За способом реалізації: *У вигляді спеціального програмно—апаратного забезпечення* . Реалізація VPN мережі здійснюється за допомогою спеціального комплексу програмно—апаратних засобів. Така реалізація забезпечує високу продуктивність і, як правило, високий ступінь захищеності. *У вигляді програмного рішення*. Використовують персональний комп'ютер зі спеціальним програмним забезпеченням, що забезпечує функціональність VPN.

Інтегроване рішення. Функціональність VPN забезпечує комплекс, вирішальний також завдання фільтрації зв'язку, організації мережевого екрану і забезпечення якості обслуговування *за призначенням*: *Intranet VPN, Remote Access VPN, Extranet VPN*

Intranet VPN . Використовують для об'єднання в єдину захищену мережу декількох розподілених філій однієї організації, які обмінюються даними по відкритих каналах зв'язку.

Remote Access VPN . Використовують для створення захищеного каналу між сегментом корпоративної мережі (центральним будівлею або філією) та одиночним користувачем, який, працюючи вдома, підключається до корпоративних ресурсів з домашнього комп'ютера або, перебуваючи у відрядженні, підключається до корпоративних ресурсів за допомогою ноутбука.

Extranet VPN. Використовують для мереж, до яких підключаються «зовнішні» кор истувачі (наприклад, замовники або клієнти). Рівень довіри до них набагато нижче, ніж до співробітників ВНЗ, тому потрібно забезпечення спеціальних «рубежів» захисту, що запобігають або обмежують доступ останніх до особливо цінної, конфіденційної інформації.

Переваги VPN очевидні. Надавши користувачам можливість з'єднуватися через Інтернет, масштабованість досягається в основному збільшенням пропускної здатності каналу зв'язку, коли мережа стає перевантаженої. VPN допомагає заощадити на телефонних витратах, оскільки вам не потрібно мати справу з багатою кількістю модемів. Крім того, VPN дозволяють отримати доступ до мережевих ресурсів, які в звичайній ситуації адміністратори змушені виносити на зовнішнє з'єднання.

Отже, VPN забезпечує:

- захищені канали зв'язку за ціною доступу в Інтернет, що в кілька разів дешевше виділених ліній;
- при установці VPN не потрібно змінювати топологію мереж, переписувати програми, навчати користувачів – все це значна економія;
- забезпечується масштабування, оскільки VPN не створює проблем росту і зберігає зроблені інвестиції;
- незалежність від криптографії і можете використовувати модулі криптографії будь—яких виробників у відповідності з національними стандартами тієї чи іншої країни;
- відкриті інтерфейси дозволяють інтегрувати вашу мережу з іншими програмними продуктами та бізнес—додатками.

До недоліків VPN можна віднести порівняно низьку надійність. У порівнянні з виділеними лініями та мережами на основі Frame relay віртуальні приватні мережі менш надійні, проте в 5—10, а іноді і в 20 разів дешевше.

На думку аналітиків, це не зупинить VPN, це не суттєво для більшості користувачів [18].

2.3. Розробка методики проведення кіберспортивних змагань і оцінки ефективності забезпечення їх інформаційної безпеки

Розробка методики проведення кіберспортивних змагань проводиться відповідно до загальної схеми, представленої на рис. 2.16

Рис. 2.16 Загальна схема проведення кіберспортивного змагання

Змагання проводиться в спеціальних місцях, де публіка може спостерігати за гравцями, що сидять за комп'ютерами, а хід змагань відстежувати на своїх ноутбуках або великому електронному екрані, де транслюється саме ігровий процес (див.рис. 2.17).

Змагання можуть також проводитись в комп'ютерних або кіберспортивних клубах, а хід його – наживо транслюватись через Інтернет і інші медіаресурси (аналоги телебачення). [54]

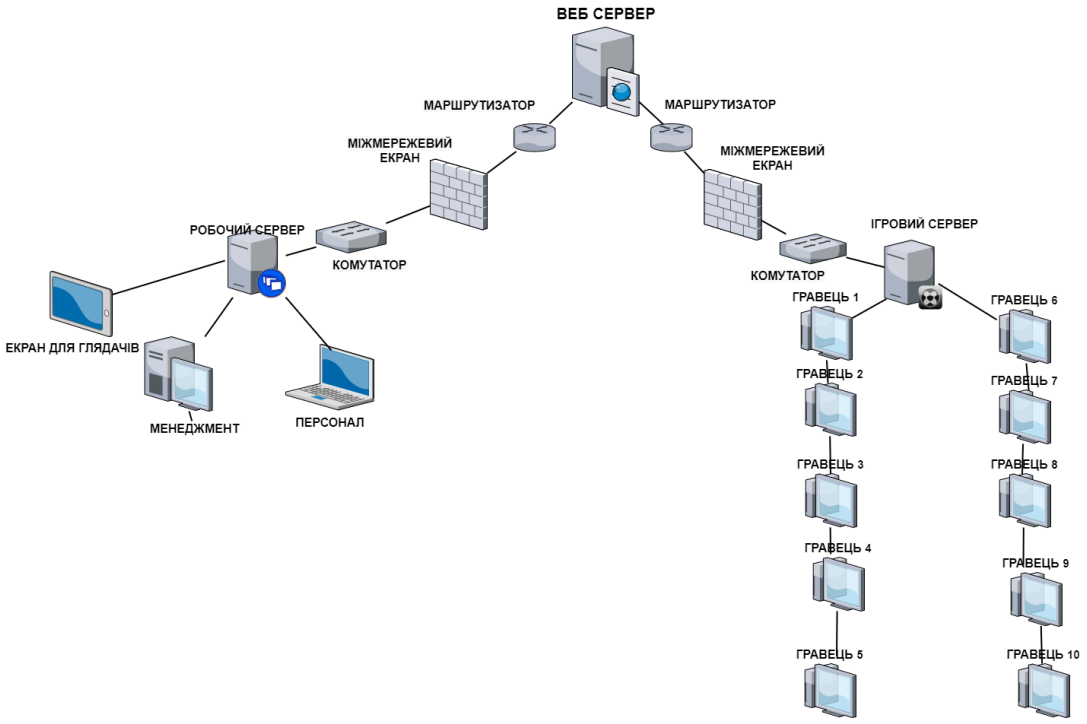

Рис. 2.17 Схема проведення кіберспортивного змагання

Велика кількість електронних пристроїв, які фіксують, обробляють, зберігають та надають до широкого доступу цифрову, друковану та відео інформацію про хід змагань, команди, гравців, тренерів, суддів та ін., змушує звертати увагу на забезпечення безпеки їх функціонування. Масове використання комп'ютерних засобів та інструментів комунікації у кіберспортивних змаганнях завжди буде пов'язано також з наявністю можливих кіберзагроз і виникненням подій інформаційною безпеки.

Тому для розробки методики проведення кіберспортивних змагань і оцінки ефективності забезпечення їх інформаційної безпеки треба визначитись з категоріями:

- інформаційних ресурсів під час проведення кіберспортивних змагань, що підлягають захисту;
- відвідувачів та учасників;
- режими використання та рівні доступу до інформації

Категорії інформаційних ресурсів під час проведення кіберспортивних змагань, що підлягають захисту. Виходячи з необхідності забезпечення різних рівнів захисту різних видів інформації, що зберігається та обробляється під час проведення кіберспортивних заходів, вводиться кілька категорій конфіденційності та кілька категорій цілісності інформації, що захищається:

«*Строго конфіденційна*» - до цієї категорії відноситься інформація, яка є конфіденційною відповідно до вимог чинного законодавства (банківська таємниці, персональні дані), а також інформація, обмеження на поширення якої запроваджені рішеннями керівництва організаторами проведення змагання (комерційна таємниця), розголошення якої може призвести до тяжких фінансово-економічних збитків для організації. Наприклад, інформація про відвідувачів, про учасників, про журналістів, дані банківських карток.

«*Конфіденційна*» - до цієї категорії належить інформація, не віднесена до категорії «Строго конфіденційна», обмеження на поширення якої запроваджуються рішенням керівництва організаторами змагання відповідно до наданих йому як власника (уповноваженої власника особи) інформації чинним законодавством правами, розголошення якої може призвести до значних збитків та втрати конкурентоспроможності організації. Інформація про порядок проведення змагань, про рішення коли і як будуть проведені визначені етапи змагання є конфіденційною;

«*Відкрита*» - до цієї категорії відноситься інформація, забезпечення конфіденційності (запровадження обмежень на поширення) якої не потрібне.

Категорії відвідувачів та учасників, режими використання та рівні доступу до інформації. *Організатори проведення кіберспортивних змагань***:** мають необмежені права доступу до всіх ділянок змагання

*Адміністратор кіберспортивних змагань***:** надає усім, хто пов’язаний з організацією та займає якусь відповідну роль щодо статусу права, які узгоджені з організатором змагань, але вони не мають доступу до системних ресурсів, до програмних файлів та баз паролів.

Менеджери по роботі з гравцями та іншими відвідувачами, що мають відношення до організації змагань: мають доступ до персональных даних.

*Преса (представники засобів масової інформації)***:** мають змогу безперешкодно відвідувати усі зони змагань, бути спостерігачами - як зі сторони глядача, так і з організаційної сторони.

