МІНІСТЕРСТВО ОСВІТИ ТА НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

Навчально-науковий інститут захисту інформації

На рецензію	захисту
Завідувач кафедри УІКБ	Завідувач кафедри УІКБ
доктор економічних наук, професор	доктор економічних наук, професор
_____ С.В. Легомінова	_____ С.В. Легомінова
«_____» _____2022 р.	___» _____2022 р.

ДИПЛОМНА РОБОТА

на тему:

ДОСЛІДЖЕННЯ КІБЕРСКЛАДОВОЇ ІНФОРМАЦІЙНОЇ ВІЙНИ РОСІЙСЬКОЇ ФЕДЕРАЦІЇ ПРОТИ УКРАЇНИ

СТУДЕНТ: Дьячук Олександр Станіславович

КЕРІВНИК: доцент кафедри Управління інформаційною та кібернетичною безпекою, к.т.н., доцент Дзюба Тарас Михайлович

НОРМОКОНТРОЛЕР: (підпис)

Київ - 2022

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
Навчально-науковий інститут захисту інформації
Кафедра управління інформаційною та кібернетичною безпекою
Освітньо-кваліфікаційних рівень – магістр
Спеціальність «Кібербезпека»
Спеціалізація «Управління інформаційною безпекою»

«ЗАТВЕРДЖУЮ»
Завідувач кафедри УІКБ
_____ С.В. Легомінова
(підпис)
“___”_____ 2021 р.

ЗАВДАННЯ
на дипломну роботу
студенту Дьячуку Олександру Станіславовичу

1. Тема роботи «ДОСЛІДЖЕННЯ КІБЕРСКЛАДОВОЇ ІНФОРМАЦІЙНОЇ ВІЙНИ РОСІЙСЬКОЇ ФЕДЕРАЦІЇ ПРОТИ УКРАЇНИ», затверджена наказом по університету від «11» жовтня 2021 р. № 170.

2. Термін здачі студентом оформленої роботи « 10 » січня 2022 р.

3. Об’єкт дослідження: інформаційна війна Російської Федерації проти України.

4. Предмет дослідження: кіберскладова інформаційної війни Російської Федерації проти України.

5. Мета дослідження: на основі аналізу змісту кіберскладової інформаційної війни Російської Федерації проти України обґрунтувати доцільні напрями забезпечення кібербезпеки України.

6. Перелік питань, які мають бути розроблені:

6.1. Дослідити особливості російської гібридної збройної агресії проти України. Визначити роль і місце в ній інформаційної війни.

6.2. Проаналізувати зміст заходів інформаційної війни проти України, які проводяться у кіберпросторі.

6.3. Обґрунтувати доцільні напрями забезпечення кібербезпеки України в умовах ведення проти України інформаційної війни.

7. Дата видачі завдання «14» жовтня 2021 р.

КАЛЕНДАРНИЙ ПЛАН

Дата видачі завдання: « 14 » жовтня 2021 р

№ з/п	Етапи дипломної роботи	Термін виконання етапів	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження	**21.10.2021**	
2.	Збір та аналіз літератури	**15.11.2021**	
3.	Дослідження особливостей російської гібридної збройної агресії проти України	**25.11.2021**	
4.	Дослідження особливостей російської гібридної збройної агресії проти України	**07.12.2021**	
5.	Обґрунтування доцільних напрямів забезпечення кібербезпеки України в умовах ведення проти України інформаційної війни	**24.12.2021**	
6.	Формулювання висновків за результатами проведеного дослідження	**25.12.2021**	
7.	Оформлення роботи	**10.01.2022**	
8.	Оформлення презентації	**11.01.2022**	
9.	Отримання рецензії на роботу	**12.01.2022**	
10.	Захист в ДЕК	**18.01.2022**	

Студент **О.С. Дьячук**

підпис

Науковий керівник **Т.М. Дзюба**

РЕФЕРАТ

Текстова частина магістерської роботи : 111 сторінок, 62 джерела.

Об’єкт дослідження: інформаційна війна Російської Федерації проти України. Предмет дослідження: кіберскладова інформаційної війни Російської Федерації проти України.

Мета дослідження: на основі аналізу змісту кіберскладової інформаційної війни Російської Федерації проти України обґрунтувати доцільні напрями забезпечення кібербезпеки України.

Методи дослідження: В роботі використаний широкий спектр різних методів аналізу: воєнно-політичного, SWOT, PEST, PMESII-ASCOPE; при обгрунтуванні пропозицій щодо забезпечення кібербезпеки України в умовах інформаційної війни, розв’язаної Російською Федерацією застосовувався системний підхід, зокрема декомпозиція всіх заходів з виділенням тих, як безпосередньо проводились в кіберпросторі, для подальшого синтезу пропозиції саме у сфері кібербезпеки.

Виконуючи поставлені завдання у магістерській роботі досліджені особливості російської гібридної збройної агресії проти України, визначені роль і місце в ній інформаційної війни, проаналізований зміст заходів інформаційної війни проти України, які проводяться у кіберпросторі, обґрунтуванні доцільні напрями забезпечення кібербезпеки України в умовах ведення проти України інформаційної війни.

Отримані результати вже частково реалізовані (розділи цілей та завдань реалізації Стратегії) в Стратегії кібербезпеки України, затвердженій Указом Президента України від 26 серпня 2021 року № 447/2021. Станом на сьогодні вони можуть використовуватись при формуванні пропозицій щодо Дорожньої карти реалізації Стратегії кібербезпеки України. Крім того, отримані результати можуть бути використані при підготовці фахівців з кібербезпеки.

ГІБРИДНА ВІЙНА, ІНФОРМАЦІЙНА ВІЙНА, ІНФОРМАЦІЙНА БЕЗПЕКА, КІБЕРБЕЗПЕКА.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ…… 7
ВСТУП……... 8
РОЗДІЛ 1. ОСОБЛИВОСТІ РОСІЙСЬКОЇ ГІБРИДНОЇ ЗБРОЙНОЇ АГРЕСІЇ ПРОТИ УКРАЇНИ……... 11
1.1 Огляд російсько-української гібридної війни…….. 11
1.2 Методи РФ……... 14
1.3 Задіяні частини, приватні компанії та громадські організації з російського боку…… 27
1.4 Задіяні частини, приватні компанії та громадські організації з українського боку…… 35
Висновки до першого розділу…… 36
РОЗДІЛ 2. АНАЛІЗ ЗМІСТУ ЗАХОДІВ ІНФОРМАЦІЙНОЇ ВІЙНИ ПРОТИ УКРАЇНИ, ЯКІ ПРОВОДЯТЬСЯ У КІБЕРПРОСТОРІ……... 39
2.1 Операція “ЗМІЯ”……. 39
2.2 Операція “Атака на «Вибори»”…… 41
2.3 Атаки на енергетичні компанії України……..… 48
2.4 Кібератаки на Мінфін, Держказначейство і Пенсійний фонд України…… 58
2.5 Компрометація ArtOS……. 58
2.6 Petya та NotPetya…….. 60
2.7 Операція «9 травня»…… 66
2.8 Операція «Прикормка»……... 66
2.9 Злам «Першого каналу»…….. 68
2.10 Блокування російських інтернет-сервісів……... 68
2.11 Псевдозамінування…… 71
Висновки до другого розділу……... 71
РОЗДІЛ 3. НАПРЯМИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ УКРАЇНИ В УМОВАХ ВЕДЕННЯ ПРОТИ УКРАЇНИ ІНФОРМАЦІЙНОЇ ВІЙНИ……. 74
3.1 Україна на 2016 – 2020 роки……... 74
3.2 Національна система кібербезпеки: засади робудови…….. 76

3.3 Національний кіберпростір виклики та кіберзагрози……... 79
3.4 Пріоритети забезпечення кібербезпеки україни та стратегічні цілі. 83
3.5 Стратегічні завдання…… 86
3.6 Напрями зовнішньополітичної діяльності України у сфері кібербезпеки……. 100
3.7 Механізми реалізації стратегії та забезпечення відкритості…….... 102
Висновки до третього розідлу…….. 104
ВИСНОВКИ……. 105
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ…… 106

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ

РФ - Російська Федерація

США - Сполучені Штати Америки

ЄС – Євро Союз

ОРДЛО - Окремі райони Донецької та Луганської областей

ООН - Організація об’єднаних націй

НАТО - Організація Північноатлантичного договору

ПАРЄ - Парла́ментська асамбле́я Ра́ди Євро́пи

ОБСЄ - Організація з безпеки і співробітництва в Європі

ДНР - Донецька Народна Республіка

ЛНР – Луганська Народна Республіка

РНБО - Рада національної безпеки і оборони України

ВСТУП

В умовах збройної агресії проти України, яка у формі кампаній, операцій та акцій гібридної війни продовжується вже восьмий рік поспіль, надзвичайно актуальною є роль інформаційної безпеки України.

Використання традиційних підходів, які базуються або на тріаді захисту конфіденційності, цілісності та доступності інформації разом зі спостережністю функціонування інформаційних систем або на захисті власного інформаційного простору сьогодні є малоефективним.

Сучасна інформаційна безпека – це динамічний процес, в якому заходи захисного характеру мають поєднуватись з активними заходами, спрямованими на формування необхідного стану інформаційного простору, просування власних змістів та ідей, превентивного знешкоджування джерел загроз інформаційній безпеці тощо.

Сьогодні ми маємо розвинене законодавство за напрямом кібербезпеки (Закон України «Про основні засади забезпечення кібербезпеки України», Стратегію кібербезпеки України та відповідні підзаконні акти). До того ж, Україна імплементує відповідні законодавчі документи міжнародного права у галузі кібербезпеки. Також, існує достатня кількість наукових публікацій, серед яких доцільно виділити монографії «Основи формування державної системи кібернетичної безпеки» В.Л. Бурячка, «Основи кібернетичної безпеки» Р.В. Грищука та Ю.Г. Даника, «Кібербезпека України на сучасному етапі державотворення: теоретико-правові основи» А.В. Тарасюка, «Кіберпростір, як новий вимір геополітичного суперництва» Д.В. Дубова, підручники, навчальні посібники та наукові праці В.Б. Толубка, В.А. Савченка, О.Г. Корченка, С.В. Толюпи, Ю.Г. Даника, Р.В. Грищука, В.Л. Бурячка, В.В. Семка, Д.В. Дубова, С.Л. Гнатюка, В.О. Бойка, Ю.І. Хлапоніна.

Також вже існує значна кількість наукових робіт за контентним напрямом інформаційної безпеки, до яких, перш за все слід віднести численні монографії Г.Г. Почепцова, наукові праці А.О. Рося, І.В. Замаруєвої, Л.Ф. Компанцевої, А.В. Баровської, О.М. Хайруліна, Я.М. Жаркова, М.Т. Дзюби, чудові дослідження Оксани Мороз «Нація овочів» та «Боротьба за правду».

Окремо слід відмітити книгу Д.Ю. Золотухіна «Біла книга спеціальних інформаційних операцій проти України: 2014-2018», в якій на прикладах реальних інформаційних операцій проти України, визначені конкретні шляхи забезпечення інформаційної безпеки.

Інтегрований підхід до забезпечення інформаційної безпеки України без її розділення на контентний та технологічний напрями викладений, перш за все, в монографії «Проблеми захисту інформаційного простору України» В.П. Горбуліна та М.М. Биченка та численних працях А.О. Рося . Серед останніх досліджень слід виділити монографії «Консолідація інформаційного законодавства України» та «Інкорпорація інформаційного законодавства України» В.А. Ліпкана, «Інформаційна безпека держави» В.М. Богуша та О.К. Юдіна, наукові праці В.Ю. Богдановича, Р.Р. Марутян, В.М. Петрика, М.М. Присяжнюка.

В усіх зазначених наукових працях викладені аргументовані авторські погляди на різні аспекти інформаційної безпеки, однак невирішеним залишається завдання інтеграції різних поглядів та підходів в єдину концепцію, яка могла б стати основою для розроблення відповідних нормативно-правових актів, визначення та практичної реалізації комплексних механізмів попередження та реагування на загрози інформаційній безпеці, активного впливу на світовий інформаційний простір для задоволення національних інтересів України.

З урахуванням зазначеного тема моєї роботи, яка присвячена дослідженню кіберскладової інформаційної війни Російської Федерації проти України є **актуальною**.

Мета роботи – на основі аналізу змісту кіберскладової інформаційної війни Російської Федерації проти України обґрунтувати доцільні напрями забезпечення кібербезпеки України.

Об’єкт дослідження: інформаційна війна Російської Федерації проти України.

Предмет дослідження: кіберскладова інформаційної війни Російської Федерації проти України.

Для досягнення поставленої мети в роботі вирішені наступні **часткові наукові завдання**:

досліджені особливості російської гібридної збройної агресії проти України, визначені роль і місце в ній інформаційної війни.

проаналізований зміст заходів інформаційної війни проти України, які проводяться у кіберпросторі;

обґрунтуванні доцільні напрями забезпечення кібербезпеки України в умовах ведення проти України інформаційної війни.

Методи дослідження. В роботі використаний широкий спектр різних методів аналізу: воєнно-політичного, SWOT, PEST, PMESII-ASCOPE; при обгрунтуванні пропозицій щодо забезпечення кібербезпеки України в умовах інформаційної війни, розв'язаної Російською Федерацією застосовувався системний підхід, зокрема декомпозиція всіх заходів з виділенням тих, як безпосередньо проводились в кіберпросторі, для подальшого синтезу пропозиції саме у сфері кібербезпеки.

Наукова новизна отриманих результатів. Результати були отримані в ході практичної роботи щодо формування проекту Стратегії кібербезпеки України та практичного виконання завдань забезпечення інформаційної безпеки в Операції Об'єднаних Сил.

Практичне значення дослідження Отримані результати вже частково реалізовані (розділи цілей та завдань реалізації Стратегії) в Стратегії кібербезпеки України, затвердженій Указом Президента України від 26 серпня 2021 року № 447/2021. Станом на сьогодні я приймаю участь в формуванні пропозицій щодо Дорожньої карти реалізації Стратегії кібербезпеки України. Крім того, отримані результати можуть бути використані при підготовці фахівців з кібербезпеки.

РОЗДІЛ 1. ОСОБЛИВОСТІ РОСІЙСЬКОЇ ГІБРИДНОЇ ЗБРОЙНОЇ АГРЕСІЇ ПРОТИ УКРАЇНИ

1.1 Огляд російсько-української гібридної війни

Три роки триває російська "гібридна" агресія, яка завдала Україні безпрецедентних людських, територіальних, економічних втрат – загинули понад 10 тис. українських громадян, 21 тис. поранені, 1,8 млн. – вимушених переселенців, окуповано 44 тис. км2 території (7%), зруйновано 20% промислового потенціалу країни.

Одним з глибинних мотивів російської агресії проти України було прагнення зірвати реалізацію українського "європейського проекту". Перспектива того, що Україна може стати прикладом проведення реформ і створити кращі умови життя для своїх громадян саме через реалізацію європейського, а не євразійського інтеграційного курсу, створює серйозну загрозу для правлячого режиму Росії.

На думку Голови Комітету Європарламенту у закордонних справах Е.Брока: "найгірше, що може трапитися з Росією – це якщо Україна стане демократичною і економічно успішною державою, де пануватиме верховенство права. Це буде ката- строфою для Кремля…"32.

З одного боку, в разі успіху європейських реформ в Україні закономірно постало б питання про нездатність керівництва Росії запропонувати привабливу для громадян модель суспільного розвитку. З іншого, – євроінтеграція України, вихід зі сфери впливу Росії означали б провал російсько центричного євразійського інтеграційного проекту, крах претензій Москви на регіональне лідерство та "особливі права" на пострадянському просторі.

Реалізація цілей "гібридної" агресії Кремля може досягатися через різні сценарії.

Перший з них передбачає доведення суспільно- політичної та соціально-економічної ситуації до вибухонебезпечного стану і формування лояльної до Росії (контрольованої нею) влади. Йдеться про формування в суспільстві та політикумі джерел нестабільності та конфліктів, створення нових

конфронтаційних ліній, формування атмосфери невпевненості і страху (в т.ч. за допомогою терактів).

Другий передбачає реалізацію неодноразово озвучених російським керівництвом цілей – федералізації України з можливістю регіонів впливати на зовнішню політику та політику безпеки держави. Це дало б можливість загальмувати європейську інтеграцію України й відмовитися від курсу вступу до НАТО, що, відповідно, викликало б опір більшості громадян і мас- штабний громадянський конфлікт. Засоби реалізації цього сценарію закладені в Мінських домовленостях, де головною вимогою до України є надання особливого статусу районам, контрольованим "ДНР-ЛНР". Розвиток подій в Україні в 2014-2016рр. характеризувався поєднанням обох сценаріїв.

На думку експертів, цілями російської агресії проти України є: зміна влади і встановлення контролю над Україною (66%), унеможливлення європейської і євроатлантичної інтеграції (59%), знищення української державності (36%).

Громадяни вважають головними причинами російсько-українського конфлікту: намагання України вийти з-під впливу РФ (46%), неприйняття Москвою євроінтеграційного курсу Києва та загалом України як самостійної держави з незалежною зовнішньою політикою (по 42%).

Російська агресія призвела до тектонічних, незворотних змін у відносинах Києва та Москви – зруйновані міждержавні інститути, демонтовані торговельні механізми, де-факто анігільована договірно-правова база (близько 350 документів).

"Гібридна" війна Росії проти України з усього модельного ряду міждержавних відносин (не кажучи про війну як таку) залишає Україні на тривалий період тільки формат вимушеного та конфронтаційного співіснування з Росією – залежно від поточної ситуації.

Нормалізація відносин з путінською Росією унеможливлена через наступні причини. По-перше, існує ряд базових проблем, де компроміс нині є неможливим. Не простежується перспектив вирішення проблеми анексованого Криму. Конфлікт на Донбасі в кращому випадку буде заморожений на

тривалий час. Для Кремля європейська інтеграція Києва є неприйнятною, а євроатлантична – неприпустимою.

По-друге, Україна під час війни отримала коло-сальний травматичний досвід від “братньої” країни. По-третє, відбулися довгострокові глибинні зміни в суспільній свідомості. За роки конфлікту докорінно змінилося ставлення громадян України до РФ, її керівництва, до політики Кремля, перспектив відносин з Росією. Виникла “прірва” відчуження, недовіри та ворожості.

Очікувати в найближчому майбутньому змін на краще в політиці Кремля на українському напрямі не доводиться. Слід нагадати, що 31 грудня 2015р. В.Путін підписав нову Стратегію національної безпеки, де повторюються тези про “підтримку США і ЄС антиконституційного перевороту в Україні”, “зміцнення ультраправої націоналістичної ідеології”. Такі тези лунали і в наступних виступах і заявах Президента РФ. Зокрема, на прес-конференції 10 серпня 2016р. В.Путін, “звинувачуючи” Україну – жертву російської агресії в тероризмі, неодноразово повторював: “люди, які захопили владу в Києві”. Аналогічні оцінки висловив В.Путін на ІІІ інвестиційному форумі 12 жовтня 2016р. Це означає, що російська сторона, як і раніше, сумнівається в легітимності української влади і не вважає європейський вибір Києва остаточним.

Прикладом безпрецедентного лицемірства та цинізму виглядає пасаж про Україну в новій Концепції зовнішньої політики РФ (затверджена В.Путіним 30 листопада 2016р.) – “РФ зацікавлена в розвитку всього різноманіття політичних, економічних культурних і духовних зв’язків з Україною, на основі взаємоповаги… Росія докладатиме необхідних зусиль для політико-дипломатичного врегулювання внутрішнього українського конфлікту”37.

З іншого боку, не варто орієнтуватися на прогнози швидкого економічного краху та розпаду Росії, близькі зміни у вищому кремлівському керівництві. (Подібні зміни в умовах авторитарного режиму не означають змін на краще). За результатами опитування російського Фонду “Громадська думка” 25 грудня 2016р., якби вибори відбулися наступної неділі, за В.Путіна проголосували б – 67%, за В.Жириновського – 8%, Г.Зюганова – 4%, а за іншого політика – лише 1% громадян РФ38. Така “прірва” між 67% і 1%

красномовно свідчить про тотальну відсутність реальної конкуренції нинішньому кремлівському лідеру. Слід додати, що в 2018р. до виборчих урн в РФ прийдуть представники нової генерації, які народилися і виросли за путінського режиму.

Експерти вважають, що найбільш реальним сценарієм розвитку відносин Україна-РФ у найближчий перспективі є продовження конфлікту в нинішньому стані (45%) або консервація конфлікту з наступним періодом конфронтації без застосування зброї (40%). Більшість громадян вважають, що найближчими роками відносини України і Росії або погіршаться (35%), або залишаться без змін (35%).

На офіційному рівні українська сторона визначила свою позицію стосовно РФ: Росія є державою-агресором і військовим противником; мета Кремля – руйнування української державності; агресія має довгостроковий характер, нормалізація відносин можлива за умови повернення окупованих територій, компенсації збитків від агресії, невтручання у внутрішні справи України.

1.2 Методи РФ

Разом з воєнними засобами агресії (окупація і анексія Криму, збройне вторгнення на Донбас), РФ використовує весь наявний арсенал засобів "гібридної" війни – від інформаційно-пропагандистської експансії, економічного, енергетичного тиску та дискредитації Києва на світовій арені до підривних, шпигунсько-диверсійних дій на українській території, підбурювання сепаратистських настроїв у регіонах і масованих кібератак на державні електронні мережи.

Серед арсеналу різноманітних засобів російської "гібридної" агресії проти України можна виокремити наступні.

Перше. Збройна агресія Росії. "Силовою" складовою "гібридної" війни РФ проти України є військова експансія – окупація і незаконна анексія Криму, згодом – вторгнення російських військ в ОРДЛО.

У лютому-березні 2014р. було окуповано півострів, блоковані українські військові частини і флот, транспортна інфраструктура, проведено псевдо-

референдум, ухвалено акт про незалежність Криму та ухвалено рішення про його входження до складу РФ. Отже, здійснена масштабна, швидка і заздалегідь ретельно спланована військово-політична спецоперація.

Окупаційна влада розпочала в Криму широкі етнічні чистки, запровадила геноцид кримсько-татарського народу, поширеною є практика політично мотивованих кримінальних переслідувань, викрадання людей, тортур, незаконних затримувань. У Криму спостерігається масове порушення прав людини, зокрема, свободи слова, віросповідання, права на мирні зібрання. У квітні 2016р. російська влада оголосила Меджліс кримськотатарського народу екстремістською організацією і заборонила його діяльність. Міжнародні правозахисні організації не мають доступу до Криму і можливості впливати на ситуацію.

Усі ці злочини російського окупаційного режиму окреслені та зафіксовані у Резолюції ГА ООН "Ситуація у сфері прав людини в Автономній Республіці Крим…" від 19 грудня 2016р. Світова спільнота загалом засудила анексію Криму. Зокрема, ще 27 березня 2014р. ГА ООН схвалила резолюцію, у якій висловила підтримку суверенітету, політичної незалежності та територіальної цілісності України. Незаконну анексію Криму засудили провідні країни світу та міжнародні організації – ООН, ЄС, НАТО, ОБСЄ, ПАРЄ, країни G-7 та ін. Відтак, у міжнародному дискурсі дедалі ширше утверджується визначення ситуації навколо Криму – як "незаконної анексії", "тимчасової окупації", а подій на Донбасі – як "російської воєнної інтервенції", "збройного конфлікту між Україною і РФ" (таблиця "Деякі між- народні документи…").

Нині тема анексії Криму перетворюється на "заморожену", відкладену проблему – не знайдено міжнародно-правових, політичних, економічних шляхів і механізмів вирішення ситуації з окупова-ним півостровом. Для керівництва РФ цієї проблеми не існує. У щорічному посланні Президента РФ Федеральним Зборам (3 грудня 2015р.) тема Криму була закрита, "возз'єднання Криму та Севастополя з Росією" оголошено як "принциповий, доленосний вибір шляху".

Три роки окупації довели, що для російського керівництва Крим є винятково стратегічно вигідною військовою базою, мілітаризованим плацдармом для зміцнення позицій у Чорноморському регіоні.

Одразу після захоплення Криму, Росія в березні 2014р. інспірувала та підтримала масові заворушення в окремих районах Донбасу, сприяла створенню сепаратистських "ДНР" і "ЛНР" і ввела туди регулярні збройні сили.

За три роки "гібридної" окупації Донбасу зусиллями РФ створено маріонеткові мілітаризовані псевдо-державні "владні" інституції. Тільки в "ДНР" налічується 20 "міністерств", всілякі: "народна рада", "рада міністрів", "прокуратура", "центробанк", "верховний суд". Діють свої профспілки, спілка журналістів та ін. Створена система ЗМІ у складі: семи телеканалів, чотирьох радіостанцій та 13 газет. Уся ця пропагандистська машина керується Міністерством пропаганди у складі 120 осіб. Громадські організації в "ДНР" представляє 140-тисячний рух "Донецька республіка".

У "республіках" створюється своя (повністю русифікована) система "патріотичного" виховання молоді за російськими методикам, що оспівує подвиги "ополченців". Система вищої освіти в "ДНР-ЛНР" повністю зав'язана на РФ. Йде відкрита і тотальна русифікація окупованих територій. Паралельно триває масова видача російських паспортів місцевим жителям.

У вересні 2015р. в "ЛНР" і "ДНР" як обов'язкова валюта введений російський рубль, за яким здійснюються розрахунки, в т.ч. виплати бойовикам. Курс на Росію однозначний і незаперечний. Лідер "ДНР" О.Захарченко ще у вересні 2015р. в зверненні до "жителів ДНР" заявляв про те, що вони не збираються повертатися в Україну і ведуть "дипломатичну битву з безжалісною терористичною бандою". У травні 2016р. він під час "прямих ліній" з жителями Одеси та Харкова закликав до розвалу України: "Може бути, навпаки, демонтувати її [Україну] та почати жити своїм власним життям". Він же 12 червня 2016р. в своєму зверненні привітав росіян з Днем Росії і заявив, що "кожен з нас захищає і готовий захищати до кінця право бути частиною "русского мира".

