ХМЕЛЬНИЦЬКА ОБЛАСНА РАДА

ХМЕЛЬНИЦЬКИЙ УНІВЕРСИТЕТ УПРАВЛІННЯ ТА ПРАВА
ІМЕНІ ЛЕОНІДА ЮЗЬКОВА
ФАКУЛЬТЕТ УПРАВЛІННЯ ТА ЕКОНОМІКИ

Кафедра: публічного управління та адміністрування

МАГІСТЕРСЬКА РОБОТА

на тему: «Удосконалення заходів захисту державних інформаційних ресурсів у сфері кібербезпеки»

Виконав: студент магістратури за спеціальністю 281 Публічне управління та адміністрування заочної форми навчанням Витвицький В.Б.

Керівник: Требик Л.П., доцент кафедри публічного управління та адміністрування, кандидат наук з державного управління

Рецензент: _____

Хмельницький – 2020 рік

АНОТАЦІЯ

Витвицький В.Б. Удосконалення заходів захисту державних інформаційних ресурсів у сфері кібербезпеки. – Рукопис.

У магістерській роботі обґрунтовано суть понять "інформаційна безпека", яке набагато ширше за поняття безпеки інформації і аж ніяк не зводиться до нього. Наразі тема щодо безпеки у кіберпросторі є найпоширенішою і найбільш затребуваною суспільством, оскільки це стосується кожного, хто стикається зі світом інформаційних технологій.

Визначено, що законодавче регулювання кібербезпеки в Україні знаходиться на початку свого створення, але найскладніший етап - визначення стратегії, меж і напрямів державної політики кібербезпеки пройдено. Ще є багато проблем, але є і досягнення. Невирішені питання державно-приватного співробітництва, ще не сформульовані списки об’єктів критичної інфраструктури та інші, розробка підходів до кіберзахисту, попереду великий пласт проблем і обсяг роботи спрямованої на нормативно-правове врегулювання в сфері кібербезпеки.

Охарактеризовано діяльності суб’єктів національної системи кібербезпеки і вияснено, що переваги сучасного цифрового світу і розвиток інформаційних технологій привели до появи нових загроз національній і міжнародній безпеці.

Запропоновано ряд рекомендацій щодо додаткових заходів по забезпеченню кіберзахисту інформаційних і телекомунікаційних систем підприємств, установ, організацій і т. д. Розробка і прийняття нормативних актів в області захисту інформації спрямоване на регулювання безпечного використання інформаційних та комунікаційних технологій, доступу до інформації, захисту інформації від несанкціонованого доступу і передачі по технічних каналах.

Ключові слова: інформаційні ресурси, кібербезпека, кіберзахист, ДС спеціального зв'язку та захисту інформації.

Summary

Vytvytsky V.B. Improving measures to protect state information resources in the field of cybersecurity. - Manuscript.

The master's thesis substantiates the essence of the concepts of "information security", which is much broader than the concept of information security and is not reduced to it. Currently, the topic of security in cyberspace is the most common and most in demand in society, as it applies to anyone who encounters the world of information technology.

It is determined that the legislative regulation of cybersecurity in Ukraine is at the beginning of its creation, but the most difficult stage - defining the strategy, boundaries and directions of state cybersecurity policy has been passed. There are still many problems, but there are also achievements. Unresolved issues of public-private cooperation, not yet formulated lists of critical infrastructure and others, the development of approaches to cybersecurity, a large layer of problems ahead and the amount of work aimed at regulatory regulation in the field of cybersecurity.

The activities of the subjects of the national cybersecurity system are described and it is clarified that the advantages of the modern digital world and the development of information technologies have led to the emergence of new threats to national and international security.

A number of recommendations for additional measures to ensure cybersecurity of information and telecommunications systems of enterprises, institutions, organizations, etc. Development and adoption of regulations in the field of information protection aimed at regulating the safe use of information and communication technologies, access to information, protection of information from unauthorized access and transmission through technical channels.

Key words: information resources, cybersecurity, cyber protection, DS of special communication and information protection.

ЗМІСТ

ВСТУП

Актуальність теми дослідження. Активний розвиток електронного урядування в Україні, реформа системи державного управління, впровадження цифрових сервісів та інструментів у кожну суспільну сферу ставить у важливість ґрунтовно визначити організаційні засади проведення огляду стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації.

Питання інформаційної безпеки України, її стану і перспектив розвитку, методологічне та теоретичне підґрунтя досліджуваної проблеми висвітлювалося в наукових працях таких вітчизняних і зарубіжних авторів, як: І. Арістова [2], В. Бебик [5], В. Петрик [32], О. Юдін [61-65], С. Бучик [62-63], І. Спасибо [55], Я. Малик [27].

Мета і завдання дослідження. Метою дослідження є обґрунтування теоретичних положень, аналіз стану та розроблення практичних рекомендацій щодо удосконалення заходів захисту державних інформаційних ресурсів у сфері кібербезпеки.

Відповідно до поставленої мети було сформульовано такі завдання:

– розкрити основні поняття та особливості кібербезпеки та інформаційної безпеки;

– дослідити нормативно-правове забезпечення та принципи кібербезпеки в Україні;

– зробити характеристику діяльності суб’єктів національної системи кібербезпеки;

– проаналізувати сучасний стан кіберзлочинів в Україні за 2017-2020 роки;

– провести методику експертного оцінювання функціональних профілів загроз державних інформаційних ресурсів;

– надати рекомендації щодо підвищення рівня захищеності інформаційних ресурсів при віддаленій роботі співробітників установи.