*ВІП відвідувачі (представники влади)***:** мають доступ до відвідування закритих павільйонів для перегляду та безпосередньо контактувати з учасниками змагань

*ІТ спеціалісти***:** налаштування усіх технологічних процесів змагання, підтримка та контроль стану функціонування технічних пристроїв.

Медіа гості: мають доступ до медіа-технічного обладнання, що пройшло перевірку перед використання під час змагання, можуть контактувати з гравцями та іншими робітниками змагання.

*Продавці сувенірів***:** мають доступ до документів і програм, що дозволяють їм здійснювати торгові операції.

*Охорона***:** мають доступ до відокремленого каналу зв'язку, можуть здійснювати перевірку та огляд підозрілих речей то пропускати електронні пристрої через сканер.

*Відвідувачі***:** мають доступ до спеціально відведених зон перегляду разом з іншими відвідувачами.

Учасники (гравці): мають доступ до відокремленої захищеної ігрової зони, можуть використовувати своє ігрове обладнання, що пройшло перевірку адміністратором змагання.

Для розробки методики проведення кіберспортивних змагань і оцінки ефективності його проведення необхідно в першу чергу знати місце забезпечення безпеки та його роль в змаганнях [37].

Рис. 2.18 Місце забезпечення безпеки та його роль в кіберспортивних змаганнях

При оцінці ефективності забезпечення інформаційної безпеки проведення кіберспортивних змагань треба також знати, які інформаційні ресурси треба захищати і як провести їх ідентифікацію.

Ресурси –це те, що має цінність під час проведення кіберспортивного змагання, усіх його етапів, операцій та безперервності цих процесів. Тому ресурси необхідно захищати для того, щоб забезпечити безперервність усіх процесів кіберспортивного змагання. Належне управління та облік ресурсів є життєво важливим і має бути основним обов'язком для керівництва всіх рівнів.

Важливі ресурси кіберспортивного заходу мають бути не тільки чітко ідентифіковані, а ще і належним чином оцінені, а реєстри цих ресурсів мають бути зібрані разом та підтримуватись у актуальному стані до кінця змагання. Об'єднання схожих або пов'язаних ресурсів у керовані набори даних дозволяють полегшити зусилля, що витрачаються на процес оцінки ризиків.

Підзвітність за ресурси дозволяє забезпечити підтримку адекватності рівня інформаційної безпеки. Для кожного з ідентифікованих ресурсів або групи ресурсів повинен бути визначений їхній власник, і відповідальність за супровід механізмів безпеки має бути покладена на цього власника.

При організації кіберспортивного змагання вимоги безпеки походять з трьох основних джерел:

- унікальний набір загроз та вразливостей, які можуть призвести до значних втрат у разі їх реалізації;
- вимоги законодавства, нормативної бази та договорів, які застосовуються до організації, її комерційних партнерів, підрядників та провайдерам з обслуговування;
- унікальний набір принципів, цілей та вимог до обробки інформації, який організація розробила для підтримки своїх управлінських операцій та процесів в інформаційних системах.

Після визначення вимог безпеки при організації кіберспортивного змагання необхідно розглядати їх у процесі визначення вартості ресурсів з формулюванням їх у термінах конфіденційності, цілісності та доступності. Таким чином, основними факторами в оцінці ефективності забезпечення інформаційної безпеки проведення кіберспортивних змагань є ідентифікація та визначення вартості ресурсів, які залежать від потреб кіберспортивного змагання. Для визначення рівня захисту ресурсів необхідно оцінити їх вартість виходячи зі ступеня важливості для проведення змагання або цінності для різних можливостей управлінської діяльності. Також необхідно враховувати ідентифіковані законодавчі вимоги, вимоги бізнесу та наслідки порушення конфіденційності, цілісності та доступності.

Одним із способів вираження вартості ресурсу є використання наслідків для проведення кіберспортивного заходу, що виникають і тісно пов’язані з порушенням професійної діяльності. Це порушення можуть бути у вигляді нанесеної прямої або непрямої шкоди внаслідок небажаних інцидентів, таких як розкриття, модифікація, недоступність та/або знищення ресурсів. Ці інциденти, у свою чергу, можуть призвести до втрати доходу або прибутку, тому ці міркування мають бути відображені у вартості ресурсів.

Вихідні дані для визначення вартості ресурсів мають надавати організатори та користувачі цих ресурсів, які можуть авторитетно міркувати про вартість ресурсів та конкретну інформацію для використання при проведенні

кіберспортивних змагань. Для рівномірного визначення вартості ресурсів необхідно визначати шкалу вартості ресурсів. Тому для кожного з ресурсів має бути визначена його вартість, що відображатиме потенційні наслідки в результатах змагання у разі порушення конфіденційності, цілісності, доступності або будь-яких інших важливих властивостей цього ресурсу. Для кожного з цих властивостей має бути визначено окреме значення вартості, оскільки вони є незалежними і можуть змінюватись для кожного з ресурсів [58] .

Інформація та інші ресурси повинні бути відповідним чином класифіковані відповідно до ідентифікованої вартості ресурсів, законодавчих та бізнес-вимог і рівням критичності. Класифікація показує потребу, пріоритети та очікуваний рівень захисту при користуванні інформацією. Визначення класифікації, а також її перегляд з метою надання гарантій того, що класифікація залишається на відповідному рівні, входить до обов'язків власника ресурсу.

Ресурси є об'єктом багатьох видів загроз. Загроза може спричинити небажаний інцидент, внаслідок якого організатору, учасникам кіберспортивного змагання або її ресурсам буде завдано шкоди. Цей збиток може виникнути внаслідок атаки на інформацію, що належить організації. Атака може привести , наприклад, донесанкціонованого розкриття, модифікації, пошкодження, знищення, недоступності або втрати цінної інформації. Загрози можуть походити від випадкових або навмисних джерел або подій. При реалізації загрози використовується одна або більше вразливостей систем, додатків або сервісів, що використовуються з метою успішного заподіяння шкоди ресурсам. Загрози можуть виходити зсередини організації, і ззовні. Тому необхідно проводити разом ідентифікацію загроз і вразливостей. Вразливості системи є місцем слабкості її захисту і завжди асоційовані з ресурсами організації. Ці слабкості можуть використовуватися однією або декількома загрозами, які є причиною небажаних інцидентів, які можуть призвести до втрати, пошкодження або шкоди для ресурсів та проведенню заходів по їх захисту [59].

Ідентифікація вразливостей повинна визначити слабкості, які пов’язані з ресурсами:

- фізичне середовище;
- персонал, процедури управління, адміністрування та механізми контролю;
- технічні засоби, програмне забезпечення або телекомунікаційне обладнання та підтримуюча інфраструктура.

Після виявлення загроз і вразливостей необхідно оцінити ймовірність їх об’єднання з ризиком. Це включає оцінку ймовірності загроз, а також те, наскільки легко вони можуть використовувати наявні вразливості.

Оцінка ймовірності загроз має враховувати таке:

- *Умисні загрози*. Імовірність навмисних загроз залежить від мотивації, знань, компетенції та ресурсів, доступних потенційному зловмиснику, а також від привабливості ресурсів для реалізації витончених атак.
- *Випадкові небезпеки*. Можливість випадкових загроз може оцінюватися з використанням статистики та досвіду. Ймовірність таких загроз може залежати від близькості організації до джерел небезпеки, таких як автомагістралі та залізничні колії, а також заводи, що мають справу з небезпечними матеріалами, такими як хімічні речовини або бензин. Імовірність людських помилок (одна з найпоширеніших випадкових загроз) та поломки обладнання також мають бути оцінені.
- *Попередні інциденти*. Ці інциденти в минулих змаганнях, що ілюструють проблеми з існуючими гарантіями.
- *Нові розробки та тенденції*. Це включає звіти, новини та тенденції, отримані з Інтернету, груп новин або від інших організацій, які допомагають оцінювати ситуацію з загрозами.

Імовірність реалізації загроз має оцінюватися на основі такого підходу до оцінки та на базі шкали, обраної для оцінки загроз та вразливостей.

Загальна можливість інциденту також залежить від вразливостей ресурсів, тобто. Наскільки легко вразливості можуть бути використані.

Обчислення рівнів ризиків здійснюватиметься шляхом комбінування вартості ресурсів, що виражає ймовірні наслідки порушення конфіденційності, цілісності та/або доступності, з оцінковою ймовірністю пов’язаних з ними загроз та величиною вразливостей, які при об’єднанні стають причиною інциденту.

Організатори проведення кіберспортивних змагань самі повинні визначати метод оцінки ризиків, що найбільш підходить для їх вимог. Обчислені рівні ризиків дозволяють ранжувати ризики та ідентифікувати ті ризики, що є найбільш проблематичними в змаганнях.

Існують різні способи встановлення відносин між вартістю, ресурсами, ймовірністю загроз та величиною вразливостей для отримання одиниць виміру ризиків.

Ризик визначається двома факторами, один з них виражає наслідки, що настають у разі здійснення ризику, а інший висловлює ймовірність того, що ця подія може статися.

Наступною частиною оцінювання ризику є порівняння обчислених рівнів ризику зі шкалою рівня ризику. Рівні ризику повинні бути виражені в термінах втрат для організаторів кіберспортивного змагання та часу відновлення, як, наприклад, «серйозні збитки для організаторів, від яких не можуть відновитися раніше, ніж за півроку». Встановлення зв'язку між рівнями ризику та впливу на змагання потрібно для того, щоб реалістично оцінювати вплив, який обчислені ризики надають на них, та доносити зміст рівнів ризику до керівництва.