Російська сторона фактично створила в “ЛНР” і “ДНР” регулярну армію, кістяк якої складають російські спецпідрозділи, офіцери та генерали, і яка забезпечується російською технікою та озброєнням і діє під командуванням Міноборони РФ.

За даними Міноборони України, станом на кінець грудня 2016р. - початок січня 2017р., “армія ДНР/ЛНР” нараховує 40 тис. бойовиків, з яких 5 000 – регулярні російські війська. На озброєнні бойовиків – близько 600 танків, 1 300 БМП, 860 артилерійських систем, 300 систем залпового вогню.

Ситуація у “республіках” тотально контролюється російськими спецслужбами. Звичайною практикою стали інспекційні візити до Донецька комісій Генштабу РФ, спільне планування силових операцій за участю ФСБ і місцевих бойовиків.

За даними західних джерел, соціально-економічною сферою “ДНР-ЛНР” керує Уряд РФ через міжвідомчу комісію (шість робочих груп, створених п’ятьма російськими міністерствами) – контролюються фінанси, податки, інфраструктура, транспорт, енергоресурси і т.ін..

“Гібридна” анексія Донбасу створила “ДНР-ЛНР” – ворожу та чужу Україні мілітаризовану зону, просочену ідеологією “русского мира”, наповнену зброєю, вкриту густою мережею агентури та резидентури російських спецслужб, контрольовану армією бойовиків на чолі з російськими офіцерами. Причому, для багатьох бойовиків зворотна мирна “реінкарнація” у “шахтарів і трактористів” уже неможлива.

Слід констатувати, що зусилля міжнародної дипломатії в рамках “Нормандської четвірки” і тристоронньої контактної групи в Мінську не призвели ні до врегулювання, ні навіть до стабільного зупинення бойових дій на Сході України. 19 жовтня 2016р. в Бер-ліні відбулася зустріч лідерів Німеччини, Франції, України і Росії, де ухвалене рішення про розробку “дорожньої карти” з виконання Мінських домовленостей. Однак, 29 листопада на переговорах глав МЗС у “нормандському” форматі не досягнуто жодного результату. Причина – блокування переговорного процесу російською стороною, намагання країни-агресора включити до складу України

терористичні проросійські утворення “ДНР/ЛНР”, закріпивши їх “особливий” статус у Конституції. Це категорично неприйнятно для української сторони.

Російський план приєднання до України “ДНР” і “ЛНР” з конституційно закріпленим “особливим статусом”, перетворення бойовиків на “місцеву міліцію”, по суті, є “міною уповільненої дії” для Європи. Інтеграція до України терористичних утворень у нинішньому вигляді може спричинити масштабні соціальні протести, викликати небезпечні відцентрові тенденції в регіонах і критично дестабілізувати внутрішньополітичну ситуацію в Україні. Особливо небезпечним такий сценарій виглядає в умовах складної соціально-економічної ситуації, росту недовіри до діючої влади. Це є прямою загрозою українській державності, цілісності країни. По суті, врегулювання конфлікту на Донбасі за російським варіантом загрожуватиме ескалацією масштабного конфлікту в центрі Європи, новою “міграційною кризою”.

Нині ситуація на Донбасі залишатиметься вибухонебезпечною, існуватиме загроза ескалації конфлікту з непередбачуваними наслідками.

Друге. Гуманітарно-інформаційна агресія. Експансія в інформаційному просторі є ключовою і найнебезпечнішою складовою “гібридної” війни Росії проти України. Медіа-вплив Москви здійснюється упродовж усієї новітньої історії українсько-російських відносин. Але можна припустити, що “гаряча фаза” інформаційної війни розпочалася восени 2013р. напередодні Вільнюського саміту, де планувалося підписання Угоди про асоціацію Україна-ЄС. Кремль задіяв проти України потужну пропагандистську машину, яка охоплює теле та радіомовлення, друковані та електронні ЗМІ, кіно, театр і книговидання, концертну, фестивальну та виставкову діяльність, молодіжні субкультури та соціальні Інтернет-мережи, різноманітні громадські та релігійні організації. Головними інструментами зовнішньої інформаційної агресії РФ є потужні державні медіа-корпорації – телеканал Russia Today та агентство Sputnik.

У щорічній доповіді міжнародної організації Freedom House за 2019р. наголошується, що “Росія стала новатором сучасної державної пропаганди…Російська влада активізувала зусилля з маніпуляції ЗМІ в

геополітично значущих питаннях політики з сусідніми державами – Україною, Молдовою, країнами Балтії".

Спеціальна робоча група при Європейській службі зовнішніх дій (East StratCom Task Force) з жовтня 2020р. по липень 2021р. зафіксувала 936 випадків дезінформації, фейкових повідомлень кремлівської пропаганди російською мовою для громадян України, Білорусі, країн Балтії.

Важливим об'єктом російського впливу є внутрішньополітична ситуація в Україні, а також окремі політичні та громадські інститути: система влади, місцеве самоврядування, політичні партії і громадські рухи, релігійні організації, ЗМІ. Мета російської інформаційної (психологічної) війни – руйнація українського суспільства "зсередини" – через дискредитацію діючої влади, її курсу на європейську та євроатлантичну інтеграцію, інспірування соціального невдоволення і сепаратистських настроїв у регіонах, просування в українському культурно-інформаційному просторі доктрини "русского мира" і правомірності захисту "співвітчизників" на українській території. Загалом йдеться про дезінтеграцію і знищення української державності.

Методами російської ворожої пропаганди є відверта брехня, спотворення фактів, інсинуації, наклепи, інформаційні диверсії, провокації, викривлення історичних подій тощо.

Ворожа антиукраїнська пропаганда за сім років інформаційної агресії сформувала стійкий фальшивий стереотип сусідньої держави. Для звичайного росіянина Україна це країна, де:

1. За допомогою Заходу відбувся антиконституційний заколот і до влади прийшли "бандерівці", які розв'язали геноцид проти російськомовного населення і братовбивчу громадянську війну;

2. Русофобська київська влада проводить каральну операцію проти повстанців Донбасу;

3. Вороги Росії втягують Україну до ЄС і НАТО всупереч волі її народу;
4.Україна – "держава, яка не відбулася" і без Росії її чекає деградація і розпад.

Інформаційна агресія Кремля зруйнувала контакти українців і росіян, створила глибинний (в масштабах поколінь) вододіл відчуження, ворожості та недовіри між двома народами.

Україна вжила певних заходів з протистояння російській інформаційній експансії. Зокрема, в грудні 2014р. створено Міністерство інформаційної політики. Згодом, у жовтні 2015р. почала діяти Мультимедійна платформа іномовлення України. У 2015-2016рр. Україна запровадила пакетні санкції проти російських ЗМІ, діячів культури, видавництв тощо. (Зокрема протягом 2014-2021рр. Національна рада з питань телебачення і радіомовлення заборонила ретрансляцію 73 російських телеканалів). Відновлюється мовлення на окуповані території Донбасу. В жовтні 2016р. під егідою РНБО України створено Міжнародний інформаційний консорціум "Бастіон" для протистояння російському інформаційному впливу.

Однак, загалом контрзаходи української сторони є певною мірою ситуативними, досить вузько спрямованими і далеко не повною мірою відповідають масштабам російської експансії. Розгортанню дієвого спротиву на всьому гуманітарному, соціокультурному полі заважає відсутність державної гуманітарної політики, отже, – комплексного ідейного, ідеологічного забезпечення інформаційної діяльності.

Очевидно, що РФ (принаймні доки існуватиме її нинішній політичний режим) продовжуватиме інформаційну агресію проти України як у власному та українському інформаційному просторах, так і на міжнародному рівні. Також очевидно, що навіть у випадку "заморожування" ситуації на Донбасі, слід очікувати зміцнення головного напряму російської агресії- інформаційного. Причому ця медіа-експансія активізуватиметься мірою просування України на європейському та євроатлантичному шляху.

Економічна війна. Починаючи з середини 2000-х років важливим інструментом політичного та економічного тиску РФ на Україну РФ стало широке запровадження різноманітних торговельних обмежень. Мета цих заходів – заблокувати євроінтеграційний курс Києва і втягнути Україну до реінтеграційних проектів Кремля на пострадянському просторі.

Початком широкомасштабних торговельних воєн вважається 20 січня 2006р., коли РФ без попередження заборонила ввезення всіх видів української продукції тваринництва, нібито за її низьку якість. Надалі РФ залучала до антиукраїнських торговельних заходів країни-союзники. Зокрема, у червні

2011р. Митний союз (під тиском РФ) запровадив мита на українські метал і труби, підвищив мита на широко- вживані продовольчі товари – зокрема, цукор, гречку, картоплю, капусту тощо. Експорт українських солодощів було заборонено зовсім.

Гостра кризова ситуація виникла влітку 2013р. Так, 14 серпня всі українські товари, які постачалися до Росії, були віднесені до категорії ризикових, що фактично створило ситуацію "митної війни" – поставки всіх українських товарів до Росії були заблоковані. Невипадково ця економічна блокада України розпочалася напередодні Вільнюського саміту, де передбачалося підписання Угоди про асоціацію Україна-ЄС.

Росія використовувала всі наявні економічні важелі впливу:

1. Підвищення мита;
2. Заборона експорту українських товарів;
3. Дискредитація українських товарів в очах європейських споживачів;
4. Блокування постачань української продукції на ринки третіх країн;
5. Заборона українського транзиту через російську територію до Кавказького регіону та Центральної Азії;
6. Економічні диверсії. Все це здійснюється з метою руйнування української економіки, встановлення економічного та політичного протекторату й утримання Києва в зоні власних "привілейованих інтересів".

Ситуація катастрофічно погіршилася після військової агресії Росії проти України. Обсяги торгівлі стрімко знижувалися. Навіть у відносно "спокійному" 2013р. обсяги торгівлі між Україною та РФ скоротилися на 15%, а упродовж наступних 2014-2016рр. щорічне зниження сягало 35-40%.

За деякими оцінками, закриття російського ринку вже обійшлося Україні в $15 млрд. З іншого боку, разом із зниженням обсягів торгівлі з РФ, Україна позбувалася монополістичної залежності від Росії у низці галузей, насамперед газовій. Знаковим стало припинення імпорту російського газу для внутрішніх потреб з 25 листопада 2015р. Україна розірвала контакти у сфері військово-технічного співробітництва з РФ, денонсувавши пакет відповідних угод.

Нині Росія втратила виключне значення, як головний торговельний партнер для України. За підсумками дев'яти місяців 2016р. український експорт (товарів) до РФ зменшився на 30,1% (порівняно з відповідним періодом 2015р.) і його частка в загальному експорті становить лише 10% (для прикладу, у 2012р. частка українського експорту до РФ перевищувала чверть загального експорту країни).

Така тенденція зберігатиметься, в т.ч. і в результаті обопільних обмежувальних заходів (запровадження Росією обмежень на українську продукцію і відповідні контрзаходи української сторони).

За словами колишнього Президента П.Порошенка: "Напевно, стратегічно це добре, що таким кардинальним чином скоротилася наша залежність від російського ринку, де балом правлять не закони економіки, а політичний шантаж та імперський тиск". Загалом економічна політика Кремля на українському напрямі спрямована на загострення соціальної кризи, зниження обороноздатності країни, підігрівання протестних настроїв і, у підсумку, – зміни нинішнього політичного режиму. З огляду на це, сама по собі торгівля з РФ викликає питання, оскільки по суті це є спонсоруванням країни-агресора.

Хоча загальні обсяги торгівлі України з рештою країн світу також суттєво скоротилися, проте, по-перше, це стало відбиттям загалом зниження глобальних темпів міжнародної торгівлі, по-друге – наслідком російської агресії, через яку Україна втрати п'яту частину свого зовнішньоекономічного потенціалу, по-третє – започаткуванням Україною структурних змін переорієнтації на нові ринки та пошук нових конкурентних ніш. Натомість частка українського експорту до країн Європи (в загальному екс-порту) зросла з 24% у 2012р. до 40% у 2016р у 2021р до 60%.

Звичайно, відбуватиметься подальша переорієнтація зовнішньої торгівлі України на нові ринки (в т.ч. висхідних країн), за збереження стратегічної орієнтації на розвинуті країни ЄС та Північної Америки.

Четверте. Енергетична агресія. Упродовж багатьох років Україна залишалася залежною від імпорту енергетичних ресурсів з Росії: природного газу (Україна змушена була імпортувати до 50 млрд. м3 на рік), нафтопродуктів, палива для АЕС (сьогодні країна закуповує понад 90%

ядерного палива), а згодом – для ТЕС, що перетворило газ, нафту, ядерне паливо та вугілля на важелі тиску на Україну з боку сусідньої держави. Така ситуація склалася через історичну тісну виробничу співпрацю, яка будувалася на доступі до дешевих енергоресурсів СРСР, що зробило їх, а згодом й енергетичну інфраструктуру інструментами ведення "гібридної" війни Росією проти України з метою збереження контрою над останньою та досягнення власних політичних цілей.

Енергетичним ресурсом, яким Росія почала шантажувати Україну, став природний газ. "Газова" війна Росії проти України розпочалася задовго до початку військових дій: першими проявами її стали газові кризи у 2006р. і 2009р., коли Росія переривала транзит природного газу територією України. Енергетична зброя стала ефективною за умов 100% залежності України від поставок газу монополістом, яким виступав ВАТ "Газпром", що давало можливість Росії диктувати ціни на газ – з 2005р. ціна підвищилася з $50 за 1 000 м3 до $420 за 1 000 м3 у 2012р.

Натомість ряд реформ, проведених в енергетичному секторі протягом 2014-2021рр., дозволили відмовитися від закупівель природного газу у Росії, чим вдалося зламати російську газову монополію. Україна диверсифікувала поставки природного газу і у 2015р. підписала договір з угорським оператором про об'єднання транскордонних газопроводів. (Однак, український оператор – ПАТ "Укртрансгаз" – не може повноцінно співпрацювати з операторами суміжних ГТС країн-членів ЄС через поточні схеми їх взаємодії з ВАТ "Газпром". Зокрема, російська компанія не надає українській стороні шипер-коди (інформацію про окремі партії газу, який транспортується територією України)).

Зрозумівши, що Україна може обходитися без російського газу, Росія у якості енергетичної зброї почала використовувати інфраструктурний компонент – створення маршрутів транспортування природного газу в обхід України, реалізація яких є досить витратною, технологічно складною та економічно необгрунтованою. Серед таких проектів – Південний потік, Турецький потік та Північний потік, метою яких є ослаблення України як надійного транзитера, а також енергетичної безпеки і України, і Європи. З

початком експлуатації “Турецького потоку” та підвищенням прокачування природного газу по OPAL Україна може втратити значний обсяг транзиту природного газу, що скоротить її валютну виручку від транзиту газу та негативно відобразиться на роботі ГТС.

Російська агресія завдала величезних збитків українській енергетичній інфраструктурі. Внаслідок анексії Криму Україна втратила ряд об’єктів ПЕК та перспективних територій для розробки вугле- водневих ресурсів, а воєнна експансія на Донбасі призвела до руйнування нафтогазової інфраструктури та енергетичних об’єктів у Донецькій і Луганській областях.

Через військові дії на Сході України відбулося суттєве зменшення видобутку антрацитового вугілля, що спричинило нарощування його імпорту, головним чином з Росії (через менші логістичні витрати та часові рамки). Натомість, поставки антрациту на вітчизняні ТЕС неодноразово заморожувалися РФ, що ставило під загрозу безперебійне електропостачання країни. Зокрема до середини 2015р. вугілля не надходило з окупованих територій Донбасу, а Росія блокувала постачання антрациту.

Нині російська енергетична експансія спрямована, з одного боку, на дискредитацію і ліквідацію України як країни-транзитера енергоресурсів, іншого – на захоплення/руйнування української енергетичної інфраструктури, що загрожує сталому функціонуванню системи життєзабезпечення країни в цілому.

П’яте. Російська кіберекспансія. Вкрай небезпечною складовою “гібридної” війни проти України є агресія в кіберпросторі. Зокрема, йдеться про масовані атаки на сайти органів влади і державних компаній, війну в соцмережах, яку розгорнули російські “фабрики тролів”, кібершпигунство. З російського боку діють численні хакерські групи, зокрема такі як Sandworm, “Кіберберкут”, “Спрут” (з території “ДНР”) та ін. Очевидно, що за ними стоять і керують їх діяльністю російські спецслужби. (Для протистояння російській кіберекспансії українські волонтери в 2014р. організували групу “Українські кібер-війська”. Також було створено український “кибералья́нс” (об’єднання груп FalconsFlame, Trinity, “Рух8” і “КиберХунта”).

Російська “гібридна” агресія в кіберпросторі набуває розмаху. Група CERT-UA (Computer Emergency Response Team of Ukraine) при Державній службі спецзв’язку в 2014р. зафіксувала 216 кібератак ззовні (більше половини з них – на державні установи). У 2015р. кількість атак збільшилася в 1,5 рази. За останні три роки проросійські хакери здійснювали масовані напади на урядові інтернет-портали та інтернет-ресурси державних органів, зокрема на сайти Адміністрації Президента, Кабінету Міністрів, Держспецзв’язку. Були атаковані портали ряду обласних державних адміністрацій, де хакери завантажували антиукраїнський контент і радянську символіку.

23 грудня 2015р. відбулася найнебезпечніша кібердиверсія, коли було завдано масований удар по диспетчеру компанії “Укренерго” і 6 енергокомпаніям, що призвело до відключення електроенергії у 103 населених пунктах на Заході України (використовувався небезпечний вірус BlackEnergy). Американські експерти встановили, що ця масована диверсія була здійснена з боку РФ. А вже в січні 2016р. були атаковані Інтернет-ресурси аеропорту “Бориспіль”.

27 січня 2016р. на засіданні РНБО України, при- свяченому створенню державної системи кіберзахисту.

15 березня 2016р. Указом Президента було введено в дію рішення РНБО “Про стратегію кібербезпеки України”. Згідно з цим документом при РНБО був створений Національний центр кібербезпеки. Попри те, що при силових структурах України були сформовані спеціальні підрозділи електронного захисту (зокрема в МВС в 2015р. було створено підрозділ кіберполіції) країна виявилася неготовою до війни в Інтернет-просторі.

У 2020 році в Україні було зафіксовано близько одного мільйона випадків кіберзагроз. Серед них – мережеві атаки, спроби мережевого сканування, спроби WEB-атак, фішинг, DDoS-атаки, поширення шкідливого програмного забезпечення. Звідки це «прилітало» – здогадатися не складно, враховуючи те, з ким наша держава на сьогодні знаходиться в стані війни де-факто. Відтак нагальна потреба у кібервійську - абсолютно очевидна.

Саме тому Президент Зеленський підписав 14 травня 2021 року указ, яким постановив ввести в дію інше рішення РНБО "Про Стратегію

кібербезпеки України", затвердити Стратегію кібербезпеки України, а також визнати такою, що втратила чинність, статтю 2 Указу президента України від 15 березня 2016 року "Про рішення РНБО від 27 січня 2016 року "Про Стратегію кібербезпеки України".

Цим указом Президент постановив ввести в дію відповідне рішення РНБО та контролювати виконання цього рішення. Указ Президента набув чинності в день його опублікування.

Рішення РНБО передбачає, що для створення у системі міністерства оборони України кібервійськ потрібно розрахувати обсяг матеріально-технічних та фінансових ресурсів, необхідний для їхнього створення та функціонування. А також потрібно укомплектувати особовий склад кібервійськ з урахуванням оптимального співвідношення військовослужбовців, працівників міністерства оборони України, а також зарахованих у запас, резервістів та інших категорій осіб.

Свідченням масштабності кібервійни РФ проти України стала нещодавня масована інтернет-диверсія проти українського фінансово-банківського сектору. 6 грудня 2016р. внаслідок хакерської атаки була забло-кована робота сайтів Державного казначейства, Міністерства фінансів, Пенсійного фонду. Згодом були атаковані Інтернет-ресурси “Укрзалізниці” і Міноборони. Російська агресія в Інтернет-просторі викликала дуже серйозне занепокоєння спецслужб ряду країн світу. Спецслужби США звинуватили вище керівництво РФ в організації ківбердиверсій під час виборчої кампанії в США. Про небезпеку російського втручання заявили представники розвідслужб Німеччини, Чехії, інших країн Європи.

Очевидно, що активність і масштаби російської інтернет-експансії проти України зростатимуть. Кібер-агресія стає однією з головних складових “гібридної” війни Кремля проти України.

Експерти вважають, що найбільш небезпечними засобами російської “гібридної” агресії є – пропагандистська експансія в українському медіа-просторі (4,4 бали за п’ятибальною шкалою), ведення бойових дій в зоні АТО (4,3), мілітаризація Криму і ОРДЛО (4,3), шпигунська діяльність російських спецслужб (4,3). Також дуже небезпечними є – підтримка “п’ятої” колони в

органах влади і ЗМІ, підбурювання сепаратистських настроїв у регіонах, кібератаки на українські комп'ютерні мережи тощо.

1.3 Задіяні частини, приватні компанії та громадські організації з російського боку

Поряд із військовим фронтом на сході України, ще у 2003 році було відкрито невидимий фронт – інформаційний.

Про інформаційну агресію РФ написано вже чимало, але, зазвичай, розглядаються традиційні ЗМІ. Кіберпростір та одна з його складових – Інтернет – довший час були відносно поза увагою.

Проте сьогодні в широкий дискурс ввійшло поняття україно-російської кібервійни, яка багатьма дослідниками вважається чи не першою у світовій історії.

Рунет швидко об'єднав навколо себе сегменти майже всіх пострадянських країн. Цьому сприяли безліч причин, що переросло в повну домінацію російських соціальних мереж (ВКонтакте, Одноклассники), поштових сервісів (mail.ru), пошукових систем (yandex.ru), програмного забезпечення (1С).

Англомовний сегмент Інтернету залишається, здебільшого, terra incognita для українського користувача, окрім ресурсів з україномовною локалізацією. Західні соціальні мережі, як Фейсбук, лише в червні 2017-го змогли обійти російські у відвідуваності.

Російська агресія в кіберпросторі має дві площини, які умовно можна поділити на інформаційну та хакерську.

Інформаційна площина. Її можна охарактеризувати як систематичне, постійне транслювання певних ідей, концепцій, гасел, закликів, ярликів, послань у кіберпросторі. Найбільше це відбувається в соціальних мережах, інформаційних порталах, тематичних групах і чатах, у коментарях під новинами.

Ззовні це виглядає як полеміка: один користувач пише коментар під новиною чи пост у соціальній мережі. Метою таких заходів є нав'язування

певних ідей, створення ілюзії "громадської" думки. На більш високому рівні – це ньюзмейкінг або створення новин.

Тривалий час суб'єкти таких інформаційних приводів зберігали відносну анонімність, проте після розкриття "тролів з Ольгіно" та зізнань британської журналістки, яка працювала в "Russia 24", Сари Фьорт (Sara Fert), стало відомо, хто за цим стоїть, та масштаби дій, які проводяться.

Слід зазначити, що такі дії спрямовані не лише проти України, але й проти США та країн ЄС. Основними акторами є так звані "тролі" – фейкові й лише в рідкісних випадках справжні аккаунти користувачів, які займаються інформаційними провокаціями, створенням фейкових новин, інформаційних приводів, коментарів, дописів.

У контексті інформаційної кібервійни проти України існують цілі фабрики тролів, які за фінансову винагороду займаються цією діяльністю.

Загалом схема впровадження атаки в інформаційному просторі виглядає так:

1. Тролі (або заангажовані чи підкуплені експерти) під виглядом очевидців, фахівців чи інших спеціалістів створюють інформаційний привід.

2. Російські ЗМІ озвучують новину, посилаючись на джерело з пункту 1 як на об'єктивне та фахове.

3. Миттєво за цим слідують тролі, які починають обговорення новини в мережі, створюючи ілюзію резонансу та правдивості інформації.

За такою простою схемою криється ефективний механізм маніпуляції свідомістю, перекручування фактів, виставлення тих чи інших подій у необхідному світлі.

Хакерська площина. Вона відрізняється від інформаційної тим, що веде боротьбу не лише на інформаційному полі, а й на фізичному рівні кіберпростору. Ця діяльність має на меті виведення з ладу техніки, програмного забезпечення, завдання економічних збитків і так далі.

У розрізі унікальних акторів, задіяних у кібервійськових заходах, можемо виділити такі:

З російського боку: згідно відкритих даних, на чолі кібервійськових операцій стоїть Федеральне агентство урядового зв’язку та інформації при президенті Російської Федерації (рос. ФАПСИ).

Цей орган є керуючим та координує інші підрозділи, зокрема:

"КіберБеркут" (англ. CyberBerkut) – інтернет-бренд, під яким відбуваються хакерські атаки, в основному на сайти державних і громадських організацій України. Американський спеціаліст з комп'ютерної безпеки Джефрі Карр 2014 року припустив, що це група проросійських хактивістів, яка працює проти України. За даними британського Національного центру комп'ютерної безпеки за фасадом «КіберБеркуту» ховається підрозділ російської військової розвідки, відомий як Fancy Bear. Це хакерська організація, якій приписують атаки на сайти ЦВК, МВС, ГПУ, президента України; оприлюднення приватних листувань посадовців, політиків, активістів Майдану та військових; розповсюдження пропагандистської інформації. Експерт з інформаційної безпеки В’ячеслав Гусаров говорить, що матеріали, які вони публікують, є необґрунтованими, позбавленими фактичної основи та мають на меті дискредитацію України.У доповіді Розвідувального управління Міноборони США "Russia Military Power" йдеться, що "КіберБеркут" створений для ведення російської державної кібердіяльності, підтримки військових операцій та стратегічних цілей Росії, з використанням технічних та пропагандистських кібератак не лише проти України, а й проти країн НАТО.

"Sandworm" – відомі після атаки на енергетичні системи в Україні та пов’язані з цим збої подачі електроенергії 23 грудня 2015 року. Їх називають причетними до атак на низку підприємств залізничного комплексу в 2014-му.