Об’єктом дослідження є суспільні відносини у сфері кібербезпеки.

Предметом дослідження є удосконалення заходів захисту державних

інформаційних ресурсів у сфері кібербезпеки.

Методи дослідження. У процесі написання магістерської роботи була використана велика кількість методів, таких як: історичний у дослідженні концептуальних засад захисту державних інформаційних ресурсів у сфері кібербезпеки; аналіз та порівняння даних щодо діяльності досліджуваної тематики; системний підхід був використаний у формулюванні напрямів удосконалення заходів захисту державних інформаційних ресурсів у сфері кібербезпеки.

Структура роботи. Відповідно до мети та завдань дослідження робота складається зі вступу, 3 розділів, 6 підрозділів, висновків, списку використаних джерел із 68 найменувань. Загальний обсяг роботи складає 63 сторінки.

РОЗДІЛ 1
ТЕОРЕТИЧНІ АСПЕКТИ ЗАХИСТУ ДЕРЖАВНИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ У СФЕРІ КІБЕРБЕЗПЕКИ

1.1. Поняття та особливості кібербезпеки та інформаційної безпеки

Поки що в публікаціях ми можемо знайти різні поняття, які використовуються як взаємозамінні, зокрема "інформаційна безпека", "безпека інформації" та "кібербезпека". Автори, які замінюють ці поняття одне одним, вводять суспільство в оману.

Поняття "інформаційна безпека" визначено в пункті 3.28 ISO/IEC 27000(informationsecurity) «Безпека інформації» - підтримка конфіденційності (3.10), цілісності (3.36) та доступності (3.7) інформації. Згідно з Приміткою [1], інші характеристики, такі як достовірність (3.6), підзвітність, неприйняття (3.48) та надійність (3.55), слід враховувати для кваліфікації інформаційної безпеки [39]. У національному вимірі концепція інформаційної безпеки передбачає захист інформації від несанкціонованих дій (випадково чи навмисно), що призводять до модифікації, розкриття чи знищення даних [52].

Вперше поняття "Інформаційна безпека" в Україні було визначено в українському Законі "Про основні принципи розвитку інформаційного суспільства в Україні на 2007-2015 роки" від 01.09.2007 р. № 537-V [11], в якому інформаційна безпека як держава визначається як захист життєво важливих інтересів людини, суспільства та держави, в якій нанесення шкоди запобігає через:

• неповна, застаріла та недостовірна інформація;

• негативний вплив на інформацію; негативні наслідки використання інформаційних технологій;

• несанкціоноване розповсюдження, використання та порушення цілісності, конфіденційності та доступності інформації.

Відповідно до Закону України "Про основні принципи розвитку інформаційного суспільства в Україні на 2007-2015 роки"[51], вирішення проблеми інформаційної безпеки має здійснюватися на основі завдань:

• створити повністю функціональну державну інформаційну інфраструктуру та забезпечити захист її важливих елементів;

• вдосконалити координацію діяльності державних органів щодо виявлення, оцінки та прогнозування загроз інформаційній безпеці, запобігання таким загрозам та забезпечення усунення їх наслідків та здійснення міжнародного співробітництва з цих питань;

• вдосконалення законодавчої бази для забезпечення інформаційної безпеки, включаючи захист інформаційних ресурсів, боротьбу з комп'ютерною злочинністю, захист персональних даних та правоохоронну діяльність;

• забезпечення та розвиток Національної системи конфіденційного зв'язку як сучасної безпечної транспортної бази, яка може інтегрувати географічно розподілені інформаційні системи, в яких обробляється конфіденційна інформація [11].

Як бачимо, поняття "інформаційна безпека" набагато ширше поняття безпеки інформації і аж ніяк не зводиться до нього.

Стандарт ISO/IEC 27032 визначає "кібербезпеку" з точки зору безпеки кіберпростору - зберігаючи конфіденційність, цілісність та доступність інформації в кіберпросторі. У той же час кіберпростір - це середовище, яке є результатом функціонування на основі єдиних принципів та згідно із загальними правилами щодо інформації, телекомунікацій та інформаційно-комунікаційних систем [31]. Відповідно до ДСТ України ISO/IEC 27032: 2016 п. 4.21 Кіберпростір - це складне середовище, яке виникає в процесі взаємодії людей, програмного забезпечення та послуг в Інтернеті за допомогою технологічних пристроїв або взаємопов'язаних мереж і не існує в жодній фізичній формі [6].

Вивчення цієї проблеми можна розпочати з термінології, визначеної у міжнародному стандарті ISO/IEC 27032: 2012. Серед вчених варто виділити роботи: Алпеєва А.С., Архипова О.Є., Чепуренко Я.А., Мохор В.В. Богданова А.Н., Грибуніна В.Г., Горбатко А.В. Напрямки розвитку кібербезпеки запропонували В. Лебедєв, Д. Огородников, М. Олейник, Д. Прозоров, А.

Свіщев, Є.В. Брежнєв, А.А. Коваленко, А.А. Ілляшенко. Робота С.П. Євсєєва присвячена аналізу оцінки ризиків кібербезпеки в банківському секторі.