Оцінка ризиків повинна також визначити прийнятні в більшості випадків рівні ризику, тобто ті рівні ризику, при яких оцінений збиток настільки малий, що організація впорається з ними, не перериваючи своєї повсякденної діяльності, і, отже, не потрібно ніяких подальших дій.

Оцінку ефективності забезпечення інформаційної безпеки проведення кіберспортивних змагань можно провести, використовуючі модель порушника – для приклада [60].

Модель порушника є свого роду опис типів зловмисників, які, навмисно або випадково, в результаті дії або бездіяльності, які здатні пошкодити інформаційну

систему, яка використовується на кіберспортивних змаганнях. Найчастіше вони поділяються на зовнішні, внутрішні та інші категорії, відповідно –на A, B і C. Однак цей поділ не є достатнім. Таким чином, рейтинг проводиться з диверсифікацією цих категорій на підкатегорії (A1, B1, B2 і C1), які показані в табл. 2.1.

Таблиця 2.1

Модель порушника

Ідентифікатор	Найменування	Опис функцій
A1	Зовнішній порушник	
B1	Інсайдер	Особи, які мають санкціонований доступ до контрольованої зони, але не мають доступу до інформаційного ресурсу.
B2	Інсайдер	Зареєстрований користувач інформаційного ресурсу, який має обмежені права на доступ до даних.
C1	Шкідлива програма	Програмні закладки («Троянський кінь», спеціальні програми: клавіатурні шпигуни, програми підбору паролів віддаленого доступу та ін.) Програмні віруси.
C2	Збої, відмови обладнання	

Для використання моделі порушника були обрані для приклада основні компоненти мережі інформаційної системи, до яких застосовуються загрози. Це основні компоненти:

- Контролер домену.
- Ігрові сервери.
- Робочі сервери.

- Маршрутизатор.
- Комутатор.
- Робочі місця представників організатор та менеджерів.
- Канал зв'язку.

Робочі місця усього персонала то компьютери організаторів змагання були обєднанні в одну групу. Також у групи були об'єднані Маршрутизатори та Комутатори. Для Серверів складався власний перелік загроз та оцінка ризиків. Було обрано також узагальнений список загроз: *повного дистанційного управління системою; порушення цілісності, правильного функціонування системи; порушення доступності системи; фізичне пошкодження апаратних засобів; можливість негласного отримання та розголошення*.

Загроза повного дистанційного управління системою включає:

- несанкціонований доступ;
- несанкціонований доступ до журналів аудиту;
- присвоєння ідентифікатора організатора;
- доступ до внутрішнбої мережі неавторизованих осіб.

Загроза порушення цілісності, правильного функціонування системи включає:

- порушення цілісності;
- помилки;
- введення несанкціонованого або неперевіреного коду;
- шкідливий код.

Загроза порушення доступності системи включає:

- відмова в обслуговуванні, відсутність системних ресурсів, інформації;
- знищення записів;
- збій обладнання;
- збій комунікаційних сервісів.

Фізичне пошкодження апаратних засобів включає:

- збій системи технічних систем (охоронні, сигналізації, кондиціонери);

- ушкодження носіїв інформації;
- лиха (природні або антропогенні);
- несанкціонований фізичний доступ;
- вандалізм.

Можливість негласного отримання та розголошення (публікація) інформації, що захищається, включає в себе:

- несанкціоноване розкриття інформації.
- витік інформації;
- розкриття інформації;
- розкриття паролів;
- перехоплення інформації;
- фальсифікація записів.

Для розрахунку інформаційних ризиків задаємо дані вартості ресурсу (Asset Value , AV):

- Характерні значення ресурсу. 1 – мінімальна вартість ресурсу, 2 – середня вартість ресурсу, 3 – максимальна вартість ресурсу.
- Міра вразливості ресурсу до загрози (Exposure Factor, EF). Цей параметр показує, якою мірою той чи інший ресурс вразливий по відношенню до аналізованої загрози. 1 – мінімальна міра вразливості, 2 – середня міра вразливості, 3 – максимальна міра вразливості.
- Оцінка ймовірності реалізації загрози (Annual Rate of Occurrence, ARO) демонструє, наскільки можлива реалізація певної загрози за певний період часу, а також ранжується за шкалою від 1 до 3 (низька, середня, висока).

На підставі отриманих даних виводиться оцінка очікуваних втрат (рівень ризику) – [17].

- Оцінка очікуваного можливого збитку від одиничної реалізації певної загрози (Single Loss Exposure, SLE) розраховується за формулою:

$$SLE = AV \times EF \quad (2.1).$$

- Підсумкові очікувані втрати від конкретної загрози за певний період (Annual Loss Exposure, ALE) характеризують величину ризику та розраховується за формулою:

$$ALE = SLE \times ARO \quad (2.2).$$

- Кінцева формула розрахунку ризиків:

$$ALE = ((AV \times EF = SLE) \times ARO). \quad (2.3).$$

Визначення значення збитків та ймовірностей проводилося технічними спеціалістами та головним спеціалістом з безпеки при проведенні кіберспортивного змагання.

Перелік загроз, що становлять потенційну небезпеку для даних, які мають місце в ресурсах при проведенні кіберспортивних змагань, результати оцінки очікуваних втрат (рівень ризику) і заходи з рішеннями щодо усунення від інформаційних загроз, представлені в табл. А.1. – А.6.

Висновки до другого розділу

Проведена робота показала, що головною метою будь-якої системи захисту інформації є забезпечення сталого функціонування об’єкта, запобігання загрозам його безпеки, захист законних інтересів організатора кіберспортивного змагання від протиправних посягань, недопущення розкрадання фінансових коштів, розголошення, втрати, витоку, перекручування та знищення інформації, забезпечення нормальної діяльності всіх підрозділів об’єкта. Іншою метою системи інформаційної безпеки є підвищення якості послуг, що надаються і гарантій безпеки майнових прав та інтересів усіх учасників та відвідувачів.

Була розроблена і запропонована методика проведення кіберспортивних змагань та оцінка ефективності забезпечення їх інформаційної безпеки.

На наступному етапі дослідження постає завдання розробки рекомендацій по комплексному забезпеченню інформаційної безпеки при проведенні кіберспортивних змагань.

Розділ 3

ПРОВЕДЕННЯ ДОСЛІДЖЕННЯ І РОЗРОБКА РЕКОМЕНДАЦІЙ ПО КОМПЛЕКСНОМУ ЗАБЕЗПЕЧЕННЮ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ КІБЕРСПОРТИВНОГО ЗМАГАННЯ.

Забезпечення інформаційної безпеки кіберспортивного змагання включає всі елементи системи управління змаганням, пов’язані з визначенням, досягненням конфіденційності, цілісності, доступності, автентичності та достовірності інформації або засобів її обробки.

Для забезпечення ефективного функціонування всіх вище визначених елементів необхідно використання комплексного підходу. Це означає, насамперед, що в межах системи управління не може бути створено окремої підсистеми, яка б відповідала за інформаційну безпеку.

Для дослідження і розробки рекомендацій в якості прикладу було взято кіберспортивне змагання міжнародного рівня з гри CS:GO PGL Major Stockholm 2021 (рис.3.1 і рис. 3.2) , яке відбулося у листопаді 2021 року. Будучи відвідувачем на цьому змаганні, можна виділити основні недоліки та на їх підставі розробити рекомендації по комплексному забезпеченню його інформаційної безпеки. [19]

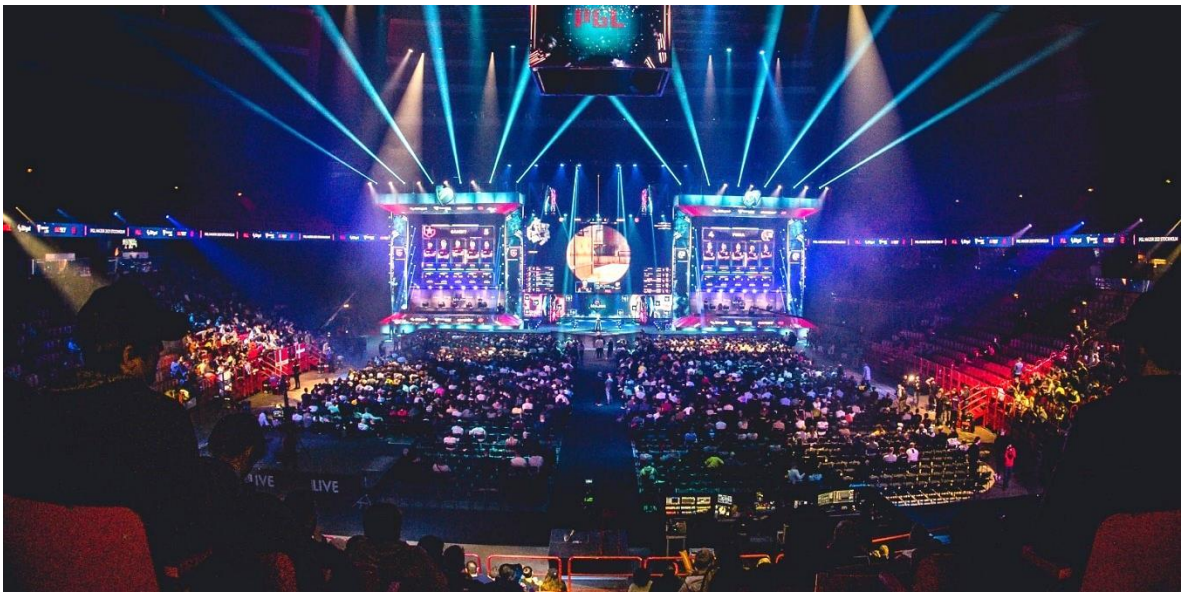

Рис. 3.1 Турнір PGL Major Stockholm 2021

Рис. 3.2 Турнір PGL Major Stockholm 2021

Результати були отримані після обробки даних з використання наступних заходів щодо захисту інформації:

1. *Зміна інформаційної мережі простору проведення кіберспортивного змагання* – виведення основних серверів в окрему підмережу і виведення робочих комп’ютерів персоналу та гравців в окрему мережу.

