МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЗАПОРІЗЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет журналістики
Кафедра соціальних комунікацій та інформаційної діяльності

КВАЛІФІКАЦІЙНА РОБОТА БАКАЛАВРА

на тему «Інструменти інфомедійної безпеки в умовах воєнного стану»

Виконала студентка 5 курсу
групи 6.0618-ІС
спеціальності 029 Інформаційна, бібліотечна
та архівна справа
ОП «Інформаційно-комунікаційна справа»
Візнюк О.В.
Керівник – доцент, канд. філол. наук
Іванюха Т.В.
Рецензент – доцент, канд. філол. наук
Романюк Н.В.

Запоріжжя – 2023

ЗМІСТ

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЗАПОРІЗЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет журналістики
Кафедра соціальних комунікацій та інформаційної діяльності
Рівень вищої освіти бакалаврський
Спеціальність 029 Інформаційна, бібліотечна та архівна справа
ОПП Інформаційно-комунікаційна справа

ЗАТВЕРДЖУЮ
Завідувач кафедри
Березенко В.В.
_____
«__»_____2023 року

З А В Д А Н Н Я
НА ДИПЛОМНУ РОБОТУ СТУДЕНТУ

Візнюк Олені Вікторовні

1. Тема роботи (проекту) «Інсрументи інфомедійної безпеки в умовах воєнного стану»
керівник роботи (проєкту) Іванюха Тетяна Валеріївна, к.філол.н., доцент,
затверджені наказом ЗНУ від «30» грудня 2022 року № 1904-с.
2. Строк подання студентом роботи 15 травня 2023 року.
3. Вихідні дані до роботи праці вітчизняних та зарубіжних медіадослідників В. Ананьїна, О. Андреєва, І. Бінько, В. Бортнікова, М. Волощук, А.Гриценко, І. Дорошенко, В.Онищенко та інших.
4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити): 1) дослідити поняття інформаційної безпеки та проаналізувати головні засади її досягнення в умовах воєнного стану;
2) розглянути основні різновиди інформаційних операцій і атак та та методи протистояння їм;
3) проаналізувати використання інформаційних технологій та їх вплив на інформаційну безпеку країни;
4) виявити основні інструменти інфомедійного захисту та охарактеризувати особливості їх застосування.
5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень) –

6. Консультанти розділів роботи (проєкту):

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Перший розділ	Іванюха Т.В., доцент	02.10.2022	02.10.2022
Другий розділ	Іванюха Т.В., доцент	12.12.2022	12.12.2022
Вступ, висновки	Іванюха Т.В., доцент	03.03.2023	03.03.2023

7. Дата видачі завдання _____

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Строк виконання	Примітка
1.	Пошук наукових джерел з теми дослідження, їх вивчення та аналіз; укладання бібліографії	Жовтень 2022 р.	Виконано
2.	Збір матеріалів для аналізу	Листопад-грудень 2022 р.	Виконано
3.	Підготовка Розділу 1	Січень 2023 р.	Виконано
4.	Написання Розділу 2	Березень 2023 р.	Виконано
5.	Формулювання вступу, висновків, оформлення роботи	Квітень 2023 р.	Виконано
6.	Одержання відгуку та рецензії, проходження нормоконтролю	Травень 2023 р.	Виконано
7.	Захист роботи	Травень 2023 р.	Виконано

Студент _____ _____
(підпис) (ініціали та прізвище)

Керівник роботи _____ _____
(підпис) (ініціали та прізвище)

Нормоконтроль пройдено
Нормоконтролер _____ _____
(підпис) (ініціали та прізвище)

РЕФЕРАТ

Кваліфікаційна робота бакалавра «Інструменти інфомедійної безпеки в умовах воєнного стану» – основний текст – 48 сторінок. Для виконання дипломної роботи опрацьовано 53 джерела.

Об'єкт дослідження: інструменти інформаційної безпеки в умовах воєнного стану.

Предмет дослідження: система забезпечення інформаційної безпеки в умовах воєнного стану.

Мета роботи: виявити провідні інструменти інформаційної безпеки в умовах воєнного стану в контексті сучасного інформаційного та воєнного протистояння.

Методи дослідження: для аналізу інформаційних технологій у військових операціях було використано такі методи: аналіз, описовий метод, аналіз літературних джерел, кейс-стаді, порівняльний аналіз, системний підхід.

Для реалізації поставленої мети необхідно виконати такі **завдання:**

5) дослідити поняття інформаційної безпеки та проаналізувати головні засади її досягнення в умовах воєнного стану;

6) розглянути основні різновиди інформаційних операцій і атак та та методи протистояння їм;

7) проаналізувати використання інформаційних технологій та їх вплив на інформаційну безпеку країни;

8) виявити основні інструменти інфомедійного захисту та охарактеризувати особливості їх застосування.

Методологічну і теоретичну основу дослідження складають праці, присвячені розгляду проблем інформаційної безпеки та інформаційного протиборства дослідників В.Ананьїна, О.Андреєва, О. Волощук, Г.Горяйнової, О.Гуляєва, Я.Жаркова, С.Квіта, Ю.Король, М.Лепського, В.Мітюхіна, Г.Почепцова, М.Присяжнюка, О.Шаповал та інших.

Наукова новизна одержаних результатів полягає в тому, що ця робота висвітлює сучасний стан використання інформаційних технологій у військових діях та їх вплив на інформаційну безпеку країни, пропонує аналіз ризиків та проблем, а також рекомендації щодо підвищення безпеки в умовах воєнного стану.

Сфера застосування: Матеріали дослідження можуть бути використані під час подальших наукових розробок, викладання навчальних дисциплін, пов’язаних з відповідною тематикою, при написанні курсових та дипломних робіт студентами факультету журналістики.

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ, ВІЙСЬКОВІ ДІЇ, ІНФОРМАЦІЙНА БЕЗПЕКА, КІБЕРАТАКИ, ВОЄННИЙ СТАН, КІБЕРБЕЗПЕКА

ВСТУП

У сучасному світі, де інформаційні технології займають велике місце в різних сферах життя, вони також мають значний вплив на військові дії та національну безпеку країни. В умовах воєнного стану інформаційна безпека стає особливо актуальною, оскільки ворог може використовувати кібератаки, кібершпигунство та інші методи для завдання шкоди важливим інформаційним системам та інфраструктурі.

В умовах сучасного світу інформаційна безпека є надзвичайно важливою складовою національної безпеки кожної країни. Умови воєнного стану вносять значні корективи у систему забезпечення інформаційної безпеки країни. У таких умовах інформаційні загрози збільшуються, а владні органи повинні мати належні засоби для ефективної боротьби з ними, що і зумовлює **актуальність роботи.**

Особливої уваги на сучасному етапі вимагають основні загрози, з якими стикається країна в умовах воєнного конфлікту, включаючи кібератаки на енергетичні системи, фінансові установи, комунікаційні мережі та військові об'єкти, а також можливі наслідки, такі як порушення функціонування електронних систем, зниження економічної активності, загроза життю і здоров'ю людей, порушення правопорядку та інші соціально-економічні проблеми, які можуть виникнути в результаті кібератак в умовах воєнного стану. Питання інформаційної безпеки в умовах інформаційного протиборства порушували у своїх працях чимало дослідників та науковців, зокрема, В. Ананьїн, В. Березенко, В. Бортніков, В. Горбатенко, М. Лепський, О. Пучков, О. Семенець та багато інших, однак у їхніх дослідженнях не враховані умови «гарячої війни» та найвищого рівня інформаційної небезпеки.

Мета роботи: виявити провідні інструменти інформаційної безпеки в умовах воєнного стану в контексті сучасного інформаційного та воєнного протистояння.

Для реалізації поставленої мети необхідно виконати такі **завдання:**

1) дослідити поняття інформаційної безпеки та проаналізувати головні засади її досягнення в умовах воєнного стану;

2) розглянути основні різновиди інформаційних операцій і атак та та методи протистояння їм;

3) проаналізувати використання інформаційних технологій та їх вплив на інформаційну безпеку країни;

4) виявити основні інструменти інфомедійного захисту та охарактеризувати особливості їх застосування.

Об’єкт дослідження: інструменти інформаційної безпеки в умовах воєнного стану.

Предмет дослідження: система забезпечення інформаційної безпеки в умовах воєнного стану.

Методи дослідження: використано такі методи дослідження, як аналіз наукових джерел, що дав змогу ознайомитися з попередніми науковими дослідженнями та теоретичними концепціями щодо використання інформаційних технологій у військових діях та їх впливу на інформаційну безпеку, кейс-стаді дозволяє аналізувати конкретні випадки використання інформаційних технологій у воєнних сценаріях та оцінювати їх ефективність і наслідки, порівняльний аналіз дав змогу порівнювати різні країни, періоди часу або стратегії використання інформаційних технологій у військових діях і визначати спільні тенденції або різницю у підходах, системний підхід був використаний для аналізу і визначення взаємозв'язків між різними складовими системи військових дій та інформаційної безпеки. Також були використані методи опису, узагальнення та метод системного аналізу.

Методологічну і теоретичну основу дослідження складають праці, присвячені розгляду проблем інформаційної безпеки та інформаційного протиборства дослідників В.Ананьїна, О.Андреєва, О. Волощук, Г.Горяйнової, О.Гуляєва, Я.Жаркова, С.Квіта, Ю.Король, М.Лепського, В.Мітюхіна, Г.Почепцова, М.Присяжнюка, О.Шаповал та інших.

Наукова новизна одержаних результатів полягає в тому, що дослідження розкриває сутність та особливості кібератак у воєнних умовах, аналізує загрози для національної безпеки, описує методи та засоби кіберзахисту, а також розглядає можливі наслідки цих атак. Висновки дослідження висувають нові ідеї та рекомендації щодо підвищення ефективності захисту від інформаційних атак у воєнних умовах.

Практичне значення одержаних результатів. Матеріали дослідження можуть бути використані під час подальших наукових розробок, викладання навчальних дисциплін, пов’язаних з відповідною тематикою, при написанні курсових та дипломних робіт студентами факультету журналістики.

Структура: кваліфікаційна робота бакалавра складається зі вступу, двох розділів, висновків, списку використаних джерел. Обсяг основної роботи – 45 сторінок. Список використаної літератури включає 50 найменувань (викладених на 5 сторінках).

РОЗДІЛ 1
ТЕОРЕТИЧНІ ЗАСАДИ ПРОТИСТОЯННЯ ІНФОРМАЦІЙНИМ ТЕХНОЛОГІЯМ У ВОЄННИЙ ЧАС

1.1 Основні поняття та принципи інформаційної безпеки

Інформаційна безпека – це комплекс заходів, спрямованих на захист інформації від несанкціонованого доступу, використання, зміни, видалення та знищення, з метою забезпечення її конфіденційності, цілісності та доступності.

Основні поняття, які використовуються в контексті інформаційної безпеки, включають:

1. **Інформація** – це будь-які дані, які можуть бути оброблені за допомогою електронних, механічних або інших технічних засобів.У контексті інформаційної безпеки, інформацію можна визначити як будь-які дані, що передаються, зберігаються або обробляються в електронному, паперовому або іншому форматі. Це може бути текст, зображення, звук, відео, або будь-який інший тип даних.