"Sofacy Group" (також: APT 29; Pawn Storm; Fancy Bear та Sednit та інші) відомі проведенням заходів "Змія" ("Уробурос", англ. "Uroburos") та резонансної кібератаки вірусом "Petya".

"APT29" - кібершпигунське угруповання типу розвиненої сталої загрози, яке діє щонайменше з 2008 року та перебуває на території Російської Федерації. Основну увагу приділяє добуванню інформації, необхідної для ухвалення рішень із зовнішньої політики та оборони. Переважно жертвами угруповання стають уряди західних країн та пов'язані з ними організації:

міністерства, агенства, аналітичні центри, виконавці державних замовлень. Також їхніми жертвами ставали уряди країн-членів СНД, Азії, Африки, Близького сходу; організації, пов'язані з чеченськими борцями за незалежність, а також російськомовні продавці наркотиків. Це угруповання діє під управлінням та в інтересах ФСБ або Служби зовнішньої розвідки РФ. Різні дослідники та компанії з кібербезпеки давали відмінні назви цьому угрупуванню. Зокрема, з ним пов'язують такі назви: APT29, Office Monkeys, CozyCar, The Dukes, CozyDuke та Grizzly Steppe.

Угруповання має у власному арсеналі широкий набір інструментів зловмисного програмного забезпечення. В середині 2010-тих можна було спостерігати здійснення угрупованням масованих операцій адресного фішингу проти сотень (інколи — навіть тисяч) кореспондентів з різних урядових та пов'язаних з ними організацій.

Типова атака складалася з грубого (надто помітного для фахівців з інформаційної безпеки) проникнення до інформаційної системи, стрімкого збирання та викрадення інформації. Якщо виявлялося, що жертва становить особливий інтерес, то угруповання переходило до використання менш помітних інструментів для забезпечення тривалого доступу до враженої інформаційної системи.

На додачу до масованих, угруповання здійснювало операції меншого масштабу, більш зосереджені та з використанням іншого набору інструментів. Жертви цих вузькоспрямованих операцій на час атак перебували в полі зору російського уряду з питань міжнародних відносин та оборони.

Угруповання було дуже чутливим до оприлюднених про нього досліджень і зазвичай змінювало тактику та застосовані інструменти щоб уникнути виявлення. Однак, попри розголос, угруповання не зупиняло операції.

У надзвичайних випадках угруповання могло здійснювати операції із незміненими інструментами навіть після їх розголошення в спеціалізованих публікаціях та ЗМІ. Таким чином, воно демонструвало свою впевненість у безкарності за скоєні злочини.

“Turla” також відоме якUroburos/Epic Turla/Snake/SnakeNet/Venomous Bear/Krypton — угрупування типу розвинена стала загроза. Служба зовнішньої розвідки Естонії вважає, що угрупування SNAKE (Turla) працює в інтересах ФСБ РФ. Угрупування спеціалізується на шпигунстві проти різних урядових установ та оборонно-промислових комплексів різних країн.

В першому бюлетені 2016 року німецька служба контррозвідки — Федеральна служба захисту конституції Німеччини (нім. BfV), надала високу оцінку здібностям російської розвідки а також представила широкий перелік відомих жертв російських кібератак. Угрупування Turla було назване серед відомих угрупувань типу розвинена стала загроза, які пов'язують з Росією або російськими підрозділами спеціального призначення.

З даним угрупуванням пов'язують сімейство гнучких модульних інструментів-зразків шкідливого ПЗ Snake. Зустрічаються назви Turla, «уроборос», англ. uroborus (також англ. ouroborus — гадюка в грецькій міфології, або англ. sengoku та англ. snark).

Фахівці із CERT-UA виявили кілька особливостей вірусу Uroborus:

1. Складність програмного коду (що обумовлює можливість його розроблення із залученням значної кількості людських, технічних і фінансових ресурсів (зокрема, це можуть бути науково-дослідні установи, IT-корпорації, державні установи, спецслужби тощо);

2. Наявність літер кирилиці у програмному коді;

3. Схожість за низкою характеристик (імена файлів, ключі шифру, основні можливості тощо) із троянською програмою Agent.BTZ, яку було знайдено в інформаційних системах ЗС США в 2008 році, що призвело до повної відмови ЗС США від використання USB-носіїв (через які вона поширювалася в автоматизованих системах військового призначення);

Географія поширення вірусу. «Уроборос» здатен поширюватись різними способами, зокрема, через так звані атаки Watering-Hole. Його складно виявляти, він працює автономно, та самостійно поширюється в інфікованих мережах. Враженими можуть бути навіть комп'ютери без прямого підключення до Інтернет.

«Тро́лі з О́льгіна» також «фабрика тролів», «кремлеботи» — загальне позначення користувачів-провокаторів (тролів), які за гроші у спеціально обладнаних офісах лишають дописи та коментарі під новинами інтернет-видань або на інших ресурсах в мережі з метою розповсюдження російської пропаганди в соціальних мережах. Робота найнятих коментаторів, які розміщували неправдиву інформацію і провокативні коментарі, стала однією зі складових масштабної інформаційної війни Росії проти України. При цьому використовувалися не лише російські інтернет-ресурси, але й інтернет-ресурси України, Європи, США за для висвітлення подій з вигідної для російської пропаганди точки зору, або для формування громадської думки щодо них. Неофіційна назва однієї з викритих установ («Агентства інтернет-досліджень» із штаб-квартирою у Санкт-Петербурзі) — «фабрика тролів», — дала широковживане алегоричне ім'я всім таким структурам.

Поняття походить від спеціально обладнаного для тролінгу офісу, який російські журналісти викрили у 2013 році в Ольгіні, історичному районі Санкт-Петербурга. Пізніше назви «тролі з Ольгіна» або «ольгінські тролі» стали загальними щодо тролів, які здійснюють російську пропаганду, без прив'язки до офісу в Ольгіні.

Російське видання «Ведомости» пов'язує ухвалену російською владою стратегію маніпулювання суспільною свідомістю через нові медіа з В'ячеславом Володіним, першим заступником голови адміністрації президента Російської Федерації.

За даними журналістів-розслідувачів, офіс в Ольгіні мав офіційну назву ТОВ «Агентство інтернет-досліджень» (рос. ООО «Агентство интернет-исследований»). Структуру заснували влітку 2013 року.

Журналісти також вказують, що до офісу в Ольгіні прямо причетним був Олексій Сосковець — виходець з молодіжного політичного середовища Росії. Його фірма «Північно-Західне агентство послуг» виграла 17 або 18 (за різними даними) конкурсів на проведення свят, форумів і спартакіад для органів влади Санкт-Петербурга. У половині конкурсів агентство брало участь одноосібно. Влітку 2013-го виграло конкурс на транспортне обслуговування учасників табору «Селіґер».

У 2014 році, за інформацією російських ЗМІ, в організації діяльності стала фігурувати компанія під назвою ТОВ «Інтернет дослідження» (рос. ООО «Интернет исследования»). Її заснували в березні 2014 року. Журналісти видання «Новая газета» називають товариство наступником ТОВ «Агентство інтернет-досліджень». ТОВ «Інтернет дослідження» пов'язують із Євгеном Пригожиним, який є головою холдингу «Конкорд». «Ольгінських тролів» у Санкт-Петербурзі називають саме його проектом. Станом на жовтень 2014 року товариство належить Михайлу Бистрову, що раніше очолював управління внутрішніх справ Московського району Санкт-Петербурга.

Російські ЗМІ вказують, що відповідно до документів, оприлюднених хакерами «Анонімного інтернаціоналу», холдинг «Конкорд» має прямий стосунок до управління тролінгом через товариство. Зокрема, дослідники наводять листування через електронні скриньки, в якому «Конкорд» дає вказівки виконавцям тролінгу, а отримує від них звіти за виконану роботу. За даними журналістів, у 2000 році цей холдинг організовував бенкети у Кремлі, а також співпрацює з «Воєнторгом» та Міністерством оборони Російської Федерації.

Попри зв'язки із Олексієм Сосковцем, заступник голови комітету з молодіжної політики Санкт-Петербурга Надія Орлова заперечила причетність її установи до офісів із здійснення тролінгу.

За свідченнями журналістів-розслідувачів і колишніх співробітників офісів, основна тематика дописів і коментарів тролів така:

1. Критика Олексія Навального, його спонсорів, а також російської опозиції в цілому;
2. Критика зовнішньої політики України та США, а також перших політиків цих країн;
3. Вихваляння політики Росії та Володимира Путіна.

Журналісти відзначають, що тематика тролення однакова з тематикою російської пропаганди, її тези збігаються у часі. Технічні завдання для тролів беруть переважно з контенту телеканалу Russia Today.

За даними американського видання BuzzFeed, із квітня 2014 року розпочалась організована кампанія із формування необхідної російській владі

думки у країнах Західного світу про російську збройну агресію проти України у 2014 році. Такі висновки журналісти роблять із документів, які опинилися у їхньому розпорядженні. Як повідомляє видання, в документах містяться інструкції для коментаторів сайтів Fox News, Huffington Post, The Blaze, Politico и WorldNetDaily. В них також викладено очікуваний об'єм робіт від тролів: в середньому за день вони мають залишати до 50 коментарів до новинних статей. Кожен блогер повинен вести 6 акаунтів у Facebook, публікуючи мінімум 3 записи в день і двічі беручи участь в обговореннях у спільнотах. Інші співробітники повинні вести по 10 акаунтів на Twitter, публікуючи по 50 твітів щодня. На підставі аналізу документів журналісти роблять висновок, що керівником проекту ймовірно є Ігор Осадчий, а саму кампаніє здійснює ТОВ «Агентство інтернет-досліджень». Осадчий свою причетність до товариства спростовує.

Українські користувачі Facebook зазначають, що проти них діє організована система російських ботів. Вони цілеспрямовано працюють на блокування сторінок відомих українських користувачів соціальної мережі. У 2015 році проблема набула скандалу найвищого рівня. З проханням відкрити офіс Facebook в Україні, який би не залежав від Росії, до Марка Цукерберга звернувся навіть Президент України Петро Порошенко. Українські користувачі збираються подавати до суду за блокування.

На початок 2016 року видання «Укрінформ», провівши журналістське розслідування, виявила систему ботів у соцмережах, які поширюють в інтернеті заклики до насилля до української влади та заклики виходити на «Третій Майдан». Згідно з розслідуванням, організатором є Сергій Жук, колишній бойовик антиукраїнських сил із Донбасу. Свою діяльність в інтернеті він вів із Внуково, що у Москві.

На початок квітня 2018 року адміністраторами було видалено 70 облікових записів Facebook, 138 сторінок Facebook та 65 облікових записів Instagram, контрольованих «фабрикою тролів». В сумі — 273 сторінки та облікових записів.

Видалені сторінки були орієнтовані на російськомовну аудиторію як в Росії, так і за її межами, в тому числі — в Україні, Азербайджані, Узбекистані.

Деякі з видалених сторінок належали «агентствам новин», але насправді ними керували працівники «фабрики». Зокрема, одне із заблокованих видань мало близько мільйона підписників у Facebook і близько 500 тисяч в Instagram. Імовірно серед видалених сторінок були «Федеральное агентство новостей», «Журналистская правда», «Невские новости» та «Экономика сегодня».

1.4 Задіяні частини, приватні компанії та громадські організації з українського боку

"Український кіберальянс" – об'єднання хакерів та кіберактивістів на основі "FalconsFlame", "Trinity", "RUH8" та "Кіберхунти". Мета діяльності – протидія російській кіберагресії.

Відомі за зламом електронних скриньок російських активістів і ватажків терористів; кібератаками на пропагандистські ЗМІ ("Анна Ньюз", "Перший Канал"), міністерства РФ та так звані "ДНР" і "ЛНР"; публікаціями електронного листування терористів та російських високопосадовців.

"Українські кібервійська" – ініціатива, створена Євгеном Докуніним. Основною метою є проведення оборонних та наступальних операцій в Інтернеті, протидія сепаратизму, тероризму та інформаційній війні проти України.

Відомі блокуванням мобільного зв'язку та близько 450-ти банківських рахунків терористів; хакерськими атаками на близько 150 веб-ресурсів та віддаленим захопленням веб-камер терористів у Криму.

Матеріали з цих камер є доказом російської агресії та інформують про переміщення живої сили й техніки противника.

"ІнформНапалм" (англ. InformNapalm) – відомі проведенням незалежного розслідування катастрофи малайзійського Боїнга; базою даних російських підрозділів, які воюють в Україні. Основний метод діяльності базується на принципі Open source intelligence – зборі інформації з відкритих джерел, соціальних мережах і тому подібне.

Характерною особливістю є переклад інформації на більш ніж два десятка мов, які неодноразово використовувалися у звітах Bellingcat про

присутність російських регулярних військ на території України та їх вину в катастрофі малайзійського "Боїнга" 17 липня 2014 року.

"Миротворець". Широко відомі завдяки ЗМІ через бази даних осіб, задіяних у сепаратизмі, незаконному відвідуванні тимчасово окупованого Криму, підтримці агресивної політики Кремля.

У контексті кібервійни відзначилися розробкою автоматизованої системи аналізу та розпізнавання облич Identigraf, що покликана обробляти масивні бази даних та виявляти порушників.

Україна на державному рівні вживає такі заходи:

1. Закон "Про основні засади забезпечення кібербезпеки"; ухвалення стратегії кібербезпеки; указ президента, який вводить в дію рішення РНБО щодо невідкладних дій та нейтралізації загроз кібербезпеці держави.

2. Створення Команди реагування на комп'ютерні надзвичайні події – CERT-UA (англ. Computer Emergency Response Team of Ukraine).

3. Національний координаційний центр кібербезпеки – робочий орган при РНБО.

4. Програма Трастового фонду НАТО зі сприяння Україні в зміцнені її спроможності у сфері кіберзахисту.

5. Створення Центрів кібернетичної безпеки в системі ЗСУ та Департаменту кіберполіції Національної поліції.

6. Санкції проти російських розробників програмного забезпечення (Доктор Веб, Лабораторія Касперського); блокування доступу до деяких веб-ресурсів.

Висновки до першого розділу

"Гібридна" агресія Кремля несе не лише загрозу державності України, її суверенітету, а загалом пост-гельсінському політичному устрою Європи. Кремль намагається дискредитувати базові європейські цінності, дезорієнтувати громадську думку, сформувати впливове проросійське лобі в європейському істеблішменті, поглибити розбіжності між європейськими державами та інституціями ЄС. Йдеться про ведення масштабної "гібридної" експансії саме на теренах ЄС з метою максимального

послаблення/фрагментації (розвалу) Європейського Союзу, мінімізації американської присутності на континенті та переформатування усталеного європейського політичного устрою за російським сценарієм.

Російсько-українська "гібридна" війна не є локальним, периферійним конфліктом. У цій війні Росія використовує весь наявний арсенал засобів – від воєнної агресії, інформаційно-пропагандистської експансії, економічного, енергетичного тиску до підривних, шпигунсько-диверсійних дій і масованих кібератак.

Нині немає підстав говорити про наявність ефективних шляхів і механізмів комплексного врегулювання російсько-українського конфлікту – довгострокового і глибинного, що охопив всі сфери двосторонніх відносин. (Нормандський і Мінський формат – лише інструменти вирішення конфлікту на Донбасі, а проблема анексованого Криму де-факто отримала "від-кладений" характер).

Тому найбільш вірогідний сценарій на середньо-строкову перспективу – конфронтаційне (вороже) співіснування Києва і Москви за наявності загрози ескалації "гібридної" агресії. Причому ця загроза, очевидно, буде посилюватися мірою поглиблення європейської та євроатлантичної інтеграції України.

Триваюча "гібридна" війна проти України унеможливлює врегулювання ситуації на Донбасі та інтеграцію до України окупованих районів, де нині російською владою створено мілітаризовані псевдо-державні "республіки", чужі і глибоко ворожі Україні. Сценарії "експрес-виборів", що легітимізують "ДНР-ЛНР", є вкрай небезпечними та загрожують масштабним "гарячим" конфліктом в Україні та Європі в цілому.

У такій ситуації Заходу вкрай важливо зберегти солідарну лінію поведінки щодо Росії, оскільки в середньостроковій перспективі доведеться співіснувати з путінською Росією – авторитарною державою з тоталітарною внутрішньою та агресивною зовнішньою політикою і зневагою до міжнародних норм і правил. Важливим є продовження/поширення анти-російських санкцій, які мають надзвичайно важливий стримуючий політико-економічний і психологічний ефект. Їх скасування (ослаблення) в нинішній

ситуації буде сприйняте Кремлем як капітуляція Заходу та сигнал до активних дій, причому не тільки на пост- радянському просторі.

Розвиток геополітичних процесів в Європі і світі дає підстави прогнозувати критичне погіршення ситуації довкола російсько-українського конфлікту. Йдеться про ймовірні зміни зовнішньополітичного курсу США, реальну можливість приходу до влади в ряді європейських країн лояльних Росії політичних сил, перегляд Заходом політики санкцій щодо Росії і несприятливу для України розстановку сил у "Нормандському" переговорному форматі. Відтак, на українську сторону буде здійснюватися потужний тиск, зокрема щодо врегулювання ситуації на Донбасі за російським сценарієм.

У цих умовах Україна в протистоянні з РФ має орієнтуватися насамперед на власні сили та можливості.

РОЗДІЛ 2. АНАЛІЗ ЗМІСТУ ЗАХОДІВ ІНФОРМАЦІЙНОЇ ВІЙНИ ПРОТИ УКРАЇНИ, ЯКІ ПРОВОДЯТЬСЯ У КІБЕРПРОСТОРІ

2.1 Операція “ЗМІЯ”

Дослідники британської фірми BAE Systems Applied Intelligence зафіксували в 2013—2014 роках сплеск виявлених випадків зараження інформаційних систем приватних підприємств та державних установ України комп'ютерним хробаком (з руткітом), який вони назвали «Змія» (англ. snake). Дослідники з німецької фірми GData назвали цього хробака «уроборос», англ. uroborus (також англ. ouroborus — гадюка в грецькій міфології, або англ. sengoku та англ. snark). На думку дослідників обох фірм, цей хробак можливо пов'язаний та був створений на основі хробака Agent.BTZ, який в 2008 році вразив інформаційні системи Центрального Командування ЗС США.

Пік виявлення атак із використанням хробака «уроборос» збігся з розвитком масових протестів. Протягом січня 2014 року було зафіксовано 22 випадки інфікування інформаційних систем, при цьому протягом 2013 року «уроборос» був виявлений не більше 8 разів. В Україні зловмисники із застосуванням «уроборос» отримували повний доступ до вражених систем. На думку британських експертів, є всі підстави вважати, що за «уроборос» стоять спецслужби Російської Федерації.

Даний зразок шкідливого програмного забезпечення отримав різні назви від різних компаній, зокрема, він відомий як:

1. «Уроборос», англ. uroborus, також англ. ouroborus — гадюка в грецькій міфології;
2. Sengoku;
3. Turla.

В інтернет-протистоянні Росії з Україною проти України вперше було застосовано троянські програми, ключовою серед яких став вірус Uroburos. З одного боку, завданням цього вірусу було формування бот-мережі із заражених комп'ютерів та отримання повноцінного доступу до їх наповнення, а з іншого — викрадення інформації з цих комп'ютерів. Об'єкти атаки також, вочевидь, були обрані не випадково — веб-ресурси органів державної влади (в тому

числі силових структур), засобів масової інформації, фінансових установ, великих промислових підприємств.

Дослідники британської фірми BAE Systems Applied Intelligence зафіксували в 2013—2014 роках сплеск виявлених випадків зараження інформаційних систем приватних підприємств та державних установ України комп'ютерним хробаком (з руткітом), який вони назвали «Змія» (англ. snake). Дослідники з німецької фірми GData назвали цього хробака «уроборос», англ. uroborus (також англ. ouroborus — гадюка в грецькій міфології, або англ. sengoku та англ. snark). На думку дослідників обох фірм, цей хробак можливо пов'язаний та був створений на основі хробака Agent.BTZ, який в 2008 році вразив інформаційні системи Центрального Командування ЗС США.

Пік виявлення атак із використанням хробака «уроборос» збігся з розвитком масових протестів. Протягом січня 2014 року було зафіксовано 22 випадки інфікування інформаційних систем, при цьому протягом 2013 року «уроборос» був виявлений не більше 8 разів. В Україні зловмисники із застосуванням «уроборос» отримували повний доступ до вражених систем. На думку британських експертів, є всі підстави вважати, що за «уроборос» стоять спецслужби Російської Федерації.

За даними CERT-UA основними відомими станом на березень 2014 року об'єктами ураження «уроборос» є:

1. Веб-ресурси органів державної влади (в тому числі силових структур);
2. Веб-ресурси засобів масової інформації;
3. Веб-ресурси фінансових установ;
4. Веб-ресурси великих промислових підприємств.

Фахівці CERT-UA не виключають, що головною метою Uroborus є порушення функціонування об'єктів інформаційної інфраструктури України для викрадення конфіденційної інформації. Ретельна підготовка, прихованість дій, спрямованість кібератак (США -2008 рік, Україна — 2014 рік), а також залучення значних ресурсів — все це опосередковано свідчить про причетність іноземних спецслужб. В цьому контексті CERT-UA та деякі українські спеціалісти з інформаційної безпеки вбачають основним мотивом ініціатора

кібератак необхідність встановлення прихованого контролю за визначеними об'єктами для подальшого спостереження за інформаційним обміном з власної території.

«Уроборос» був застосований не лише проти України, а й проти інших країн. Зокрема, дане ПЗ згадане в річному звіті німецької контррозвідки за 2015 рік. Німецька контррозвідка зазначила, що як і раніше, в 2015 році російська розвідка використовувала «змію» (він же — «Turla») проти установ по всьому світу. В Німеччині жертвами кібератак з його застосуванням стали посольства, заклади вищої освіти, дослідницькі інститути, та приватні підприємства.

2.2 Операція “Атака на «Вибори»”

Під час дочасних Президентських виборів в Україні 2014 фахівцями CERT-UA було знешкоджено атаки на автоматизовану систему «Вибори».

21 травня 2014 року зловмисники з угрупування КіберБеркут здійснили успішну кібератаку на інформаційну систему «Вибори» Центральної виборчої комісії України. Їм вдалось вивести з ладу ключові мережеві вузли корпоративної мережі та інші компоненти інформаційної системи ЦВК. Майже 20 годин поспіль програмне забезпечення, яке мало показувати поточні результати підрахунку голосів, не працювало як слід. В день виборів, 25 травня, за 12 хвилин до закриття виборчих дільниць (19:48 EET), зловмисники розмістили «картинку Яроша» на серверах ЦВК.

Увечері 25 травня фахівцями CERT-UA було отримано інформацію про те, що на російських телеканалах анонсували новину про нібито виграш Дмитра Яроша на «президентських перегонах». З метою підтвердження цієї інформації на російському ТБ була продемонстровано картинку, яку в мережі вже назвали як «Картинка Яроша». 25 травня, о 20:16:56 було зафіксоване перше звернення до веб-сайту ЦВК виключно за IP-адресою внутрішнього веб-сервера з вказівкою в GET-запиті повного шляху до картинки «result.jpg» з IP-адреси 195.230.85.129. Ця адреса входить до діапазону IP-адрес телеканалу ОРТ.

В результаті атаки «Перший канал» російського телебачення повідомив своїм глядачам про те, що найбільшу кількість голосів виборців в першому турі на виборах президента України набрав лідер «Правого сектора» Дмитро Ярош. Про це йшлося у випуску вечірніх новин, присвяченому позачерговим виборам президента України. Ведуча повідомила, що незважаючи на дані екзит-полів, які свідчать про перемогу Петра Порошенка в першому турі, на сайті ЦВК з'явилася «дивна картинка» (так звана «Картинка Яроша»). За їхньою інформацією, Дмитро Ярош набрав 37,13 % голосів виборців, натомість за фаворита Петра Порошенка проголосувало лише 29,63 %.

Рано вранці наступного дня, 26 травня, сервери системи «Вибори», які приймали та обробляли дані про підрахунок голосів, зазнали розподіленої DoS-атаки, та були не доступні в проміжку між 1-3 годинами ранку.

Окрім інформаційної системи ЦВК, кібератак зазнали інші організації, які мали дуже віддалений зв'язок до виборів, жертвою міг стати сайт, який містив сторінку зі словом «вибори». Однак, більшість атак проти таких сайтів відрізнялись низьким рівнем технічної реалізації. Натомість, атака проти ЦВК відрізнялась високою складністю та технологічністю. За словами Миколи Коваля, тогочасного голови CERT-UA, атака на інформаційну систему ЦВК стала однією з найскладніших кібератак, які йому тоді довелось розслідувати.

І хоча відповідальність за атаки взяло на себе угрупування начебто хактивістів КіберБеркут, Микола Коваль припускає, що велика складність атаки може свідчити про те, що за нею стояли підрозділи іншої держави. Також в мережі ЦВК було виявлене шкідливе програмне забезпечення, яке пов'язують з угрупуванням APT28/Sofacy Group.

Опитані американською газетою Christian Science Monitor фахівці з комп'ютерної безпеки назвали атаку на інформаційною систему «Вибори» надзвичайно небезпечною, а також попередженням на майбутнє про вразливість комп'ютерних систем, залучених у виборчий процес. Можливість зриву виборів, або маніпуляція результатами виборів, набула нової ваги під час виборів Президента США 2016 року після успішної кібератаки проти Демократичної партії.

Схожа кібератака була здійсненна на Національний комітет Демократичної партії США – це несанкційоване втручання до інформаційної системи Національного комітету Демократичної партії США, яке стало відоме широкому загалу у червні 2016. Несанкційоване втручання було виявлене іще наприкінці квітня, тоді ж до розслідування була залучена фірма CrowdStrike. В результаті проведеного розслідування було встановлено, що зламати інформаційну систему вдалось двом угрупуванням російських хакерів - Cozy Bear та Fancy Bear. Група Cozy Bear отримала несанкційований доступ до інформаційної системи іще влітку 2015 року, а Fancy Bear - в квітні 2016 року. Разом обидва угрупування спромоглись викрасти скриньки електронної пошти, а також зібраний компромат на конкурента демократів на виборах Президента - Дональда Трампа.