2. *Правильний вибір міжмережевих екранів* для захисту інформації.

3. *Встановлення Intrusion Detection System (IDS)*

4. *Організаційні заходи щодо захисту інформації*

1. *Зміна інформаційної мережі простору проведення кіберспортивного змагання* .Під час змагання всі сервери, а також комп’ютери персоналу, точок магазинів та гравців знаходилися разом в одній підмережі (наприклад 192.168.100.0/24). [20] Ця обставина може дуже вразливо впливає на усі процеси що проходять під час змагання і, крім того, негативно впливає на безпеку серверів та саме змагання в цілому. Наприклад, включення через патчкорд (через який працюють термінали оплати або комп'ютери співробітників під час змагання)

принесеного «лівого» ноутбука дозволяє отримати йому по DHCP адресу цієї підмережі, в якій знаходяться всі сервери цього змагання.

Щоб таке не сталося, запропоноване рішення згідно з яким – вивести важливі для змагання сервери в окремі мережи (див. табл. 3.1) і також відокремити від інших мереж робочі комп'ютери співробітників і гравців.

Таблиця 3.1

План розподілу серверів на підмережі

№	Підмережа	Вміст
1	vlan100 (DEFAULT) – 192.168.100.0/24	Персонал
2	vlan120 (Terminals) – 192.168.120.0/27	Магазини
3	vlan130 (Gamers) - 192.168.130.0/31	Ігрові потреби

2. *Правильний вибір міжмережевих екранів для захисту інформації.*

В даний час вибір міжмережевих екранів дуже широкий, починаючи від простого (і безкоштовного) Windows Firewall, що захищається, до високопродуктивних міжмережевих екранів з перевіркою стану пакетів вартістю в десятки тисяч доларів. При виборі міжмережевого екрану слід враховувати два основних фактори: вимоги безпеки та вартість. Головний акцент в огляді мережних міжмережевих екранів для змагань різних розмірів та вимог до безпеки зроблено на рівні захисту, а не характеристик маршрутизації або додаткових функціях пристрою.

Вимоги до безпеки постійно змінюються. Адміністратор змагання повинен поєднувати надійний захист із зручністю користувальницького доступу до даних, а також обмежувати програми, автори яких не звертають уваги на безпеку хост-машини та мережі. Головна перешкода на шляху до високої безпеки – витрати, які готові або можуть нести організатори змагання. Ринок міжмережевих екранів надзвичайно великий та різноманітний і чим вище його вартість, тим надійніший захист. Багато постачальників міжмережевих екранів стягують додаткову плату за передові функції маршрутизації, які не впливають на рівень безпеки. Було обрано

кілька постачальників пристроїв, що охоплюють весь спектр надійності та вартості, від традиційних міжмережевих екранів з перевіркою пакетів до змішаних пристроїв з перевіркою пакетів та програм для усунення універсальних загроз (universal threat management, UTM). Запропоновані такі постачальники, як Cisco Systems, Network Engines, Rimapp, SonicWall та Symantec.

Для малих та регіональних змагань з низьким рівнм безпеки пропонується пристрій SonicWall 170 (ціновой діапазон— близько 500 дол.), який працює майже автоматично.

В середньому при організації масштабного кіберспортивного змагання (в т.ч. і міжнародних змагань) витрачається від 5000 до 6000 дол. За надійний міжмережевий екран. Пропонуються пристрої SonicWALL PRO 4060 та Cisco PIX 515E-UR-FE-BUN. Обидві моделі відрізняються високою продуктивністю, але їм не вистачає можливостей балансування навантаження і передачі функцій від пристрою. На відміну від них пристрій RoadBLOCK F302PLUS на базі ISA Server 2004 компанії RimApp забезпечує вичерпний контроль на прикладному рівні за прийнятною ціною.

Такі високорівневі міжмережові екрани, як SonicWALL Pro 4060, Cisco PIX-515E UR-FE-BUN, RimApp RoadBLOCK F302PLUS забезпечують високі рівні безпеки та продуктивність для локальних та міжнародних змагань. При виборі оптимального міжмережевого екрану слід звернути увагу на контроль на прикладному рівні та вичерпні можливості протоколювання та підготовки звітів про доступ користувачів та додатків. Крім того, при виборі апаратного міжмережевого екрана важливо пам'ятати про стійкість до відмови.

3. Встановлення Intrusion Detection System (IDS). IDS є програмними або апаратними системами, які автоматизують процес перегляду подій, що виникають у комп’ютерній системі або мережі, та аналізують їх з точки зору безпеки. Оскільки кількість мережевих атак зростає, IDS стають необхідним доповненням безпеки інфраструктури.

Виявлення проникнення є процесом моніторингу подій, що відбуваються в комп'ютерній системі або мережі, та аналізу їх. Проникнення визначаються як

спроби компрометації конфіденційності, цілісності, доступності чи обходу механізмів безпеки комп'ютера чи мережі. Проникнення можуть здійснюватися як атакуючими, які отримують доступ до систем з Інтернету, так і авторизованими користувачами систем, які намагаються отримати додаткові привілеї, яких вони не мають. IDS є програмними або апаратними пристроями, які автоматизують процес моніторингу та аналізу подій, що відбуваються в мережі чи системі, з метою виявлення проникнень.

IDS складаються з трьох функціональних компонентів: інформаційних джерел, аналізу та відповіді. Система отримує інформацію про подію з одного або більше джерел інформації, виконує аналіз даних події, що визначається конфігурацією, а потім створює спеціальні відповіді – від найпростіших звітів до активного втручання при визначенні проникнень.

Виявлення проникнення дозволяє організаторам проведення захищати свої системи від загроз, пов'язані зі зростанням мережевої активності та важливістю інформаційних систем. При розумінні рівня та природи сучасних загроз мережевій безпеці, питання не в тому, чи слід використовувати системи виявлення проникнень, а в тому, які можливості та особливості систем виявлення проникнень слід використовувати.

IDS служать механізмами моніторингу, спостереження активності та прийняття рішень про те, чи спостерігаються події підозрілими. Вони можуть виявити атакуючих, які обійшли міжмережевий екран, і видати звіт про це адміністратору, який, у свою чергу, зробить кроки для запобігання атакі.

IDS стають необхідним доповненням інфраструктури безпеки кіберспортивного змагання. Технології виявлення проникнень не роблять систему абсолютно безпечною. Тим не менш, практична користь від IDS існує.

Використання IDS допомагає досягти кількох цілей:

1. Можливість мати реакцію на атаку дозволяє змусити атакуючого відповідати за власну діяльність.

2. Можливість блокування означає можливість розпізнати деяку активність або подію як атаку і потім виконати дію блокування джерела. IDS може визначити,

коли атакуючий здійснив проникнення в систему, використовуючи некоректовану або некоректовану помилку. Більше того, IDS може бути важливою ланкою в захисті системи, вказуючи адміністратору, що система була атакована, щоб вона могла ліквідувати завдані збитки.

3. Виконує документування існуючих загроз для мережі та систем. При складанні звіту про бюджет на мережеву безпеку корисно мати документовану інформацію про атаки.

4. Забезпечення контролю якості розробки та адміністрування безпеки, особливо у великих та складних мережах та системах.

5. Отримання корисної інформації про проникнення, які мали місце, з наданням покращеної діагностики для відновлення та коригування факторів, що викликали проникнення.

6. Допомагає визначити розташування джерела атак по відношенню до локальної мережі (зовнішні або внутрішні атаки), що важливо при прийнятті рішень про розташування ресурсів у мережі.

Технологія виявлення проникнень є необхідним доповненням для інфраструктури мережевої безпеки міжнародного кіберспортивного змагання PGL Major. Ефективне розгортання IDS вимагає ретельного планування, підготовки, прототипування, тестування та спеціального навчання.

Для захисту мережі кіберспортивного змагання завжди рекомендується розглядати *комбінацію network-based IDS та host-based IDS.*

Розгортання network-based IDS є більш простими для встановлення та супроводу. Існує багато варіантів розташування системних сенсорів network-based IDS, кожен з яких має свої переваги (див.рис. 3.3):

Позаду зовнішнього міжмережевого екрану DMZ-мережі (розташування 1)

Переваги:

- Бачить атаки, що виходять із зовнішнього світу, яким вдалося подолати першу лінію оборони мережевого периметра.