Основне завдання інформаційної безпеки полягає в тому, щоб забезпечити захист інформації від несанкціонованого доступу, використання, зміни або руйнування. Для досягнення цієї мети використовуються різні технічні та організаційні заходи, які включають у себе шифрування, автентифікацію, контроль доступу та інші.Основна мета інформаційної безпеки – забезпечення конфіденційності, цілісності та доступності інформації. Конфіденційність означає, що інформація доступна лише обмеженому колу осіб, які мають право на її знання. Цілісність означає, що інформація зберігається та передається без змін та порушень. Доступність означає, що інформація доступна користувачам в потрібний момент та має відповідний рівень якості.

В інформаційній безпеці інформація є важливим ресурсом, який потрібно захищати. Конфіденційна інформація, така як персональні дані, бізнес–секрети або державні таємниці, є особливо вразливими і потребують додаткових заходів

захисту. Окрім того, інформаційна безпека повинна забезпечувати захист інформації від різних загроз, таких як несанкціонований доступ, шпигунство, злам, вірусні атаки та інші. Захист інформації забезпечується за допомогою застосування різноманітних технологій, таких як криптографія, аутентифікація, авторизація, контроль доступу, аудит та інші.

Також, важливо знати, що інформація може бути вразливою внаслідок людських помилок або несанкціонованої дії, такої як хакерські атаки або соціальний інжиніринг. Тому, одним з найважливіших аспектів інформаційної безпеки є підвищення свідомості користувачів та навчання їх основам кібербезпеки.

Отже, інформація в контексті інформаційної безпеки – це основний об'єкт захисту, який вимагає застосування різних технологій та принципів захисту для забезпечення конфіденційності, цілісності та доступності.

2. **Конфіденційність** – це властивість інформації, яка гарантує, що вона буде доступна лише обмеженому колу осіб, які мають на це дозвіл. Конфіденційність інформації може бути забезпечена за допомогою різних технічних та організаційних заходів. Конфіденційність є одним із основних принципів інформаційної безпеки, який відображає ступінь захищеності інформації від несанкціонованого доступу. Під поняттям конфіденційності розуміють стан захищеності інформації від несанкціонованого доступу та розголошення.

Конфіденційна інформація повинна бути доступна тільки обмеженому колу осіб, які мають необхідне дозволення на її отримання та оброблення. Конфіденційність забезпечується за допомогою різноманітних методів захисту, таких як шифрування, автентифікація користувачів, контроль доступу та інші.

Особливу увагу до забезпечення конфіденційності інформації приділяють у сферах, які пов'язані з національною безпекою, оборонною промисловістю, банківською справою, медициною, державному управлінні, а також у сфері комерції та бізнесу.

З метою забезпечення конфіденційності, слід використовувати заходи захисту, такі як шифрування, контроль доступу, аутентифікація користувачів, збереження даних на захищених носіях, захист мережі від несанкціонованого доступу та інші. Важливо забезпечити не тільки технічний захист, але й правильно організувати роботу з інформацією, контролювати дії користувачів, вести моніторинг та аудит інформаційної безпеки. Для забезпечення конфіденційності необхідно встановити дієві заходи захисту, такі як регулювання прав доступу до інформації, контроль доступу, аудит безпеки, криптографічний захист інформації, захист інформації під час транспортування і зберігання.

При розробці стратегії інформаційної безпеки необхідно враховувати конфіденційність інформації та забезпечити її захист від несанкціонованого доступу. Організації повинні забезпечувати відповідність політики захисту інформації законодавству і вимогам стандартів.

3. **Цілісність** – це властивість інформації, яка гарантує, що вона не буде змінена без належної авторизації та контролю. Цілісність інформації може бути забезпечена за допомогою механізмів контролю цілісності та перевірки цифрових підписів. Цілісність в контексті інформаційної безпеки – це здатність зберігати інформацію в незмінному вигляді і захищати її від несанкціонованих змін. Це означає, що інформація повинна бути захищена від несанкціонованого доступу, модифікації або видалення.

Один з основних способів забезпечення цілісності інформації полягає в застосуванні методів контролю цілісності даних, таких як хеш-функції, цифрові підписи та інші методи контролю цілісності. Ці методи дозволяють перевірити, чи була змінена інформація після того, як вона була збережена.

Збереження цілісності інформації є важливою складовою інформаційної безпеки, оскільки порушення цілісності може призвести до втрати довіри до інформації, що може негативно вплинути на діяльність організації або іншого суб'єкта. Наприклад, втрата цілісності фінансової інформації може призвести до недостовірної звітності та іншої фінансової шахрайства. Тому збереження

цілісності інформації є важливим аспектом інформаційної безпеки і повинен бути реалізований за допомогою відповідних технологій та політик захисту інформації.

4. **Доступність** – це властивість інформації, яка гарантує, що вона буде доступна тим особам, які мають на це дозвіл. Доступність інформації може бути забезпечена за допомогою механізмів захисту від вірусів, захисту від DoS–атак та ін. По суті, це принцип інформаційної безпеки, що означає, що інформаційні ресурси та системи повинні бути доступні тільки авторизованим користувачам у разі необхідності, але в будь–який час, коли вони потребують цього. Забезпечення доступності інформаційних ресурсів є однією з ключових складових їх функціонування та успішної роботи організацій.

Організації повинні забезпечувати доступність інформаційних ресурсів у межах припустимої загальної кількості запитів, що надходять до системи, та захищати їх від перевантажень та збоїв. Важливо також забезпечувати доступність інформаційних ресурсів у випадку катастроф, аварій та інших непередбачених ситуацій.

Для забезпечення доступності інформаційних ресурсів необхідно використовувати заходи захисту від вірусів, хакерських атак та інших небезпек. Організації повинні також мати плани надзвичайних ситуацій та процедури відновлення роботи систем у разі їх відмови.

Доступність є важливим принципом інформаційної безпеки, оскільки від неї залежить робота організації та можливість її успішної діяльності. Водночас, недоступність інформаційних ресурсів може призвести до важких наслідків для організації та викликати значні фінансові втрати. Тому важливо забезпечувати доступність інформаційних ресурсів та систем з дотриманням вимог інших принципів інформаційної безпеки.

5. **Аутентифікація** – це процес перевірки ідентифікаційних даних користувача з метою встановлення його ідентичності та визначення рівня дозволів для доступу до ресурсів. Аутентифікація – це процес перевірки ідентифікаційних даних користувача з метою визначення його прав на доступ до

певної інформації або ресурсу. Цей процес забезпечує ідентифікацію користувача за допомогою унікальних ідентифікаторів, таких як ім'я користувача та пароль, біометричні дані, токени або сертифікати.

В інформаційній безпеці аутентифікація використовується для перевірки дійсності ідентифікаційних даних користувача перед наданням доступу до конфіденційної інформації або ресурсу. Це важливий механізм для запобігання несанкціонованому доступу до інформації, викраденню даних, а також забезпечення захисту від кібератак.

Для забезпечення ефективної аутентифікації, потрібно використовувати сильні паролі, двофакторну аутентифікацію, біометричні дані або інші методи, які забезпечують надійний рівень ідентифікації користувача. Крім того, важливо використовувати захист від підбору паролів та зберігати ідентифікаційні дані в безпечному місці.

Аутентифікація є одним з основних засобів захисту інформації в умовах воєнного стану, коли збільшується ризик несанкціонованого доступу до конфіденційної інформації. У таких умовах важливо використовувати найбільш сучасні технології аутентифікації та системи захисту, щоб забезпечити надійний захист від кібератак і зламів.

6. **Аудит** – система контролю та моніторингу дій користувачів з метою виявлення можливих загроз. Аудит в контексті інформаційної безпеки – це процес систематичного та незалежного огляду, перевірки та аналізу заходів забезпечення інформаційної безпеки організації з метою виявлення потенційних загроз та порушень інформаційної безпеки. Аудит є важливим елементом системи контролю за інформаційною безпекою, який дозволяє забезпечити дотримання політик, процедур та стандартів інформаційної безпеки.

Основні завдання аудиту інформаційної безпеки включають:

- виявлення порушень та загроз інформаційній безпеці;
- оцінка рівня ризику та розробка заходів щодо його зменшення;
- перевірка відповідності політик, процедур та стандартів інформаційної безпеки;

– виявлення слабких місць в системі захисту інформації та розробка рекомендацій щодо їх усунення;
– оцінка ефективності заходів забезпечення інформаційної безпеки.

Аудит інформаційної безпеки може бути внутрішнім (проводиться самою організацією) або зовнішнім (здійснюється сторонньою організацією). Внутрішній аудит дозволяє організації забезпечити високий рівень контролю за інформаційною безпекою та забезпечити відповідність внутрішніх політик та процедур вимогам стандартів інформаційної безпеки.

7. **Фізична безпека** – є однією з ключових складових інформаційної безпеки. Вона охоплює заходи та процедури, спрямовані на захист фізичних об'єктів, які містять конфіденційну інформацію або можуть бути використані для її отримання. Фізичні об'єкти, які вимагають захисту, можуть бути різного типу: офісні приміщення, дата–центри, серверні кімнати, склади тощо.

Основні елементи фізичної безпеки включають:

– контроль доступу – захист від несанкціонованого доступу до приміщення або обладнання шляхом встановлення системи контролю доступу, включаючи електронні картки, кодові замки та біометричні системи.

– відеоспостереження – встановлення камер відеоспостереження для контролю за доступом до об'єктів та забезпечення доказів в разі порушення безпеки.

– захист обладнання – фізичний захист обладнання від несанкціонованого доступу, відключення або викрадення шляхом установки замків, кабельних захистів та інших заходів.

– захист від стихійних лих – захист обладнання від знищення, пошкодження або втрати в разі стихійних лих, таких як пожежа, повінь, землетрус.

– захист від крадіжок – захист від крадіжок та викрадення відомостей та іншого майна, встановлення системи сигналізації, фізичне охоронення тощо.

Фізична безпека є надзвичайно важливою для забезпечення інформаційної безпеки в організаціях. Недостатня фізична безпека може призвести до витоку конфіденційної інформації.

Принципи інформаційної безпеки – це встановлені правила та стратегії, що використовуються для захисту конфіденційності, цілісності та доступності інформації в організаціях, урядових структурах та приватних секторах. Нижче розглянемо детальніше кожен з принципів інформаційної безпеки:

1. Принцип найменшого доступу: цей принцип передбачає, що доступ до інформації має бути наданий тільки необхідним особам та тільки в мінімально необхідному обсязі. Це забезпечує, що інформація буде захищена від несанкціонованого доступу та використання. Для реалізації цього принципу можуть використовуватися методи аутентифікації та авторизації користувачів, системи контролю доступу та інші заходи.

Принцип найменшого доступу – це принцип інформаційної безпеки, який передбачає обмеження рівня доступу до конфіденційної інформації лише до необхідного мінімуму для здійснення конкретної роботи чи виконання певної функції. Застосування цього принципу забезпечує зменшення ризиків порушення конфіденційності, цілісності і доступності інформації.

Принцип найменшого доступу має на меті запобігти неналежному використанню або зловживанню інформацією. Застосування цього принципу передбачає, що користувачам будуть надані лише ті рівні доступу, які необхідні для виконання їх робочих обов'язків і завдань. Надання вищих рівнів доступу повинно бути обґрунтованим і підтвердженим документально.