Згодом стало відомо про можливу кібератаку типу тайпосквотинг різновид кіберсквотингу - навмисного створення фальшивих сайтів з доменими іменами дуже схожими на оригінальні проти DCCC - організації, що збирає пожертви для кандидатів у Конгрес від Демократичної партії. Атака розпочалась приблизно в червні 2016 року.

У спільній заяві Міністерство національної безпеки США та директора Національної розвідки 7 жовтня 2016 року повідомили, що американська розвідка впевнена у причетності російського уряду до "нещодавніх кібератак проти окремих осіб та політичних організацій". Розкриття викраденої інформації сайтами DCLeaks.com та WikiLeaks та інтернет-персонажем Guccifer 2.0 цілком вкладається у методи та цілі російського керівництва. Такі кібератаки з метою впливу на суспільну думку вже спостерігались в Європі та Євразії та мали бути схвалені на найвищих рівнях.

Згодом стало відомо про можливу кібератаку типу тайпосквотинг різновид кіберсквотингу - навмисного створення фальшивих сайтів з доменими іменами дуже схожими на оригінальні проти DCCC англ. Democratic Congressional Campaign Committee - організації, що збирає пожертви для кандидатів у Конгрес від Демократичної партії. Атака розпочалась, приблизно, в червні 2016 року.

Для спуфінгу справжньої адреси веб-сервера DCCC була створена адреса actbluescom, використане для типосквотингової атаки на підрядника Нацкомітету Демократичної партії.

У жовтні 2015 - травні 2016 року угрупування Sofacy Group Fancy Bear, APT28 здійснило масовану направлену фішингову англ. spearfishing атаку на користувачів поштовими послугами Gmail як корпоративними, так і приватними. Всього було виявлено 3907 поштових скриньок, на які були відправлені фішингові листи. Для введення жертв в оману, зловмисники скористались інтернет-службою Bitly, яка дозволяє скорочувати і приховувати справжні адреси гіперпосилань. Прямого звязку між направленою фішинговою атакою та зламом інформаційної системи Національного комітету Демократичної партії США встановити не вдалось, проте можна припустити, що аналогічні методи допомогли розпочати проникнення до системи.

19 березня 2016 року фішингова атака проти Джона Подести, керівника передвиборчого штабу Гіларі Клінтон, завершилась вдало. 9 жовтня того ж року, у розпал передвиборчої кампанії, "Вікілікс" розпочав оприлюднення листів у тому числі компрометуючих з його поштової скрині.

Слід зазначити, що злам поштової скриньки із викраденням приватного листування Джона Подести під час виборчої кампанії був не першим таким випадком - під час виборів 2008 року була зламана поштова скриня Сари Пейлін, кандидата у віце-президенти США та партнера кандидата в президенти Джона Маккейна. Відповідальним виявився Девід Кернел англ. David Kernell. Листування Пейлін було спочатку оприлюднене на інтернет-форумах, а потім розміщене Вікілікс. Кернел ретельно дослідив профілі Сари Пейлін в соціальних мережах, звідки дізнався її біографічні дані, необхідні для проходження процедури "відновлення" паролю до поштової скрині. Його звинуватили у вчиненні низки злочинів із сукупним терміном покарання 50 років у вязниці, визнали винним у скоєнні двох та засудили до увязнення на термін 1 рік + 1 день.

Заради легалізації викрадених даних було створене "опудало", що мало служити фасадом для угрупування - "хакер" на прізвисько "Гуцифер 2.0" англ. Guccifer 2.0. Це прізвисько було запозичене в іншого хакера - румунця

Марселя Лазара Лехеля рум. Marcel Lazar Lehel, котрий назвав себе англ. Guccifer злиття слів Gucci та Lucifer. Марсель Лехель став відомим завдяки зламу поштових скриньок відомих людей зокрема, сестри Джорджа Вокера Буша. В 2014 році його засудили в Румунії до 7 років увязнення, але згодом передали до Сполучених Штатів, де станом на 2016 рік він очікував на вирок суду. Після того, як Лехеля доставили до США, він заявив, що неодноразово зламував особистий поштовий сервер Гілларі Клінтон, коли та була державним секретарем США див. Імейлгейт. Проте, він не зміг навести жодного доказу, а слідчі не знайшли жодних свідчень на підтвердження його слів. У липні 2016 року директор ФБР Джеймс Комі заявив, що Лазар збрехав, коли заявив про злам поштового серверу Клінтон.

Утім, саме завдяки Лехелю широкий загал дізнався про існування приватної поштової скрині Гілларі Клінтон, коли він поширив листи зі зламаної ним же поштової скрині близького партнера Клінтон Сідні Блюменталя Оприлюднені листи стосувались подій навколо терористичних атак на консульство США в Бенгазі в 2012 році. Сідні Блюменталь на той час не мав доступу до таємної інформації, однак деякі з отриманих ним від Клінтон текстів були згодом визнані такими, що підпадають під гриф "таємно".

На відміну від першого Гуцифера, Guccifer 2.0 не зміг навести переконливі докази своєї автентичності, або що за цим фасадом стоїть реальна жива людина. На думку аналітиків фірми ThreatConnect, швидше за все, Guccifer 2.0 - лише спроба російських спецслужб облудою відвернути увагу від їхньої ролі у зламі інформаційних систем Демократичної партії Серед іншого:

1. його поведінка була нетиповою для звичайних політичних хактивістів - замість оприлюднення документів одразу після їх отримання, він чекав більше року;

2. дивним виглядало й те, що хакер-одинак скористався невідомою "вразливістю нульового дня" у нішевому пропрієтарному програмному забезпеченні, коли набагато краще оснащені російські спецслужби скористались набагато простішим направленим фішингом.

3. незрозуміло, навіщо Guccifer 2.0 змінював метадані документів або навіть їх вміст перед оприлюдненням, адже це ставило під сумнів їхню справжність.

На думку фахівця з компютерної безпеки Дейва Айтеля, оприлюднивши викрадені файли російські спецслужби перетнули червону лінію припустимого. Він запропонував вважати таке нахабне втручання в перебіг президентських виборів іззовні країни прикладом кібервійни.

У березні 2018 року американське видання The Daily Beast із посиланням на власні "джерела" повідомило, що фахівцям фірми Threat Connect та співробітникам американської розвідки вдалось знайти докази, що за персонажем Guccifer 2.0 стояли співробітники ГРУ, які працювали в офісах ГРУ на вулиці Гризодубової в Москві. Оператори цього інтернет-персонажа заходили в соціальні мережі через анонамізатор Elite VPN з точкою виходу у Франції, але штаб-квартирою в Москві. Одного разу оператор припустився помилки і зайшов до соц. мереж зі своєї справжньої IP-адреси.

Наступним кроком з легалізації викрадених даних, який отримав набагато більше розголосу, стала публікація решти файлів на сайті організації Вікілікс, яку колишній співробітник АНБ Джон Р. Шиндлер назвав "сурогатом російських спецслужб". Засновник Вікілікс, Джуліан Ассанж, анонсував оприлюднення даних в інтервю телеканалу ITV 12 червня 2016 року. При цьому, він визнав, що цим витоком намагається зашкодити Гілларі Клінтон виграти вибори. Оприлюднення сталось шість тижнів по тому, 22 липня 2016 року - організація розмістила у вільному доступі у себе на сайті 19 252 електронних листів з 8034 вкладеними файлами. Листи були викрадені з поштових скриньок 7 ключових осіб в DNC та охоплювали період від січня 2015 року до 25 травня 2016 року. Серед листів з вкладеними файлами були й повідомлення голосової пошти.

Про передачу оприлюднених листів до Вікілікс заявив Гуцифер 2.0, який першим виступив публічно як особа, що стоїть за кібератаками на Демократичну партію. Попри те, Джуліан Ассанж заперечив будь-яку причетність російських спецслужб до витоку даних, а також пообіцяв оприлюднити ще більше компромату на Гілларі Клінтон. При цьому, він

припустив, що "колись джерело або джерела інформації дадуть про себе знати". 9 серпня 2016 року Ассанж зробив натяк, що можливим джерелом отриманих файлів був співробітник Демократичної партії Сес Річ англ. Seth Rich, якого вбили вранці 10 липня поблизу його квартири. Однак, він відмовився прямо підтвердити чи спростувати причетність Річа до витоку даних.

Оприлюднені листи, серед іншого, містили приватну інформацію деяких донорів Демократичної партії - номери соціального страхування, номера паспортів, інформацію про кредитні картки. Один лист містив перелік осіб, запрошених на зустріч ЛГБТ активістів, організовану Демократичною партією. Серед файлів голосової пошти був запис співробітника Демократичної партії про відвідання зоопарку з дітьми.

Вікілікс оприлюднила викрадені листи напередодні зїзду Демократичної партії, на якій відбулась формальне висування Гілларі Клінтон у кандидати на виборах Президента США 2016 року. Однак, з оприлюднених листів випливало, що Національний комітет Демократичної партії протягом праймеріз віддавав деяку перевагу Гілларі Клінтон перед Берні Сандерсом. Унаслідок спричиненого цим викриттям скандалу голова Національного комітету Демократичної партії, Деббі Вассерман-Шульц, була змушена терміново піти у відставку.

Низка експертів з питань національної безпеки Республіканської партії 28 липня 2016 року звернулись з відкритим листом до політичних лідерів Конгресу провести ретельне розслідування кібератаки на Демократичну партію з наступним оприлюдненням викраденої інформації, оскільки такий випадок вважали "атакою на цілісність всього політичного процесу".

31 липня Гілларі Клінтон звинуватила спецслужби Росії в кібератаці на штаб Демократичної партії. У відповідь АНБ, можливо, зламує російських хакерів.

Російський уряд заперечував свою причетність до інциденту.

Після цього випадку міністерство національної безпеки США стало вивчати можливість зарахування інформаційних систем, залучених у виборчий процес, до переліку обєктів "критичної інфраструктури".

На початку листопада 2017 року видання The Wall Street Journal повідомило із посиланням на власні джерела, що міністерству юстиції США вдалось встановити особи шістьох російських високопосадовців, причетних до хакерської атаки на комітет демократичної партії.

2.3 Атаки на енергетичні компанії України

Кібератака на енергетичні компанії України — перша зареєстрована успішна кібератака на енергетичну систему з виведенням її із ладу. Сталась 23 грудня 2015 року. Російським зловмисникам вдалось успішно атакувати комп'ютерні системи управління трьох енергопостачальних компаній України. Наступна, і набагато менш масштабна за наслідками, кібератака сталась вночі з 17 на 18 грудня 2016 року. Протягом трохи більше однієї години була виведена з ладу підстанція «Північна» енергокомпанії «Укренерго», без струму залишились споживачі північної частини правого берегу Києва та прилеглих районів області.

Найбільше від першої кібератаки постраждали споживачі «Прикарпаттяобленерго»: було вимкнено близько 30 підстанцій, близько 230 тисяч мешканців залишались без світла протягом однієї-шести годин. Атака відбувалась із використанням троянської програми BlackEnergy.

Водночас синхронних атак зазнали «Чернівціобленерго» та «Київобленерго», але з меншими наслідками. За інформацією одного з обленерго, підключення зловмисників до його інформаційних мереж відбувалося з підмереж глобальної мережі Internet, що належать провайдерам в Російській Федерації.

Загалом кібератака мала комплексний характер та складалась щонайменше з таких складових:

1. попереднє зараження мереж за допомогою підроблених листів електронної пошти з використанням методів соціальної інженерії;
2. захоплення управління АСДУ з виконанням операцій вимикань на підстанціях;
3. виведення з ладу елементів IT інфраструктури (джерела безперебійного живлення, модеми, RTU, комутатори);

4. знищення інформації на серверах та робочих станціях (утилітою KillDisk);

5. атака на телефонні номери кол-центрів, з метою відмови в обслуговуванні знеструмлених абонентів.

Перерва в електропостачанні склала від 1 до 3,5 годин. Загальний недовідпуск — 73 МВт·год (0.015 % від добового обсягу споживання України).

Внаслідок другої кібератаки, в грудні 2016 року, струм був відсутній протягом трохи більше однієї години.

Інформаційні системи, відповідальні за управління роботою об'єктів інфраструктури відносять до класу автоматизованих систем керування технологічним процесом (скорочено АСК ТП; або англ. industrial control systems, ICS). Усі АСК ТП ділять на три класи: системи диспетчерського управління і збирання даних (SCADA), розподілені системи керування (РСК), програмовані логічні контролери (ПЛК).

Або загальних рисах, електрична мережа є об'єктом інфраструктури, який сполучає споживачів електричної енергії з її виробниками. У будь-якому процесі управління існує об'єкт, яким управляють (вимикач, трансформатор, генератор) і орган, який здійснює управління (технічний засіб, людина). У процесі управління цей орган отримує інформацію про стан зовнішнього середовища, де перебуває об'єкт і з яким він пов'язаний. Уся ця інформація сприймається управляючим органом, який виробляє на її основі управляючу інформацію (приймає рішення). На основі прийнятого рішення виконавчий орган здійснює управляючий вплив на об'єкт управління. При цьому оператор засобами людино-машинної взаємодії може впливати на параметри роботи АСУ ТП, керувати об'єктом управління, здійснювати діагностику, переглядати за поточним станом системи та виправляти виявлені несправності.

Складні інформаційні системи управління роблять системи автоматизації електричними мережами вразливими перед кібератаками. В праці дослідники виокремили три категорії можливих кібератак:

1. Націлені на компоненти: електронно-обчислювальні прилади, такі як віддалені термінали (rtu) або людино-машинного інтерфейсу (hmi) зазвичай мають інтерфейс для віддаленого налаштування або управління. Через

віддалений доступ зловмисник може перехопити управління пристроєм та спричинити несправності, наприклад:

1.1. Спотворити передані дані оператору;

1.2. Пошкодити обладнання, якщо оператор здійснює управління на основі спотворених даних;

1.3. Взагалі повне або часткове виведення пристрою з ладу.

2. Націлені на протоколи: майже всі сучасні протоколи передачі даних добре задокументовані та їхнє описання знаходиться у відкритому доступі. Наприклад, стандарт dnp3 поширений в системах управління електричними мережами у північній америці. Його специфікація доступна всім охочім за невелику ціну. Документація протоколу полегшує завдання зворотної розробки для здійснення атаки типу «людина посередині». Серед іншого, зловмисник може відправляти спотворені дані, які можуть призвести до:

2.1. Фінансові втрати через перевиробництво електричної енергії;

2.2. Небезпека для працівників: наприклад, зловмисник може увімкнути живлення леп коли там працюють інженери;

2.3. Пошкодження обладнання, якщо внаслідок відправлених команд станеться перенавантаження окремих ланок системи.

3. Націлені на топологію: зловмисники можуть скористатись також і вразливостями топології мережі. Наприклад, масована відправка коректних запитів на віддалені термінали може створити затримки у відправленні повідомлень в режимі реального часу. Це призведе до спотвореного представлення стану системи оператору, через що він може ухвалювати помилкові рішення.

Так само, як під час звичайної війни, об'єкти інфраструктури є мішенями атак і під час кібервійни.

Станом на 2016 рік вже були відомі успішні віддалені кібератаки на об'єкти інфраструктури. Наприклад, в 2000 році розлючений інженер Вайтек Боуден вирішив провчити своє керівництво і здійснив успішну кібератаку на очисні споруди в графстві Маручі (Квінсленд, Австралія). Внаслідок атаки до навколишнього середовища потрапило понад 800 тис. літрів неочищених стічних вод, природа та живі істоти зазнали істотної шкоди.

Приклад типової атаки. Для здійснення атаки на системи промислового управління зловмисник спочатку має отримати до них доступ. В праці названо три поширених шляхи отримання несанкційованого доступу:

1. атака на шлюз між корпоративною мережею та мережею SCADA;
2. атака на зовнішні канали доступу до мережі SCADA через VPN;
3. зв'язок зі сторонніми серверами.

Для нормальної роботи систем управління необхідний певний обмін інформацією . Зазвичай, інформація зі SCADA потрапляє до тих чи інших баз даних, і долає деякий мережевий шлюз між комерційною та промисловою підмережами. Шлях для обміну інформацією може бути вразливим до атак.

Також системи SCADA можуть обмінюватись інформацією з терміналами операторів. Злам операторського терміналу також може бути використаний зловмисником для проникнення до мережі SCADA.

Вразливим до атак може бути і віддалений доступ операторів або інших інженерів до систем SCADA через VPN, особливо у випадку невірного налаштування.

Вразливість можуть становити сторонні сервери (архівування даних, розробників, аналітиків, тощо) та їхнє підключення до системи промислового управління.

Після здобуття доступу до мережі промислового управління, зловмисник має здійснити розвідку, аби вивчити схему роботи SCADA. Інколи, надзвичайна складність систем SCADA посилює захист від атаки та примушує зловмисника витрачати час та сили на її вивчення.

Одразу після вторгнення зловмисник, швидше за все, матиме дуже обмежений доступ до решти мережі.

Серед доступних йому джерел інформації можуть бути внутрішні веб-сервери, робочі станції операторів, мережеві диски, інші інтерфейси до керованих систем. Ці джерела інформації можуть бути доступними всім терміналам у мережі, інколи навіть без автентифікації користувача.

Іншим джерелом інформації може стати пасивна розвідка комп'ютерної мережі. Успіх цього методи істотно залежить від знаходження скомпрометованої системи в мережі та вимагає від операторів виконувати

якісь дії (аби генерувати потоки даних). На відміну від попереднього підходу, може надати інформацію про облікові дані користувачів, використані ними протоколи, налаштування, тощо. Також пасивна розвідка мережі не потребує відправки пакетів даних і тому непомітна системам виявлення вторгнень. Якщо скомпрометована система знаходиться в одній мережі з основними складовими SCADA, зловмисник матиме можливість розвідки використаних протоколів та команд.

Зловмисник може вдатись і до активної розвідки мережі. Для цього йому знадобиться доступ до скомпрометованої системи з правами адміністратора, оскільки цей метод передбачає можливість відправляти мережею спеціально сформовані пакети даних. Однак, ці пакети можуть бути помічені системою виявлення вторгнень, внаслідок чого системні адміністратори дізнаються про існування в мережі скомпрометованої системи. На противагу попереднім методам, цей метод дозволяє зловмисникові дізнатись про доступні зі скомпрометованої системи пристрої та інші термінали в мережі.

Нарешті, для розуміння та відтворення промислового процесу зловмисникові доведеться ретельно вивчити отриману ним інформацію. Наприклад, із перехоплених повідомлень він може дізнатись про існування терміналу «Вимикач-4А», але йому доведеться докласти додаткових зусиль аби збагнути, що це за вимикач, та як він впливає на систему в цілому.

Після вивчення промислового процесу, зловмисник може перейти до перехоплення управління ним. Різні методи можуть надавати різний рівень контролю, а відповідно, і результати атаки.

Серед найважливіших об'єктів для атаки є головний диспетчерський блок (англ. front-end processor, FEP), який відповідає за взаємодію між програмованими логічними контролерами та іншими компонентами системи SCADA, зокрема, з людино-машинним інтерфейсом з оператором.

Іще однією важливою мішенню для зловмисника може бути людино-машинний інтерфейс (HMI), оскільки він доступно представляє стан всієї системи та надає можливість оператору керувати нею. Однак, можливості для атаки будуть обмежені можливостями людино-машинного інтерфейсу і тому

зловмисникові може не вдатись вивести систему з ладу або завдати якоїсь істотної шкоди.

Атака на людино-машинний інтерфейс є атакою націленою на компоненту. З її переваг можна назвати те, що вона може бути здійснена із використанням звичайних підходів та інструментів, не пов'язаних з промисловими системами управління. Також атака на людино-машинний інтерфейс дозволить зловмисникові приховати свою діяльність під виглядом звичайної роботи оператора.

Схожою на атаку на людино-машинний інтерфейс може бути атака на робочі станції інженерів (англ. engineering workstation, EWS), залучених в розробці програмного забезпечення для людино-машинного інтерфейсу та іншого системного ПЗ. Перевага атаки на робочі станції полягає в тому, що вони можуть не мати обмежень, які накладає людино-машинний інтерфейс.

Зловмисник, після вивчення протоколу між людино-машинним інтерфейсом і контролерами, може здійснити спуфінгову атаку — відправляти підроблені команди контролерам або спотворювати дані, передані оператору.

Програмовані логічні контролери, особливо під'єднані до мережі, можуть бути іще одним об'єктом атаки. Інколи програмовані контролери доступні через веб-служби, модеми, протокол Telnet. Погано захищений контролер може видати зловмиснику не лише інформацію про свій стан, а й навіть про запрограмовану логіку та вбудовану програму.

Перша хвиля атаки. Нападники змогли отримати доступ до корпоративної мережі компанії “Прикарпаттяобленерго” завдяки вдалому зараженню комп'ютера одного із співробітників трояном BlackEnergy третьої версії. Проте, мережі цифрових контролерів, які власне і керують обладнанням, знаходились за мережевими екранами.

Протягом багатьох місяців вони проводили масштабну розвідку, досліджували та описували мережі і здобували доступ до служби Windows Domain Controllers, яка керує обліковими записами користувачів мереж. Тут вони зібрали реквізити співробітників, у тому числі паролі від захищеної мережі VPN, яку працівники енергокомпаній використовували для віддаленого підключення до мережі SCADA.

Здобувши доступ до внутрішньої мережі нападники переконфігурували пристрої безперебійного живлення (UPS), відповідальні за енергопостачання двох диспетчерських центрів.

Кожне обленерго використовувало власну систему управління розподілом енергії у своїх мережах, і під час фази розвідки нападники ретельно вивчили кожну з них. Тоді вони написали шкідливий мікрокод, яким замінили справжній вбудований мікрокод на конвертерах із серійного інтерфейсу на інтерфейс Ethernet у понад десяти підстанціях (ці конвертери застосовуються для обробки команд, які надходять від мережі SCADA до систем управління підстанцією).

Виведення з ладу конвертерів не давало операторам змогу посилати віддалені команди для повторного включення запобіжників після того, як енергію було вимкнено.

Приблизно о 3:30 по обіді 23 грудня вони зайшли в мережі SCADA через вкрадені облікові записи і віддали команди на вимкнення систем безперебійного живлення, які вони вже переконфігурували раніше. Після цього вони почали вимикати запобіжні системи, які переривали живлення.

Але перед цим вони запустили атаку за методикою «відмова від обслуговування» на кол-центри обленерго, аби користувачі не могли повідомити про аварію. Фіктивні дзвінки, судячи з усього, надходили з Москви.

Після того, як нападники вимкнули запобіжники і відключили низку підстанцій від мережі, вони також переписали програмний мікрокод на конвертерах із серійного інтерфейсу на інтерфейс Ethernet, замінивши «справжнє» програмне забезпечення шкідливим, і тим самим вивівши з ладу конвертери, які перестали виконувати команди.

Завершивши всі ці дії, зловмисники застосували програму під назвою KillDisk для знищення файлів з комп'ютерів операторів підстанцій, тим самим вивівши і їх з ладу. KillDisk стирає чи перезаписує дані в критично важливих системних файлах, викликаючи їхнє «зависання».

Деякі з компонентів KillDisk потрібно запускати вручну, але нападники у двох випадках застосували так звану «логічну бомбу», яка запустила KillDisk автоматично через 90 хвилин після початку атаки.

Через півгодини, коли KillDisk мав зробити свою справу і в операторів не залишилось сумнівів щодо причини масштабного зникнення світла, компанія розмістила друге повідомлення — про те, що до цього причетні хакери.

Одночасно з атаками на західноукраїнські обленерго, хакери завдали потужного удару по комп'ютерних мережах «Київобленерго»: 23 грудня 2015 року сторонніми особами було здійснено несанкційоване втручання в інформаційно-технологічну систему віддаленого доступу до телеуправління обладнанням підстанцій 35-110 кВ ПАТ «Київобленерго».

В результаті втручання виникли збої в роботі телемеханіки та було відключено 30 вузлових підстанцій (7 — ПС-110 кВ та 23 — ПС-35 кВ) від яких живиться низка стратегічних об'єктів області: підприємства, державні установи, заклади та населення. З 15:31 хв. до 16:30 хв. було повністю або частково відключено близько п'ятдесяти населених пунктів у Білоцерківському, Кагарлицькому, Миронівському, Фастівському, Сквирському, Макарівському, Рокитнянському, Іванківському та Яготинському адміністративних районах, без електричної енергії були понад 80 378 споживачів. Електропостачання було відновлено всім споживачам о 18:56 того ж дня.

Друга хвиля атаки. Невстановлені зловмисники здійснили наприкінці лютого 2016 року другу хвилю кібератак на компанії енергетичного сектора України: 19 та 20 лютого ними було розіслано близько 100 отримувачам «вірусні» листи електронною поштою.

Перший етап «вірусної розсилки» розпочався надвечір 19 лютого 2016, другий етап розпочався зранку, до початку робочого дня 20 лютого (вівторок та середа відповідно). Тоді НЕК «Укренерго», довідавшись про масову розсилку листів начебто від її імені виступила із заявою на офіційному веб-сайті.

Як і в попередній хвилі (грудень 2015 року), зловмисники скористались поширеним прийомом соціальної інженерії: електронний лист мав вкладений

документ-приманку, при перегляді якого жертві пропонується активувати макрос для коректнішого зображення вмісту.