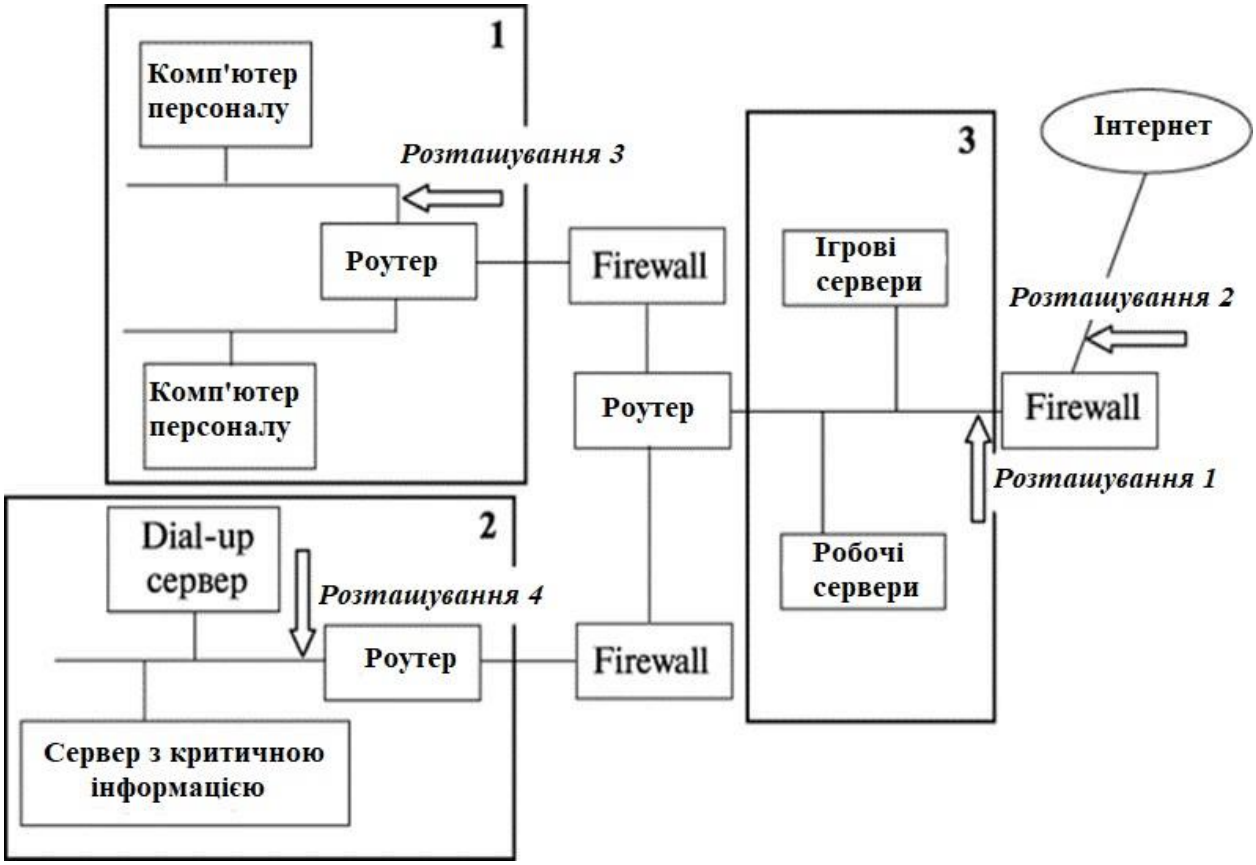

Рис. 3.3. Можливі варіанти розташування сенсорів network-based IDS

- Може аналізувати проблеми, пов'язані з політикою чи продуктивністю міжмережевого екрана, що забезпечує першу лінію оборони.
- Бачить атаки, метою яких є прикладні сервери (такі як web або ftp), які зазвичай розташовані в DMZ.
- Навіть якщо вхідна атака не розпізнана, IDS іноді може розпізнати вихідний трафік, що виникає внаслідок компрометації сервера.

Перед зовнішнім міжмережевим екраном (розташування 2)

Переваги:

- Документує кількість атак, що походять з Інтернету, метою яких є мережа.
- Документує типи атак, що походять з Інтернету, метою яких є мережа.

На основній магістральній мережі (розташування 3)

Переваги:

- Переглядає основний мережевий трафік; цим збільшується ймовірність розпізнання атак.
- Визначає неавторизовану діяльність авторизованих користувачів усередині периметра безпеки організації.

У критичних підмережах (розташування 4)

Переваги:

- Визначає атаки, метою яких є критичні системи та ресурси.
- Дозволяє фокусуватися на обмежених ресурсах найважливіших інформаційних цінностей, розташованих у мережі.

Після розташування системних сенсорів network-based IDS переходять до додаткового захисту критичних серверів за допомогою host-based IDS. Рекомендується, щоб насамперед host-based IDS був інстальований на критичних серверах. Це може зменшити загальну вартість розгортання та дозволить основну увагу приділити реагуванню на тривоги, що стосуються найважливіших хостів. Після того, як host-based IDS почали функціонувати у звичайному режимі, організації з підвищеними вимогами до безпеки можуть обговорити можливість інсталяції host-based IDS на інші хости. У цьому випадку слід використовувати host-based системи, які мають централізоване управління та функції створення звітів. Такі можливості можуть істотно знизити складність управління повідомленнями про тривоги від великої кількості хостів. Найчастіше ефективність конкретної host-based IDS залежить від можливості адміністратора розрізняти помилкові і вірні тривоги.

4. *Впровадження організаційних заходів щодо захисту інформації і їх ефективність в забезпеченні інформаційної безпеки під час проведення кіберспортивного змагання були досліджені на системах:* ігрових та робочих серверів, маршрутизаторів, комутаторів, робочих місць представників організатора та менеджерів, каналів зв'язку.

Результати дослідження комплексного забезпечення інформаційної безпеки кіберспортивного змагання (на базі розглянутого прикладу) представлені в Додатку Б (у розширеному вигляді) і є наступними:

За рахунок наступних заходів вдалося знизити загрозу отримання повного віддаленого контролю над системою для ігрових та робочих серверів.

За рахунок наступних заходів вдалося знизити загрозу порушення цілісності, правильного функціонування системи для ігрових та робочих серверів.

За рахунок наступних заходів вдалося знизити загрозу порушення доступності системи для ігрових та робочих серверів.

За рахунок наступних заходів вдалося знизити загрозу підміни мережевої адреси для ігрових та робочих серверів.

За рахунок наступних заходів вдалося знизити загрозу фізичного пошкодження апаратних засобів для ігрових та робочих серверів.

За рахунок наступних заходів вдалося знизити загрозу отримання повного віддаленого контролю над системою для Маршрутизаторів.

За рахунок наступних заходів вдалося знизити загрозу порушення цілісності, правильного функціонування системи для Маршрутизаторів.

За рахунок наступних заходів вдалося знизити загрозу порушення доступності системи для Маршрутизаторів.

За рахунок наступних заходів вдалося знизити загрозу фізичного пошкодження апаратних засобів для Маршрутизаторів.

За рахунок наступних заходів вдалося знизити загрозу порушення цілісності, правильного функціонування системи для Комутаторів.

За рахунок наступних заходів вдалося знизити загрозу порушення доступності системи для Комутаторів.

За рахунок наступних заходів вдалося знизити загрозу фізичного пошкодження апаратних засобів для Комутаторів.

За рахунок наступних заходів вдалося знизити загрозу отримання повного віддаленого контролю над системою для робочих місць представників організатора та менеджерів.

За рахунок наступних заходів вдалося знизити загрозу порушення цілісності, правильного функціонування системи для робочих місць представників організатора та менеджерів.

За рахунок наступних заходів вдалося знизити загрозу порушення доступності системи для робочих місць представників організатора та менеджерів.

За рахунок наступних заходів вдалося знизити загрозу підміни мережевої адреси для робочих місць представників організатора та менеджерів.

За рахунок наступних заходів вдалося знизити загрозу фізичного пошкодження апаратних засобів для робочих місць представників організатора та менеджерів.

За рахунок наступних заходів вдалося знизити загрозу витоку видової інформації для робочих місць представників організатора та менеджерів.

За рахунок наступних заходів вдалося знизити загрозу перехоплення мережевого трафіку з метою подальшого аналізу для каналів зв'язку.

За рахунок наступних заходів вдалося знизити загрозу фізичного пошкодження для каналів зв'язку.

Висновки до третього розділу

У третьому розділі розглянуті результати дослідження та надані рекомендації щодо комплексного забезпечення інформаційної безпеки кіберспортивного змагання на прикладі «PGL MAJOR CS:GO 2021».

Було рекомендовано раціональне використання інформаційної мережі простору проведення кіберспортивного змагання – виведення основних серверів в окрему підмережу, виведення робочих комп’ютерів персоналу, гравців в окрему мережу, правильний вибір міжмережевих екранів для захисту інформації, встановлення Intrusion Detection System (IDS) та виділено основні організаційні заходи щодо захисту інформації.

Проведений аналіз та запропоновані рекомендації дозволяють побудувати захищену систему безпеки, якщо використовувати на вибір з декілька досліджених їх варіантів, в залежності від спеціальних потреб.