Застосування принципу найменшого доступу допомагає уникнути ситуацій, коли невідомі або неуповноважені особи мають доступ до конфіденційної інформації, а також зменшує ризик несанкціонованого внесення змін у систему чи програмне забезпечення. Окрім того, цей принцип є важливим для забезпечення доступності інформації, оскільки він дозволяє використовувати ресурси ефективніше і зменшує ризик перевантаження системи.

Принцип найменшого доступу є основою багатьох систем захисту інформації, таких як системи контролю доступу та системи управління правами користувачів. Дотримання цього принципу є необхідним у всіх сферах діяльності, де використовується конфіденційна інформація, включаючи фінансовий сектор.

2. Принцип конфіденційності: цей принцип передбачає захист інформації від несанкціонованого доступу, використання та розголошення. Це забезпечується за допомогою криптографічних методів, систем контролю доступу, фізичних заходів безпеки та інших заходів. Організації можуть використовувати різні заходи для захисту конфіденційної інформації, такі як шифрування, відокремлення, маркування, огляд та інші.

Принцип конфіденційності є одним з основних принципів інформаційної безпеки. Він передбачає забезпечення захисту інформації від несанкціонованого доступу та використання.

Захист конфіденційної інформації є особливо важливим у воєнний період, коли державна безпека та оборона мають вирішальне значення. Інформація може бути конфіденційною, якщо її розголошення може призвести до відкриття державної таємниці, порушення прав людини, збитку для держави або підприємства тощо. Захист конфіденційної інформації передбачає запобігання несанкціонованому доступу до неї, забезпечення її нерозголошення та захисту від втрати або зловживання. Конфіденційна інформація може включати такі дані, як особисті дані, комерційну інформацію, бізнес–таємниці, державні та військові таємниці та ін.

Заходи забезпечення конфіденційності можуть включати захист від несанкціонованого доступу до даних, шифрування даних та забезпечення контролю за доступом до інформації. Також можуть застосовуватися організаційні заходи, такі як регламентація доступу до даних, організація тренінгів та навчання персоналу з питань інформаційної безпеки та інші. Захист конфіденційної інформації може бути забезпечений за допомогою таких технічних та організаційних засобів, як шифрування даних, системи

аутентифікації та авторизації користувачів, забезпечення фізичної безпеки, обмеження доступу до інформації лише за необхідності та належним дозволом, застосування політики контролю доступу до інформації, внутрішньої звітності та інші.

Принцип конфіденційності має під собою велику кількість законодавчих норм та правил, які регулюють обіг та захист конфіденційної інформації. Водночас, важливим аспектом є також свідоме ставлення користувачів до захисту конфіденційної інформації, включаючи зміну паролів, встановлення міцних паролів, збереження конфіденційної інформації на безпечних носіях, непоширення її без належної потреби та інші. Важливо зазначити, що забезпечення конфіденційності інформації не є абсолютним і може бути порушено через технічні недоліки, людський фактор або соціально–психологічні методи атак. Тому важливо розробляти комплексну стратегію забезпечення конфіденційності інформації, що передбачає використання як технічних засобів, так і організаційних заходів, таких як навчання працівників, розробка процедур управління конфіденційною інформацією, аудит системи безпеки.

3. Принцип цілісності: цей принцип передбачає захист інформації від несанкціонованого змінення, видалення та втручання. Це забезпечується за допомогою захисту від вірусів, систем виявлення вторгнень та інших заходів. Організації можуть використовувати різні методи захисту цілісності інформації, такі як контроль цілісності даних, резервне копіювання, аудит інформації та інш.

Принцип цілісності є одним з основних принципів інформаційної безпеки, що передбачає збереження та захист цілісності інформації від несанкціонованого доступу, модифікації та втрати.

Цілісність інформації означає, що дані зберігаються і передаються в незміненому вигляді, без спотворень та втрати інформації. Принцип цілісності допомагає запобігти порушенням конфіденційності, а також гарантує правильність та достовірність інформації.

З метою забезпечення цілісності інформації застосовуються різні методи та технології, зокрема:

– Контроль цілісності даних: цей метод передбачає створення контрольної суми для кожного блоку даних, яка дозволяє виявити будь–які зміни в цих даних.

– Криптографічний захист: застосування криптографічних методів дозволяє захистити інформацію від несанкціонованого доступу та модифікації.

– Автентифікація та контроль доступу: ці методи дозволяють перевірити ідентичність користувача, що намагається отримати доступ до інформації, а також обмежити доступ до неї для несанкціонованих користувачів.

– Зберігання копій даних: збереження резервних копій даних дозволяє відновити відомості у випадку їх втрати або пошкодження.

Цілісність інформації означає, що дані повинні зберігатися і передаватися в безпечному стані і не підлягати змінам без належного дозволу. Якщо дані були змінені без належного дозволу, то цілісність інформації порушується, що може привести до серйозних наслідків.

Забезпечення цілісності інформації потребує використання таких технічних засобів, як системи контролю цілісності даних, системи контролю версій, системи контролю доступу, електронних підписів та інших.

Однак, важливо зазначити, що принцип цілісності може бути порушений не тільки технічними методами, але і через людський фактор, такий як зловживання повноваженнями, недбалість, недостатня кваліфікація або злочинні наміри.

Отже, для забезпечення цілісності інформації необхідно вживати комплексних заходів, що охоплюють як технічні засоби, так і організаційні заходи, такі як контроль за доступом до інформації, створення процедур зміни даних, моніторинг доступу до даних та ін.

4. Принцип доступності – цей принцип передбачає, що інформація повинна бути доступна за потребою користувачів. Принцип доступності (Availability) в інформаційній безпеці визначається як забезпечення того, що інформація та ресурси доступні користувачам у необхідному обсязі та вчасно.

Важливість принципу доступності полягає в забезпеченні можливості користувачів звертатися до інформації та ресурсів в будь–який момент часу, коли вони цього потребують. Недоступність інформації або ресурсів може призвести до втрати можливості вчасно приймати рішення, виконувати завдання, а також до великих збитків для бізнесу або інших організацій.

Щоб забезпечити доступність інформації та ресурсів, необхідно вживати заходів забезпечення стійкості систем та мереж перед негативним впливом зовнішніх та внутрішніх загроз, в тому числі технічних, організаційних та процедурних.

Серед технічних заходів можна відзначити:

- захист мереж та систем від DDOS–атак та інших внутрішніх та зовнішніх загроз;
- використання захисту від вірусів та інших шкідливих програм;
- застосування резервування та архівування даних, що забезпечує можливість відновлення даних у разі їх втрати або пошкодження.

Організаційні заходи полягають у розробці політики доступності, створенні процедур управління ризиками, плануванні аварійного відновлення, контролю доступу до інформації та ресурсів та управління змінами.

Процедурні заходи включають в себе регулярну перевірку наявності та ефективності механізмів.

1.2 Особливості інформаційної безпеки в умовах воєнного стану. Різновиди інформаційних операцій

Воєнний стан є загрозою національної безпеки будь-якої країни, оскільки він створює складну ситуацію для захисту населення, території та державних інтересів. У таких умовах інформаційна безпека стає ще більш актуальною, оскільки інформація є ключовим ресурсом для забезпечення національної безпеки в умовах воєнного стану.

Особливості інформаційної безпеки в умовах воєнного стану можуть відрізнятися від стандартних підходів до захисту інформації, які використовуються в звичайних умовах. Основними особливостями інформаційної безпеки в умовах воєнного стану є:

1. Збільшений обсяг інформації, що обробляється: умови воєнного стану передбачають швидкий розвиток подій, тому інформація має бути отримана та оброблена надзвичайно швидко. Умови воєнного стану супроводжуються значним збільшенням обсягу інформації, що обробляється. Це може бути пов’язано зі збільшенням кількості зв’язків, кількістю та обсягом документів, які потрібно обробляти та зберігати, збільшенням кількості електронних повідомлень та інформаційних систем.

Для забезпечення інформаційної безпеки в умовах збільшеного обсягу інформації необхідно використовувати спеціальні технічні та організаційні заходи. Один з основних заходів – це використання систем захисту інформації, які забезпечують надійний захист від несанкціонованого доступу до інформації.

Одним з можливих рішень є використання систем контролю доступу, які дозволяють забезпечити контроль за доступом до різних рівнів інформації в залежності від ролі та повноважень користувача. Також необхідно забезпечити захист інформації на різних рівнях – від захисту даних на окремих комп’ютерах та мережевих пристроях до захисту даних в цілому інформаційному просторі.

Крім того, необхідно використовувати системи резервного копіювання даних, що забезпечують можливість відновлення інформації в разі її втрати або пошкодження. Важливим елементом є також захист від вірусів та інших загроз, що можуть виникнути під час військових дій.

У збільшеному обсязі інформації, яку необхідно обробляти, також можуть виникати проблеми з її організацією та зберіганням.

2. Підвищений ризик витоку інформації: умови воєнного стану можуть призвести до підвищення ризику витоку чутливої інформації, оскільки ворог може мати більше можливостей для здійснення шпигунської діяльності. Умови

воєнного стану призводять до збільшення ризику витоку інформації. З одного боку, це може бути пов'язано зі збільшеним обсягом інформації, який обробляється в умовах конфлікту, з іншого боку, з підвищеним рівнем небезпеки з боку злочинних елементів та спецслужб ворога.

Підвищений ризик витоку інформації може бути пов'язаний з недостатнім захистом інформації від несанкціонованого доступу та зламу. Зокрема, умови воєнного стану можуть призвести до необхідності роботи з конфіденційною інформацією, яка є цінним ресурсом для ворога, що створює підвищений ризик її витоку.

Одним із способів зменшення ризику витоку інформації є встановлення систем захисту інформації, які дозволяють контролювати доступ до неї та перехоплення даних в мережі з боку злочинних елементів та спецслужб. Застосування криптографічних методів та створення систем ідентифікації та автентифікації також є важливими для захисту конфіденційної інформації в умовах воєнного стану.

Крім того, розробка та впровадження стратегії управління ризиками можуть допомогти зменшити ризик витоку інформації. Це може включати проведення аудиту та інвентаризації інформації, оцінку ризиків та визначення методів захисту інформації, а також планування та реалізацію заходів щодо захисту інформації.

Підвищений ризик кібератак: умови воєнного стану можуть також збільшити ризик кібератак на системи зберігання та обробки інформації. Умови воєнного стану суттєво збільшують ризик кібератак на критичну інфраструктуру, в тому числі на військові об’єкти та комунікації, що може серйозно підірвати обороноздатність та національну безпеку держави. Кібератаки можуть мати різні форми та наслідки, такі як переривання роботи важливих систем, витік чутливої інформації, фальшиві повідомлення, розповсюдження шкідливого програмного забезпечення, пошкодження обладнання та інше.

Підвищений ризик кібератак у воєнний час пояснюється кількома факторами. По-перше, збільшується кількість сторін, які можуть мати інтерес у проведенні кібератак, включаючи державних та недержавних акторів, кіберзлочинців, хакерів, терористів тощо. По-друге, умови воєнного стану зазвичай призводять до збільшення обсягу інформації, яку необхідно обробляти та зберігати, що робить її більш вразливою до кібератак. По-третє, умови воєнного стану можуть призвести до зниження рівня кібербезпеки, оскільки увага керівництва та ресурси можуть бути спрямовані на інші пріоритети.