В ЗУ «Про основні засади забезпечення кібербезпеки України» [51] наведені терміни, що вживаються в такому значенні (Додаток А).

Зараз тема безпеки у віртуальному просторі є найпоширенішою та найпопулярнішою темою в суспільстві, оскільки вона стосується кожного, хто стикається зі світом інформаційних технологій.

З огляду на такі ризики, кожній державі представляється необхідним виробити власний підхід до гарантування кібербезпеки. Тому розвиток нового виду протистояння, такого як інформаційна війна та перехід технічної гонки озброєнь до кіберпростору, також визначає актуальність дослідження відносин між державами у галузі кібербезпеки.

За словами експертів з питань кібербезпеки збройних сил США, станом на 2008 рік, технічно повністю адекватна система кіберзахисту була розроблена для побудови та використання таких базових підсистем:

• захисні підсистеми (Protection Capabilities), що гарантують конфіденційність випромінювання від радіоелектронних засобів, систем та зв'язку, комп'ютерної безпеки (Computer Security) та інформаційної безпеки (InfoSec).

• підсистеми виявлення (Detection Capabilities), що забезпечують виявлення аномалій у мережі завдяки використанню їх систем;

• підсистеми реагування на зміни технічних параметрів та умов (Reaction Capabilities), що дозволяють відновлення (включаючи реконфігурацію) та виконання інших процесівоперацій з інформацією [3].

На думку деяких авторів, система кібербезпеки, створена відповідно до вищезазначених вимог, не в повному обсязі гарантує кібербезпеку IT-об'єкта і, перш за все, держави та оборонних відомств. Кібербезпека цих організацій повинна здійснюватися єдиною інтелектуальною системою кібербезпеки, яка є частиною системи інформаційної безпеки. У той же час концепція розвитку систем повинна бути основою для побудови перспективної системи кібербезпеки, тобто можливості її адаптації шляхом зміни параметрів під

впливом зовнішніх та внутрішніх кіберзагроз (кібератак) та технологій, за допомогою яких з ними борються протягом їх життєвого циклу [54, С. 5 - 7].

Звичайно, створення такої системи можливе лише за умови поєднання всього спектру державних регуляторних заходів від правового регулювання до ефективного та відповідального правозастосування на основі управління ризиками.У сучасних умовах структура американського кіберкомандування налічує понад 50 000 осіб і є складною багаторівневою структурою, яка поєднує зусилля Міністерства оборони США, АНБ та американського кіберкомандування та включає 133 бойові групи з понад 6 200 чоловік.

Каталізатором законодавчих змін у галузі кібербезпеки в нашій державі стала гібридна війна, яку Російська Федерація розпочала як з класичною, так і з нелетальною зброєю, також у кіберпросторі та через кіберпростір. Завдяки методам інформаційної війни лише за кілька днів Україна втратила 27 000 км² лише в Криму, частину населення, яка перевищує 2 500 000 осіб [51], 21.-25 травня у 2014 році під час президентських виборів відбулися DDoS-атаки та хаккерські атаки на веб-сайті ЦВК, що дало неправдиві результати. Незважаючи на повідомлення про хакерські атаки, ці дані були озвучені на російському Першому каналі як фактичні результати виборів в Україні. 23 грудня 2015 року програма BlackEnergy3 Trojan, якою раніше користувались російські хакери, зупинила роботу близько 30 підстанцій зв'язку, в результаті чого понад 200 000 жителів Івано-Франківської області залишились без електроенергії на одну-п’ять годин. Напади на "Київобленерго" та "Чернівціобленерго" відбувалися тоді ж. Ці та багато інших, але не настільки відомих, кібератак не лише змусили провідні технологічні компанії серйозно задуматись і переосмислити підходи до кібербезпеки, а й загалом вивести цю проблему на державний рівень. Виклики та загрози для нацбезпеки Українив кіберпросторі призвели до створення Стратегії кібербезпеки України, що була впроваджена указом Президента України від 15 березня 2016 року [46], а реалізація її положень призвела до прийняття Закону України «Про основні засади забезпечення кібербезпеки України» [51].

Як бачимо, поняття "інформаційна безпека" набагато ширше поняття безпеки інформації і аж ніяк не зводиться до нього. Наразі тема щодо безпеки у кіберпросторі є найпоширенішою і найбільш затребуваною суспільством, оскільки це стосується кожного, хто стикається зі світом інформаційних технологій.

1.2. Нормативно-правове забезпечення та принципи кібербезпеки в Україні

Розвиток правового та нормативного забезпечення інформаційної безпеки в Україні зумовлений появою якісно нових соціальних явищ, пов’язаних з інформацією, та посиленою увагою законодавчої влади до впорядкування цієї сфери суспільних відносин. Важливість інформації в різноманітних соціальних процесах сьогодні зростає. Активне використання засобів обробки та передачі інформації, а також розвиток нових технологій призводять до значних змін в економічній, політичній та інших сферах суспільного життя. Багато дослідників ставлять питання про формування інформаційного суспільства нового типу, яке замінить індустріальне.