ВИСНОВКИ

1. В результаті роботи були досліджені основні та популярні змагання з кіберспорту, виділені основні загрози їх проведення. Найпоширенішими загрозами є комп'ютерні віруси, DdoS атаки, недосконаліть програмного забезпечення, платформи, серверу та людський фактор.

2. Були виділені основні загрози, створена модель порушника під час проведення кіберспортивних змагань. Були запропоновані рішення щодо організаційних та програмно-технічних засобів захисту під час проведення кіберспортивних змагань. Було рекомендовано виведення основних серверів в окрему підмережу, виведення робочих комп'ютерів персоналу, гравців в окрему мережу, правильний вибір міжмережевих екранів для захисту інформації, встановлення Intrusion Detection System (IDS) та виділено основні організаційні заходи щодо захисту інформації.

3. Була розроблена методика проведення кіберспортивних змагань і оцінка ефективності забезпечення їх інформаційної безпеки. Головною метою системи захисту інформації під час проведення кіберспортивних змагань є забезпечення сталого функціонування об'єкта, запобігання загрозам його безпеки, захист законних інтересів організатора кіберспортивного змагання від протиправних посягань, недопущення розкрадання фінансових коштів, розголошення, втрати, витоку, перекручування та знищення інформації, забезпечення нормальної діяльності всіх підрозділів змагання.

4. Було проаналізовано головне кіберспортивне змагання з гри CS:GO PGL Major Stockholm 2021 та виділено основні заходи щодо захисту інформації:

1. Зміна інформаційної мережі простору проведення кіберспортивного змагання.
2. Правильний вибір міжмережевих екранів для захисту інформації.
3. Встановлення Intrusion Detection System (IDS).
4. Організаційні заходи щодо захисту інформації.

Практична значимість дипломної роботи полягає в тому, що її матеріали та результати можуть бути використані при організації інформаційної безпеки на кіберспортивних змаганнях.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Команди, турніри, призові та як влаштован кіберспорт. URL: https://tech.liga.net/technology/article/igra-na-million-kak-ustroen-kibersport-i-kto-na-nem-zarabatyvaet-rasskaz-weplay

2.Правила спортивних змагань з кіберспорту (електронного спорту) 55с. URL: http://dsmsu.gov.ua/media/2021/01/26/3/pravila_Kibersport.pdf

3.Поляков Д.А. Застосування системного підходу при організації захисту інформації / Д.А. Поляков, Ю.М. Якименко//Інтернет-конференція «Актуальні проблеми інформаційної та кібернетичної безпеки», 26 жовтня 2018 року. Тези доповідей — Київ: ДУТ(ННІЗІ), 2018. — С. с.44-45.

4.Поляков Д.А. Методичні підходи до аналізу систем виявлення мережевих вторгнень і виявлення ознак комп'ютерних атак безпеки / Д.А. Поляков, Ю.М. Якименко, //Конференція «Цифрова трансформація кібербезпеки», 26 квітня 2020 року. Тези доповідей — Київ: ДУТ(ННІЗІ), 2020. — С. 24-25.

5.Поляков Д. А. Забезпечення кібербезпеки в кіберспортивних заходах // Матеріали: Всеукраїнська наукова конференція, Актуальні проблеми кібербезпеки, 27 жовтня 2021. Тези доповідей — Київ: ДУТ, 2021.- С.124-126 - URL : http://www.dut.edu.ua/uploads/p_2099_79407917.pdf

6.Поляков Д., Якименко Ю. Аналіз загроз при проведенні кіберспортивних змагань. V Всеукраїнська НПК молодих учених, студентів і курсантів, 26 листопада 2021 року. Інформаційна безпека та інформаційні технології: збірник тез доповідей / Д.А. Поляков, Ю.М. Якименко // Конференція ІБІТ-2021. – Львів: ЛДУ БЖД, 2021- С.94-95.- URL: https://drive.google.com/drive/search?q=parent:1fdKL4ySYWfvT6JoAdqs76Fc47yO3S6L

7. Топ-10 кіберспортивних ігор за розміром призового фонду URL:https://itc.ua/articles/dengi-za-pobedu-top-10-kibersportivnyh-igr-po-razmeru-prizovogo-fonda/

8. Найпопулярніші турніри листопада 2021 URL: https://escharts.com/ru/blog/top-tournaments-november-2021

9.Річниця офіційного кіберспорту в Україні: головні досягнення індустрії URL: https://sport.nv.ua/other-sport/kibersport-v-ukraine-pervaya-godovshchina-oficialnogo-priznaniya-cybersport-parimatch-50181851.html

10.Федерація кіберспорту України: історія, досягнення та плани на майбутнє URL: https://tsn.ua/ru/cybersport/federaciya-kibersporta-ukrainy-istoriya-dostizheniya-i-plany-na-buduschee-1717865.html

11. Як організувати успішний кіберспортивний турнір? Кейс WePlay! Esports URL: https://ain.ua/ru/2020/02/24/kak-organizovat-uspeshnyj-kibersportivnyj-turnir-kejs-weplay-esports/

12. Модель побудови системи інформаційної безпеки. URL:http://pidruchniki.com/1237070651274/ekonomika/model_pobudovi_sistemi_informatsiynoyi_bezpeki

13. Інформаціна безпека: нові підходи до визначення поняття / Ірина Залєвська // Український науковий журнал "ОСВІТА РЕГІОНУ". – 2016. – URL: http://social-science.com.ua/article/352.

14. Загрози інформаційної безпеки. URL: https://searchinform.ru/informatsionnaya-bezopasnost/osnovy-ib/ugrozy-informatsionnoj-bezopasnosti

15. Збитки від віруса WannaCry. URL: https://www.rbc.ua/rus/news/ushcherb-virusa-wannacry-otsenili-1-mlrd-1495683784.html

16. Загрози інформаційної безпеки. URL: https://searchinform.ru/informatsionnaya-bezopasnost/osnovy-ib/ugrozy-informatsionnoj-bezopasnosti/

17. Ризики кібербезпеки в кіберспорті URL:https://thebridge.in/esports/esports-cybersecurity-risks-how-stay-protected/

18.Віртуальна приватна мережа URL: https://sites.google.com/site/zahistlokalnoiemerezi/zahist/virtualna-privatna-mereza

19. PGL Major Stockholm 2021 URL: https://liquipedia.net/counterstrike/PGL/2021/Stockholm

20. Privacy and Gaming. How to setup a private VPN and a VLAN on a single machine URL: https://forum.level1techs.com/t/guide-openvpn-for-security-privacy-and-gaming-how-to-setup-a-private-vpn-and-a-vlan-on-a-single-machine/140013

21. «Делойт». Управление рисками. Правила игры меняются. URL: https://www2.deloitte.com/content/dam/Deloitte/ru/Documents/risk/russian/rules-of-game-changing.pdf.

22. Федерация европейских ассоциаций риск менеджеров. Стандарты управления рисками. – URL: https://www.ferma.eu/app/uploads/2011/11/a-risk-management-standard-russian-version.pdf.

23. Обработка рисков информационной безопасности. URL: https://www.securitylab.ru/blog/personal/aguryanov/30003.php.

24. Невизначеність та ризик. URL: http://www.risk24.ru/neopred.htm.

25. Беспалова О. В. Отличительные особенности понятий «неопределенность» и «риск». URL: https://cyberleninka.ru/article/n/otlichitelnye-osobennosti-ponyatiy-neopredelennost-risk/viewer.

26. Критерий среднего выигрыша. URL: https://studopedia.su/18_5233_kriteriy-srednego-viigrisha.html.

27. Рейтинг украинских CS: GO-коллективов на портале HLTV.org. URL: https://tsn.ua/ru/cybersport/reyting-ukrainskih-cs-go-kollektivov-na-portale-hltv-org-1788478.html

28. How can esports players protect themselves against security risks? URL: https://win.gg/news/how-can-esports-players-protect-themselves-against-security-risks-question-mark/

29. Threats to the Esports Industry. URL: https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/cheats-hacks-and-cyberattacks-threats-to-the-esports-industry-in-2019-and-beyond

30. E-sports is a billion-dollar industry—it could be a risky one. URL: https://www.verisk.com/insurance/visualize/e-sports-is-a-billion-dollar-industry-it-could-be-a-risky-one-too/

31. Esports Industry Analysis. URL: https://medium.com/stg-blog/esports-industry-swot-analysis-6d8265a9fe54

32. The Latest Trends and Threats in the Esports Entertainment Industry. URL: https://thegameofnerds.com/2021/01/09/the-latest-trends-and-threats-in-the-esports-entertainment-industry/

33. CYBER SECURITY FOR EGAMING & ESPORTS. URL: https://riela-cyber.com/esports-and-egaming-cyber-security/

34. IT Operations Analytics for eGames & eSports. URL: https://www.extrahop.com/solutions/industry/egaming/

35. Esports gaming skills pave the way for cybersecurity careers. URL: https://portswigger.net/daily-swig/esports-gaming-skills-pave-the-way-for-cybersecurity-careers

36. The Cost-Effective Path to Meeting All eSports Security Requirements. URL: https://theiabm.org/the-cost-effective-path-to-meeting-all-esports-security-requirements/

37. US Cyber Games and TikTok turn cybersecurity into an esport. URL: https://venturebeat.com/2021/08/02/us-cyber-games-and-tiktok-make-an-esport-out-of-cybersecurity/

38. How Cyber Security is Bringing Value to Esports. URL: https://thedalesreport.com/esports/internet-security-brings-value-to-esports/

39. eSports and Data Privacy: A Game Worth Winning. URL: https://www.dentons.com/en/insights/articles/2020/november/24/esports-and-us-data-privacy-a--game-worth-winning

40.Kaspersky becomes brand’s Esports team partner. URL: https://www.kaspersky.com/about/press-releases/2021_kaspersky-extends-partnership-with-scuderia-ferrari-and-becomes-brands-esports-team-partner

41. Playing with privacy? Privacy and cybersecurity considerations in esports. URL: https://esportsinsider.com/2021/06/playing-with-privacy-privacy-and-cybersecurity-considerations-in-esports/

42. Optimise the Gaming experience using IBM Tech. URL: https://www.ibm.com/sites/b/eSports

43. Will Cybersecurity Become a Popular eSport? URL: https://www.makeuseof.com/cybersecurity-popular-esport/

44. Filling in the Security Gaps within Esports! URL: https://www.esportssafeguards.com/

45. Выбор оптимальной стратегии защиты компании. URL: http://www.lghost.ru/lib/security/kurs2/theme04_chapter03.htm.