Для підвищення інформаційної безпеки в умовах воєнного стану необхідно вживати заходів з попередження кібератак, виявлення та реагування на них. Зокрема, до таких заходів можуть відноситися створення сучасних систем захисту інформації, застосування шифрування та інших технологій забезпечення конфіденційності.

3. Залежність від інформаційних технологій: в умовах воєнного стану, військові дії можуть бути більш ефективними, якщо вони підтримуються сучасними інформаційними технологіями. В сучасному світі інформаційні технології стали необхідним елементом життя, зокрема в галузі бізнесу, науки, освіти, медицини та багатьох інших. Проте, залежність від цих технологій також створює нові ризики для інформаційної безпеки.

Залежність від інформаційних технологій може бути причиною вразливості для кібератак, які можуть призвести до витоку конфіденційної інформації або пошкодження даних. Крім того, залежність від інформаційних технологій може створити нові ризики для бізнесу, такі як втрата клієнтів або погіршення репутації після витоку даних.

Одним з головних ризиків, пов'язаних з залежністю від інформаційних технологій, є можливість витоку даних через хакерські атаки, соціальну інженерію або інші методи. Це може призвести до втрати довіри клієнтів та шкоди бізнесу. Також існує ризик залежності від постачальників інформаційних технологій, що може стати причиною втрати контролю над даними та сервісами.

Залежність від інформаційних технологій може також стати причиною низької культури безпеки серед користувачів. Це може призвести до втрати конфіденційної інформації через невірну обробку даних або зловживання привілеями доступу. Брак знань і умінь користувачів щодо захисту даних може стати причиною багатьох проблем в галузі інформаційної безпеки.

Одним із різновидів інформаційних операцій є кібератака. Кібератака є процесом або дією, спрямованою на шкоду або здобуття несанкціонованого доступу до інформації, виконання операцій з метою перешкодити роботі комп'ютерних систем або навіть заволодіти ними. Кібератаки можуть бути спрямовані на різноманітні об'єкти, такі як урядові відомства, компанії, інфраструктуру та громадські сервіси, що підкреслює необхідність інформаційної безпеки.

До основних різновидів кібератак як інформаційно-комунікаційних операцій відносять:

Фішинг: це шахрайський процес, в якому зловмисник намагається отримати доступ до інформації, такої як паролі або фінансові дані, використовуючи вимогливі повідомлення або імітуючи легітимні веб–сайти.

Фішинг (англ. phishing) – це форма кібератаки, яка спрямована на отримання конфіденційної інформації, такої як логіни, паролі, номери банківських карток тощо. Зазвичай, атака проводиться шляхом відправлення підробленого електронного листа або повідомлення, що містить запит про оновлення або підтвердження даних на відомому вам веб-сайті, банківському рахунку, соціальній мережі або іншому сервісі. Коли користувач переходить на сторінку, яка здавалося б підтвердженням даних, він повинен ввести свої особисті дані, які згодом можуть бути використані зловмисниками для шахрайства.

Фішинг є дуже поширеною кібератакою, оскільки залежно від рівня кваліфікації зловмисників, ці атаки можуть бути досить ефективними. Щоб запобігти фішингу, користувачам рекомендується бути дуже обережними при відкриванні електронних листів або повідомлень, особливо якщо вони містять

запити про введення особистих даних або викликають сумніви. Крім того, слід завжди перевіряти URL-адресу веб-сайту, на який вас перенаправляють, перш ніж вводити будь-яку інформацію, та не використовувати однакові логіни та паролі для різних веб–сайтів.

Існують різні види фішингу, серед яких:

1. Електронна пошта фішингу (Phishing email) – це один з найпоширеніших видів фішингу, коли зловмисники надсилають листи електронної пошти, які здаються легітимними. Листи можуть містити логотипи та іншу інформацію відомих компаній або урядових установ, а також посилання на підроблені веб–сайти. Користувачі, які натискають на ці посилання, потрапляють на сайти, що виглядають аналогічно легітимним, але насправді належать зловмисникам.

2. Соціальний фішинг (Social engineering) – це метод обману, коли зловмисники використовують соціальні інженерні техніки, щоб вплинути на жертву та переконати її розкрити конфіденційну інформацію. Наприклад, зловмисники можуть увійти в роль представника компанії та надіслати електронний лист, що запитує у жертви логін та пароль.

3. Фішинг–атаки на мобільні пристрої (Mobile phishing) – це фішинг, який спрямований на мобільні телефони та інші пристрої, що працюють на платформах Android та iOS. Ці атаки можуть включати надсилання текстових повідомлень та електронних листів, які містять посилання на підроблені веб–сайти.

Малвар – це загальна назва для вірусів, черв'яків, троянів та іншого зловмисного програмного забезпечення. Вони можуть завдати шкоди комп'ютерній системі, виконувати операції без дозволу користувача, збирати інформацію та навіть керувати комп'ютером здалеку. Малвар (від англ. malware – malicious software) – це програмне забезпечення, створене з метою завдання шкідливої дії на комп'ютері чи мобільному пристрої користувача. Малвар може проникнути на пристрій шляхом завантаження з інтернету, відкриття електронної пошти, підключення до зараженої мережі і т.д.

Малвар може мати різноманітні цілі: від крадіжки особистої інформації (логіни, паролі, банківські реквізити) до знищення файлів, зміни конфігурації системи та встановлення додаткового шкідливого програмного забезпечення.

Існує безліч різновидів малвару, зокрема:

1. Віруси (viruses) – це програмне забезпечення, що вкрапляється в інші файли та програми на комп'ютері та розповсюджується з їх допомогою. Вони можуть завдати шкоди шляхом знищення або зміни файлів, розповсюдження спаму, крадіжки інформації та інших дій.

2. Троянські програми (Trojan horses) – це програмне забезпечення, що приховано від користувача, що виконується в тлі та намагається отримати несанкціонований доступ до комп'ютера або розповсюджується на інші комп'ютери через Інтернет.

3. Рансомвар (ransomware) – це програмне забезпечення, що блокує доступ користувача до даних на комп'ютері або кодує їх, а потім вимагає викупу в обмін на доступ до даних.

4. Руткіти – це малвар, який надає зловмисникам повний контроль над комп'ютером. За допомогою руткітів зловмисники можуть виконувати будь–які дії на комп'ютері користувача без його знання.

5. Шпигунське програмне забезпечення (spyware) – це програми, які приховано встановлюються на комп'ютері користувача з метою відстежування його дій та перехоплення особистої інформації.

Деніал–оф–сервіс (DoS) та дистриб'ютивний деніал–оф–сервіс (DDoS): це атаки, спрямовані на перевантаження мережі або веб-сайти шляхом надсилання великої кількості запитів. Це призводить до відмови в обслуговуванні для легітимних користувачів та може призвести до втрати доходів або навіть до втрати клієнтів.

DoS–атака полягає у намаганні перевантажити ресурси комп'ютерної системи, щоб зробити її недоступною для користувачів. Це можна зробити за допомогою різноманітних методів, таких як відправка великої кількості запитів до сервера, спроба виконати невірний код на сервері, переповнення буферу

пам'яті та інші. DDoS–атака полягає в тому, що низка комп'ютерів–зомбі (botnet) надсилають велику кількість запитів до цільового сервера або мережі, що призводить до перевантаження та недоступності ресурсів.

Основним наслідком DoS та DDoS–атак є зниження доступності сервісів та інфраструктури, що може призвести до великих втрат. Наприклад, якщо атака спрямована на сайт електронної комерції, то це може призвести до зупинки продажів та втрати доходів. Якщо ж атака спрямована на критичні інфраструктурні об'єкти, такі як електростанції або транспортні системи, то це може викликати серйозні наслідки для національної безпеки.

Вимагається викуп (ransomware): це зловмисний код, який блокує доступ до комп'ютерної системи або файлив, накладає шифрування на файли. Це різновид кібератаки, під час якої зловмисники шифрують файли на комп'ютері або в мережі користувача, після чого вимагають викуп за розшифрування. Це один з найбільш широко поширених та ефективних методів атак на користувачів та організації.

Основним механізмом дії ransomware є шифрування файлів, що знаходяться на комп'ютері або в мережі потенційної жертви. Зловмисники використовують сильні алгоритми шифрування, щоб зробити файли недоступними для користувачів, а потім вимагають викуп в обмін на розшифрування файлів. Як правило, вимога викупу подається у вигляді повідомлення на екрані комп'ютера або в електронному листі.

У більшості випадків, для того, щоб розшифрувати файли, жертва повинна заплатити зловмисникам у вигляді криптовалюти. Вимоги викупу можуть бути різними, від кількох доларів до тисяч доларів, в залежності від об'єму та значущості зшифрованих даних.

Отже, підсумовуючи вищевикладене, зазначимо, що воєнний стан може суттєво вплинути на інформаційно-комунікаційну сферу України. Хоча існують потенційні перспективи розвитку, є й значні виклики. Для сприяння розвитку інформаційно-комунікаційної сфери в Україні уряду важливо збалансувати потребу безпеки з потребою прозорості та свободи слова.

У теоретичному розділі ми розглянули сутність, характеристики та механізми реалізації інформаційної війни. Інформаційна війна має значення в сучасній цифровій епосі і передбачає використання різних форм та тактик, зокрема дезінформаційних кампаній, кібератак та психологічного маніпулювання.

Вплив інформаційної війни здійснюється на різні сфери, зокрема політику, національну безпеку, бізнес та суспільство в цілому. Досліджено наслідки інформаційної війни, такі як підрив громадської довіри, дестабілізація демократичних процесів та економічні збурення.

До основних понять інформаційної безпеки – її складових – відносять такі: інформація, доступність, конфіденційність, цілісність, аутентифікація, аудит, фізична безпека. Серед головних принципів інформаційної безпеки науковці наголошують на таких, як принцип найменшого доступу, конфіденційності, цілісності, доступності. Усі вони в сукупності працюють на досягнення інформаційної безпеки держави.

РОЗДІЛ 2
АНАЛІЗ СУЧАСНИХ ІНФОРМАЦІЙНИХ ЗАГРОЗ І ЗАСОБІВ ІНФОМЕДІЙНОЇ БЕЗПЕКИ В УМОВАХ ВОЄННОГО СТАНУ

2.1 Визначення основних загроз для національної безпеки від кібератак в умовах воєнного стану

У сучасних умовах кібератаки можуть стати серйозною загрозою для національної безпеки в умовах воєнного стану. Важливим завданням є визначення основних загроз, що можуть виникнути в таких умовах, та розробка заходів для захисту від них.

Основні загрози від кібератак в умовах воєнного стану

1. Втрати інформації: Кібератаки можуть призвести до втрати важливої інформації, такої як розробки військової техніки, плани наступу або збройних сил, інформація про технічні засоби забезпечення безпеки, тощо. Такі втрати можуть значно ускладнити ведення бойових дій та знизити ефективність військових дій.