Після відкриття документа на комп'ютері жертви створюється і запускається завантажувач, завданням якого є завантаження, декодування, та запуск шкідливої програми (файл: «root.cert»). У випадку цієї атаки шкідлива програма — бекдор був завантажений із зламаного іще в середині серпня 2015 року сервера, який фізично знаходився в Україні

На цьому етапі можна виокремити дві риси подібні до попередньої хвилі атак із застосуванням BlackEnergy:

1. Для відправлення електронного листа зі шкідливим вкладенням «Ocenka.xls» був використаний відомий сервер:

Received: from mx2-mail.com (mx1-mail.com [5.149.248.67])

2. Електронний лист, як і в першій хвилі, містив в тілі рядок (гіперпосилання на файл), назва якого містила закодовану в base64 адресу електронної пошти жертви

На відміну від попередньої хвилі, цього разу як бекдор була використана програма з відкритими кодами Gcat, а не потужніший та гнучкіший BlackEnergy. Програма Gcat написана мовою програмування Python та перетворена на .EXE файл програмою PyInstaller, як канал керування використана служба електронної пошти Gmail. Попри простоту цієї програми (в порівнянні з BlackEnergy версій 2 та 3), вона має низку переваг, одна з яких — ускладнення її виявлення методом глибокого інспектування пакетів (DPI) каналу керування бекдором в інформаційних потоках (оскільки він нічим не відрізняється від звичайного використання поштової служби Gmail).

Оскільки зловмисники залишили в обфускованому коді бекдору дані облікового запису каналу керування, стало можливим дослідити управління інфікованою системою з точки зору зловмисника. З проведеного дослідження випливало, що зловмисник здійснював атаку цілеспрямовано, скеровано на конкретну, вибрану ним жертву.

Завдяки вчасній реакції служб захисту інформаційних систем CyS-CERT та втручання CERT-UA була встановлена адреса сервера керування, задіяного в атаці, 20 лютого о 10:51 інтернет-провайдер Dream Line закрив до нього

доступ. Цим були припинені подальші спроби завантаження бекдору. До роботи із збереження електронних доказів, збирання даних для ідентифікації причетних до атаки осіб, були залучені співробітники СБУ.

В результаті додаткового розслідування було встановлено, що після першої розсилки надвечір 19 лютого щонайменше два співробітника із двох компаній відкрили документ-приманку, запустили макрос, в результаті чого був успішно завантажений бекдор, але завантажені бекдори встановитись не змогли.

20 лютого 2016 року, вже після першої та другої розсилок, був для зловмисників успішнішим днем. В проміжок між 08:42 та 10:39 бекдор був завантажений 9 співробітниками із 4 компаній. Однак, успішне встановлення бекдору з відкриттям каналу керування сталась лише на одному комп'ютері однієї компанії. При цьому зловмисники почали скеровану розвідку комп'ютерної мережі жертви, що може свідчити про те, що зловмисники були обізнані про структуру інформаційної системи компанії та були причетні до атак в грудні 2015 року.

Кібератака на Укренерго. У вечорі та вночі з суботи на неділю, 17 на 18 грудня 2016 року на підстанції «Північна» стався збій в автоматиці управління, через що споживачі північної частини правого берегу Києва та прилеглих районів області залишились без струму. Несправності були усунуті протягом 1 години 15 хвилин. Основною версією стала кібератака — зовнішнє втручання через мережі передачі даних. Оператор підстанції, компанія «Укренерго» спочатку не стала підтверджувати кібератаку, проте залучені до розслідування фахівці з комп'ютерної безпеки підтвердили, що збій стався внаслідок кібератаки. Проміжні результати розслідування були представлені фахівцями Олексієм Ясінським від компанії Information Systems Security Partners (Україна) та Мариною Кротофіл від Honeywell Industrial Cyber Security Lab 10 січня 2017 року на конференції S4 у Флориді, США. Однак, нападники не стали завдавати істотної шкоди, натомість дана атака мала послужити «демонстрацією сили». Як і у попередніх випадках, дана атака була частиною масштабнішої фішингової операції проти державних установ України.

На початку червня 2017 року були оприлюднені доповіді фахівців компаній ESET та Dragos, в яких було наведено результати ретельного аналізу шкідливого ПЗ, використаного в атаці. Дане ПЗ отримало назву Industroyer або Crash Override.

2.4 Кібератаки на Мінфін, Держказначейство і Пенсійний фонд України

6 грудня 2016 року хакерська атака на урядові сайти (Держказначейства України та інших) і на внутрішні мережі держорганів призвела до масштабних затримок бюджетних виплат. Вже 7 грудня Кабмін виділив 80 млн гривень для захисту від хакерів. Для виведення з ладу серверів використовувався вірус KillDisk. Атака відбувалась із використанням троянської програми BlackEnergy, тої самої, що і в атаці на «Прикарпаттяобленерго». Українські чиновники приписують кібератаки Росії, припускаючи, що та таким чином хотіла помститися за відімкнення офіційним Києвом електроенергії у Криму. В Міністерстві фінансів, де інцидент охарактеризували як «скоординовану професійну хакерську атаку», також заявили, що інцидент призвів до пошкодження їхнього мережевого обладнання. Хакери намагались зірвати бюджетний процес та реформи Мінфіну. Намагались підірвати довіру бо кібербезпеки уряду.

2.5 Компрометація ArtOS

ArtOS — програмно-апаратний комплекс, призначений для скорочення часу для розрахунку на ураження об'єкту. Використання комплексу економить час в чотири рази — до двох хвилин. Крім того, комплекс здатен розв'язувати до 70 % тактичних та бойових завдань, які постають перед артилеристами

Компрометація ArtOS - історія, що позиціювалася російською групою хакерів Fancy Bear як злам артилерійського додатку для планшетів Android, розробленого українським офіцером Ярославом Шерстюком.

Програма-додаток для планшетів Android була розроблена капітаном 55-ї окремої артилерійської бригади Ярославом Шерстюком десь в проміжку між 20 лютого та 13 квітня 2013 року. Додаток слугував як калькулятор для

розрахунку артилерійських поправок. 28 квітня 2013 року обліковий запис соціальної мережі ВКонтакті з ідентичним іменем став поширювати цю програму зі своєї сторінки «рос. Программное обеспечение современного боя». Як запобіжник неконтрольованому розповсюдженню, після завантаження та встановлення програми користувач мав звернутись до розробника за ключем для розблокування її роботи.

21 грудня 2014 року на українському військовому інтернет-форумі було вперше помічено файл установки програми, скомпрометований імплантатом X-Agent. Згідно припущення, висловленого у звіті CrowdStrike, скомпрометований варіант був створений у проміжку між кінцем квітня 2013 та початком грудня 2014 року — саме тоді, коли політична криза переросла у російсько-українську війну з анексією Криму та бойовими діями на сході України.

22 грудня 2016 році видання CrowdStrike, посилаючись на дані The Military Balance, опублікувало звіт, у якому зазначало, що Україна нібито втратила у боях до 80 % гаубиць Д-30. Згідно звіту, додаток для планшетів, яким користувалися українські артилеристи, був зламаний російськими хакерами, що дозволило їм отримати доступ до GPS-даних планшетів і визначити розташування української артилерії.

Новину того ж дня поширила низка західних видань: Forbes, Reuters, Guardian.

Українські журналісти розкритикували підхід CrowdStrike, вказуючи на те, що у своєму матеріалі видання посилається на дані з публікації кримського блогера Бориса Рожина (Colonel Cassad), і засумнівалися в тому чи CrowdStrike користувалися справжнім звітом The Military Balance, випуск якого коштує 350 фунтів-стерлінгів. Після критики щодо своїх висновків і припущень, CrowdStrike вніс зміни до свого звіту, вказавши кількість втрат українських гаубиць Д-30 на рівні 15 %—20 %.

Зважаючи на те, що дослідники з CrowdStrike не змогли встановити точну кількість заражених пристроїв та наслідки цієї операції: невідомо, чи були взагалі випадки виходу в інтернет з планшетів під час бойових дій, наскільки масовою була програма з інтернету, адже оригінальне ПЗ було

поширене у закритий спосіб, тощо. Цілком може бути, що сам факт існування скомпрометованого варіанту програми ворожа сторона використовує для ускладнення використання важливої та ефективної артилерійської програми на планшетах ЗСУ, або навіть як чергову компанію «зради» для деморалізації супротивника.

У звіті Associated Press, оприлюдненому 2 листопада 2017 року, було зазначено, що Ярослав Шерстюк як розробник програми був одним із 545 членів політичної та військової еліти України, які стали мішенню хакерської групи. Автор звіту Рафаель Сеттер оприлюднив дані, згідно з якими спроба зламу пошти Шерстюка відбулася 3 квітня 2015 року.

2.6 Petya та NotPetya

Petya — сімейство шкідливих програм, що вражає комп'ютери під управлінням сімейства ОС Microsoft Windows. Перші представники були виявлені в 2016 році та були звичайними зразками здирницьких вірусів[3][4]. 27 червня 2017 року сталась масштабна атака останнім представником сімейства, який запозичив деякі модулі з попередніх зразків, але можливо був створений іншими розробниками та вже був вірусом-винищувачем даних, замаскованим під програму-вимагач.

Програма шифрує файли на жорсткому диску комп'ютера-жертви, а також перезаписує і шифрує головний завантажувальний запис (MBR) — дані, необхідні для завантаження операційної системи. В результаті всі файли, що зберігаються на комп'ютері, стають недоступними. Потім програма вимагає грошовий викуп у біткоїнах за розшифровку і відновлення доступу до файлів. При цьому перша версія вірусу шифрувала не самі файли, а MFT-таблицю — базу даних з інформацією про файли, що зберігаються на диску.

На думку Адміністрації Президента США Дональда Трампа атака із використанням вірусу NotPetya в червні 2017 року стала найбільшою хакерською атакою в історії. У спільній заяві країни альянсу Five Eyes поклали відповідальність за дану атаку на російську владу. Відповідальність за атаку покладають на Росію також уряди Данії та України

Вперше вірус Petya був виявлений в березні 2016 року. Компанія Check Point тоді зазначила, що, хоча йому вдалося заразити менше комп'ютерів, ніж іншим програмам-здирникам початку 2016 року, таким як CryptoWall, поведінка нового вірусу помітно відрізняється, завдяки чому він негайно був відзначений, як наступний крок в еволюції програм-вимагачів". За відновлення доступу до файлів програма вимагала від користувача 0,9 біткоїнів, що, за станом на березень 2016 року, становило близько 380 доларів США.

На думку частини аналітиків, називати нову загрозу «Petya», строго кажучи, невірно. Шкідливе ПЗ дійсно володіє значною кількістю коду з більш старої області, призначеної для вимагання, яка ідентифікується антивірусними системами як Petya. Проте вже через кілька годин після початку епідемії деякі дослідники інформаційної безпеки помітили, що ця схожість досить поверхова. Дослідники з Лабораторії Касперського відмовилися називати шкідливу програму «Petya» — замість цього вони використовують терміни New Petya, NotPetya, ExPetr. Поширюються й інші варіанти цієї назви — Petna, Pneytna та інші. Крім того, інші дослідники, які самостійно виявили шкідливе ПО, визначили його зовсім іншими назвами: наприклад, румунська компанія Bitdefender назвала його Goldeneye. З іншого боку, американська компанія Symantec вважає нову загрозу різновидом вірусу Petya, не привласнюючи їй якоїсь іншої назви.

27 червня 2017 року почалося масове поширення нової модифікації програми. На цей раз вірус використовує ті ж вразливості системи, що і WannaCry (наприклад, експлойт EternalBlue і бекдор DoublePulsar), а за відновлення доступу до даних вимагає відправити 300 доларів в біткоїнах. При цьому фахівці не рекомендують користувачам йти на поводу у вимагачів, оскільки це все одно не допоможе їм відновити доступ до даних; електронна адреса, на яку зловмисники просять відправити дані після здійснення платежу, вже заблокована провайдером. На думку головного інженера компанії McAfee Крістіана Біка, ця версія була розроблена так, щоб максимально швидко поширюватися. Вірус отримував пароль адміна завдяки утиліті Mimikatz. У компанії ESET заявили, що поширення шкідливої програми почалося в Україні.

Атака була в основному спрямована проти України, на яку припало 75 % всіх постраждалих від атаки комп'ютерів. Атаці піддалися енергетичні компанії, українські банки, Аеропорт Харкова, Чорнобильська АЕС, урядові сайти, київський метрополітен. Національний банк України опублікував на своєму сайті офіційну заяву про хакерську атаку на банки країни і боротьби з нею. Пізніше стали з'являтися повідомлення про хакерську атаку на російські банки, компанії Хоум Кредит, Роснафта і Башнафта. Також повідомлення про зараження стали надходити з Італії, Ізраїлю, Сербії, Угорщини, Румунії, Польщі, Аргентини, Чехії, Німеччини, Великої Британії, США, Данії, Нідерландів, Іспанії, Індії, Франції та Естонії.

Попри зовнішню схожість новий вірус має істотні відмінності від вже відомого Petya й тому отримав нові назви від різних дослідників (NotPetya, Eternal Petya, Petna, тощо). У цілому він має добре написаний код, який використовує для свого поширення низку шляхів:

1. Вразливості EternalBlue та EternalRomance (CVE-2017-0144 та CVE-2017-0145 відповідно, обидві виправлені в оновленні MS17-010)

2. Виявлення гешів паролів зареєстрованих на комп'ютері користувачів і навіть адміністраторів (алгоритм LSA Dump, схожий на Win32/Mimikatz).

3. Використання стандартних можливостей операційної системи: спочатку передає свої файли установки через мережеві диски (Windows Share), а потім намагається їх запустити або віддаленим виконанням команд PowerShell (psexec), або ж через систему WMIC (Windows Management Instrumentation Command-line).

Таким чином, заражений цим хробаком комп'ютер здатен, за певних умов, вражати інші комп'ютери в мережі, навіть ті, які отримали останні оновлення операційної системи.

Аби не бути виявленим антивірусними програмами, бінарні коди вірусу застосовують:

1. Підроблений цифровий підпис Microsoft,

2. Шифрування алгоритмом XOR (для обходу перевірок на сигнатуру).

Проте, попри досить високий рівень реалізації самого вірусу, його розробники скористались вкрай вразливим та ненадійним способом спілкування з жертвами, що створює враження, що здирництво не було основним мотивом:

1. Всім жертвам пропонується перерахувати криптовалюту біткоїн вартістю 300$ на гаманець автора вірусу,

2. Та передати вказаний на екрані довгий код на вказану адресу електронної пошти.

Поштова служба, де була зареєстрована скринька зловмисників, заблокувала її вже через кілька годин після початку атаки і, таким чином, унеможливила спілкування між жертвами та зловмисниками. Тобто, сплата викупу не має сенсу, оскільки гарантовано не дасть бажаного результату. В оприлюдненій заяві компанія-провайдер поштової скриньки повідомила, що не лише заблокувала скриню, а й активно працює з німецькою федеральною службою інформаційної безпеки в розслідуванні цієї події.

Шкідлива дія вірусу складається з двох частин та залежить від прав, який має його процес, та від того, які процеси працюють в операційній системі. Вірус обчислює нескладний хеш назв запущених процесів, і якщо буде знайдено наперед задані коди може або припинити своє поширення, або ж, навіть, відмовитись від шкідливої дії[29].

Першим кроком вірус шифрує файли з наперед заданого переліку типів (їх понад 60) з використанням алгоритму AES-128. Для кожного комп'ютера вірус обчислює новий ключ симетричного алгоритму шифрування AES-128, який шифрує 800-бітним відкритим ключем RSA з пари ключів зловмисників та зберігає на жорсткому диску. Повідомлення з вимогою викупу для дешифрування файлів залишається на жорсткому диску. Це повідомлення має інший ключ, відмінний від ключа на другому кроці (так званий «ідентифікатор жертви») та доведена можливість відновлення втрачених файлів за умови отримання правильного коду від зловмисників. Проте навіть тут зловмисники припустились помилок, внаслідок яких відновлення даних істотно ускладнене,

а оскільки сам вірус Petya не містить модуля для відновлення даних, то для цього необхідна іще одна, інша програма.

Після завершення першого кроку (шифрування файлів), якщо вірус має достатньо системних прав та за певних інших умов, він переходить до другого кроку (знищення файлової системи).

Другим кроком вірус:

1. Змінює головний завантажувальний запис (MBR) кодами свого запуску,
2. Обчислює «ідентифікатор жертви» (англ. Victim ID) із застосуванням випадкових чисел,
3. Обчислює ключі шифрування із використанням криптографічно стійкого генератора псевдовипадкових чисел, зберігає його у MBR,
4. Встановлює випадковий таймер (не менше 10, але не більше 60 хвилин) на перезавантаження комп'ютера, та
5. Знищує всі записи в системних журналах.

При завантаженні комп'ютера, завдяки змінам в головному завантажувальному записі (MBR) замість операційної системи буде завантажено шкідливий код вірусу, який малює на екрані підробку під інтерфейс програми перевірки цілісності жорсткого диску Chkdsk. Основна шкідлива дія на цьому кроці полягає в шифруванні таблиці файлів (англ. Master File Table, MFT) файлової системи NTFS алгоритмом шифрування Salsa20. При цьому, ключ шифрування після завершення процесу безповоротно стирається, а жертві пропонується відправити зловмисникам для отримання ключа дешифрування «ідентифікатор жертви» (англ. Victim ID), який жодним чином не пов'язаний з тим ключем.

Така поведінка відрізняється від поведінки оригінального хробака Petya/Mischa. Оригінальний вірус Petya зберігав ключ шифрування Salsa20 й тим самим зберігав можливість для відновлення даних. Хоча, через помилку в реалізації відновити дані виявилось можливим навіть без сплати викупу (поки ця помилка не була виправлена у третій версії та вірусі Goldeneye).

Слід зазначити, що шкідлива дія вірусу цим не обмежена: через ваду в реалізації вірус здатен повторно вражати одну й ту саму систему. Тоді

зашифровані на першому кроці файли будуть зашифровані вдруге, а необхідний для їхнього дешифрування ключ буде затертий новим, чим унеможливить їхнє відновлення.

Використання вірусом одного-єдиного відкритого ключа RSA означає, що розкривши за викуп бодай один код для відновлення даних жертви (фактично — приватний ключ в парі RSA), зловмисники водночас відкрили б можливість усім іншим відновити втрачені дані (за допомогою цього ключа). Це, разом з іншими ознаками, може свідчити, що здирництво не було основним мотивом атаки, а навпаки, під здирництво була замаскована масштабна кібератака на інформаційні системи українських підприємств (від найбільших до найменших) та органів державної влади.

Компанія Symantec стверджує, що для своєї роботи вірус створює файл «C:\Windows\perfc», а якщо він вже існує, то вірус припиняє роботу. Тому якщо користувач сам створить цей файл і зробить його доступним тільки для читання, то це, імовірно, захистить його від вірусу.

Створити порожні та захищені від запису файли

1. C:\Windows\perfc
2. C:\Windows\perfc.dat
3. C:\Program Data\perfc
4. C:\Program Data\perfc.dat

Це захистить від шифрування файлів на комп'ютері, але не захистить від його використання для поширення вірусу.

Аби завадити зараженню та поширенню вірусу, слід, перш за все, виконувати звичайні поради з комп'ютерної безпеки, зокрема: не відкривати вкладені файли від незнайомих осіб або підозрілих листів від знайомих (захист від фішингу), встановити останні оновлення для операційної системи (зокрема, латку MS17-010) та антивірусних програм. Для захисту мережі від поширення вірусу слід також вимкнути підтримку застарілого протоколу SMBv1, вимкнути або обмежити використання систем PowerShell, WMIC та мережевих тек (Windows Share). Також в мережевих екранах слід заблокувати трафік на порти 139 та 445. Виконання цих порад, однак, може порушити звичну роботу інформаційної системи та вимагатиме додаткових зусиль від адміністраторів.

Для ефективного захисту не лише від цього конкретного вірусу-хробака, а подібних інцидентів взагалі, слід ретельно впровадити політики комп'ютерної-інформаційної безпеки, наприклад, Defence-in-Depth.

2.7 Операція «9 травня»

Українські хакери кіберальянсу анонімних груп FalconsFlame та Trinity з 00:00 9 травня 2016 року провели операцію OpMay9, у рамках якої здійснили не менше 9 успішних зломів сайтів терористичної організації «ДНР», а також російських сайтів агресивної антиукраїнської пропаганди й ресурсів російських приватних військових компаній (ПВК), що діють під протекцією ФСБ РФ в Україні та Сирії.

На зламаних сайтах хакери залишили хештеги OpMay9 оп9Травня, а також по 3 коротких відео про Другу світову війну і внесок українського народу в перемогу над нацизмом.

Перед тим, 29 квітня 2016 року, ті самі групи хакерів припинили існування популярного сайту російських пропагандистів, який позиціював себе як мережеве інформаційне агентство «Anna News». Альянс хакерських груп Falcons Flame та Trinity записав відеозвернення і розмістив його на сайті після повного знищення інформації (статей, баз даних і бекапів). У відео також був згаданий мем «Львівське метро».

Окрім зламу пропагандистських сайтів, групи хакерів спільно з волонтерами групи InformNapalm змогли знайти докази застосування російськими терористами сучасних засобів РЕБ у війні на сході України, зокрема — Р-330Ж «Житель».

2.8 Операція «Прикормка»

У травні 2016 року компанія ESET (з головним офісом в Братиславі) оприлюднила доповідь за результатами проведеного аудиту, в якому викрила компанію кібершпигунства українських хакерів (ймовірно афілійованих зі спецслужбами) за інформаційними системами маріонеткових утворень російських терористів на окупованому сході України. Доповідь була підготовлена вихідцем з Росії, випускником Південно-Уральського державного

університету (Челябінськ, Росія) Антоном Черепановим. Автор дослідження виступив з доповіддю на форумі Positive Hack Days, який проходив 17-18 травня в Москві.

У третьому кварталі 2015 року спеціалісти ESET виявили раніше невідоме модульне сімейство шкідливих програм — Prikormka. Подальші дослідження показали, що дана загроза почала поширюватися щонайменше з 2008 року. За період активності найбільше шкідливих програм зафіксовано в Україні. Тривалий час Prikormka залишалася непоміченою через відносно низьке співвідношення загроз до 2015 року. Однак у 2015 році кількість цього небезпечного програмного забезпечення суттєво зросла.

Основним способом інфікування, який був визначений спеціалістами ESET в ході дослідження, стало поширення фішингових електронних листів з прикріпленими шкідливими файлами або з посиланнями для завантаження небезпечного файлу, розміщеного на віддаленому сервері. Після відкриття замаскованого небезпечного вкладення, Prikormka відображає документ-приманку для обману та відволікання уваги потенційної жертви, яка очікує безпосередньо відкриття документу, не підозрюючи про загрозу. Цей метод спрацьовує у випадках, коли користувачі не є технічно обізнаними та не дотримуються правил безпеки під час роботи за комп'ютером.

Зловмисники використовують прийоми соціальної інженерії для переконання жертви відкрити шкідливе вкладення, серед яких використання провокативних та привабливих назв вкладень електронної пошти. Приклади таких назв:

1. Нацгвардейцы со шприцами сделали из донецкого мальчика мишень для ракет.exe
2. Последнее обращение командира бригады 'Призрак' Мозгового Алексея Борисовича к солдатам и офицерам ДНР и ЛНР.scr
3. Места дислокации ВСУ в зоне проведения АТО.scr

Також були виявлені ознаки, що операція «Прикормка» була спрямована і на інформаційні системи «Правого сектора» та інших організацій.

Слід зазначити, що антивірус розробки ESET досить поширений серед державних установ України, що може створити для компанії можливості отримувати доступ до інформації в цих системах.

2.9 Злам «Першого каналу»

На початку червня 2016 року волонтери команди Інформнапалм повідомили про успішний злам корпоративного сервера російського «Першого каналу» українським кібер-альянсом хакерів FalconsFlame, Trinity та Рух8. Операція почалася 25 травня, а перші результати з'явилися 5 червня. Внаслідок злому було опубліковано анкетні дані всіх співробітників «Першого каналу». Крім цього, з'явилась можливість зламати особисті поштові скриньки і хмарні сховища співробітників.

Першим російським пропагандистом, інформацію про якого розкрили активісти, став журналіст Сергій Зенін. Було з'ясовано, що російський пропагандист звертався за консультаціями до компанії ESET Russia при створенні проекту з головним завданням «Показати, як далеко зайшли США у своїй уявній боротьбі з тероризмом і наскільки небезпечні ігри АНБ із цифровими технологіями». В червні 2014 року відбулось перше відрядження Зеніна на захоплений російськими терористами Донбас. Отримав «акредитацію» в «ДНР» під номером 116.

Також було з'ясовано, що Зенін обговорював з журналістом московського офісу Reuters Антоном Звєрєвим (акредитація в «ДНР» під номером 232) різні версії збиття Боїнгу малайзійських авіаліній. При чому Звєрєв наводив уривки інтерв'ю з російськими бойовиками, з яких можна було дізнатись про надання Росією установки ЗРК «Бук», її маршрут, приблизне місце пуску ракети.

2.10 Блокування російських інтернет-сервісів

Наказом № 133/2017 від 15 травня 2017 року Президент України Петро Порошенко ввів у дію рішення РНБО України від 28 квітня 2017 року «Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)» яким заборонив інтернет-провайдерам надавати послуги з

доступу користувачам мережі інтернет до низки російських інформаційних ресурсів та порталів, зокрема, й соціальних мереж ВКонтакте і Одноклассники. Згідно думки аналітиків, прямий доступ до бази даних соціальних сервісів із надзвичайною легкістю дозволяє російським спецслужбам виявити якнайширший спектр інформації, яку звичайні громадяни і військовослужбовці завантажують до соцмереж.

За словами Валентина Петрова, керівника служби з питань інформаційної безпеки Апарату РНБО України, коли проводилось розслідування атаки на фінансовий сектор України, які відбулися у грудні 2016 року, то виявилося, що на значній більшості вражених машин було встановлено російське програмне забезпечення. Відповідно, було висловлене припущення, що російське програмне забезпечення, перш за все, надає потенційну можливість несанкціонованого доступу до інформації.

За словами представників СБУ пакет програм 1С також становить небезпеку. «1С» присутня на українському ринку вже тривалий час та завоювала статус монополіста. Однак, вся інформація, яку отримує «1С», та оновлення програми йде через російські сервери. Функціонує зворотній зв'язок, тож збираються дані, типу як big data, яка може бути використана в інтересах підриву економіки, збору даних, підриву окремих галузей окремих секторів економіки нашої держави.