46. Safran. An introduction to qualitative risk analysis. URL: https://www.safran.com/content/introduction-qualitative-risk-analysis.

47. Esports tournaments facing huge cyber-attack threats. URL: https://www.techradar.com/news/esports-tournaments-facing-huge-cyberattack-threats

48. Switches are the MVP of eSports. URL: https://www.dlink.com.au/Switches%20are%20the%20MVP%20of%20eSports

49. Cloud Hacking eSports. URL: https://www.cloudsecuritypodcast.tv/season-2/cloud-hacking-esports-ultimate-hacking-championship

50. Engineering Safety Consultants. Quantitative risk assessment – QRA. URL: https://esc.uk.net/quantitative-risk-assessment/.

51. Software Engineering Institute. Introducing OCTAVE Allegro: Improving the information security risk assessment process. URL: https://resources.sei.cmu.edu/library/asset-view.cfm?assetID=8419.

52. Современные методы и средства анализа и управления рисками информационных систем компаний. URL: http://citforum.ru/products/dsec/cramm/cramm1.shtml.

53. Microsoft Solutions for Security and Compliance. The Security Risk Management Guide. San Francisco: Microsoft Corporation, 2006. 129 p

54. Effective Risk Analysis. URL: https://csrc.nist.gov/csrc/media/publications/conference-paper/2000/10/19/proceedings-of-the-23rd-nissc-2000/documents/papers/304slide.pdf.

55. Классификация угроз Digital Security (Digital Security Classification of Threats). URL: http://www.dsec.ru/products/grif/fulldesc/classification.

56. Staying Secure While Online: An eSports Security Guide. URL: https://thechrisvossshow.com/staying-secure-while-online-an-esports-security-guide/

57. Anybrain receives €1 million investment from Trust Esport. URL: https://gamingstreet.com/anybrain-receives-e1-million-investment-from-trust-esport/

58. An introduction to qualitative risk analysis. URL: https://www.safran.com/content/introduction-qualitative-risk-analysis.

59. 8 Online Gaming Security Risks – Are You Protected? URL: https://www.pandasecurity.com/en/mediacenter/security/online-gaming-risks/

60. Cheats, hacks, and cyber-attacks: Esports cybercrime. URL: https://portswigger.net/daily-swig/cheats-hacks-and-cyber-attacks-esports-cybercrime-poised-to-soar

Додаток А

Перелік загроз для даних при проведенні кіберспортивних змагань, результати оцінки очікуваних втрат і заходи з рішеннями щодо їх усунення

Таблиця А.1

Перелік загроз, що становлять потенційну небезпеку для даних

Ресурс	AV	Загроза	Модель порушника	EF	ARO	SLE	ALE
1	2	3	4	5	6	7	8
Контролер домену	3	Загроза отримання повного віддаленого контролю за системою	A1, B2	3	2	9	18
		Загроза порушення цілісності, правильного функціонування системи.	A1, B2, C1, C2	3	3	9	27
		Загроза порушення доступності системи	A1, B2, C1	3	2	9	18
		Підміна мережевої адреси.	A1, B2	3	3	9	27
		Фізичне ушкодження апаратних засобів	B1	1	1	3	3

Продовження табл. А.1

1	2	3	4	5	6	7	8
Ігрові сервери	3	Загроза отримання повного дистанційного контролю над системою.	A1, B2	3	2	9	18
		Можливість негласного отримання та розголошення (публікація) інформації, що захищається.	A1, B2, C1	2	2	6	12
		Загроза порушення цілісності, правильного функціонування системи.	A1, B2, C1, C2	3	3	9	27
		Загроза порушення доступності системи.	A1, B2, C1	3	2	9	18
		Підміна мережевої адреси	A1, B2	3	3	9	27
		Фізичне пошкодження апаратних засобів	B1	1	1	3	3

Продовження табл. А.1

1	2	3	4	5	6	7	8
Робочі сервери	3	Загроза отримання повного дистанційного контролю над системою.	A1, B2	3	2	9	18
		Загроза порушення цілісності, правильного функціонування системи.	A1, B2, C1, C2	3	2	9	18
		Загроза порушення доступності системи.	A1, B2, C1	3	2	9	18
		Підміна мережевої адреси	A1, B2	3	3	9	27
		Загроза отримання повного віддаленого контролю за системою	A1, B2	2	2	6	12

Продовження табл. А.1

1	2	3	4	5	6	7	8
Маршрутизатор	3	Загроза порушення цілісності, правильного функціонування системи.	A1, B2, C1, C2	2	2	6	12
		Загроза порушення доступності системи	A1, B2, C1	3	2	9	18
		Підміна мережевої адреси.	A1, B2	3	3	9	27
		Фізичне ушкодження апаратних засобів.	B1	1	1	3	3
		Загроза отримання повного віддаленого контролю за системою	A1, B2	2	2	6	12
Комутатор	3	Загроза порушення цілісності, правильного функціонування системи.	A1, B2, C1, C2	2	2	6	12
		Загроза порушення доступності системи	A1, B2, C1	3	2	9	18
		Загроза	Модель порушника	EF	ARO	SLE	ALE
Ресурс	AV	Підміна мережевої адреси.	A1, B2	3	3	9	27

Продовження табл. А.1

1	2	3	4	5	6	7	8
Комутатор	3	Фізичне ушкодження апаратних засобів.	B1	1	1	3	3
		Загроза отримання повного дистанційного контролю над системою.	A1, B2	3	2	3	6
Робочі місця представників організатор та менеджерів	1	Загроза порушення цілісності, правильного функціонування системи.	A1, C1, C2	3	3	3	9
		Загроза порушення доступності системи.	A1, C1	3	2	3	6
		Підміна мережевої адреси	A1	3	3	3	9
		Фізичне пошкодження апаратних засобів	A1, B1	3	2	3	6
		Загроза витоку видової інформації	A1, B1	3	2	3	6
		Загроза перехоплення мережевого трафіку з метою подальшого аналізу	A1, C1	3	1	9	9
Канал зв'язку	3	Фізичне пошкодження	A1, C2	3	2	9	18

Технічні та організаційні заходи усунення інформаційних загроз:

Сервера:

Таблиця А.2

Заходи щодо усунення інформаційних загроз серверів

Загроза	Технічне рішення	Організаційне рішення
1	2	3
Загроза отримання повного віддаленого контролю за системою	Своєчасне оновлення операційної системи Розгортання ліцензійного антивірусного ПЗ Фільтрування мережного трафіку, довірений список портів. Застосування жорстких шаблонів безпеки. Періодична перевірка рівня безпеки (використання спеціалізованих сканерів) Налаштування системи виявлення вторгнень (на рівні маршрутизатора cisco)	Інструкція по оновленню серверних систем. Інструкція з антивірусного захисту серверних систем. Інструкція з парольного захисту. Регламент ІБ.
Загроза порушення цілісності, правильного функціонування системи.	Своєчасне оновлення операційної системи Розгортання ліцензійного антивірусного програмного забезпечення Регулярне резервне копіювання Тестування оновлень на спеціалізованих комп'ютерах для виявлення можливих проблем	Інструкція по оновленню серверних систем. Інструкція з антивірусного захисту серверних систем. Інструкція з резервного копіювання серверних систем.
Загроза порушення доступності системи	Забезпечення резервного харчування. Наявність резервного сервера. Контроль доступу до серверного приміщення.	Регламент ІБ.

Продовження табл. А.2

1	2	3
Підміна мережевої адреси.	Виведення в окремий сегмент мережі. Впровадження системи сертифікатів (налаштування аутентифікації лише на рівні комутаторів для аутентифікації робочих станцій). Portsecurity на комутаторах cisco	Регламент ІБ.
Фізичне ушкодження апаратних засобів.	Контролює температуру, вологість серверного приміщення. Забезпечення резервного харчування. Контроль доступу до серверного приміщення.	Інструкція з експлуатації обладнання. Регламент ІБ.