2. Пошкодження критичної інфраструктури: Кібератаки можуть спрямовуватися на критичну інфраструктуру, таку як енергетичні мережі, телекомунікаційні системи, системи водопостачання та інші. Пошкодження таких систем може призвести до серйозних наслідків для національної безпеки.

3. Вплив на військові операції: Кібератаки можуть впливати на військові операції, зокрема на системи зв'язку, навігації та управління. Наприклад, атаки на системи зв'язку можуть зробити неможливим зв'язок між різними частинами армії, а атаки на системи навігації можуть спричинити неконтрольоване рухання техніки.

Варто навести такі приклади кібератак на країни в умовах воєнного конфлікту, що завдали значної шкоди під час війни в Україні. Україна стала однією з перших країн, що дійшла до війни з Росією в електронному просторі. Починаючи з 2014 року, коли Росія окупувала Крим та підтримує бойовиків на

сході України, було зафіксовано численні кібератаки на різні об’єкти та інфраструктуру України.

За останні роки Україна стала однією з найбільш активних цілей для кібератак, зокрема у контексті воєнного конфлікту на сході країни. Нижче розглянуто кілька прикладів кібератак, які сталися в Україні в останні роки.

Кібератака на енергетичну систему: 23 грудня 2015 року українська енергетична система була атакована хакерами, що призвело до вимкнення електропостачання в декількох районах країни. Кібератака була спрямована на підприємства, які виробляють електроенергію та контролювали її розподіл, а також на компанії, які забезпечують інфраструктуру енергосистеми. Кібератака спричинила перерву у постачанні електроенергії для понад 225 тисяч людей в західній частині України, що призвело до серйозних проблем у житті людей та підприємств. Зокрема, були зафіксовані відключення світла у містах Івано–Франківськ, Львів та Тернопіль.

Атака була проведена за допомогою шкідливої програми, яка була занурена в систему керування енергопостачанням підприємств. Шкідлива програма змогла зламати захист системи, отримати доступ до неї та призначити команди для виконання певних операцій, таких як відключення електрики.

Ця кібератака була важливим поворотним моментом в історії кібербезпеки, оскільки вона показала, що кіберзлочинці можуть направляти свої атаки на критичну інфраструктуру та наносити реальну шкоду національній безпеці та життю людей. Такі атаки можуть мати серйозні наслідки, які важко передбачити та контролювати.

У зв'язку з цим, держави повинні приділяти належну увагу розробці та застосуванню заходів кіберзахисту для критичної інфраструктури, зокрема енергетичних систем, щоб запобігти подібним кібератакам у майбутньому.

Кібершпигунство: у 2017 році було виявлено, що українська компанія–розробник програмного забезпечення M.E.Doc була скомпрометована хакерами, що призвело до кібератаки на українську фінансову систему. У 2017 році було виявлено один з найбільших кібератак в історії України, який здійснили через

вразливість в програмному забезпеченні M.E.Doc, популярної бухгалтерської програми, яка використовується в Україні та інших країнах. Атака вплинула на десятки тисяч комп'ютерів, включаючи комп'ютери урядових установ, банків, медичних закладів та інших організацій.

Атака почалася у червні 2017 року, коли хакери використали вразливість в програмному забезпеченні M.E.Doc, щоб вставити вредоносний код в оновлення програми. Коли користувачі оновили програму, вірус поширився на їх комп'ютери та почав виконувати свої завдання.

Ця кібератака використовувала шкідливе програмне забезпечення, відоме як Petya, яке шифрує дані на жертві та вимагає викуп за їх розшифрування. Але на відміну від звичайного розшифрування, Petya видаляє та перезаписує збережені дані. Це стало причиною того, що великі корпорації, такі як Maersk та Merck, зазнали втрат у мільйони доларів.

Серйозні наслідки кібератаки M.E.Doc породили серйозні запитання про кібербезпеку в Україні та за її межами. Крім того, ця атака показала, що навіть маленька компанія може мати великий вплив на національну безпеку країни.

Кібератака на Банк: у липні 2017 року, хакери використали уразливість в програмному забезпеченні банківської системи, щоб вкрасти мільйони гривень з банку в Україні.

У липні 2017 року була виконана одна з найбільших кібератак на банківську галузь. Кіберзлочинці використали шкідливий код під назвою "NotPetya", який був поширений через оновлення програмного забезпечення бухгалтерської програми M.E.Doc, що використовується в Україні. Оскільки банки теж використовували цю програму, вони стали жертвами кібератаки.

"NotPetya" використовував вразливість в операційній системі Windows, що дозволяло зламувачам зашифрувати диск комп'ютера, вимагаючи від жертви викуп у вигляді біткоїнів. Крім того, вірус заблокував доступ до системи банків, що призвело до великих фінансових втрат.

У результаті цієї кібератаки, деякі банки в Україні були змушені зупинити свою роботу та призупинити обслуговування клієнтів. Крім того, було

пошкоджено багато комп'ютерів, що призвело до втрат даних та великих витрат на відновлення комп'ютерної інфраструктури.

Ця кібератака є однією з найбільших в історії та показує, як вразливо можуть бути фінансові установи та інші організації перед кіберзагрозами. Для запобігання таким атакам, необхідно вживати заходів кібербезпеки, таких як регулярне оновлення програмного забезпечення, міцні паролі, шифрування даних та багато іншого.

Кібератаки на військові об'єкти: останнім часом кібератаки на військові об'єкти стали більш поширеними і складними. Військові об'єкти зазвичай мають велику кількість конфіденційної інформації, яка може бути цінною для кіберзлочинців та кібершпигунів. Такі атаки можуть бути спрямовані на викрадення конфіденційних даних, завдання матеріальних збитків, або на завдання шкоди самій обороноздатності країни.

Останніми роками світ ставки на цифрові технології і інформаційні системи військових об'єктів вище ніж будь-коли. За даними інформаційно–аналітичної компанії Recorded Future, кількість кібератак на військові об'єкти зросла втричі між 2019 та 2020 роками.

У квітні 2020 року Ізраїль звинуватили в кібератаках на іранський ядерний комплекс, під час яких хакери використали хитрий план для того, щоб знищити частину обладнання комплексу.

У грудні 2020 року Росію звинуватили в кібератаках на десятки американських установ та компаній, у тому числі на Міністерство фінансів, американські розвідувальні агентства та компанії–виробники програмного забезпечення.

Одним з відомих прикладів кібератаки на військові об'єкти є атака на компанію Lockheed Martin в 2011 році. Компанія є одним з найбільших постачальників обладнання для військової техніки США. Кібератака, яка була спрямована на викрадення конфіденційних даних, була виконана за допомогою шкідливих програм, які були встановлені на комп'ютерах підрядників компанії.

Інший приклад кібератаки на військові об'єкти стався у 2015 році, коли хакери взломали систему Міністерства оборони ФРН. У результаті цієї атаки було викрадено близько 16 Гб конфіденційних даних. Інформація, яка була викрадена, включала в себе дані про військову техніку, обладнання та системи зв'язку.

Один з прикладів кібератак на військові об'єкти відбувся в 2017 році, коли хакерська група Fancy Bear або APT28 (Advanced Persistent Threat 28), пов'язана з російською розвідкою, вдерлася в комп'ютерну мережу української армії. Ця атака, відома як Operation Armageddon, стала однією з найбільш руйнівних кібератак в історії України. Хакери використали спеціальний шпигунський софт, який дозволив їм перехоплювати повідомлення та дані, що передавалися між військовими об'єктами.

Іншим прикладом кібератак на військові об'єкти є атака на систему керування китайського літаконесущого корабля "Ліанонін". В липні 2020 року хакерська група українського походження, що працює на користь китайської розвідки, використала уразливість в програмному забезпеченні корабля, щоб отримати необмежений доступ до систем керування та управління. Атака не спричинила фізичної шкоди, але показала, що кіберзагрози можуть стати серйозними загрозами для військової безпеки.

В Україні військові об'єкти теж не змогли уникнути кібератак. У 2017 році група хакерів, відома під назвою SandWorm, взяла на себе відповідальність за кібератаки на українські електростанції, що спричинило масштабний відключення електроенергії в окремих регіонах країни.

Також у 2017 році, група хакерів відома як Dragonfly 2.0 або Energetic Bear, влаштувала кібератаку на підприємства української енергетики та водопостачання, використовуючи вразливості в програмному забезпеченні для отримання доступу до систем керування.

Зазначимо також, що на тлі зростаючої кількості кібератак на військові об'єкти, з'являється все більше заходів з підвищення кібербезпеки.

Кібератаки на країни в умовах воєнного стану можуть мати серйозні наслідки, що можуть відчутно вплинути на функціонування суспільства та загрожувати національній безпеці. Деякі з можливих наслідків таких атак включають:

1. Порушення функціонування електронних систем: Кібератаки можуть викликати збій роботи електронних систем, включаючи системи енергопостачання, транспорту, комунікації та інформаційні системи. Це може призвести до зниження ефективності роботи країни та викликати суттєві економічні збитки. Одним з найбільш очевидних наслідків кібератаки на країну в умовах воєнного стану є порушення функціонування електронних систем. Це може охоплювати різні аспекти життя країни, такі як:

- Енергетична система: кібератаки на енергетичну систему можуть призвести до зупинки електропостачання, що може спричинити значні збитки для населення та економіки країни.
- Транспортна система: кібератаки на транспортну систему можуть призвести до зупинки руху транспортних засобів, що може викликати серйозні проблеми з транспортуванням товарів та послуг, а також здійсненням екстреної медичної допомоги.
- Фінансова система: кібератаки на фінансову систему можуть призвести до зупинки роботи банків та інших фінансових установ, що може призвести до великих збитків для бізнесу та громадян.
- Медична система: кібератаки на медичну систему можуть призвести до зупинки роботи лікарень та інших медичних установ, що може ставити під загрозу життя та здоров'я людей.
- Комунальна система: кібератаки на комунальну систему можуть призвести до зупинки роботи водопроводів, каналізаційних систем та інших комунальних послуг, що може викликати серйозні проблеми зі здоров'ям населення та гігієною.

Ці наслідки можуть мати серйозний вплив на економіку та життя країни, що може стати причиною зниження економічної активності, зростання безробіття, зниження рівня життя та загрози правопорядку.

2. Зниження економічної активності: Кібератаки можуть спричинити зниження економічної активності, оскільки підприємства можуть бути змушені припинити свою діяльність на деякий час або втратити значну кількість конфіденційної інформації. Крім того, такі атаки можуть призвести до зменшення довіри інвесторів та споживачів, що може спричинити зниження економічного зростання та розвитку країни.

3. Загроза життю і здоров'ю людей: Кібератаки можуть мати велику загрозу для життя та здоров'я людей, особливо якщо атакуються системи, які відповідають за критичну інфраструктуру, таку як системи медичного обслуговування або авіаційні системи. Такі атаки можуть мати небезпечні наслідки та призвести до смерті та серйозних травм.

4. Порушення правопорядку: кібератаки можуть призвести до порушення правопорядку, зокрема, до крадіжок конфіденційної інформації, зловживання даними, відкриття доступу до захищених об'єктів тощо. Це може стати причиною серйозних правових наслідків для тих, хто бере участь у кібератаках.