В травні 2017 року на слуханнях в Конгресі США було підняте питання використання продуктів російської компанії «Лабораторія Касперського». Керівники американських розвідувальних служб (в тому числі ЦРУ, АНБ, військової розвідки) висловили певне занепокоєння стосовно продуктів компанії та заявили, що не радять ними користуватись.

Результати дослідження компанії gemiusAudience показали, що частка користувачів на заблокованих соціальних мережах знизилася: Вконтакте втратив 3,7 мільйона користувачів, що заходили на сайт через персональні комп'ютери або ноутбуки, а Однокласники — 2,6 мільйона. До введення санкцій ВКонтакте охоплював 50,5 % відвідувачів Уанету, за тиждень охоплення аудиторії скоротилось до 30,8 %. Охоплення аудиторії на Одноклассниках впало з 22,3 % до 8,5 %.

У той же час введення санкцій позитивно позначилось на кількості відвідувань Facebook. Тижнева аудиторія мережі до заборони російських ресурсів становила 5,3 мільйона користувачів (охоплення 28,5 %), а після блокування виросла на 2,2 мільйона. З 22 по 28 травня соціальну мережу відвідали 7,5 мільйона аудиторії Уанету, 40 % всіх інтернет-користувачів за тиждень. За цим показником Facebook вперше обійшов ВКонтакте. Станом на 7 червня 2017 року за даними внутрішньої статистики для рекламодавців цим порталом користувалось вже 8,6 млн українців. За перший тиждень червня до Facebook приєднались ще 300 тисяч користувачів з України.

Разом з користувачами з соцмережі пішли й рекламодавці. Особливо це видно у відеорекламі, що розміщувалась у ВКонтакте. Там спад охоплення аудиторії відеорекламою склав 92 % (2,17 млн користувачів). В Одноклассниках з 22 по 28 травня відеореклама охопила 400 тисяч користувачів, що на 77 % менше, ніж протягом тижня до заборони ресурсів.

Аудиторія Yandex.ua скоротилась на 1,9 мільйона користувачів: перед забороною ресурсу сайт охоплював 38,1 % всіх користувачів Уанету за тиждень, після заборони — 28,0 %. Mail.ru втратив більше користувачів — 2,5 мільйона: з 8 по 14 травня портал відвідали 31,7 % тижневої аудиторії української мережі, а з 22 по 28 травня — 18,6 %.

За даними SimilarWeb станом на середину червня 2017 року аудиторія російської соцмережі ВКонтакте в Україні скоротилась на 61 %, якщо порівнювати дані за квітень 2017 року і за перші 16 днів червня. Відвідуваність зупинилося на рівні 3,8 млн візитів у день. Відвідуваність соцмережі «Одноклассники» впала на 64 % — з 4,6 млн до 1,6 млн візитів на день. Падіння відвідуваності інтернет-порталу yandex.ua дорівнює близько 65 % — з 5,9 млн до 2 млн візитів на день. Mail.ru втратив 55 % української аудиторії. Кількість щоденних візитів зменшилась з 4,9 млн до 2,2 млн.

Натомість, станом на 25 червня 2017 року, українська аудиторія Facebook зросла з 7,4 млн користувачів у травні 2017 до 10 млн користувачів.

1 червня 2017 року в ЗМІ стало відомо про рішення компанії Яндекс закрити офіси в Україні та запропонувати своїм співробітникам переїхати в

інші країни для продовження роботи на компанію. Аналогічне рішення — закрити офіси в Україні — ухвалило й керівництво Mail.ru.

Одразу після підписання указу стався сплеск інтересу серед інтернет-користувачів з України до технології VPN. Але вже за три тижні інтерес став згасати, а кількість пошукових запитів зменшилась в 7 разів. Також було помічено зменшення інтенсивності використання VPN для доступу до російських веб-сайтів.

У червні 2017 року в ТОП-5 сайтів, якими користуються українці, вперше за історію дослідження були відсутні російські.

За даними Kantar TNS CMeter у вересні 2017 року в Топ-10 найпопулярніших сайтів не було жодного російського, хоча майже третина українців продовжувала щонайменше раз на місяць відвідувати ВКонтакте.

2.11 Псевдозамінування

Протягом 2018—2021 років в Україні зафіксована хвиля масових повідомлень про замінування низки об'єктів: вокзалів, аеропортів, торгових центрів, навчальних закладів, лікарень, урядових установ та інших місць, які передбачають велике скупчення людей. Зокрема у жовтні 2021 року надійшло 211 електронних повідомлень та викликів про закладення вибухових пристроїв за різними адресами міста. Схожа ситуація відбулася у Харкові, де зафіксовано 42 неправдивих виклики про замінування та м. Київ — 12 викликів. За даними міністерства внутрішніх справ дані повідомлення надходять з території Російської Федерації та ОРДЛО з використанням тимчасових електронних скриньок та інтернет-телефонії.

Висновки до другого розділу

Забезпечити повну безпеку України в кіберпросторі можливо лише застосувавши досвіду Китаю, проте це суперечитиме як нормам міжнародного права, так і прагненню України до інтеграції з Заходом.

Ефективного захисту кіберпростору можна досягнути розробкою власних технічних засобів та програмного забезпечення, розвитком українського сегменту Інтернету. Як, наприклад, в Естонії, де це щорічно додає

кілька відсотків до ВВП, а такі розробки, як Skype, стали всесвітньо популярними.

Для мінімізації ризиків у Європі в 2018 році наберуть чинності закони про захист даних. Вони передбачають різке підвищення штрафів за розголошення або втрату персональних даних, що змусить компанії вже в цьому році переглянути свої підходи і стандарти щодо забезпечення інформаційної та кібернетичної безпеки, в тому числі ввести окрему посаду відповідального за захист інформації та кібернетичну безпеку. Важливим фактором посилення заходів кібернетичної безпеки є збереження балансу між комфортом, свободою доступу до інформації та забезпеченням надійного захисту інформації, від яких багато в чому залежить благополуччя громадян і мир в Україні. Однак це завдання непросте, і його доведеться вирішувати ще довгий час. Масштабна кібератака на корпоративні та державні мережі за допомогою вірусу «NotPetya», яка відбулася 27 червня 2017 року, — яскравий приклад важливості кібернетичної безпеки для функціонування держави. Подібні кібератаки спрямовані на дестабілізацію України. **«Відключити, знищити, дестабілізувати»,** — ось їхня мета. Масові відключення електроенергії, телефонного зв'язку та Інтернету, труднощі з обслуговуванням клієнтів і проведенням банківських операцій, реальні фінансові збитки — це те, що використовує ворог вже сьогодні.

Використовуючи кіберпростір, хакери можуть зламати захищені мережі та отримати необхідну інформацію, тому ми мусимо спрямувати зусилля на захист своїх мереж і забезпечити їх безпеку, використовуючи такі рівні захисту інформації:

1. запобігання — доступ до інформації та технології надається тільки для персоналу, який отримав допуск та має відповідні фахові навички;

2. виявлення — забезпечується раннє виявлення злочинів і зловживань, навіть якщо механізми захисту були обійдені;

3. обмеження — зменшується розмір втрат, якщо злочин все-таки відбувся, незважаючи на заходи щодо його запобігання та виявлення;

4. відновлення — забезпечується ефективне відновлення інформації за наявності документованих і перевірених планів з відновлення.

Висновок, який ми повинні зробити для себе, — це збільшення інвестування в кібербезпеку, щоб запобігати атакам на великі державні й приватні компанії і протистояти намірам дестабілізувати суспільство.

Досвід України у веденні кібервійни вже є безцінним і може бути взірцем для інших країн.

РОДІЛ 3. НАПРЯМИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ УКРАЇНИ В УМОВАХ ВЕДЕННЯ ПРОТИ УКРАЇНИ ІНФОРМАЦІЙНОЇ ВІЙНИ

3.1 Україна на 2016 – 2020 роки

Прийняття у 2016 році Стратегії кібербезпеки України стало важливим кроком у запровадженні підходів довгострокового планування в цій сфері, а отже, сам факт її прийняття є позитивним результатом. За ці роки було докладено зусиль до становлення та розвитку національної системи кібербезпеки. Важливим етапом її інституалізації стало прийняття Закону України «Про основні засади забезпечення кібербезпеки України», який є правовим підґрунтям для створення національної системи кібербезпеки та виконання її основними суб'єктами завдань у сфері кібербезпеки.

Удосконалено нормативне забезпечення з питань кіберзахисту критичної інформаційної інфраструктури, ухвалено порядок її визначення та загальні вимоги до її кіберзахисту.

Утворено центри (підрозділи) забезпечення кібербезпеки або кіберзахисту в Державній службі спеціального зв'язку та захисту інформації України, Службі безпеки України, Національному банку України, Міністерстві інфраструктури України, Міністерстві оборони України (Збройних Силах України).

Розбудовується Національна телекомунікаційна мережа, функціонують захищені центри обробки даних (дата-центри), утворюється Національний центр резервування державних інформаційних ресурсів, розпочато функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки.

З метою покращення координації діяльності суб'єктів забезпечення кібербезпеки було утворено робочий орган Ради національної безпеки і оборони України – Національний координаційний центр кібербезпеки, рішення якого сприяють вирішенню найбільш складних проблем у цій сфері.

Активно розвивається співпраця з іноземними партнерами, поглиблюється співробітництво України з ЄС та НАТО, проводяться кібернавчання за участю

інших держав та міжнародних організацій.

Започатковано проведення щорічного заходу – місяця кібербезпеки.

Водночас діяльність суб'єктів національної системи кібербезпеки залишається недостатньо скоординованою і такою, що спрямована на виконання лише поточних завдань. За результатами експертних оцінок, стан реалізації Стратегії за визначеними показниками не перевищує 40 %. Невирішеними залишилися питання оперативного обміну інформацією про кіберзагрози, ефективної системи підготовки кадрів та дієвої моделі державно-приватного партнерства. Організація і проведення наукових досліджень у сфері кібербезпеки всіма експертами визначаються як недостатні.

Отриманий протягом часу дії Стратегії досвід надав змогу виокремити низку системних проблем, які або ускладнювали, або унеможливлювали її ефективну реалізацію.

Однією з виявлених проблем стала недостатня чіткість визначених пріоритетів та напрямів забезпечення кібербезпеки України, значна частина яких не мала зрозумілої кінцевої мети та була не конкретною. Незадовільним був рівень планування заходів з реалізації Стратегії, заплановані заходи не завжди корелювались із завданнями Стратегії. Реалізація Стратегії ускладнена відсутністю цілісного бачення (програми) розвитку спроможностей основних суб'єктів національної системи кібербезпеки, обмеженістю ресурсного забезпечення функціонування цієї системи, відсутністю належної державної підтримки розвитку її інституційного забезпечення.

Не були розроблені індикатори виконання Стратегії, що ускладнило процес оцінки її результативності та виокремлення незавершених завдань. Участь у реалізації Стратегії переважно брали суб'єкти сектору безпеки і оборони, недостатньо залучались інші міністерства і відомства, наукові установи, громадськість. До виконання завдань із розвитку наукового потенціалу та поширення кіберграмотності недостатньо залучались освітні установи та наукові заклади.

Надзвичайно важливі для розвитку національної системи кібербезпеки завдання Стратегії не були виконані: не сформовано перелік критичної інформаційної інфраструктури, не створено модель державно-приватного

партнерства. Розвиток цифрової грамотності здійснювався без чіткої програми, кібернавчання проводились епізодично.

Нова Стратегія кібербезпеки України враховує цей досвід і проблеми та визначає механізми реалізації Стратегії на наступний п’ятирічний період.

3.2 Національна система кібербезпеки: засади робудови.

Україна прагне створити максимально відкритий, вільний, стабільний і безпечний кіберпростір, де враховуються права і свободи людини, підтримуються соціальний, політичний і економічний розвиток.

Реалізуючи Стратегію кібербезпеки України на 2016 – 2020 роки, держава змогла сформувати ядро національної системи кібербезпеки. Україна наростила потенціал, який дає можливість здійснювати подальшу розбудову національної системи кібербезпеки на засадах стримування, кіберстійкості, взаємодії.

З цією метою Україна:

посилить спроможності національної системи кібербезпеки для унеможливлення збройної агресії проти України у кіберпросторі або з його використанням, нейтралізації розвідувально-підривної діяльності, мінімізації загроз кіберзлочинності та кібертероризму (стримування);

набуде здатності швидко адаптуватися до внутрішніх і зовнішніх загроз у кіберпросторі, підтримуватиме стале функціонування національної інформаційної інфраструктури, насамперед об’єктів критичної інформаційної інфраструктури (кіберстійкість);

забезпечить розвиток комунікації, координації та партнерства між суб'єктами забезпечення кібербезпеки на національному рівні, розвиток стратегічних відносин у сфері кібербезпеки із ключовими іноземними партнерами, передусім з Європейським Союзом і НАТО та їх державам

членами, співробітництво у цій сфері з іншими державами та міжнародними організаціями на основі національних інтересів України (взаємодія).

Розбудова національної системи кібербезпеки на таких засадах дасть можливість розширити запропоновані та рекомендовані дії на всі галузі економіки та сфери діяльності.

З цією метою держава залучить до вирішення завдань щодо забезпечення кібербезпеки в національному масштабі крім основних суб'єктів національної системи кібербезпеки, на яких спиралася на початковій стадії формування національної системи кібербезпеки, широке коло суб'єктів забезпечення кібербезпеки, у тому числі суб'єктів господарювання, громадські об'єднання та окремих громадян України.

Ключову об'єднувальну та координаційну роль у цьому процесі відіграватиме Національний координаційний центр кібербезпеки.

Держава розбудовуватиме національну систему кібербезпеки, ґрунтуючись на:

всеохоплюючому розумінні та аналізі цифрового середовища, глобальних трендів кібербезпекового середовища (з одночасним урахуванням особливостей нашої країни), неухильному захисті національних інтересів України у сфері кібербезпеки;

перманентності заходів з удосконалення законодавства у сфері кібербезпеки та оперативності дій щодо її актуалізації відповідно до безпекових умов, що змінюються;

орієнтованості на суспільство, що сприятиме його економічному і соціальному зростанню;

використанні принципу мінімальної достатності ролі держави у процесах розвитку та забезпечення безпеки кіберпростору, встановлення вимог (правил, настанов) щодо безпечного використання мережі Інтернет;

збалансованому забезпеченні потреб держави і прав громадян, дотриманні законності, процесуальних гарантій та засобів правового захисту, повазі до основоположних цінностей, прав людини і особи на свободу вираження думки, такому самому захисті загальновизнаних основоположних прав в онлайн-середовищі, як і в офлайновому; засудженні практики перевищення

встановлених меж необхідності щодо обмеження прав громадян та юридичних осіб під час використання кіберпростору та ІКТ-технологій;

відкритості та створенні умов для активної участі всіх заінтересованих сторін з урахуванням їх потреб і зобов'язань в умовах, коли кібербезпека цифрового середовища набула надважливого значення для держави, суспільства і громадян;

визначенні чітких ролей, потреб, зобов'язань під час розв'язання завдань кібербезпеки різного ступеня складності, застосування стимулюючих механізмів та обміну унікальними знаннями і досвідом;

ризик-орієнтованому підході в частині заходів забезпечення кібербезпеки та кіберзахисту;

співпраці та інклюзивному діалозі всіх суб'єктів забезпечення кібербезпеки, зокрема в рамках державно-приватного партнерства, задля досягнення стратегічних цілей, заснування ініціатив, вироблення узгоджених планів та проєктів у сфері кібербезпеки;

впровадженні сучасних принципів, методів, підходів та механізмів публічного управління у сфері кібербезпеки, у тому числі тих, що базуються на стратегічному плануванні та управлінні, кризовому управлінні, партнерських відносинах між державою, бізнесом та суспільством;

збалансованому розподілі наявних матеріальних і фінансових ресурсів, а також оптимальному застосуванні для вирішення кожного конкретного завдання у сфері кібербезпеки таких важелів, як законодавство, стандартизація, освітні програми, механізми стимулювання та зміцнення довіри, обмін інформацією і передовим досвідом;

проактивному підході, що передбачає здійснення випереджувальних заходів, зокрема застосування систем попередження кібератак, зміщуючи організаційний та технологічний фокус від боротьби з наслідками до протидії кібератакам на ранніх стадіях;

забезпеченні демократичного цивільного контролю за функціонуванням національної системи кібербезпеки, а саме дотриманням вимог Конституції і законів України суб'єктами забезпечення кібербезпеки, станом реалізації стратегічних документів, концепцій, державних програм та планів у сфері

кібербезпеки, ефективністю використання ресурсів, зокрема бюджетних коштів.

3.3 Національний кіберпростір виклики та кіберзагрози

Інформаційних технологій поряд із потужними соціально значимими перевагами супроводжується масштабуванням кіберзагроз на всі сфери життєдіяльності, їх еволюцією вбік високотехнологічних рішень та урізноманітненням інструментарію реалізації.

Україна має необхідний потенціал для нарощування спроможностей у сфері кібербезпеки для адекватної протидії сучасним викликам і загрозам.
Викликами для України у сфері кібербезпеки є:

активне використання кіберзасобів у міжнародній конкуренції за світове лідерство, змагальний характер розвитку засобів кібербезпеки та реалізації кіберзагроз у процесі швидких прогресуючих змін інформаційно-комунікаційних технологій, хмарних обчислень, 5G-мереж, великих даних, Інтернету речей, машинного навчання/штучного інтелекту (AI) тощо;

мілітаризація кіберпростору та зростаючі технологічні можливості кіберзброї, які дають можливість здійснювати приховане проведення противником кібератак та кібероперацій, віддаленого взяття під контроль систем управління, завдання шкоди та руйнування критичної інформаційної інфраструктури;

зростання технологічного рівня протиправних посягань на інтереси держави, суспільства та окремих громадян із застосуванням методів соціальної інженерії, використання технологій штучного інтелекту та криптотехнологій;

вплив на економічну діяльність та соціальну поведінку поширення пандемії COVID-19, що спричинило швидку трансформацію і організацію значного сегмента суспільних відносин у дистанційному режимі з широким використанням електронних сервісів та інформаційно-комунікаційних систем. Це посилило загрозу порушення прав громадян під час використання кіберпростору.

Цифрова трансформація, що є одним із пріоритетів розвитку України, створює нові виклики у сфері кібербезпеки. Упровадження нових технологій,

цифрових послуг та механізмів взаємодії громадян з державою, включаючи виборчий процес, створює велику кількість прихованих взаємозв'язків на рівні технологій і процесів. Без системного підходу до кібербезпеки та оцінки ризиків існує ймовірність втрати довіри громадян до процесів цифрової трансформації.

Сучасні світові тренди розвитку кібербезпекового середовища, виклики для країни, внутрішні процеси та явища сформували такі загрози кібербезпеці України.

З 2014 року Росія активно використовує кіберпростір у гібридній агресії проти України шляхом здійснення деструктивного впливу на органи державної влади, системи управління військами та зброєю сил оборони, а також на об'єкти критичної інфраструктури. Держава-агресор невпинно нарощує арсенал кіберзброї наступального, розвідувального та підривного призначення, застосування якої може викликати невиправні, незворотні руйнівні наслідки. Зазначені чинники вимагають постійного нарощування можливостей забезпечення кібербезпеки органами сектору безпеки і оборони.

Надзвичайно актуальною загрозою на сьогодні є розвідувально-підривна діяльність у кіберпросторі проти України, яка пов'язана з проведенням спецслужбами іноземних держав, насамперед Російської Федерації, розвідувальної діяльності з метою викрадення інформації (кібершпигунство) та підривних акцій з порушення штатного режиму функціонування об'єктів критичної інформаційної інфраструктури, передусім систем управління державою, об'єктів життєзабезпечення, електроенергетики, транспорту, ядерної і хімічної промисловості, банківської сфери (актів кібердиверсій).

В Україні в останні роки відчутно зросла загроза кібертероризму. Насамперед, це пов'язано з кіберможливостями держави-агресора Російської Федерації, яка веде проти України кібервійну із застосуванням кіберзброї. Спостерігається використання кіберпростору для фінансування терористичних угруповань. Водночас недостатньою є взаємодія України з міжнародними партнерами щодо опрацювання на взаємовигідній основі механізмів протидії кібертероризму.

Зростання кіберзлочинності в національному сегменті кіберпростору є

масштабною загрозою, яка завдає шкоди державним інформаційним ресурсам, суспільним процесам, особисто громадянам, що знижує довіру суспільства до інформаційних технологій та призводить до значних матеріальних втрат. Набуває поширення використання кіберпростору для вчинення інших злочинів (проти основ національної безпеки, легалізації доходів, одержаних злочинним шляхом, торгівлі людьми, незаконного обігу зброї, наркотичних засобів та інших предметів і речовин, які загрожують життю та здоров'ю людей). Ситуація ускладнюється через низький рівень кіберграмотності населення, зокрема пересічних користувачів електронних послуг.

Державні інформаційні ресурси та об'єкти критичної інформаційної інфраструктури, які призначені для забезпечення задоволення життєво важливих потреб громадянина, особи, суспільства і держави, є недостатньо захищеними від кібератак.

Державні органи, приймаючи рішення про автоматизацію процесів державного управління, не завжди оцінюють ризики, що виникають у кіберзахисті державних інформаційних ресурсів. Захист інформаційно-комунікаційних систем державних органів та суб'єктів господарювання, в яких обробляється значна частина службової інформації та персональних даних громадян, не відповідає вимогам законодавства, що посилює ризики втручання в такі системи, загрожує конфіденційності, цілісності та доступності інформації (реєстри, бази даних), яка призначена для задоволення потреб та забезпечення конституційно гарантованих інтересів, громадян, суспільства і держави.

Висока технологічна залежність України від іноземних виробників продукції ІКТ та програмного забезпечення управління нею, відсутність сучасних національних стандартів щодо вимог з безпеки ланцюга поставок відповідного обладнання, розроблення програмного забезпечення та інформаційно-комунікаційних систем, систем сертифікації або оцінки відповідності з безпеки такої продукції підвищують ступінь уразливості об'єктів військової, політичної, фінансово-економічної та промислової інфраструктури держави від шкідливих і незадекларованих функцій у такому обладнанні та звужують вітчизняні спроможності протидії кіберзагрозам.

Значна частина підприємств, установ та організацій усіх форм власності не забезпечують кіберзахист електронних інформаційних ресурсів, якими вони розпоряджаються, що призводить до порушень прав користувачів цифрових послуг та дискредитує процеси цифрової трансформації в державі. Базовий ландшафт інструментарію реалізації окреслених кіберзагроз характеризується зростанням високотехнологічної складової та різноманіттям.

Безперервно збільшується кількість кібератак, спрямованих на викрадення персональних та інших конфіденційних даних громадян та організацій із використанням методів соціальної інженерії.

Зростає рівень ризику застосування фішингових атак, ботнетів, шкідливого програмного забезпечення, у тому числі програм-вимагачів, як з боку фінансово мотивованих кіберзлочинних груп, так і з боку хакерських угруповань, підконтрольних країні-агресору та іншим країнам.

Збільшення інформації у базах даних та інформаційних системах та посилення відповідальності за витоки персональних даних громадян у провідних країнах створило глобальний ринок для розвитку програм-вимагачів, які вимагають кошти за розблокування доступу до інформації або нерозміщення викраденої інформації в мережі Інтернет.

Усе частіше спрямовані кібератаки не здійснюються напряму на уряди та організації. Кібератак зазнають розробники та постачальники програмних і апаратних засобів з метою зараження популярних додатків, внесення змін у вихідні коди та процеси оновлень. У подальшому це використовується для проникнення до великої кількості їх клієнтів та завдання масштабної шкоди.

Популярні веб-сайти, соціальні мережі, реєстри збирають велику кількість ідентифікаційних та персональних даних користувачів. Витоки інформації з баз даних, які їм належать, створюють загрозу використання цих даних з метою атаки на інші ресурси та інформаційні системи.

Передумови та чинники, які формують окреслені загрози:

недосконалість нормативно-правової бази у сфері кібербезпеки, а також її застарілість у сфері захисту інформації, повільна імплементація положень європейського права у вітчизняне законодавство, недостатня врегульованість цифрової складової частини розслідування злочинів, а також низький рівень

правової відповідальності за порушення вимог законодавства у цій сфері;

відсутність у значної частини міністерств і відомств відповідних структурних підрозділів, необхідного кадрового забезпечення та належного контролю за кіберзахистом. Фінансування робіт із кіберзахисту здійснюється за залишковим принципом з технологічними помилками;

відсутність системи незалежного аудиту інформаційної безпеки та механізмів розкриття інформації про вразливості в умовах динамічної цифровізації всіх сфер державного управління та життєдіяльності країни, що вимагає суворого дотримання відповідних стандартів;

невідповідність сучасним вимогам рівня підготовки та підвищення кваліфікації фахівців з питань кібербезпеки та кіберзахисту, зокрема неефективні механізми їх стимулювання до роботи в державному секторі;

відсутність законодавчого акта про критичну інфраструктуру України та її захист, що значно ускладнює формування системи кіберзахисту такої інфраструктури;

незавершеність заходів з упровадження організаційно-технічної моделі кіберзахисту, яка відповідатиме сучасним загрозам, викликам у кіберпросторі та глобальним тенденціям розвитку індустрії кібербезпеки;

відсутність системи підвищення цифрової грамотності громадян та культури безпекового поводження в кіберпросторі, підвищення рівня обізнаності суспільства щодо кіберзагроз та кіберзахисту.

3.4 Пріоритети забезпечення кібербезпеки україни та стратегічні цілі.

Пріоритетами забезпечення кібербезпеки України є:

убезпечення кіберпростору задля захисту суверенітету держави та розвитку суспільства;

захист прав, свобод і законних інтересів громадян України у кіберпросторі;

європейська і євроатлантична інтеграція у сфері кібербезпеки.

Формування нової якості національної системи кібербезпеки потребує чіткого та зрозумілого визначення стратегічних цілей, що мають бути досягнуті протягом періоду реалізації Стратегії.