До прийняття українського Закону "Про основні принципи забезпечення кібербезпеки України" [51] була Конституція України [20], Закони України "Про інформацію" [45], "Про захист інформації в інформаційно-телекомунікаційних системах" [42] та інші закони, що забезпечують правову основу кібербезпеки України, Конвенція Ради Європи про кіберзлочинність [37], інші міжнародні договори, затверджені Верховною Радою України, Доктрина інформаційної безпеки України та інші нормативно-правові акти.Закон України "Про основні принципи забезпечення кібербезпеки України" визначає правову та організаційну основу захисту життєво важливих інтересів людини та громадянина, суспільства та держави, національних інтересів України в кіберпросторі , основні цілі, напрямки та принципи державної політики у галузі кібербезпеки, повноваження державних установ, компаній, установ, організацій, приватних осіб та громадян у цій галузі, основні принципи координації їх діяльності щодо забезпечення кібербезпеки.

Слід зазначити, що застосування українського Закону «Про основні принципи реалізації кібербезпеки України» не поширюється на відносини та послуги, пов'язані зі змістом інформації, що обробляється (передається, зберігається) розміщеної в комунікаційних та/або технологічних системах, соціальних мережах та приватна електронна інформація в Інтернеті (включаючи платформи для ведення блогів, веб-сайти для відеохостингу, інші веб-ресурси) та для інформаційних та телекомунікаційних систем, в яких циркулює інформація, що представляє державну таємницю. Однак запровадження норм закону в цій галузі може становити серйозне порушення прав людини у значенні положень Європейської конвенції про захист прав людини та основоположних свобод, ст. 10 Конвенції [38].

Забезпечення кібербезпеки в Україні ґрунтується на таких принципах:

- верховенство права, законність, повага прав людини та основних свобод та їх захист у порядку, встановленому законом;

- захист національних інтересів України;

- відкритість, доступність, стабільність та безпека віртуального простору, розвиток Інтернету та відповідальна поведінка у віртуальному просторі;

- державно-приватна взаємодія, широка співпраця з громадянським суспільством у галузі кібербезпеки та кіберзахисту, зокрема шляхом обміну інформацією щодо інцидентів кібербезпеки, проведення спільних науково-дослідних проектів, навчання та підвищення кваліфікації персоналу в цій галузі;

-пропорційність та доцільність заходів кіберзахисту щодо реальних та потенційних ризиків, реалізація невід'ємного права держави на самооборону відповідно до норм міжнародного права на випадок агресивних дій у кіберпросторі;

- пріоритетність запобіжних дій;

- неминучість покарання за вчинення кіберзлочинності;

- пріоритетний розвиток та підтримка вітчизняних наукових, науково-технічного та виробничого потенціалу;

- забезпечення демократичного цивільного контролю за утвореними відповідно до законів України військовими формуваннями та правоохоронними органами, що провадять діяльність у сфері кібербезпеки та ін.

Закон України "Про основні принципи кібербезпеки України" [51] встановив загальну архітектуру національної системи кібербезпеки та розподілив завдання та повноваження з основних питань кібербезпеки (Національний координаційний центр з кібербезпеки, Міністерство оборони, Генеральний штаб Збройних Сил, Державна служба спеціального зв'язку та захисту інформації, Служба безпеки, Національна поліція, Національний банк розвідувальними органами України), створює умови для залучення компаній, установ та організацій, незалежно від форми власності, що діють у сфері електронної комунікації, захист інформації та/або власниками (менеджери) критично важливих інфраструктур, наукових установ, навчальних закладів, організацій, громадських об'єднань та громадян.

Реалізація положень Стратегії кібербезпеки України та українського Закону "Про основні принципи забезпечення кібербезпеки України" [51] розробку та застосування якісно нового законодавства у галузі кібербезпеки, заснованого на досвід, накопичений за п'ять років гібридної війни, підвищення обізнаності та впровадження досвіду та норм ЄС та НАТО. Зокрема, мають бути розроблені такі нормативно-правові акти: Закон України "Про критичну інфраструктуру та її захист"[47], Постанови Кабінету Міністрів України, зокрема: "Порядок створення переліку критично важливих об'єктів інформаційної інфраструктури" [33], «загальні вимоги щодо захисту об'єктів критичної інфраструктури від кіберзагроз» (прийнятий 19 червня 2019 р. № 518), «Про затвердження протоколу спільних дій основних суб'єктів кібербезпеки, питання кіберзахисту та власників (менеджерів) об'єктів критичної інформаційної інфраструктури під час запобігання, виявлення та припинення кібератак та кіберінцидентів та усунення їх наслідків"[41], «Вимоги до незалежного тестування інформаційної безпеки на об'єктах критичної інфраструктури та процедура для незалежного тестування інформаційної безпеки на об'єктах критичної інфраструктури ".

Потрібно створити:

- реєстр об'єктів критичної інформаційної інфраструктури,

- перелік об'єктів критичної інфраструктури,

- реєстр аудиторів інформаційної безпеки.

Результатом впровадження цих норм має стати всебічний огляд сектору безпеки та оборони, який також повинен включати огляд стану кіберзахисту критично важливих інформаційних інфраструктур, державних інформаційних ресурсів та інформації, яка охороняється законом.

Важливим кроком у створенні сучасної системи кіберзахисту в Україні було прийняття Постанови Кабінету Міністрів від 19 червня 2019 р. № 518 "Про затвердження загальних вимог до кіберзахисту критичних інфраструктур" [38], в якій було визначено:

- визначення загальних вимог до кіберзахисту об’єктів критичної інфраструктури;

- визначення обов'язкових заходів для захисту від кібератак;

- запобігання порушенням конфіденційності;

- цілісність та доступність інформаційних ресурсів;

- стійке функціонування.