2.2 Використання інформаційних технологій у військовій галузі та їх вплив на інформаційну безпеку країни

У сучасному світі інформаційні технології відіграють важливу роль у військових діях і можуть мати великий вплив на інформаційну безпеку країни. Технології, такі як кібератаки, кібершпигунство та інші, стали невід'ємною частиною воєнних конфліктів і впливають на безпеку країн, оскільки вони можуть призвести до різноманітних наслідків, включаючи зниження економічного потенціалу, порушення політичної стабільності та загрозу безпеці населення. Використання інформаційних технологій відіграє важливу роль у

військових діях країн у сучасному світі. Ці технології дозволяють збирати, обробляти та аналізувати великі обсяги інформації, що допомагає забезпечити ефективність військових операцій та знизити ризик втрат серед військовослужбовців та населення.

Один з головних аспектів використання інформаційних технологій у військових діях – це здатність до швидкого збору та обробки великої кількості інформації, що може бути важливою складовою успішності військових операцій. Інформаційні технології також можуть допомогти в забезпеченні безпеки військового персоналу, наприклад, за допомогою систем контролю за діяльністю військового персоналу, систем комунікацій та обміну даними.

Однак, з іншого боку, використання інформаційних технологій також може призвести до різних видів кібератак та кібершпигунства, що можуть призвести до викриття та порушення військової та національної безпеки. Кібератаки на військові об'єкти, наприклад, можуть призвести до порушення зв'язку між військовими підрозділами, зниження ефективності військових дій та загрози життю і здоров'ю військового персоналу.

Зростання використання інформаційних технологій військовими структурами призводить до збільшення загрози кібератак та інших форм кіберзлочинності. У разі успішної кібератаки на військові інформаційні системи може бути скомпрометована вся інформація про військові операції, що може призвести до тяжких наслідків для військової безпеки та життєвої безпеки людей.

Також, використання інформаційних технологій у військових діях може привести до порушення приватності особистих даних військовослужбовців та населення, що може мати наслідки для національної безпеки країни.

Крім того, зростання кількості кіберзлочинності та кібератак на військові об'єкти призводить до збільшення витрат на кіберзахист та розробку нових інформаційних технологій, що може вплинути на економічну активність країни.

Отже, використання інформаційних технологій у військових діях дозволяє забезпечити ефективність військових операцій та зменшити ризик втрат, але одночасно призводить до збільшення загрози кібератак.

У сучасних війнах використання інформаційних технологій має вирішальне значення, адже забезпечення інформаційної безпеки є ключовою складовою забезпечення національної безпеки країни. У цілому, інформаційні технології можуть використовуватися військовими в різних аспектах, включаючи:

1. Розвідку та збір інформації: Спеціальні служби країн можуть використовувати різні інформаційні технології для збору та аналізу інформації про потенційних ворогів, зокрема з використанням дронів, супутникових знімків, електронної пошти та соціальних мереж. Це важлива складова військових дій, яка дозволяє здобувати важливу інформацію про супротивника, його стратегії та тактики. За допомогою інформаційних технологій розвідка може отримати широкий спектр даних про ворога, такі як розташування військових об'єктів, чисельність військ, склад зброї та техніки, технічні характеристики обладнання, системи комунікацій та зв'язку, та інші важливі дані.

Збір інформації може здійснюватися різними способами, включаючи перехоплення електронних повідомлень та зв'язку, використання супутникових систем спостереження, взлом систем безпеки, інтеграцію з мережами джерел відкритої інформації, та багато інших методів.

Однак, використання інформаційних технологій для розвідки та збору інформації може також стати загрозою для інформаційної безпеки країни, яка розглядається як цінний ресурс. Ворог може здійснювати кібершпигунство з метою здобуття важливої інформації, такої як військові секрети, технології виробництва зброї та техніки, та інші важливі дані, що можуть негативно вплинути на військову потужність країни.

2. Комунікації та зв'язок: Військові можуть використовувати інформаційні технології для забезпечення швидкої та ефективної комунікації

між собою. Це може включати використання радіо, супутникових зв'язків, мобільних телефонів та інших технологій. У військовій сфері використовуються різноманітні засоби зв'язку, які дозволяють передавати інформацію на різних рівнях (від командира роти до вищого командування) та на різні відстані (від кількох метрів до тисяч кілометрів). Засоби зв'язку можуть бути провідними (наприклад, кабельні з'єднання) або безпровідними (радіозв'язок, супутниковий зв'язок).

Окрім традиційних засобів зв'язку, в останні роки військові використовують інформаційні технології, що дозволяють швидко передавати великі обсяги даних. Наприклад, для передачі відео– та аудіоматеріалів використовуються спеціальні протоколи передачі даних, які забезпечують стійкість передачі при великих відстанях та поганій якості зв'язку.

Однак використання інформаційних технологій у зв'язку також може стати об'єктом кібератак, які можуть перервати комунікаційну інфраструктуру військ та позбавити їх зв'язку. Такі атаки можуть мати серйозні наслідки для успішності військових дій та безпеки військовиків.

Підсумовуючи, комунікації та зв'язок відіграють важливу роль у військових діях та керуванні військами. Ефективна комунікація і зв'язок є ключовими елементами для координації дій, передачі інформації та прийняття рішень у реальному часі. Основні аспекти комунікаційного процесу та зв'язку у військових діях включають:

- Комерційні системи зв'язку: Використання сучасних комерційних систем зв'язку, таких як радіо, супутникові зв'язок, мережі зв'язку, дозволяє забезпечити швидку та надійну передачу інформації між різними пунктами командування та військовими одиницями.

- Шифрування і захист інформації: Захист інформації є важливим аспектом комунікаційного процесу у військових діях. Застосування шифрування та інших методів захисту інформації допомагає запобігти несанкціонованому доступу до конфіденційних даних та забезпечити конфіденційність та цілісність переданих повідомлень.

- Командно–штабні системи: Використання спеціалізованих командно–штабних систем дозволяє забезпечити збір, обробку та аналіз інформації, а також координацію дій між різними рівнями командування. Ці системи включають централізовані бази даних, системи візуалізації та аналізу інформації, системи спільного доступу до даних тощо.

- Безпроводові мережі зв'язку: Використання безпроводових мереж зв'язку, таких як мережі 4G/5G, Wi–Fi та інші, дозволяє забезпечити мобільність комунікації та зв'язку для військових сил у різних областях. Вони забезпечують можливість передачі голосових, відео– та даних в режимі реального часу, що дозволяє військовим одиницям швидко обмінюватись інформацією, координувати свої дії та приймати оперативні рішення.

- Системи управління комунікаціями: Військові організації використовують спеціалізовані системи управління комунікаціями для керування та контролю комунікаційними мережами. Ці системи дозволяють забезпечити ефективне планування, моніторинг та управління комунікаційними ресурсами, що забезпечує надійність та швидкість комунікаційних засобів.

- Супутникові комунікації: Використання супутникових комунікаційних систем дозволяє забезпечити зв'язок на великі відстані та в умовах, коли інфраструктура зв'язку на землі є недоступною або пошкодженою. Супутникові системи забезпечують глобальне покриття та стійкість зв'язку.

- Автоматизовані системи командування і контролю: Використання автоматизованих систем командування і контролю допомагає забезпечити ефективну обробку та передачу інформації, управління військовими діями та координацію різних військових сил та одиниць. Ці системи включають інтегровані платформи, бази даних, засоби візуалізації та прийняття рішень.

- Аерокосмічні засоби зв'язку: Використання аерокосмічних засобів зв'язку, таких як супутники та дрони, дозволяє забезпечити широкий охоплення зв'язку та незалежність від земних інфраструктур. Це особливо важливо в умовах воєнного стану, коли земні комунікаційні мережі можуть бути пошкоджені або знищені.

Ці аспекти використання інформаційних технологій у військових діях мають великий вплив на інформаційну безпеку країни. Високий рівень інформаційної безпеки військових комунікаційних систем є критичним для успішного проведення військових операцій та захисту національних інтересів. Тому розробка та використання ефективних інструментів інформаційної безпеки є невід'ємною частиною військової стратегії країни.

3. Керування військами та зброєю: Інформаційні технології можуть використовуватися для керування військовими діями та зброєю. Це може включати використання різноманітних систем керування бойовими діями, таких як системи керування вогнем та системи навігації. За допомогою комп'ютерних систем та програмного забезпечення можна керувати військовими підрозділами, забезпечувати координацію дій та обмін інформацією між ними.Один з найважливіших аспектів керування військами – це забезпечення точної та швидкої передачі інформації між різними військовими підрозділами, а також з центральним командуванням. Це може бути здійснене за допомогою військових комунікаційних систем, таких як супутникові зв'язки, радіозв'язок, кабельні мережі та інші.

Іншим аспектом керування військами є використання систем управління бойовими діями (C4I – Command, Control, Communications, Computers and Intelligence), що дозволяють отримувати дані зі спостережень та розвідки, проводити аналіз даних та приймати рішення. Системи C4I можуть бути використані для побудови стратегічних та тактичних планів, розподілу ресурсів та керування бойовими діями.

Ще одним аспектом керування військами є використання бойових дронів та інших безпілотних систем (UAV – Unmanned Aerial Vehicle), які можуть бути використані для збору інформації та проведення ударів на ворожі цілі. Бойові дрони можуть мати різну функціональність, включаючи збір інформації, вогневу підтримку, а також виконання спеціальних завдань, таких як знищення командного пункту або здійснення зв'язку.

Узагальнюючи основні аспекти керування військами та зброєю, можно виявити, що інформаційні технології використовуються на етапах:

- Планування військових операцій: розроблення стратегічних та тактичних планів для досягнення військових цілей. Це включає визначення цілей, призначення завдань, виділення ресурсів та координацію дій між різними військовими підрозділами.

- Командування та контролю: ефективне управління військами включає прийняття рішень, видачу команд, координацію дій та контроль за їх виконанням. Командування здійснюється через ієрархічну систему командування, де керівники на різних рівнях військової структури забезпечують керування та надсилають відповідні команди підлеглим підрозділам.

- Інформаційна система керування: використання інформаційних технологій та комунікаційних систем для обміну інформацією між військовими підрозділами, збору даних, аналізу інформації та прийняття рішень. Інформаційна система керування забезпечує швидке та точне передавання команд та інформації, що є критичним для успішного керування військами.

- Логістика: забезпечення потрібних ресурсів (зброї, боєприпасів, техніки, палива, харчування, медичного забезпечення тощо) для військових операцій.

- Тактичне управління: керування військами на полі бою, включаючи координацію дій, переміщення підрозділів, розстановку сил та здійснення бойових операцій. Тактичне управління забезпечує ефективне використання розташованих на полі бою ресурсів та досягнення поставлених завдань.

- Планування та здійснення навчань: розроблення навчальних програм, проведення тренувань та навчань з метою підготовки військ до виконання завдань та підвищення їх ефективності. Навчання включає тактичні, технічні, фізичні та стратегічні аспекти, а також враховує специфіку воєнних дій та використання сучасних інформаційних технологій.

- Аналіз та оцінка результатів: систематичний аналіз та оцінка результатів військових операцій з метою виявлення помилок, вдосконалення

стратегії, тактики та процесів керування. Цей етап допомагає вдосконалити ефективність та ефективність керування військами та зброєю у майбутніх операціях.