Для формування потенціалу **стримування** (С) до 2026 року маємо досягти таких стратегічних цілей:

Ціль С.1. Дієва кібероборона. Україна має не лише створити та розвивати ефективні (у тому числі кадрово та технологічно) підрозділи з повноваженнями ведення збройного протиборства в кіберпросторі, але й сформувати належну правову, організаційну, технологічну модель їх функціонування та застосування, що неможливо без: ефективної взаємодії основних суб'єктів національної системи кібербезпеки та сил оборони під час проведення заходів з кібероборони, належного навчання та фінансового забезпечення таких структур, систематичного проведення кібернавчань, оцінки спроможностей та ефективності підрозділів, розроблення та імплементації індикаторів оцінки їх діяльності.

Ціль С.2. Посилення спроможностей у протидії розвідувально-підривній діяльності у кіберпросторі та кібертероризму. Україна забезпечить безперервне здійснення контррозвідувальних заходів з виявлення, попередження та припинення розвідувально-підривної діяльності іноземних держав, актів кібершпигунства та кібертероризму, усунення умов, що їм сприяють, та причин їх виникнення для убезпечення інтересів держави, суспільства і окремих громадян.

Ціль С.3. Посилення спроможностей у протидії кіберзлочинності. Правоохоронні та державні органи спеціального призначення з правоохоронними функціями набудуть спроможностей для мінімізації загроз кіберзлочинності, посилять свій технологічний і кадровий потенціал для проведення превентивних заходів та розслідування кіберзлочинів.

Ціль С.4. Розвиток асиметричних інструментів стримування. Створимо необхідні умови для забезпечення стримування агресивних дій у кіберпросторі проти України шляхом застосування економічних, дипломатичних, розвідувальних заходів, а також залучення потенціалу неурядового сектору.

Для набуття **кіберстійкості** (К) національною системою кібербезпеки маємо до 2026 року досягти таких стратегічних цілей:

Ціль К.1. Посилення національної кіберготовності та кіберзахист.

Запровадити і реалізовувати чіткі та зрозумілі для всіх стейкхолдерів заходи з посилення національної кіберготовності в інтересах забезпечення економічного добробуту та захисту прав та свобод кожного українського громадянина. Кіберготовність полягає у здатності всіх стейкхолдерів, насамперед суб'єктів сектору безпеки і оборони, своєчасно й ефективно реагувати на кібератаки, забезпечити режим постійної готовності до реальних та потенційних кіберзагроз, виявлення та усунення передумов до їх виникнення, забезпечивши тим самим кіберстійкість, насамперед об’єктів критичної інформаційної інфраструктури.

Ціль К.2. Професійне вдосконалення, кіберобізнане суспільство та науково-технічне забезпечення кібербезпеки.

Провести докорінну реформу системи підготовки та підвищення кваліфікації фахівців у сфері кібербезпеки. Забезпечити збереження наявного кваліфікованого кадрового потенціалу суб’єктів кібербезпеки. Стимулювати дослідження і розробки у сфері кібербезпеки з урахуванням появи нових кіберзагроз і викликів, створення національних інформаційних систем, платформ і продуктів. Вітчизняний науково-технічний потенціал першочергово залучатиметься до вирішення завдань забезпечення кібербезпеки держави. Кібергігієна, цифрові навички, кіберобізнаність щодо сучасних кіберзагроз та протидії ним мають стати невід’ємними елементами освіти кожного українського громадянина.

Ціль К.3. Безпечні цифрові послуги.

Досягнемо балансу між потребами українського суспільства, вітчизняного ринку, економіки держави та необхідністю забезпечити безпеку в кіберпросторі. Забезпечимо надійність та безпеку цифрових послуг з моменту створення та протягом усього їхнього життєвого циклу.

Взаємодія (В) буде вдосконалена досягненням до 2026 року таких стратегічних цілей:

Ціль В.1. Зміцнення системи координації.

Держава створить умови для ефективної взаємодії суб’єктів забезпечення кібербезпеки в процесі розбудови та функціонування національної системи кібербезпеки, а також для результативних спільних дій під час попередження,

відбиття та нейтралізації наслідків кібератак та кіберінцидентів. Скоординуємо діяльність усіх стейкхолдерів задля подолання кризових ситуацій у кібербезпеці.

Ціль В.2. Формування нової моделі відносин у сфері кібербезпеки.

Ми запровадимо сервісну модель державної участі у заходах з кіберзахисту, за якої держава сприйматиметься не як джерело вимог, а як партнер у розбудові національної системи кібербезпеки.

Ціль В.3. Прагматичне міжнародне співробітництво.

Спрямуємо відносини з міжнародними партнерами як на розвиток взаємної довіри для спільної відповіді на кібератаки і подолання кризових ситуацій у кібербезпеці, так і на суто практичну співпрацю: обмін інформацією про кібератаки та кіберінциденти, проведення спільних кібероперацій та розслідування міжнародних кіберзлочинів, регулярні кібернавчання та тренінги, обмін досвідом та найкращими практиками.

3.5 Стратегічні завдання.

Посилення спроможностей національної системи кібербезпеки здійснюється шляхом виконання стратегічних завдань, спрямованих на досягнення визначених цілей.

На засадах стримування:

Україна сформує систему дієвої кібероборони шляхом *(ціль С.1):*

утворення у складі Збройних Сил України окремого роду військ – сил кібероборони, забезпечивши його належними фінансовими, кадровими та технічними ресурсами для стримування збройної агресії у кіберпросторі та надання відсічі агресору;

запровадження ефективних механізмів взаємодії основних суб'єктів національної системи кібербезпеки та сил оборони в частині спільного виконання завдань кібероборони;

забезпечення постійного моніторингу електронних комунікаційних мереж та інформаційних ресурсів домену «ua», здійснення аналізу вторгнень щодо цих мереж і ресурсів, а також виявлення в режимі реального часу аномалій щодо їх функціонування;

розроблення та виконання плану кібероборони як складової частини Плану оборони України;

проведення щонайменше двічі на рік спільних тематичних навчань із відповідними підрозділами держав – членів НАТО задля досягнення оперативної сумісності;

створення MIL.CERT-UA в інтересах Міністерства оборони України та Збройних Сил України, налагодивши на постійній основі співпрацю із європейською військовою CERT-мережею (Military CERT-Network);

забезпечення оцінки спроможностей суб'єктів сектору безпеки і оборони в частині спільного виконання завдань кібероборони, зокрема під час проведення оборонних оглядів та оглядів у сфері кібербезпеки;

запровадження у систему військово-патріотичного виховання та систему територіальної оборони навчальних програм підготовки та проведення практичних навчань у сфері кібербезпеки.

Україна забезпечить ефективну протидію розвідувально-підривній діяльності у кіберпросторі та кібертероризму шляхом *(ціль С.2):*

створення відповідно до схвалених концептуальних засад загальнодержавної системи виявлення кібератак, протидії актам кібертероризму і кібершпигунства щодо об'єктів критичної інформаційної інфраструктури, призначеної для моніторингу кіберпростору з метою своєчасного виявлення, запобігання кіберзагрозам і їх нейтралізації, оперативного реагування на цільові та масштабні кібератаки;

удосконалення аналітичного і криміналістичного забезпечення контррозвідувального захисту кібербезпеки держави за рахунок впровадження інноваційних методик обробки та оцінки цифрових даних, формування електронних доказів;

забезпечення максимального охоплення об'єктів критичної інфраструктури негласною перевіркою стану їх готовності до можливих кібератак та кіберінцидентів з метою превентивного усунення передумов до реалізації кіберзагроз;

забезпечення постійного моніторингу розвитку кіберспроможностей міжнародних терористичних угруповань, спрямованого на своєчасне

виявлення і нейтралізацію реальних та потенційних загроз скоєння на території України актів кібертероризму;

посилення контррозвідувального захисту сфери електронних комунікацій, ІТ-галузі, афілійованого з ними середовища, спрямованого на виявлення, попередження і припинення розвідувально-підривних посягань спецслужб іноземних держав на національну безпеку України у сфері кібербезпеки;

створення технологічних можливостей для автоматичного виявлення кібератак у режимі реального часу в потоках даних загальнодержавних інформаційно-комунікаційних систем та на окремих об'єктах критичної інфраструктури, їх блокування та визначення пріоритетності;

вдосконалення нормативно-правового, організаційного та кадрового забезпечення загальнодержавної системи боротьби з тероризмом у частині, що стосується залучення правоохоронних органів до здійснення заходів з попередження, виявлення і припинення актів кібертероризму.

Україна посилить спроможності у протидії кіберзлочинності *(ціль С.3)*, задля цього необхідно:

провести аудит імплементації в українське законодавство положень Конвенції про кіберзлочинність та завершити цей процес шляхом внесення необхідних змін до законів України;

врегулювати на законодавчому рівні питання щодо електронних доказів, використовуючи кращі практики та підхід країн-членів ЄС з цих питань;

вдосконалити законодавство України, передбачивши внесення необхідних змін з урахуванням сучасних викликів та тенденцій у сфері кібербезпеки;

запровадити практику проведення загальнонаціональної інформаційної роз'яснювальної кампанії щодо дій громадян у випадку, коли вони стикаються із кібершахрайством, поширенням шкідливого програмного забезпечення або порнографічного контенту, іншими кіберзлочинами, а також роз'яснення процедур звернення до правоохоронних органів;

розробити методику збору кіберстатистики та щороку оприлюднювати статистичну інформацію щодо кібератак, кіберінцидентів та заходів протидії за сферами відповідальності основних суб'єктів національної системи кібербезпеки на їх офіційних сайтах;

розробити методику проведення щорічних соціологічних досліджень щодо кіберзагроз, з якими стикається населення України, з оцінками ефективності діяльності державних органів у протидії ним і забезпечити проведення таких досліджень;

розробити методику комунікації між державою та суспільством щодо протидії масштабним кібератакам і кіберінцидентам, створити всі необхідні умови для її практичної реалізації;

запровадити механізми ідентифікації суб'єктів електронної комерції у кіберпросторі, забезпечивши внесення відповідних змін до законодавства України;

врегулювати на законодавчому рівні правовий статус криптовалют, визначити правові механізми щодо операцій із криптовалютами та створення ринків;

провести спільні з ЄС заходи в рамках Програми з питань розбудови зовнішнього кіберпотенціалу ЄС та підтримки партнерів для підвищення їхньої стійкості в кіберпросторі та спроможності розслідувати, переслідувати кіберзлочинність та реагувати на кіберзагрози;

забезпечити підвищення рівня кваліфікації, матеріально-технічного забезпечення судових експертів за напрямами досліджень комп'ютерної техніки та програмних продуктів, комунікаційних систем та засобів;

сприяти розвитку інноваційних методів та технологій цифрової криміналістики;

забезпечити підвищення рівня знань оперативних працівників, працівників органів досудового розслідування, прокуратури, суддів у сфері інформаційних технологій та кібербезпеки, насамперед за напрямами збирання та дослідження цифрових (електронних) доказів;

сприяти залученню приватних експертів до проведення комп'ютерно-технічних і телекомунікаційних досліджень та експертиз, досліджень програмного забезпечення, які необхідні для швидкого реагування на кіберінциденти та ефективного розслідування кіберзлочинів.

Держава запровадить асиметричні інструменти стримування *(ціль С.4), для цього буде*:

утворено постійно діючу робочу групу з питань кіберрозвідки, налагоджено її ефективну співпрацю з Розвідувальним та ситуативним центром ЄС (INTCEN) з метою просування стратегічної співпраці України у сфері розвідки щодо кіберзагроз та діяльності у сфері кібербезпеки;

удосконалено систему розвідувального забезпечення кібербезпеки держави в частині створення, розвитку сил, засобів та інструментів упередження загроз національній безпеці у кіберпросторі;

посилено заходи щодо забезпечення кібербезпеки інформаційної інфраструктури та кіберзахисту інформаційних ресурсів дипломатичних представництв, консульських установ та об'єктів державної власності України за кордоном;

створено технологічні можливості підключення постачальниками електронних комунікаційних мереж та/або послуг технічних засобів для здійснення оперативно-розшукових, контррозвідувальних та розвідувальних заходів;

запроваджено гармонізований з євроатлантичною спільнотою підхід до накладання санкцій у відповідь на підривну діяльність у кіберпросторі, розроблено та узгоджено з іноземними партнерами механізм спільних дипломатичних та економічних дій та заходів, зокрема запровадження обмежувальних заходів у вигляді економічних санкцій, у відповідь на деструктивну кіберактивність;

визначено чіткий порядок всебічної дипломатичної реакції із застосуванням доступних на міжнародному рівні інструментів задля протидії зловмисній діяльності у кіберпросторі проти України;

налагоджено систематичний обмін інформацією про деструктивну діяльність у кіберпросторі з міжнародними партнерами, насамперед країнами-членами ЄС та НАТО, створено платформи такого обміну;

врегульовано на законодавчому рівні питання щодо всебічного залучення приватного сектору та громадянського суспільства до здійснення заходів із стримування деструктивної діяльності в кіберпросторі;

розроблено дієві механізми залучення фахівців приватного сектору з кібербезпеки до участі у стримуванні та протидії агресії проти України в кіберпросторі.

Держава у співпраці із суб'єктами приватного сектору, академічною спільнотою та громадськістю забезпечить досягнення національної кіберготовності та кіберзахисту *(ціль К.1). Для цього необхідно:*

розробити Національний план реагування на надзвичайні (кризові) ситуації в кіберпросторі, який визначить механізми реагування, з подальшим відновленням, на масштабні кібератаки та кіберінциденти щодо об'єктів критичної інформаційної інфраструктури, у ньому визначити ролі і відповідальність усіх суб'єктів забезпечення кібербезпеки та об'єктів критичної інфраструктури під час надзвичайної ситуації, ключові процеси та заходи для подолання надзвичайної ситуації, критерії віднесення ситуації до надзвичайної, механізми інформування громадян, проведення навчань для перевірки стану готовності до надзвичайних ситуацій;

розробити базові вимоги та рекомендації з питань забезпечення кібербезпеки та кіберзахисту;

розгорнути систему обміну інформацією про кіберінциденти між усіма суб'єктами забезпечення кібербезпеки;

впровадити ризик-орієнтований підхід у частині заходів забезпечення кібербезпеки та кіберзахисту об'єктів критичної інфраструктури та державних органів, зокрема розробити методики ідентифікації та оцінки кіберризиків на національному рівні та для секторів критичної інфраструктури держави, врегулювати на законодавчому рівні обов'язковість здійснення періодичної оцінки ризиків на підставі розроблених методик;

впровадити систему сертифікації продукції, яка використовується для функціонування та кіберзахисту інформаційно-комунікаційних систем, насамперед об'єктів критичної інформаційної інфраструктури;

забезпечити розвиток організаційно-технічної моделі кіберзахисту, впровадити механізми своєчасної ідентифікації загроз, інструменти виявлення кібератак для оперативного реагування на них та швидкого відновлення стабільної роботи під час та після кібератак;

завершити процеси визначення об’єктів критичної інфраструктури та об’єктів критичної інформаційної інфраструктури, створити і забезпечити функціонування державного реєстру об’єктів критичної інформаційної інфраструктури, постійно переглядати та оновлювати вимоги до їх кіберзахисту з урахуванням сучасних міжнародних стандартів з питань кібербезпеки;

запровадити загальнонаціональну програму виявлення вразливостей інформаційно-комунікаційних систем, проводити на регулярній основі аудит захищеності комунікаційних і технологічних систем об’єктів критичної інфраструктури на вразливість;

запровадити постійну оцінку стану захищеності об'єктів критичної інформаційної інфраструктури та державних інформаційних ресурсів, встановити заохочення, обов'язковість та періодичність проведення такої оцінки з урахуванням категорій критичності об'єктів, передбачити можливість участі у цих заходах фахівців з кібербезпеки приватного сектору;

впровадити систему аудиту інформаційної безпеки, насамперед на об’єктах критичної інфраструктури, визначити механізми та базові методики проведення незалежних аудитів, встановити вимоги до аудиторів інформаційної безпеки, їх сертифікації, атестації (переатестації), навчання та підвищення кваліфікації, а також щодо обов’язковості та періодичності проведення аудитів, надання узагальненої інформації про результати аудитів до Національного координаційного центру кібербезпеки;

забезпечити розвиток систем технічного і криптографічного захисту інформації, пріоритетність використання засобів технічного і криптографічного захисту інформації вітчизняного виробництва для кіберзахисту державних інформаційних ресурсів та об’єктів критичної інформаційної інфраструктури;

популяризувати застосування вітчизняних засобів криптографічного захисту інформації в інтересах приватних компаній;

проводити щорічні командно-штабні кібернавчання стратегічного рівня за участю представників державного та приватного секторів;

забезпечити розвиток мережі галузевих (секторальних) центрів реагування

на кібератаки та кіберінциденти;

створити Національний центр резервування державних інформаційних ресурсів, провести модернізацію системи захищеного доступу державних органів до мережі Інтернет;

завершити розгортання Національної телекомунікаційної мережі, збільшити її пропускну здатність, передбачити під час її функціонування використання виключно вітчизняних засобів криптографічного захисту інформації.

В Україні буде проведено наукові дослідження у сфері кібербезпеки, реформовано систему підготовки та підвищення кваліфікації кадрів, а також розгорнуто навчальні програми, курси, тренінги з кібернавчання для всіх верств населення *(ціль К.2), для чого буде:*

забезпечено стимулювання досліджень і розробок у сфері кібербезпеки з урахуванням розвитку новітніх інформаційно-комунікаційних технологій, 5G, штучного інтелекту, Інтернету речей, технологій хмарних і квантових обчислень, а також появи нових засобів реалізації кіберзагроз з метою створення вітчизняних систем, платформ і продуктів у сфері кібербезпеки;

проведено аналіз та оцінено поточний стан підготовки фахівців у сфері кібербезпеки, розроблено на основі проведеного аналізу пропозиції щодо реформування системи підготовки та підвищення кваліфікації таких фахівців, схвалено відповідну концепцію;

розроблено Загальнонаціональну програму кібергігієни, спрямовану на підвищення рівня кіберграмотності населення України;

утворено центри, що будуть здійснювати узагальнення та обмін досвідом у сфері кібербезпеки, підтримку інновацій та вітчизняних розробок у цій сфері;

встановлено вимоги щодо необхідності підвищення кваліфікації співробітників суб'єктів сектору безпеки і оборони, об'єктів критичної інфраструктури та державних службовців з питань кібербезпеки та кіберзахисту із запровадженням коротко- та довгострокових курсів і програм з цих питань;

забезпечено періодичне проведення навчання, у тому числі за рахунок держави, та отримання принаймні одного сертифіката (а також нового кожні

три роки) з кібербезпеки для фахівців державних органів, що безпосередньо виконують функції із забезпечення кібербезпеки та кіберзахисту, а також співробітників освітніх закладів, що безпосередньо здійснюють підготовку фахівців з кібербезпеки;

створено механізми підготовки фахівців з кібербезпеки як на рівні вищої освіти, так і на рівнях середньої та професійно-технічної освіти;

забезпечено періодичне проведення з урахуванням відомчої специфіки атестації (переатестації) фахівців, що відповідають за забезпечення кібербезпеки та кіберзахисту державних органів та об'єктів критичної інфраструктури;

забезпечено матеріальне стимулювання фахівців у сфері кібербезпеки, які проходять військову, державну службу (у тому числі державну службу особливого характеру), службу в правоохоронних органах або працюють за трудовим договором у державному секторі і безпосередньо виконують функції із забезпечення кібербезпеки та кіберзахисту, з урахуванням рівнів оплати праці таких фахівців у приватному секторі;

започатковано проведення щорічних національних кіберзмагань для школярів старших класів навчання та студентів як інструменту відбору найкращих молодих фахівців у сфері кібербезпеки;

забезпечено включення кібербезпекової складової до програми підготовки шкільних вчителів у вищих навчальних закладах усіх рівнів акредитації при одночасному запровадженні підвищення кваліфікації діючого педагогічного складу з питань кібербезпеки;

включено питання кібергігієни, цифрових навичок, кіберобізнаності щодо сучасних кіберзагроз та протидії ним до програм середньої, професійно-технічної та вищої освіти;

забезпечено координацію наукового співтовариства під час проведення наукових розробок у сфері кібербезпеки та залучення його до заходів з реалізації державної політики у сфері кібербезпеки;

визначено довгострокові напрями проведення досліджень та розробок у сфері кібербезпеки, а також розроблено дієву програму державної підтримки (на основі проєктного підходу) стратегічно важливих для кібербезпеки

держави наукових установ і організацій, проведення наукових досліджень з питань кібербезпеки та кіберзахисту для потреб національної безпеки і оборони;

долучено основних суб'єктів національної системи кібербезпеки до програм навчання і підвищення кваліфікації персоналу, що проводяться за підтримки ЄС, зокрема Агентства ЄС з кібербезпеки (ENISA), поступово охоплюючи такими заходами інших суб'єктів забезпечення кібербезпеки.

Визнаючи безпечні цифрові послуги запорукою економічного розвитку, держава здійснюватиме такі заходи *(ціль К.3):*

зміцнюватиме довіру приватного сектору та окремих громадян до цифрових послуг, які надаються державою, безумовно виконуючи вимоги щодо забезпечення кібербезпеки та кіберзахисту під час їх надання та інформуючи громадськість про їх безпечність та надійність;

впроваджуватиме цифрові послуги для населення та розвиватиме національну інформаційну інфраструктуру, передбачаючи виділення коштів на заходи кібербезпеки та кіберзахисту в розмірі не менше ніж 5% від загальної вартості відповідного об'єкта інформаційної інфраструктури (інформаційно-комунікаційної системи);

розробить нові національні стандарти у сфері кібербезпеки, організаційні та технічні вимоги, що стосуються безпеки застосунків, мобільних пристроїв, робочих станцій, серверів і мереж, моделей хмарних обчислень, з урахуванням європейських та міжнародних стандартів;

створюватиме органи з оцінки відповідності надавачів електронних довірчих послуг вимогам для кваліфікованих надавачів кваліфікованих електронних довірчих послуг;

запровадить електронні довірчі послуги на основі кваліфікованого сертифіката автентифікації веб-сайту;

розбудовуватиме систему органів оцінки відповідності інформаційно-комунікаційних технологій, що використовуються для створення таких систем, вимогам з безпеки, управління інформаційною безпекою суб'єктами, що надають цифрові послуги;

створить необхідні передумови (нормативні, організаційні, технологічні)

для автентифікації користувачів сервісів цифрових послуг (там, де це потрібно) з використанням технологій електронної ідентифікації та/або електронних довірчих послуг;

підвищить ефективність системи захисту персональних даних громадян, визначивши базові вимоги до їх зберігання та обробки та посиливши відповідальність за порушення цих вимог, гармонізує вітчизняне законодавство з відповідним законодавством ЄС.

Національний координаційний центр кібербезпеки забезпечить скоординовану діяльність усіх стейкхолдерів у процесі розбудови та функціонування національної системи кібербезпеки *(ціль В.1) шляхом:*

розроблення та затвердження порядку проведення огляду стану національної системи кібербезпеки, забезпечивши його проведення не менше ніж раз на рік протягом реалізації Стратегії;

запровадження обов'язкового надання в режимі реального часу інформації про кібератаки та кіберінциденти всіма відомчими та галузевими (секторальними) центрами кібербезпеки або кіберзахисту до Національного координаційного центру кібербезпеки;

забезпечення розгляду найважливіших питань у сфері кібербезпеки України на засіданнях Національного координаційного центру кібербезпеки, рішення якого є обов'язковими для виконання всіма суб'єктами забезпечення кібербезпеки;

розширення мережі обміну інформацією про кібератаки, кіберінциденти та індикатори кіберзагроз на базі технологічної платформи Національного координаційного центру кібербезпеки, охопивши всі державні органи та об'єкти критичної інфраструктури, уніфікації форматів обміну інформацією;

запровадження за досвідом країн-членів ЄС скоординованого виявлення та розкриття вразливостей інформаційно-комунікаційних систем під егідою Національного координаційного центру кібербезпеки;

розроблення та запровадження механізмів заохочення приватного сектору, наукового співтовариства, громадських організацій та окремих громадян до участі у формуванні та реалізації заходів із забезпечення кібербезпеки держави;

забезпечення щорічного оприлюднення основними суб’єктами національної системи кібербезпеки публічних звітів про стан кібербезпеки за сферами відповідальності.

Держава у взаємодії з приватним сектором сформує ефективну модель відносин у сфері кібербезпеки, засновану на довірі *(ціль В.2), здійснюючи такі заходи:*

врегулює на законодавчому рівні питання державно-приватного партнерства у сфері кібербезпеки, визначивши форми і методи здійснення такого партнерства, зміцнивши взаємну довіру та передбачивши можливість запровадження експериментальних проєктів у цій сфері;

запровадить на регулярній основі проведення консультацій заінтересованих сторін та надання методичної допомоги з питань утворення підрозділів кіберзахисту, галузевих (секторальних) центрів забезпечення кібербезпеки та команд реагування на кіберінциденти, всебічно сприятиме їх розвитку;

залучатиме на регулярній основі представників наукових установ, громадських організацій та незалежних експертів у сфері кібербезпеки до розроблення нормативно-правових актів, нормативних документів та стандартів у цій сфері;

підвищить ефективність залучення громадськості до прийняття рішень у сфері кібербезпеки шляхом проведення відповідних опитувань (анкетувань) та розміщення їх результатів на інформаційних ресурсах Національного координаційного центру кібербезпеки та основних суб'єктів національної системи кібербезпеки;

стимулюватиме розроблення вітчизняних програмних продуктів, зокрема програмного забезпечення з відкритим кодом, що пріоритетно використовуватимуться для обробки та захисту державних інформаційних ресурсів, а також на об’єктах критичної інформаційної інфраструктури;

впровадить програму розвитку ринку товарів і послуг у сфері кібербезпеки, що включатиме стимулювання його розвитку та міжнародного визнання;

розробить систему оцінки новітніх технологій, що безпосередньо мають

вплив на кіберстійкість країни, створить інструменти (стандарти, протоколи, сертифікати тощо) з оцінки ефективності використання новітніх технологій з протидії кібератакам;

запровадить пілотні менторські програми підвищення кваліфікації фахівців державних органів, що безпосередньо виконують функції із забезпечення кібербезпеки та кіберзахисту, шляхом залучення сертифікованих за міжнародними стандартами фахівців приватного сектору;

продовжить практику щорічного проведення місяця кібербезпеки в Україні із залученням широкого кола профільних фахівців та експертів державних органів, академічних і освітніх установ, а також громадського та приватного секторів, закріпивши необхідність його проведення відповідним нормативно-правовим актом;

сприятиме, зокрема шляхом надання організаційно-технічної підтримки, функціонуванню у всіх регіонах України постійно діючих діалогових майданчиків (конференцій, семінарів, форумів тощо), діяльність яких спрямована на розбудову довіри між суб'єктами забезпечення кібербезпеки;

сприятиме впровадженню на підприємствах, в установах і організаціях незалежно від форми власності культури кібербезпеки, що полягає у постійному підвищенні кіберобізнаності їх керівників та працівників;

сприятиме взаємному визнанню результатів оцінки відповідності та сертифікації з кібербезпеки, здійснених відповідними органами як в Україні, так і за кордоном;

впровадить механізм оцінки втрат суб'єктів господарювання внаслідок кібератак для можливості їх відшкодування та як елемент подальшого впровадження системи кіберстрахування.