Слід зазначити, що розвиток законодавства у сфері кібербезпеки в Україні безпосередньо пов’язаний із прагненнями України до європейської інтеграції та розвитком правового регулювання електронної комерції в рамках СОТ.

27 червня 2014 року Україна підписала Угоду про асоціацію між Україною, з одного боку, та Європейським Союзом, Європейським співтовариством з атомної енергії та його державами-членами, з іншого боку [67]. В статті з Додатку XVII (Нормативно-правове наближення до набуття повного режиму внутрішнього ринку в конкретному секторі) зазначено: "1. Відповідно до статей 114, 124, 133 і 139 глави 6 "Створення бізнесу, торгівля послугами та електронна торгівля"та глава 7 " Поточні платежі та рух капіталу"У розділі IV цієї Угоди та у статті 2 (1) цього Додатку Україна впроваджує чинне законодавство ЄС, перелічене у Додатку, відповідно до

статті 2 цього Додатку [69] у свої національні правові системи та впроваджує її на постійній основі.

У січні 2012 року ЄС розпочав реформу законодавства Європейського Союзу про захист персональних даних з метою адаптації їх до вимог "цифрової ери" та до реалізації Стратегії Єдиного Цифрового Ринку Європи (DigitalSingleMarketStrategy). У цьому контексті було складено два документи - Директиву 2016/680 Європейського Парламенту та Ради ЄС від 27 квітня 2016 року про захист фізичних осіб при обробці персональних даних компетентними органами з метою запобігання, розслідування, виявлення або притягнення до відповідальності за кримінальні правопорушення або застосування кримінальних санкцій та вільне розпорядження такими даними, а також скасування Рамкового рішення Ради 2008/977 Ради та скасування Директиви 95/46 / ЄС (Загальний регламент про захист даних (GDPR)).

Стратегія та порядок денний були опубліковані навесні 2015 р., У липні 2016 р. Європейська Комісія представила "Додаткові заходи для сприяння розвитку галузі кіберзахисту", а 6 липня 2016 р. була прийнята Директива ЄС щодо заходів про забезпечення високого рівня загальної безпеки мережевих та інформаційних систем в усьому Союзі (DIRECTIVE (EU) 2016/1148 - NIS Directive). Ця Директива встановлює єдині правила та вимоги в галузі кібербезпеки для всіх країн ЄС, але залишає за кожною державою-членом право вживати власних заходів для впровадження стандартів Директиви у національне законодавство (це має бути зроблено в країнах ЄС до 9-го травня 2018 р.).

Для досягнення мети Директиви (забезпечення більш високого рівня мережевої та інформаційної безпеки в Європейському Союзі) необхідно вжити заходів у трьох основних сферах:

- збільшити потенціал системи кібербезпеки на національному рівні;

-збільшення загальноєвропейської співпраці;

- заздалегідь керувати ризиками та бути зобов’язаним повідомляти про кіберінциденти операторам базових послуг постачальників цифрових послуг.

Директива Ради 2008/114 / ЄС від 8 грудня 2008 року про ідентифікацію та визначення європейських критичних інфраструктур та оцінку необхідності вдосконалення їх захисту та покращення також є важливою для подальшого розвитку законодавства у галузі кібербезпеки. Ми вважаємо, що необхідно враховувати положення цього документа при розробці національного нормативного законодавства, а також місцевого законодавства компаній-господарників.

В Постанові Кабінету Міністрів України від 29.03.2006 № 373 «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» [40] сказано, про реалізацію вимог стандартів сімейства систем управління інформаційної безпеки (СУІБ) для певних категорій інформації. Важливо, щоб ці вимоги діяли для забезпечення інформаційної та кібербезпеки в ЄС та наближували Україну до європейських стандартів.

Відповідно до Закону, підтвердження відповідності інтегрованої системи захисту інформації (КСЗІ) буде ґрунтуватися на результатах державної експертизи.

Тепер головне, що державні інформаційні ресурси і інформація з обмеженим доступом, за винятком державної таємниці, можуть оброблятися в системі без використання КСЗІ при дотриманні наступних умов:

• підтвердження відповідності системи менеджменту інформаційної безпеки національним стандартам України щодо систем управління інформаційної безпеки;

• використання для захисту інформації в системі криптографічного захисту інформації, що має позитивний експертний висновок за результатами державної експертизи;

• жоден з елементів системи не може перебувати на території України, де органи державної влади тимчасово не здійснюють свої повноваження, на територіях держав, визнаних Верховною Радою України державами-агресорами, на територіях держав, що підпадають під дію санкції за Законом

України, а також на територіях держав, що входять до митних союзів з такими державами;

• виконання спеціальних вимог, встановлених Урядом, для забезпечення захисту інформації в системах в залежності від категорії державних інформаційних ресурсів або інформації з обмеженим доступом, вимога захисту якої встановлена законом.

Затверджений закон вводить альтернативний спосіб підтвердження відповідності інформаційної системи вимогам захисту інформації. Цікаво, що подібна практика законодавства вже застосовується в Україні в сфері держзакупівель.