Важливо зазначити, що керування військами та зброєю є складним та багатогранним процесом, який вимагає сполучення стратегічного мислення, лідерства, використання сучасних інформаційних технологій та ефективного взаємодії між різними рівнями командування.

4. Кібербойові дії: Кібербойові дії можуть бути використані для здійснення кібератак на ворожі військові об'єкти. Наприклад, можливо взламати системи керування військами, знищити важливі файл. Кібербойові дії (англ. cyber operations) – це використання комп'ютерних систем та мереж для здійснення військових дій. Вони можуть бути як нападом, так і захистом від нападу. Кібербойові дії можуть бути використані як окремо, так і в поєднанні з традиційними засобами ведення війни.

Основні завдання кібербойових дій полягають в:

- Руйнуванні інфраструктури противника
- Розкритті та зборі розвідувальної інформації
- Поширенні дезінформації та пропаганди
- Відстеженні, контролі та знищенні військових об'єктів противника
- Знищенні ворожих військ та важливих місць їх дислокації.

Кібербойові дії можуть бути виконані різними способами, такими як відправка вірусів, троянів, шкідливих програм, злам веб–сайтів, злам соціальних мереж тощо. Вони можуть бути виконані як звичайними хакерами, так і військовими відділами та розвідувальними службами.

Також треба зазначити, що кібер бойові дії можуть мати серйозні наслідки, які можуть вплинути на життя та безпеку людей, економіку та інфраструктуру країни. Оскільки такі події можуть бути виконані з будь–якої точки світу, вони можуть бути складні для виявлення та попередження. Тому важливо мати ефективну систему кіберзахисту для захисту країни від кібер бойових дій.

2.3 Інструменти інформаційного та кіберзахисту та їх застосування в умовах воєнного стану

Інформаційна безпека є важливою складовою національної безпеки країни. Залежно від ситуації, можуть виникнути різноманітні загрози для інформаційної безпеки, зокрема в умовах воєнного стану. З метою забезпечення безпеки інформаційних систем в таких умовах, необхідно використовувати різні інструменти інформаційного та кіберзахисту.

Один з найважливіших інструментів кіберзахисту – це антивірусне програмне забезпечення. Антивірусні програми захищають інформаційну систему від шкідливих програм, виявляють і блокують їх дії. В умовах воєнного стану, коли збільшується кількість кібератак та злочинів у кіберпросторі, застосування антивірусного програмного забезпечення є надзвичайно важливим.

Ще одним важливим інструментом є перехоплення та фільтрація мережевого трафіку. Це дозволяє відслідковувати та блокувати небажаний трафік, що може містити шкідливі програми або спрямовувати на фішингові сайти. Застосування таких інструментів є особливо важливим в умовах воєнного стану, коли можуть бути проведені широкомасштабні кібератаки.

Одним з найважливіших інструментів кіберзахисту є системи раннього виявлення інцидентів (SIEM). Ці системи збирають та аналізують інформацію про події, що відбуваються в мережі та на комп'ютерах, та виявляють небезпечні події.

Основні інструменти кіберзахисту, які застосовуються в умовах воєнного стану, включають наступні:

1. Фірмові мережеві брандмауери (firewalls) – це програмне забезпечення або апаратне забезпечення, яке встановлюється на мережеві пристрої для контролю доступу до мережі. Вони перевіряють кожен пакет даних, який проходить через мережу, та забезпечують захист від шкідливих атак на мережу.

2. Системи виявлення вторгнень (Intrusion Detection Systems, IDS) – це системи, які аналізують трафік на мережі на наявність потенційно шкідливих дій,

які можуть бути здійснені зовні або всередині мережі. Ці системи виявляють потенційні загрози та повідомляють про них адміністратора мережі.

3. Антивірусні програми – це програми, які виявляють та видаляють віруси, троянські програми та інші шкідливі програми з комп'ютерів та мережі.

4. Системи безпеки електронної пошти – це системи, які контролюють електронну пошту, що надходить та відправляється з комп'ютерів та серверів. Вони перевіряють електронну пошту на наявність вірусів та інших шкідливих програм.

Використання інформаційних технологій у військових діях стало невід'ємною частиною сучасних збройних конфліктів. Це пов'язано з широким впровадженням військових інформаційних систем, автоматизацією процесів управління, збору та аналізу інформації. Але використання інформаційних технологій також створює нові виклики та загрози, що потребують ефективних методів захисту.

Один з головних викликів, пов'язаних з використанням інформаційних технологій у військових діях, полягає у забезпеченні безпеки військових інформаційних систем та даних, що обробляються. Небезпека витоку чутливої інформації може призвести до серйозних наслідків, включаючи розкриття військових та дипломатичних секретів, порушення прав людини та навіть загрози національній безпеці.

Одним з інструментів захисту військової інформації є криптографія – наука про захист інформації від несанкціонованого доступу шляхом шифрування даних. Криптографія може використовуватися для захисту від перехоплення, зламу та інших типів кібератак. Крім того, розробка військових інформаційних систем з урахуванням принципів кібербезпеки, таких як захист від деніал-оф-сервіс та захист від шкідливих програм, є дуже важливою.

Використання інформаційних технологій у військових діях є важливою складовою багатьох військових операцій. Сучасні технології дозволяють забезпечити швидкий обмін інформацією, відслідковувати рух військових формувань та дозволяють проводити точність ударів з високою точністю. У цій

теоретичній главі будуть розглянуті основні аспекти використання інформаційних технологій у військових діях, а також інструменти та методи захисту від кібератак та інших загроз.

Інформаційні технології (ІТ) є важливим інструментом для розв'язання різноманітних завдань військової діяльності. Використання ІТ дозволяє значно покращити ефективність ведення війни та зменшити ризик для людей, а також забезпечити більш точне та оперативне прийняття рішень військовими лідерами.

Отже, основні аспекти використання інформаційних технологій у військових діях можуть бути розділені на декілька категорій:

1. Комунікації та зв'язок: ІТ забезпечують безперервний потік інформації між військовими одиницями та керівництвом. Засоби комунікації включають в себе радіозв'язок, супутникову зв'язок, інтернет–зв'язок та інші форми зв'язку. Це дозволяє військовим одиницям отримувати інформацію про стан ворожих сил та здійснювати взаємодію між собою для досягнення спільних цілей.

2. Розвідка та збір інформації: ІТ забезпечують широкі можливості для збору та обробки розвідувальної інформації. Використання дронів, супутників та інших технічних засобів дозволяє отримувати інформацію з великої відстані та безпечності для людей. Крім того, використання програмного забезпечення для обробки та аналізу інформації дозволяє здійснювати більш точну та оперативну розвідку. Керування військовими операціями: ІТ дозволяють керівникам військових одиниць здійснювати керування військовими операціями більш точно

У цьому розділі ми розглянули інформаційні війни на конкретних прикладах та навели перелік необхідних дій для забезпечення захисту від цієї загрози. Дослідження базувалося на аналізі реальних інцидентів і використанні відповідних методів та інструментів. У результаті дослідження було виявлено різні форми інформаційної війни, зокрема дезінформаційні кампанії, фейкові новини та кібератаки. Було проаналізовано їхні наслідки для організацій та індивідів, такі як пошкодження репутації, фінансові втрати та порушення кібербезпеки.

З метою протидії інформаційній війні було розроблено план заходів, що включав у себе моніторинг та аналіз інформаційного простору, підвищення кібербезпеки, попередження дезінформації та підготовку персоналу.

Впровадження кібербезпечних заходів дозволить зменшити ризик кібератак та зберегти конфіденційні дані. Розроблення стратегії протидії дезінформації сприятиме відповідному реагуванню та недопущенню поширення фейкової інформації.

Отже, проведене дослідження та виконані практичні дії підтверджують важливість боротьби з інформаційною війною та необхідність прийняття ефективних заходів для захисту від її наслідків. Запропоновані рекомендації та висновки можуть бути використані як основа для подальшого вдосконалення стратегій протидії інформаційній війні і забезпечення безпеки інформаційного простору.

ВИСНОВКИ

У даній бакалаврській роботі було розглянуто тему «Інструменти інфомедійної безпеки в умовах воєнного стану». У ході дослідження було виявлено, що використання інформаційних технологій стало невід'ємною складовою сучасної війни. Було проаналізовано використання інформаційних технологій у у різних сферах та їх вплив на інформаційну безпеку країни.

У ході роботи було досліджено різні аспекти використання інформаційних технологій в військових діях, зокрема розвідку та збір інформації, комунікації та зв'язок, керування військами та зброєю, кібер бойові дії та інші. Було досліджено можливі наслідки кібератак на країну в умовах воєнного стану, включаючи порушення функціонування електронних систем, зниження економічної активності, загрозу життю і здоров'ю людей, порушення правопорядку та інші.

В результаті дослідження було виявлено, що інформаційні технології стали невід'ємною частиною військових дій та мають значний вплив на інформаційну безпеку країни. Крім того, було проаналізовано різні засоби та технології кіберзахисту, які можуть зменшити ризик кібератак на країну.

У рамках теоретичного розділу було проведено детальний аналіз теоретичних аспектів, пов'язаних з використанням інформаційних технологій у військових діях. Виявлено, що інформаційні технології є невід'ємною складовою частиною сучасної військової сфери, впливають на різні аспекти військових дій і мають значний потенціал для підвищення ефективності та забезпечення інформаційної переваги воєнних сил.

У результаті аналітичного дослідження було виявлено, що використання інформаційних технологій у військових діях має як позитивний, так і негативний вплив на інформаційну безпеку країни. З одного боку, інформаційні технології дозволяють поліпшити комунікації, забезпечити швидкий обмін інформацією, впровадити нові стратегічні та тактичні методи ведення військових операцій. З іншого боку, вони створюють нові загрози, пов'язані з кібератаками, витоком інформації, знищенням інформаційних систем тощо.

Отже, дослідження показало, що розвиток інформаційних технологій має як позитивний, так і негативний вплив на військові дії та безпеку країни. Для зменшення ризику кібератак та забезпечення інформаційної безпеки, необхідно розвивати та вдосконалювати засоби та технології кіберзахисту. Використання інформаційних технологій у військових діях має велике значення для успішного виконання військових операцій. Однак, це також може мати серйозні наслідки для національної безпеки країни, тому необхідно забезпечувати високий рівень інформаційної безпеки та розробляти заходи для запобігання можливим кібератакам.

У майбутньому, можна провести додаткові дослідження з цієї теми, зокрема, дослідження ефективності заходів забезпечення.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Ананьїн В., Пучков О. Інформаційна безпека у контексті сучасних подій в Україні. *Вісник Київського національного університету імені Тараса Шевченка*. 2007. № 14–15. С. 28–29.

2. Андреєва О.М. Національна безпека України в контексті національної ідентичності і взаємовідносин з Росією. Київ : Парламентське видавництво, 2009. 360 с.

3. Аніщенко В.О. Сутність операцій з підтримки миру (миротворчі операції). *Труди академії оборони України*. Київ : НОАУ, 2001. Вип. 34. С. 67–72.

4. Бабіч О. Особливості маніпуляції масовою свідомістю в друкованих ЗМІ під час висвітлення воєнних подій. *Вісник Київського національного університету імені Тараса Шевченка: військово–спеціальні науки.* 2007. Вип. 14 – 15. С. 89–92.