Україна розвиватиме міжнародне співробітництво у сфері кібербезпеки, спрямоване, передусім, на забезпечення незалежності і державного суверенітету, відновлення територіальної цілісності України *(ціль В.3). Для цього:*

забезпечимо участь України у роботі міжнародної платформи Програми дій із заохочення відповідальної поведінки держав у кіберпросторі Генеральної Асамблеї ООН та Групи урядових експертів ООН з питань інформаційної

безпеки (UNGGE);

забезпечимо участь України у доопрацюванні Другого додаткового протоколу до Будапештської конвенції Ради Європи про кіберзлочинність щодо вироблення заходів та гарантій для вдосконалення міжнародної співпраці між правоохоронними та судовими органами, а також між органами влади та постачальниками послуг в інших країнах;

розширимо шляхом діалогу з міжнародними партнерами доступ правоохоронних органів України до ресурсів Європейського центру боротьби з кіберзлочинністю (EC3), до телекомунікаційної системи Інтерполу I-24/7 (за технологією FIND);

продовжимо співробітництво з Агентством ЄС з кібербезпеки (ENISA), зокрема з питань скоординованого розкриття вразливостей та імплементації Директиви Європейського Парламенту і Ради Європи (ЄС) 2016/1148 від 6 липня 2016 року про заходи для високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу (NIS Директиви) як елементу євроінтеграції України;

поглибимо співпрацю з Міжнародним союзом електрозв'язку (ITU) у сферах кібербезпеки та електронних комунікацій, зокрема з питань стандартизації у цих сферах;

налагодимо співпрацю з Інтернет-корпорацією з присвоєння імен та номерів (ICANN) щодо вироблення державної політики у мережі Інтернет;

розширимо в межах Організації за демократію та економічний розвиток ГУАМ взаємодію з питань кібербезпеки;

вивчимо можливість приєднання України до стратегії ЄС з диверсифікації розпізнавання імен DNS, надання підтримки ініціативі «DNS4EU» з метою уникнення екстремальних сценаріїв реалізації кібератак на глобальну кореневу систему DNS, її ієрархічну та делеговану систему зон; забезпечимо імплементацію Україною Положення ЄС про обмеження строку дії IPv4 для управління ринком, що прискорить впровадження в Україні IPv6, а також інших усталених стандартів безпеки в Інтернеті, передових практик розпізнавання імен DNS, маршрутизації та безпеки електронної пошти;

розвиватимемо міжнародне співробітництво у сфері кібербезпеки шляхом

підтримки міжнародних ініціатив у сфері кібербезпеки, які відповідають національним інтересам України, поглиблюючи діалог України з Європейським Союзом, Організацією Північноатлантичного договору, Організацією з безпеки і співробітництва в Європі щодо зміцнення довіри при використанні кіберпростору, спільного розуміння ландшафту кіберзагроз та вдосконалення механізмів такої співпраці;

створимо постійно діючу робочу групу з питань взаємодії із провідними ІТ-компаніями, світовими провайдерами цифрових послуг, соціальними мережами з метою протидії гібридним загрозам, поширенню дезінформації, можливості застосування санкцій відповідно до законів України;

визначимо та затвердимо перелік пріоритетних напрямів залучення міжнародної технічної допомоги у сфері кібербезпеки України.

3.6 Напрями зовнішньополітичної діяльності України у сфері кібербезпеки.

Головним зовнішньополітичним пріоритетом України у сфері кібербезпеки є поглиблення євроінтеграційних процесів шляхом уніфікації підходів, методів і засобів забезпечення кібербезпеки з усталеними практиками ЄС і НАТО, вжиття інших узгоджених із ключовими іноземними партнерами заходів, спрямованих на посилення кіберстійкості України, розвиток спроможностей національної системи кібербезпеки та захист національних інтересів у кіберпросторі.

Україна приділятиме особливу увагу спільній з партнерами протидії міжнародному тероризму, виявленню, попередженню і припиненню злочинів проти миру і безпеки людства, іншим протиправним діям, що порушують міжнародний правопорядок та інтереси демократичної світової спільноти, розвиватиме на договірній основі з партнерськими спецслужбами країн- членів ЄС і НАТО взаємовигідний обмін інформацією та досвідом щодо забезпечення національної безпеки у кіберпросторі, використовуватиме кращі світові практики, активно здійснюватиме інші спільні заходи, що сприятимуть зміцненню наукової, матеріально-технічної бази та кадрового потенціалу у сфері кібербезпеки.

Україна співпрацюватиме з міжнародними партнерами, організаціями та іншими заінтересованими сторонами, які поділяють наше спільне бачення майбутнього кіберпростору як глобального, відкритого, вільного, стабільного та безпечного, в основі якого дотримання прав людини, основних свобод та демократичних цінностей, що є запорукою соціально-економічного та політичного розвитку України.

Україна продовжить активну участь у міжнародному діалозі з питань відповідальної поведінки держав у кіберпросторі на основі дотримання принципів міжнародного права, Статуту ООН, а також добровільних необов'язкових норм, правил та принципів відповідальної поведінки держави. Це потребуватиме більшої координації та консолідації заінтересованих сторін на міжнародних форумах, в яких Україна буде не лише учасником, але й ініціатором та організатором.

Виходячи з того, що Інтернет давно став суспільним надбанням, істотно вийшов за межі суто національних інтересів, держава максимально підтримуватиме мультистейкходерську (багатосторонню) модель управління Інтернетом, сприяючи міжнародним, регіональним та національним дискусіям з цього питання, сприяючи залученню до цього процесу приватного сектору, наукових та освітніх кіл, громадянського суспільства. Спроби окремих авторитарних держав суверенізувати Інтернет суперечать довгостроковим інтересам України та її моделі соціально-економічного розвитку.

Україна буде сприяти подальшому дотриманню міжнародного права та стандартів у галузі прав людини, заохочуватиме застосування найкращих практик, а також активізує свої зусилля щодо запобігання зловживанню новими технологіями. Для цього держава активізує свою участь і партнерство в міжнародних процесах стандартизації та сертифікації у сфері кібербезпеки, розширить представництво в міжнародних, регіональних та інших органах стандартизації, організаціях, що займаються розробленням стандартів та сертифікацією у цій сфері.

У питаннях розроблення стандартів у сферах нових технологій (зокрема щодо штучного інтелекту, хмарних технологій, квантових обчислень та квантових комунікацій) та базової архітектури Інтернету Україна виходить з

того, що Інтернет має залишатися глобальним та відкритим, технології повинні орієнтуватися на людину, забезпечувати її базові свободи, гарантувати невтручання у її особисте життя, забезпечувати її конфіденційність у кіберпросторі, а будь-які обмеження в цій частині повинні здійснюватися лише відповідно до закону. Використання технологій має бути законним, безпечним та етичним. Водночас у зв'язку з ускладненням міжнародної безпеки в кіберпросторі Україна займатиме більш активну позицію в дискусіях ООН та інших міжнародних форумах для просування, координації та консолідації її позиції у сфері кібербезпеки, зменшуючи небезпеки мілітаризації кіберпростору.

Ураховуючи взаємопов'язаність сучасного віртуального простору та з метою розвитку співпраці між державою, приватним сектором економіки, науковими і освітніми колами та громадянським суспільством у сфері кібербезпеки, Україна розвиватиме національний кіберпростір як глобальний, відкритий, вільний, стабільний і, насамперед, безпечний, що є запорукою успішного розвитку країни.

Протягом реалізації Стратегії Україна зробить кібербезпеку одним з основних питань своєї міжнародної діяльності, посилюючи для цього потенціал своїх зовнішньополітичних структур та кіберпотенціал держави. З цією метою Україна розвиватиме мережу партнерства у сфері кібербезпеки, розбудовуючи наявні та створюючи нові формати і механізми міжнародного співробітництва.

3.7 Механізми реалізації стратегії та забезпечення відкритості.

Стратегія діє на період 2021 – 2025 років. Координатором реалізації Стратегії є робочий орган Ради національної безпеки і оборони України – Національний координаційний центр кібербезпеки.

Основним критерієм результативності Стратегії є досягнення мети та стратегічних цілей шляхом виконання визначених стратегічних завдань.

Національний координаційний центр кібербезпеки у визначених законодавством формах забезпечує (на весь період дії Стратегії) планування заходів з реалізації Стратегії, координує їх проведення і контролює стан виконання та ефективність.

Загальний план, розроблений Національним координаційним центром кібербезпеки та схвалений Радою національної безпеки і оборони України, є основою для формування Кабінетом Міністрів України щорічних планів заходів з реалізації Стратегії, а також для здійснення дієвого контролю за виконанням запланованих завдань і відповідних заходів.

Ефективність реалізації Стратегії визначається у проведених у встановленому порядку оглядах стану:

національної системи кібербезпеки;

кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом.

Результати оглядів можуть стати підставою для внесення змін до загального плану та/або щорічних планів заходів з реалізації Стратегії, що обумовлено необхідністю адаптації до змін у безпековому середовищі, усунення та мінімізації негативних тенденцій у сфері кібербезпеки.

Стратегія є основою для розроблення інших нормативно-правових актів у сфері кібербезпеки України, а також для обґрунтування розподілу необхідних матеріальних, кадрових та інших ресурсів.

Фінансування заходів з реалізації Стратегії здійснюватиметься в межах видатків, передбачених Державним бюджетом України для сектору безпеки і оборони, які розглядатимуться Радою національної безпеки і оборони України в порядку, визначеному Бюджетним кодексом України. Відповідно до законодавства державні органи, підприємства, установи та організації передбачатимуть у своїх планах фінансові витрати на кібербезпеку. У рамках державно-приватного партнерства, міжнародної технічної допомоги залучатимуться інвестиції, які спрямовуватимуться на розбудову національної

системи кібербезпеки.

Щороку Національний координаційний центр кібербезпеки оприлюднює публічний звіт про стан реалізації Стратегії за загальними оцінками.

Процес реалізації Стратегії має бути максимально прозорим, відкритим та супроводжуватися демократичним цивільним контролем. З цією метою основними суб'єктами національної системи кібербезпеки в межах компетенції додатково буде здійснюватися щорічне інформування громадськості через власні офіційні сайти про стан реалізації ними Стратегії та стан фінансування відповідних заходів.

Висновки до третього розділу.

В умовах інформаційної війни проти України з боку Російської Федерації кібербезпека України має базуватись на основних засадах забезпечення Національної безпеки України: стримування, стійкості та взаємодії, передбачати проведення заходів активного впливу на кіберпростір разом з традиційним захистом інформаційних ресурсів та, відповідно до міжнародного законодавства, бути чіткою, зрозумілою і прозорою.

В третьому розділі роботи наведені пропозиції щодо визначення пріоритетів, стратегічних цілей і завдань, в розробці яких я приймав безпосередню участь і які стали основою чинної Стратегії кібербезпеки України. Досягнення всіх визначених цілей дозволить гарантувати кібербезпеку України в сучасних умовах.

ВИСНОВКИ

В магістерській роботі було досягнуто визначеної мети – на основі аналізу змісту кіберскладової інформаційної війни Російської Федерації проти України обґрунтувати доцільні напрями забезпечення кібербезпеки України.

1. Під час дослідження особливостей гібридної війни Російської Федерації проти України, розв'язаної у 2014 році, були визначені всі різні складові російської агресії і в кожній з них визначені питання, які безпосередньо стосуються забезпечення кібербезпеки.

2. При проведенні аналізу змісту заходів інформаційної війни проти України у кіберпросторі розглядались кібероперації та кібератаки, спрямовані на різні об'єкти та сфери суспільного життя України, а також ті заходи, які Україна проводила у відповідь. Це дало змогу визначити спектр завдань забезпечення кібербезпеки України.

3. Практичні заходи, які проводились для зриву кібероперацій Російської Федерації проти України та відбиття кібератак на різні об'єкти разом з визначеними засадами забезпечення Національної безпеки України дозволили обґрунтувати пріоритетні напрями забезпечення кібербезпеки України, визначити відповідні стратегічні цілі та завдання.

Результати роботи можуть використовуватися для подальшої роботи щодо формування Дорожньої карти реалізації Стратегії кібербезпеки України а також, для визначення, планування, організації та проведення практичних заходів. Крім того, на мій погляд, отримані результати доцільно використовувати в навчальному процесі підготовки фахівців за спеціальністю «Кібербезпека».

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Аналітичний огляд проблем інформаційного й електронного права в Україні Електронний ресурс // Сайт “AMB” group. – Режим доступу: http://www.itsway.kiev.ua/index.php?language=ru&main_managemen=about&mana gemen=eGov_Zak.

2. Бєлай С. В. Державні механізми протидії кризовим явищам соціально-економічного характеру: теорія, методологія, практика : монографія / С. В. Бєлай. – Х. : Національна акад. НГУ, 2015. – 349 с.

3. Брижко В. М. Інформаційне суспільство. Дефініції / В. М. Брижко, О. М. Гальченко, В. С. Цимбалюк, О. А. Орєхов, А. М. Чорнобров. – К., 2002. – 220 с.

4. Васильєва О. І. Трансформація регіонального управління в умовах реформування владних відносин в Україні : автореф. дис. ... д-ра наук з держ. упр. : 25.00.02 / О. І. Васильєва ; НАН України, Рада по вивч. продуктив. сил України. – К., 2010. – 38 с.

5. Вербицький О. В. Поняття соціальної напруженості та роль держави в управлінні нею й інформаційною безпекою / О. В. Вербицький // Проблеми управління соціальним і гуманітарним розвитком : матеріали наук.-прак. конф. (01.12.2017 р.). – Дніпро, 2017. – С. 47–49.

6. Глобалізація і безпека розвитку : монографія / О. Г. Білорус, Д. Г. Лук’яненко та ін. ; кер. авт. колективу і наук. ред. О. Г. Білорус. – К. : КНЕУ, 2001. – 733 с.

7. Дзюндзюк В. Б. Ефективність діяльності публічних організацій /В. Б. Дзюндзюк ; Укр. акад. держ. упр-ня при Президентові України, Харк. регіон. ін-т. – Х. : Вид-во ХарРІ УАДУ «Магістр», 2003. – 236 с.

8. Древаль Ю. Д. Безпека особистості як фактор сучасних державно-управлінських відносин [Елеткронний ресурс] / Ю. Д. Древаль // Наукові записки Інституту законодавства Верховної Ради України. – С. 123–127. – Режим доступу: http://instzak.rada.gov.ua/instzak/doccatalog/document?id=72940.

9. Домбровська С. М. Механізми інформаційної безпеки як складові державної безпеки України / С. М. Домбровська // Державне управління науково-освітнього забезпечення підготовки конкурентоспроможних фахівців у сфері цивільного

захисту : матеріали Всеукраїнської наук.-практ. конф. / за заг. ред. В. П. Садкового. – Х., 2015. – С. 282–286.

10. Енциклопедія державного управління: у 8 т. / Нац. акад. держ. упр. при Президентові України ; наук.-ред. колегія : Ю. В. Ковбасюк (голова) та ін. – К. : НАДУ, 2011. Т. 1 : Теорія державного управління / наук.-ред. колегія : В. М. Князєв (співголова), І. В. Розпутенко (співголова) та ін. – 2011. – 748 с.

11. Енциклопедія державного управління: у 8 т. / Нац. акад. держ. упр. при Президентові України ; наук.-ред. колегія : Ю. В. Ковбасюк (голова) та ін. – К. : НАДУ, 2011. Т. 2 : Методологія державного управління / наук.-ред. колегія : Ю. П. Сурмін, П. І. Надолишній та ін. – 2011. – 692 с.

12. Іщенко В. М. Міжнародний досвід упровадження електронного урядування [Електронний ресурс] / В. М. Іщенко // Держава та регіони, 2012. – № 4. – Режим доступу: http://pa.stateandregions.zp.ua/archive/4_2012/5.pdf.

13. Карпенко О. В. Механізми формування та реалізації сервісно-орієнтованої державної політики в Україні : автореф. дис. ... д-ра наук з держ. упр. : 25.00.02 / О. В. Карпенко ; Нац. акад. держ. упр-ня при Президентові України. – К., 2016. – 39 с.

14. Колот А. Соціальна згуртованість як доктрина забезпечення стійкості розвитку суспільства в умовах глобальних викликів / А. Колот // Україна: аспекти праці, 2009. – № 7. – С. 11–19.

15. Корженко В. В. Теоретико-методологічні засади державного управління: формування понятійного апарату: метод. рек. / авт. кол. В. В. Корженко, В. В. Говоруха, О. Ю. Амосов та ін. – К. : НАДУ, 2009.

16. Кузнецов А. О. Інноваційні технології в державному регулюванні соціально-економічного розвитку регіону : автореф. дис... канд. наук з держ. упр.: 25.00.02 / А. О. Кузнецов ; Нац. акад. держ. упр. при Президентові України, Харк. регіон. ін-т держ. упр. – Х., 2006. – 20 с.

17. Лелеченко А. П. Децентралізація системи державного управління в Україні: теоретико-методологічний аналіз : автореф. дис... канд. наук з держ. упр. :

25.00.01 / А. П. Лелеченко ; Нац. акад. держ. упр. при Президентові України. – К., 2006. – 20 с.

18. Матвієнко А. С. Політико-правові засади децентралізації влади в контексті адміністративної реформи в Україні : автореф. дис... канд. політ. наук : 23.00.02 / А. С. Матвієнко ; Ін-т держави і права ім. В.М. Корецького НАН України. – К., 2010. – 20 с.

19. Михайлов А. О. Оптимізація причинно-наслідкового зв'язку функцій держави та механізмів державного управління в Україні : автореферат дис. ... канд. наук з держ. упр. : 25.00.02 / А. О. Михайлов ; Акад. муніц. управління. – К., 2015. – 20 с.

20. Никитин В. А. Проблемы становления публичной политики в Украине / В. А. Никитин // Публичная полтика – 2006 : сб. ст. / под ред. А. Ю. Сунгурова. – СПб. : Норма, 2006. – 32 с.

21. Опанасенко Я. О. Електронне врядування як складова державного управління соціально-економічним розвитком регіонів / А. Л. Помаза-Пономаренко, Я. О. Опанасенко // Діяльність органів публічної влади щодо забезпечення стабільності та безпеки суспільства : матеріали Міжнарод. наук.-практ. конф., м. Суми, 22 березня 2016 р. – Суми : Сумський державний ун-тет. – С. 360–363.

22. Опанасенко Я. О. Роль і місце організаційної, соціальної й інформаційної складових у реалізації державної регіональної політики в умовах невизначеності регіонів / А. Л. Помаза-Пономаренко, Р. Т. Лукиша, Я. О. Опанасенко // Вісник Національного університету цивільного захисту України (Серія: Державне управління), 2016. – № 1 (4). – С. 203–209.

23. Офіційний веб-сайт Міністерства інформаційної політики України [Електронний ресурс]. – Режим доступу: http://mip.gov.ua/ru/.

24. Почепцов Г. Інформаційна політика : навч. посіб. / Г. Почепцов, С. Чукут. – К. : Вид-во УАДУ, 2002. – 88 с.

25. Про місцеві державні адміністрації [Електронний ресурс] : Закон України від 1990 р. (у редакції від 16.04.2017 р.). – Режим доступу: http://zakon3.rada.gov.ua/laws/show/586-14.

26. Бондаренко В. О. Інформаційна безпека сучасної держави: концептуальні роздуми [Електронний ресурс] / В. О. Бондаренко, О. В. Литвиненко. – Режим доступу: http://www.crime-research.iatp.org.ua/library/strateg.htm

27. Горбань Ю. О. Інформаційна війна проти України та засоби її ведення [Електронний ресурс] / Ю. О. Горбань. –Режим доступу: http://www.visnyk.academy. gov.ua/wp-content/uploads/2015/04/20.pdf

28. Гусаров В. Кремль розпочав нову інформаційну операцію проти України [Електронний ресурс] / В. Гусаров. – Режим доступу: http://www.osvita. mediasapiens.ua/material/34281

29. Доктрина інформаційної безпеки України [Електронний ресурс]. –Режим доступу: http://www.zakon3.rada.gov.ua/laws/show/514/2009

30. Захист інформаційної безпеки як функція держави [Електронний ресурс]. – Режим доступу: http://www.mego.info/матеріал/23-захист-інформаційної-безпеки-як-функція-держави

31. Інформаційна безпека держави у контексті протидії інформаційним війнам: Навчальний посібник / за заг. ред. В. Б. Толубка. – К. : НАОУ, 2004. – 315 с.

32. Концепція національної безпеки України [Електронний ресурс]. – Режим доступу: http://www.w1 . c1.rada.gov.ua/pls/zweb2/webproc4_1

33. Ліпкан В. А. Інформаційна безпека України в умовах євроінтеграції [Текст] : навч. посіб. / В. А. Ліпкан, Ю. Є. Макименко, В. М. Желіховський. – К. : КНТ, 2006.

34. Марутян Р. Р. Рекомендації щодо вдосконалення політики забезпечення інформаційної безпеки України [Електронний ресурс] / Р. Р. Марутян. – Режим доступу: http://www.dsaua.org/index. php?option=com_content&view=article&id=198%3A2014-08

35. • Літнарович Р. М. Сучасні технології інформаційної безпеки – Навчальний посібник – Рівне 2011.

36. Газета “Вести” 16.09.2015. ст. 9, стаття Владислава Бовсуновського.

37.Информационная безопасность (2-я книга социально-политического проекта «Актуальные проблемы безопасности социума»). М.: «Оружие и технологии», 2009 (рос.).

38.Anticyber.ua/fraud.php?id=12 (Правила безпеки при роботі з банкоматом).

39.WebHelper.info/publ/internet/3 (Вредоносное программное обеспечение: разновидности, симптомы заражения, способы защиты).

40. Богуш В. М., Кривуца В. Г., Кудін А. М., «Інформаційна безпека: Термінологічний навчальний довідник» За ред. Кривуци В. Г. — Київ. 2004. — 508 с.

41. Дорошев В. В., Домарев В. В. Рекомендации по обеспечению безопасности конфиденциальной информации согласно “Критериев оценки надежных компьютерных систем TCSEC (Trusted Computer Systems Evaluation Criteria)”, США, “Оранжевая книга”. – Бизнес и безопасность, 1998, № 1.

42. Степанов И. Шпиономания или обыкновенный промышленный шпионаж? – Бизнес и безопасность, 1997, № 5.

43. Брягин О. Простая арифметика. – Бизнес и безопасность, 1998, № 1,с.

44. Закон України “Про інформацію” // Відом. Верховної Ради УРСР. – 1992. - № 48.

45. Низенко Е., Камняк В. Забезпечення інформаційної безпеки підприємництва. – К.: МАУП, 2006.

46. Кормич Б. Інформаційна безпека: організаційно-правові основи. – К.: Кондор, 2004.

47. Зубок М. Правове регулювання безпеки підприємницької діяльності. – К.: КНТЕУ, 2005.

48. Зубок М. Безпека банківської діяльності. – К.: КНЕУ, 2002.

49. Зубок М. Інформаційна безпека. – К.: КНТЕУ, 2005.

50. Берлач А. Безпека бізнесу. – К.: Університет «Україна», 2007.

51. Електронна комерція: Навч. посібник / А.М. Береза, І.А. Козак, Ф.А. Шевченко та ін. – К.: КНЕУ, 2002. – 326 с.

52. Голдовский И. Безопасность платежей в Интернете. – СПб.: Питер, 2001. – 240 с.

53. Закон України "Про електронні документи та електронний документообіг" від 22 травня 2003 р. №851-IV.

54. Быков ВЛ. Электронный бизнес и безопасность. – М.: Радио и связь, 2000.

55. Вербицкий О.В. Вступление к криптологии. - Львов: Издательство научно-технической литературы, 1998.

56. Яскевич В. Секьюрити. Организационные основы безопасности фирмы. – М.: Ось-89, 2005.

57. Степанов Е., Корнеев И. Информационная безопасность и защита информации. – М. Инфра – М, 2001.

58. Поздняков Е. Защита объектов. – М.: БДЦ, 1997.

59. Кузнецов И. Бизнес-безопасность. – М.: ИД «Дашков и К», 2006.

60. Кожем'яко Володимр Прокопович, Тимченко Леонід Іванович, Яровий Андрій Анатолійович Паралельно-ієрархічні мережі як структурно-функціональний базис для побудови спеціалізованих моделей образного комп'ютера. – Вінниця: Універсум, 2005. – 162 с.

61. Глазунова, Олена Святославівна Методи управління стратегією дилерської мережі транснаціональної корпорації: Автореф. дис. канд. економ. наук: Спец. 08.02.03 / За заг. ред. М. Гормана і П. Вінклера. – Донецьк, 2004. – 16 с. – 44.82.

62. Зайченко Ю.П. Комп'ютерні мережі: Навчальний посібник. – К.: Слово, 2003. – 286 с. – 20.00.