Таким чином, законодавче регулювання кібербезпеки в Україні знаходиться на початку свого створення, але найскладніший етап - визначення стратегії, меж і напрямів державної політики кібербезпеки пройдено. Звичайно, на шляху ще багато проблем, але є і досягнення. Невирішені питання державно-приватного співробітництва, ще не сформульовані списки об’єктів критичної інфраструктури та інші, розробка підходів до кіберзахисту, попереду великий пласт проблем і обсяг роботи спрямованої на нормативно-правове врегулювання в сфері кібербезпеки.

РОЗДІЛ 2
АНАЛІЗ СТАНУ ЗАХИСТУ ДЕРЖАВНИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ У СФЕРІ КІБЕРБЕЗПЕКИ

2.1. Характеристика діяльності суб'єктів національної системи кібербезпеки

Швидкий розвиток інформаційних технологій поступово змінює світ. Відкритий і вільний кіберпростір розширює свободу і можливості людей, збагачує суспільство, створює новий глобальний інтерактивний ринок ідей, досліджень та інновацій, стимулює відповідальний і ефективний метод роботи уряду і активну участь громадян в управлінні та вирішенні місцевих питань, забезпечує гласність і прозорість влади, а також сприяє запобіганню корупції.

У той же час переваги сучасного цифрового світу і розвиток інформаційних технологій привели до появи нових загроз національній і міжнародній безпеці. Поряд з інцидентами природного (ненавмисного) походження зростає кількість і потужність кібератак, мотивованих інтересами окремих держав, груп і окремих осіб.

Є випадки незаконного захоплення, зберігання, використання, знищення, поширення особистих даних, незаконних фінансових операцій, крадіжок і шахрайства в Інтернеті. Кіберзлочинність стає транснаціональної і може завдати значної шкоди інтересам людей, суспільства і держави.

Триваюча агресія з боку Російської Федерації та інші радикальні зміни в середовищі зовнішньої і внутрішньої безпеки України вимагають негайного створення національної системи кібербезпеки як частини системи національної безпеки України.

Ці умови стали приводом для підписання Указу Президента України про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» [54].

Метою стратегії кібербезпеки України є створення умов для безпечного функціонування кіберпростору і його використання в інтересах особистості, суспільства і держави.

Національна система кібербезпеки - це комплексна система взаємодії Державної служби спеціального зв'язку та захисту інформації України, Національної поліції України, Служби безпеки України, Міністерства оборони України та Генерального штабу Збройних сил України, спецслужб, Національного банку України і взаємопов'язані заходи політичних, науково-технічних, інформаційних, освітніх, організаційних, правових, оперативно-розшукових, розвідувальних, контррозвідувальних, оборонних, інженерно-технічних заходів, а також заходи криптографічного та технічного захисту національних інформаційних ресурсів та Кібер об'єктів критичної інформаційної інфраструктури.

Основним суб`єктом національної системи кібербезпеки є Державна служба спеціального зв'язку та захисту інформації України, на яку припадає близько 80% навантаження і яка виконує наступні функції:

- забезпечення формування та реалізації державної політики щодо захисту державних інформаційних ресурсів та інформації в кіберпросторі, вимоги до захисту яких встановлені законодавством, кіберзахист критичних інформаційних інфраструктур, здійснює державний контроль у цих сферах;
- координує діяльність інших суб'єктів кібербезпеки в сфері кіберзахисту;
- забезпечення створення і функціонування Національної телекомунікаційної мережі, впровадження організаційно-технічної моделі кіберзахисту;
- реалізує організаційні і технічні заходи щодо запобігання, виявлення і реагування на кіберінциденти і кібератаки і усунення їх наслідків;
- нформує про кіберзагрози і відповідні методи захисту від них;
- забезпечує проведення аудиту інформаційної безпеки на об'єктах критичної інфраструктури, визначає вимоги до аудиторів інформаційної безпеки і визначає процедуру їх сертифікації (відновлена сертифікація);
- координує, організовує і проводить аудит захищеності комунікаційних і технологічних систем об'єктів критичної інфраструктури на наявність вразливостей;

- забезпечує функціонування державного центру кіберзахисту.

У Державному центрі кіберзахисту і протидії кіберзагрозам Державної спеціалізованої служби зв'язку існує структурований підрозділ Computer Response Team of Ukraine (далі: CERT-UA) - група з реагування на комп'ютерні надзвичайні ситуації в Україні, основною метою якої є - забезпечення захисту інформаційних ресурсів, а також інформаційних і телекомунікаційних систем від несанкціонованого доступу, неправомірного використання і порушення їх конфіденційності, цілісності та доступності. CERT-UA регулярно публікує рекомендації з безпеки поштового сервісу, по боротьбі із загрозою з боку інсайдерів, щодо усунення вразливостей, пов'язаних з некоректним настроюванням DNS-серверів, по самостійному пошуку і видалення веб-Шелл і т. д.

Національна поліція України займається захистом від кримінального вторгнення в кіберпростір, реалізує заходи щодо запобігання, розкриття, боротьбі і виявлення кіберзлочинності, підвищенню обізнаності громадськості про безпеку кіберпростору;

Кіберполіція (Управління кіберполіції Національної поліції України) - міжрегіональний територіальний орган Національної поліції України, який входить до складу кримінальної поліції Національної поліції і відповідно до законодавства України забезпечує реалізацію державної політики в боротьбі з кіберзлочинністю, організовує і здійснює оперативну діяльність. Спеціалізується на:

- запобіганні, виявленні, припиненні і розкритті кримінальних злочинів, механізмів підготовки, вчинення або приховування яких включають використання комп'ютерів, телекомунікацій і комп'ютерних інтернет-мереж і систем.