Маршрутизатор:

Таблиця А.3

Заходи щодо усунення інформаційних загроз маршрутизаторів

Загроза	Технічне рішення	Організаційне рішення
1	2	3
Загроза отримання повного віддаленого контролю за системою	Своєчасне оновлення. Виведення керуючого інтерфейсу окремий сегмент мережі. Використання ssh. Використання стійких паролів.	Інструкція з парольного захисту. Регламент ІБ.
Загроза порушення цілісності, правильного функціонування системи.	Своєчасне оновлення Регулярне резервне копіювання конфігурації	Інструкція по оновленню серверних систем. Інструкція з резервного копіювання.
Загроза порушення доступності системи	Забезпечення резервного харчування. Наявність резервного маршрутизатора. Резервування конфігурації устаткування. Контроль доступу.	Регламент ІБ.

Продовження табл. А.3

1	2	3
Фізичне ушкодження апаратних засобів.	Забезпечення резервного харчування. Контроль доступу.	Регламент ІБ.

Комутатор:

Таблиця А.4

Заходи щодо усунення інформаційних загроз комутаторів

Загроза	Технічне рішення	Організаційне рішення
1	2	3
Загроза порушення цілісності, правильного функціонування системи.	Застосування ACL листів. Фільтрація трафіку за списком довірених портів. Використання надійних паролів. Впровадження системи аудиту.	Інструкція з парольного захисту Регламент ІБ.
Загроза порушення доступності системи	Забезпечення резервного харчування. Наявність резервного комутатора. Резервування конфігурації устаткування. Контроль доступу.	Регламент ІБ.
Фізичне ушкодження апаратних засобів.	Забезпечення резервного харчування. Контроль доступу.	Регламент ІБ.

Робочі місця представників організатор та менеджерів:

Таблиця А.5

Заходи щодо усунення інформаційних загроз робочих місць представників організатор та менеджерів

Загроза	Технічне рішення	Організаційне рішення
1	2	3
Загроза отримання повного віддаленого контролю за системою	Своєчасне оновлення операційної системи. Розгортання ліцензійного антивірусного ПЗ. Настроювання персонального міжмережевого екрану. Застосування політик безпеки.	Інструкція по оновленню операційних систем. Інструкція з антивірусного захисту. Інструкція з парольного захисту. Регламент ІБ.
Загроза порушення цілісності, правильного функціонування системи.	Своєчасне оновлення операційної системи. Розгортання ліцензійного антивірусного ПЗ. Регулярне резервне копіювання.	Інструкція по оновленню операційних систем. Інструкція з антивірусного захисту. Інструкція з резервного копіювання.
Загроза порушення доступності системи	Забезпечення резервного харчування. Наявність резервного копіювання.	

Продовження табл. А.5

1	2	3
Підміна мережевої адреси.	Виведення в окремий сегмент мережі. Впровадження системи сертифікатів (налаштування аутентифікації лише на рівні комутаторів для аутентифікації робочих станцій). Налаштування аутентифікації за протоколом eap на базі мережного обладнання та робочих станцій. Налаштування portsecurity на комутаторах.	Регламент ІБ.
Фізичне ушкодження апаратних засобів.	Забезпечення резервного харчування. Контроль доступу до приміщення.	Інструкція з експлуатації робочого місця.
Загроза витоку видової інформації	Контроль доступу до приміщення. Правильне розташування моніторів на робочих місцях. Примусове увімкнення заставок екрану	Інструкція з парольного захисту

Канал зв'язку:

Таблиця А.6

Заходи щодо усунення інформаційних загроз каналів зв'язку

Загроза	Технічне рішення	Організаційне рішення
1	2	3
Загроза перехоплення мережевого трафіку з метою подальшого аналізу	Організація IPsec site-to-site vpn	Регламент ІБ. Інструкції по підключенню віддалених місць розташування та філій.
Фізичне ушкодження	Організація резервного каналу зв'язку	Інструкція з підключення віддалених місць та філій.

Додаток Б

Результати дослідження комплексного забезпечення інформаційної безпеки кіберспортивного змагання (на базі розглянутого прикладу)

За рахунок наступних заходів вдалося знизити загрозу отримання повного віддаленого контролю над системою для ігрових та робочих серверів:

· Своєчасне оновлення операційної системи

· Розгортання ліцензійного антивірусного ПЗ

· Фільтрування мережного трафіку.

· Періодична перевірка рівня безпеки

· Інструкція з антивірусного захисту серверних систем.

· Інструкція з парольного захисту.

· Регламент ІБ

За рахунок наступних заходів вдалося знизити загрозу порушення цілісності, правильного функціонування системи для ігрових та робочих серверів:

· Своєчасне оновлення операційної системи

· Розгортання ліцензійного антивірусного ПЗ

· Регулярне резервне копіювання

· Інструкція з антивірусного захисту серверних систем.

· Інструкція з резервного копіювання серверних систем.

За рахунок наступних заходів вдалося знизити загрозу порушення доступності системи для ігрових та робочих серверів:

· Забезпечення резервного харчування.

· Наявність резервного сервера.

· Контроль доступу до серверного приміщення.

· Регламент ІБ.

За рахунок наступних заходів вдалося знизити загрозу підміни мережевої адреси для ігрових та робочих серверів:

· Виведення в окремий сегмент мережі

· Впровадження системи сертифікатів

· Регламент ІБ.

За рахунок наступних заходів вдалося знизити загрозу фізичного пошкодження апаратних засобів для ігрових та робочих серверів:

· Контролює температуру, вологість серверного приміщення.

· Забезпечення резервного харчування.

· Контроль доступу до серверного приміщення.

· Регламент ІБ.

За рахунок наступних заходів вдалося знизити загрозу отримання повного віддаленого контролю над системою для Маршрутизаторів:

· Виведення керуючого інтерфейсу окремий сегмент мережі.

· Використання ssh.

· Інструкція з парольного захисту.

За рахунок наступних заходів вдалося знизити загрозу порушення цілісності, правильного функціонування системи для Маршрутизаторів:

· Своєчасне оновлення

· Регулярне резервне копіювання конфігурації.

· Інструкція з резервного копіювання.

За рахунок наступних заходів вдалося знизити загрозу порушення доступності системи для Маршрутизаторів:

· Забезпечення резервного електроживлення.

· Наявність резервного електроживлення.

· Резервування конфігурації устаткування.

· Контроль доступу.

· Інструкція з резервного копіювання.

За рахунок наступних заходів вдалося знизити загрозу фізичного пошкодження апаратних засобів для Маршрутизаторів:

· Забезпечення резервного електроживлення.

· Контроль доступу.

За рахунок наступних заходів вдалося знизити загрозу порушення цілісності, правильного функціонування системи для Комутаторів:

· Застосування листів ACL.

· Фільтрування трафіку за довіреним списком портів.

· Використання стійких паролів.

· Інструкція з парольного захисту.

За рахунок наступних заходів вдалося знизити загрозу порушення доступності системи для Комутаторів:

· Забезпечення резервного електроживлення.

· Наявність резервного комутатора.

· Резервування конфігурації устаткування.

· Контроль доступу.

· Регламент ІБ.

За рахунок наступних заходів вдалося знизити загрозу фізичного пошкодження апаратних засобів для Комутаторів:

· Забезпечення резервного електроживлення.

· Контроль доступу.

За рахунок наступних заходів вдалося знизити загрозу отримання повного віддаленого контролю над системою для робочих місць представників організатора та менеджерів:

· Своєчасне оновлення операційної системи.

· Розгортання ліцензійного антивірусного ПЗ.

· Застосування політик безпеки.

· Інструкція з антивірусного захисту.

· Інструкція з парольного захисту.

· Регламент ІБ.

За рахунок наступних заходів вдалося знизити загрозу порушення цілісності, правильного функціонування системи для робочих місць представників організатора та менеджерів:

· Своєчасне оновлення операційної системи.

· Розгортання ліцензійного антивірусного ПЗ.

· Інструкція з антивірусного захисту.

За рахунок наступних заходів вдалося знизити загрозу порушення доступності системи для робочих місць представників організатора та менеджерів:

· Забезпечення резервного харчування.

· Наявність резервного робочого місця.

За рахунок наступних заходів вдалося знизити загрозу підміни мережевої адреси для робочих місць представників організатора та менеджерів:

· Виведення в окремий сегмент мережі.

· Впровадження системи сертифікатів

· Регламент ІБ.

За рахунок наступних заходів вдалося знизити загрозу фізичного пошкодження апаратних засобів для робочих місць представників організатора та менеджерів:

· Забезпечення резервного харчування.

· Контроль доступу до приміщення.

За рахунок наступних заходів вдалося знизити загрозу витоку видової інформації для робочих місць представників організатора та менеджерів:

· Контроль доступу до приміщення.

· Правильне розташування моніторів на робочих місцях.

· Примусове увімкнення заставок екрану

За рахунок наступних заходів вдалося знизити загрозу перехоплення мережевого трафіку з метою подальшого аналізу для каналів зв'язку:

· Організація Ipsec site-to-site vpn

· Регламент ІБ

· Інструкція з підключення віддалених місць та філій.

За рахунок наступних заходів вдалося знизити загрозу фізичного пошкодження для каналів зв'язку:

· Організація резервного каналу зв'язку

· Інструкція з підключення віддалених місць та філій.