5. Бінько І. Інформаційний простір України: стан та тенденції розвитку. *Бібліотечний вісник*. К., 2001. № 2. С. 15–18.

6. Бортніков В.І. Політична участь і демократія : українські реалії : монографія. Луцьк : РВВ «Вежа» Волинь. держу н–ту ім. Л.Українки, 2007. 524 с.

7. Васютинський В.О. Психологічні виміри спільноти : монографія. Київ : Золоті ворота, 2010. 119 с.

8. Верстюк В.Ф. Україна і Росія в історичній ретроперспективі / під ред. Верстюк В.Ф. Київ : Наукова думка, 2004. 504 с.

9. Волощук М., Жебровський О. Інформаційні війни: сутність, особливості, механізми реалізації. *Наукові записки Національного університету «Острозька академія». Серія «Філологічна»*. Острог : Вид–во Острозької академії, 2014. Вип. 53. С. 221–226.

10. Ганжа О., Гаращенко В. Міжнародна політика ЄС: актуальні проблеми та виклики. *Політичний менеджмент: теорія і практика*. 2011. № 3. С. 32–38.

11. Горбатенко В.М. Інформаційна безпека держави. Харків : Вид–во ХНУ ім. В. Н. Каразіна, 2006. 248 с.

12. Горбулін В.П., Додонов О.Г., Ланде Д.В. Інформаційні операції та безпека суспільства: загрози, протидія, моделювання : монографія. Київ : Інтертехнологія, 2009. 164 с.

13. Горяйнова, Г. В., Морозов, А. В., Попов, С. В. Розбудова системи інформаційної безпеки держави в умовах воєнного конфлікту. *Системні технології.* 2019 (6). С. 86–92.

14. Гриценко А.Д. Інформаційна війна в демократичному суспільстві. *Проблеми права, безпеки та оборони*. Київ : КНУБА, 2009. Вип. 6. С. 139–141.

15. Гуляєв О. В. Спін–операції як специфічна форма інформаційного впливу в сучасному політичному процесі. *Гілея : науковий вісник. Збірник наукових праць.* Київ : ВІР УАН, 2011. Випуск 44. С. 548–553.

16. Дахновський Ю. Військова інформація: від битви до розвідки. *Наукові записки Національного університету «Острозька академія». Серія «Історична».* Острог : Вид–во Острозької академії, 2010. Вип. 23. С. 252–256.

17. Дженніфер С., Джеффрі К. Тюрнер. Кібербезпека в умовах збройного конфлікту: зв'язки між кібер–загрозами та кібер–стратегіями. *Журнал стратегічних студій.* 2016. Том 39, № 6–7. С. 899–924.

18. Діденко Н.Г. Управління, влада, держава: філософські аспекти взаємодії : монографія. Донецьк : ДонДУУ, 2005. 128 с.

19. Дорошенко І., Дмитрук В. Військова інформація: сучасні тенденції розвитку. *Наукові записки Національного університету «Острозька академія». Серія «Історична*». Острог : Вид–во Острозької академії, 2010. Вип. 23. С. 241–245.

20. Едвард Лукас, Бен Баллоу. Кібербезпека в умовах війни: проблеми та виклики. *Безпека*. 2018, том 60. № 3. С. 107–116.

21. Європейський союз. Стратегія кібербезпеки ЄС. URL : https://ec.europa.eu/info/publications/cybersecurity–strategy–eu–an–open–safe–and–secure–cyberspace_en

22. Жарков Я., Онищук М. Інформаційно–психологічне протиборство в сучасному світі: проблемно–історичний аналіз. *Вісник Київського національного університету імені Тараса Шевченка*. 2007. № 14–15. С. 101–104.

23. Інститут кібербезпеки України. Офіційний сайт: URL : https://www.isss.kiev.ua/

24. Квіт С., Демидюк О. Управління інформаційною безпекою в умовах гібридної війни. *Безпека та оборона: щоквартальник*. № 25 (1). С. 38–51.

25. Кейтлін Лі, Керрі М. Кібербезпека в умовах збройних конфліктів: дослідження доктрин та політик. *Кібербезпека.* 2019. Том 2, № 1. С.3–15.

26. Кібербезпека в Україні: захист держави, бізнесу та громадян в інтернет. URL : https://www.slideshare.net/IIIZakharov/cyber–security–in–ukraine

27. Кібербезпека в Україні: стан та перспективи розвитку. URL : https://www.slideshare.net/IgorDubovoy/cybersecurity–in–ukraine–2019–148109150

28. Король Ю., Дідик В. Кібербезпека держави в умовах гібридної війни. *Економічні аннали–XXI*. 2018. № 174(3–4). С. 68–72.

29. Майкл Ч., Пурді Р. Кібербезпека в умовах війни. *Журнал міжнародних відносин*. 2018. № 19. С. 51–60.

30. Медіакультура в контексті міждисциплінарних досліджень : монографія / за загал. наук. ред. В. В. Березенко, М. А. Лепського, О.О. Семенець ; відп. ред. К. Г. Сіріньок–Долгарьова. Запоріжжя : Кераміст, 2017. 309 с.

31. Міжнародна організація з кібербезпеки (ICSPA). Офіційний сайт. URL : https://www.icspa.org/

32. Міжнародний інститут кібербезпеки (IICS). Офіційний сайт. URL : https://iics.com/

33. Мітюхін А. М., Корнієнко А. О., Зорін, О. В. Кібербезпека об’єктів критичної інфраструктури в умовах гібридної війни. *Науково–технічний вісник інформаційних технологій, механіки та оптики.* 2019. Вип. 19(2). С. 266–276.

34. Національний інститут стандартів та технологій (NIST) США. Спеціальна публікація NIST 800–53, що визначає стандарти та рекомендації з кібербезпеки. URL : https://www.nist.gov/publications/sp–800–53–rev–5

35. Полянський П. Освіта як об’єкт інформаційної війни Росії проти України і як ресурс протидії такій війні. URL : http//maidanua.org/2015/03

36. Почепцов Г. Сучасні інформаційні війни. Київ : Києво–Могилянська академія, 2015. 496 с.

37. Почепцов Г. Токсичний інфопростір. Як зберегти ясність мислення і свободу дії. Київ : Віват, 2021. 384 с.

38. Присяжнюк М., Жарков Я. Аналіз засобів ведення інформаційної боротьби з використанням інформаційних технологій, форм і способів їх застосування. *Вісник Київського національного університету імені Тараса Шевченка*. 2007. № 14–15. С. 42–44.

39. Прибутько П.С., Лук’янець І.Б. Інформаційні впливи: роль у суспільстві та сучасних воєнних конфліктах. Київ : Вид. А. В. Паливода, 2007. 252 с.

40. Радковець Ю. Гібридна політика сучасної Росії. *Урядовий кур’єр.* 2015. 20 жовтня. URL : https://ukurier.gov.ua/uk/articles/gibridna–politika–suchasnoyi–rosiyi/

41. Рижков М.М., Кучмій О.П., Бєлоусова Н.Б., Є.А. Макаренко, О.М. Фролова та ін. Інформаційний потенціал України в міжнародних відносинах : монографія Київ : Центр вільної преси, 2014. 284 с.

42. Русак І.С., Телелим В.М. Розвиток форм і засобів ведення інформаційної боротьби на сучасному етапі. *Наука і оборона*. 2000. № 2. С. 18–23.

43. Сідак В. С., Вронська Т. В. Спецслужба держави без території: люди, події, факти. Київ : Темпора, 2003. 240 с.

44. Сохань Л.В. Маргіналізація особистості в контексті глобалізації. *Українське суспільство: десять років незалежності*. 2001. С. 307–315.

45. Сучасні технології та засоби маніпулювання свідомістю, ведення інформаційних війн і спеціальних інформаційних операцій : навч. посіб. / за ред. В. М. Петрик, О. А. Штоквиш, В. І. Полевий. Київ : Росава, 2006. 208 с.

46. Тихомирова Є.Б. PR – формування відкритого суспільства. Київ : Наша культура і наука, 2003. 196 с.

47. Требін М. Інформаційне суспільство. Війни нової епохи. *ВІЧЕ*. 2002. № 4 (121). С. 64–68.

48. Україна в сучасному геополітичному просторі: теоретичний і прикладний аспект / за ред. Ф.М.Рудича. Київ : МАУП, 2002. 488 с.

49. Фісун А. О. Теоретично–категоріальне осмислення поняття «інформаційна війна» в структурі інформаційно–політичного простору. *Інформаційне суспільство*. 2011. Вип. 13. С. 43–48.

50. Центр кібербезпеки Міністерства оборони України. Офіційний сайт: URL : https://cyber.mil.gov.ua/

51. Центр кібербезпеки України. Офіційний сайт: URL : https://cybersecurity.ua/

52. Шаповал О., Фединяк О. та Кравченко В. Теоретико–методологічні засади забезпечення інформаційної безпеки держави в умовах гібридної війни. *Економіка і менеджмент*. 2018. Вип. 23(1). С. 7–15.

53. Яцко Н.Б. PR та маніпуляції: практичний словник. Київ : Карпенко В.М., 2013. 472 с.

Декларація академічної доброчесності
здобувача ступеня вищої освіти ЗНУ

Я_____, студент(ка)____курсу,
форми навчання _____, факультету_____,
спеціальність_____, адреса електронної пошти_____,

- підтверджую, що написана мною кваліфікаційна робота на тему «_____»

відповідає вимогам академічної доброчесності та не містить порушень, що визначені у ст. 42 Закону України «Про освіту», зі змістом якихознайомлений/ознайомлена;

- заявляю, що надана мною для перевірки електронна версія роботи є ідентичною її друкованій версії;
- згоден/згодна на перевірку моєї роботи на відповідність критеріям академічної доброчесності у будь–який спосіб, у тому числі за допомогою інтернет–системи а також на архівування моєї роботи в базі даних цієї системи.

Дата_____Підпис_____ПІБ (студент)__

Дата_____Підпис_____ПІБ(науковий керівник)_____

SUMMARY

This bachelor's thesis provides an analysis of the essence, characteristics, and implementation mechanisms of information warfare. The research is based on an examination of various scholarly articles, books, and case studies related to the topic.

The thesis begins by defining information warfare and exploring its significance in the contemporary digital age. It delves into the various forms and tactics employed in information warfare, including disinformation campaigns, cyberattacks, and psychological manipulation.

Furthermore, the thesis examines the actors involved in information warfare, such as state–sponsored groups, hacktivist collectives, and criminal organizations. It investigates their motivations, strategies, and tools used to exploit information vulnerabilities. The study also highlights the impact of information warfare on different sectors, including politics, national security, business, and society at large. It explores the consequences of information warfare, such as erosion of public trust, destabilization of democratic processes, and economic disruptions.

In addition, the thesis analyzes the countermeasures and defense mechanisms employed to mitigate the effects of information warfare. It discusses the role of governments, international organizations, and individuals in addressing this growing threat.

The findings of this research contribute to a deeper understanding of information warfare and its implications for the modern world. By examining its essence, characteristics, and implementation mechanisms, this study provides valuable insights into the evolving landscape of information warfare and offers recommendations for safeguarding against its harmful effects.