- виявляє, розробляє і забезпечує реалізацію комплексу заходів щодо попередження та боротьби зі злочинністю в сфері кіберзлочинності;

- приймає в межах своїх повноважень необхідні оперативні та слідчі заходи для виявлення причин і умов, що призвели до вчинення кіберзлочинів;

- вживає заходів, передбачених чинним законодавством, для збору та узагальнення інформації про юридичних осіб, в тому числі про телекомунікації, інтернет-послуги, організаціях банківських і платіжних систем, з метою запобігання, виявлення і припинення злочинів;

- організовує і контролює діяльність підпорядкованих підрозділів кіберполіції з метою дотримання вимог законодавства України у сфері протидії кіберзлочинності;

- проводить роботу з інформування громадськості про дотримання законодавства України в галузі використання новітніх технологій, а також про захист та протидію кіберзагрозам в повсякденному житті;

- забезпечує формування та заповнення інформаційних полів даних, автоматизованих інформаційних систем відповідно до вимог діловодства;

- організовує в межах своєї компетенції виконання вказівок слідчого, прокурора про проведення слідчих заходів (обшуків) і негласних розслідувань (обшуків) в кримінальному провадженні;

- інше.

Служба безпеки України, поряд з Державною службою спеціального зв'язку та захисту інформації України (Держспецслужби України), Національною поліцією України, Міністерством оборони України та Генеральним штабом Збройних сил України, Національним Банком України, розвідувальними органами була визначена як один з ключових гравців у національній системі кібербезпеки. [53, ст. 8].

Служба безпеки України запобігає, виявляє, припиняє і розкриває злочини проти миру і безпеки людства що здійснюються в кіберпросторі. Проводить контррозвідувальні та розшукові операції по боротьбі з кібертероризмом і кібершпіонажем і таємно перевіряє готовність критично важливих об'єктів інфраструктури до можливих кібератак і кіберінцідентам; протидіє кіберзлочинності, наслідки якої можуть поставити під загрозу життєво важливі інтереси держави; розслідує кіберінціденти і кібератаки на державні електронні інформаційні ресурси, конфіденційну інформацію і критично

важливу інформаційну інфраструктуру; пропонує відповідь на кіберінциденти в сфері державної безпеки [53, ст. 8].

Закон України «Про національну безпеку України» [50] від 21 червня 2018 року визначив Службу безпеки України як державну установа зі спеціальним призначенням і правоохоронними функціями, яке забезпечує безпеку держави при строгому дотриманні прав і свобод людини і громадянина:

1) протидія спецслужбам і підривна діяльність проти України;

2) боротьба з тероризмом;

3) противошпигунський захист кібербезпеки та інформаційної безпеки держави, об'єктів критичної інфраструктури [50, ст. 19].

Відповідно до Закону України «Про основні засади кібербезпеки України» національна система кібербезпеки складається з підрозділів кібербезпеки і взаємопов'язаних заходів політичного, науково-технічного, інформаційного, освітнього, організаційного, правового, оперативного і слідчого характеру, розвідувальних, контррозвідувальних, оборонних, інженерно - технічних заходів, а також заходи з криптографічного і технічного захисту національних інформаційних ресурсів, кіберзахисту критичних інформаційних інфраструктур [51, стаття 8].

Слід зазначити, що Закон про кібербезпеку Міністерства оборони та Генерального штабу Збройних сил (пункт 8 другій частині статті 8) визначає без змін перші два основні завдання Стратегії, а саме:

1. Здійснення заходів з підготовки держави до захисту від військової агресії в кіберпросторі (кіберзахист);

2. Військова співпраця з НАТО та іншими суб'єктами оборони для забезпечення безпеки кіберпростору і спільного захисту від кіберзагроз. "

Третє завдання цих органів визначене інакше, ніж в стратегії, і передбачає «реалізацію заходів щодо забезпечення кіберзахисту критичних інформаційних інфраструктур в умовах надзвичайного та воєнного стану».

Також в жовтні 2017 року Закон України «Про оборону України» були внесені поправки, які обумовлюють, що підготовка держави до оборони в мирний час серед іншого включає «Заходи кіберзахисту (активний кіберзахист)

для захисту державного суверенітетету і запобігання збройним конфліктам і захист від збройної агресії».

І тільки через майже півтора року, на початку січня 2019 року, Кабінет Міністрів України вніс зміни до постанов Міністерства, в яких, зокрема, прописано, що «Міністерство оборони вживає заходів щодо забезпечення інформаційної безпеки, кібербезпеки і кіберзахисту, відповідно до його юрисдикції, і підготовка держави до захисту від військової агресії в кіберпросторі (кіберзахист) » (стаття 3 (п.21)).

Пізніше, в кінці січня 2019 року, було прийнято Положення про Генеральний штаб Збройних Сил України. Зокрема, передбачено, що цей основний орган військового управління державного оборонного планування:

- організовує, керує і забезпечує функціонування єдиної системи захисту інформації та кіберзахисту в інформаційних і телекомунікаційних системах Міністерства оборони та збройних сил (стаття 4 (п.71));

- бере участь у створенні національної системи кібербезпеки і її періодичному перегляді (стаття 4 (п.73));

- організовує планування і реалізацію заходів з підготовки держави до захисту від військової агресії в кіберпросторі (кіберзахист), координує виконання завдань з підготовки до кіберзахисту правоохоронними органами, органами місцевого самоврядування та іншими компонентами сил оборони (п. 74 статті 4);

- забезпечує інформаційну безпеку в збройних силах і протидіє системним і широкомасштабним заходам іноземних держав (груп держав) проти інтересів України в кіберпросторі, зокрема шляхом залучення кіберпідрозділів іноземних збройних сил, шляхом використання спеціальних засобів (кіберозброєння) (стаття 4 п.77).

Слід зазначити, що в 2016-2019 роках вищевказані законодавчо встановлені завдання Міністерства оборони та Генерального штабу Збройних сил України по реалізації заходів кіберзахисту, підвищенню їх можливостей кіберзахисту і т. д. не були належним чином реалізовані в документах оборонного планування.

В кінці березня 2020 були внесені зміни в положення про Генеральний штаб Збройних Сил, згідно з якими цей орган також:

- організовує планування дій збройних сил і інших компонентів сил оборони в кіберпросторі;

- організовує кіберзахист інформаційної інфраструктури Міноборони і Збройних Сил спільно з Державною службою спеціального зв'язку та захисту інформації України та Службою безпеки України.

Національний банк України визначає порядок, вимоги та заходи щодо забезпечення кібербезпеки та інформаційної безпеки в банківській системі України та контролює їх виконання з питань грошових переказів, створює центр кібербезпеки Національного банку України, забезпечує функціонування системи кібербезпеки в банківській системі України; забезпечує оцінку стану кібербезпеки і дослідження інформаційної безпеки об'єктів критичної інфраструктури в банківській системі України.

За результатами такого короткого аналізу положень законодавства, фактів і існуючих проблем в сфері кіберзахисту держави доцільно зробити наступні висновки.

Кібероборона, кібербезпека і кіберзахист багато в чому незалежні і відрізняються за змістом, тематикою та напрямками діяльності в кіберпросторі України. Структура державної системи кіберзахисту, склад, функції та завдання її суб'єктів, а також об'єкти кіберзахисту все ще не визначені відповідними нормативними актами. Відповідно до закону, основні завдання кіберзахисту покладаються на Міністерство оборони і Генеральний штаб Збройних сил, які повинні спільно вживати заходів кіберзахисту (активний кіберзахист) для захисту суверенітету та обороноздатності держави, запобігання збройних конфліктів і відсічі збройної агресії.

Оскільки за оборонні завдання України в першу чергу несуть відповідальність її сили оборони, ми вважаємо, що вони повинні включати спільні сили/війська кіберзахисту. На цьому тлі, крім відповідних підрозділів збройних сил, повинні бути включені збройні сили і ресурси державної спеціальної служби, служба безпеки, служба охорони державного кордону,

національна гвардія, національна поліція і спецслужби, яким доручено забезпечувати державну оборону. Використання таких сил управляється Головнокомандувачем Збройними Силами України через Командувача Об'єднаними силами.

2.2. Аналіз сучасного стану кіберзлочинів в Україні за 2017-2020 роки

Слід вказати, що світові тенденції зростання рівня проникнення, використання інтернету та соціальних медіа приватними особами і компаніями, с характерними і для України, що, в свою чергу, сприяє розвитку інтернет-бізнесу. Такі факти знайшли своє підтвердження в ряді досліджень.

Так, у 2017 році загальна сума витрат на покупки товарів через електронні платформи склала 1,474 трлн, доларів, що на 16% більше, ніж в 2016 році [66].

Аналіз основних статистичних показників, які характеризують рівень використання інформаційно-комунікаційних технологій на підприємствах України (табл.2.1), дозволив констатувати зростання кількості комп'ютерної техніки, підвищення доступу до мережі Інтернет та збільшення рівня використання інформаційно-комунікаційних технологій в своїй діяльності, що проявилось у наступних тенденціях:

зростання кількості комп'ютерної техніки (+2 % у 2017 р. у порівнянні із 2016 р.),

підвищення доступу до мережі Інтернет (+2% у 2017 р.) та збільшення рівня використання інформаційно-комунікаційних технологій у своїй діяльності, зокрема у 2017р.:

+4 % підприємств, що мали веб-сайт;

+8 % підприємств, які використовували соціальні медіа (соціальні мережі, блоги чи мікроблоги підприємства, веб-сайти з мультимедійним вмістом, засоби обміну знаннями);

+ 13,6% підприємств, що купували послуги хмарних обчислень упродовж року;

Таблиця 2.1

Використання інформаційно-комунікаційних технологій на підприємствах України

№	Назва показника	2017р.	2018р.	2019р.
1	Кількість підприємств, які використовували комп'ютери, протягом року, од	41597	39540	40327
2	Частка підприємств, які використовували комп'ютери, у % до загальної кількості підприємств, які взяли участь в обстеженні.	95,2	95,1	95,4
3	Кількість підприємств, які мали доступ до мережі Інтернет, од	40747	38825	39572
4	Частка підприємств, які мали доступ до мережі Інтернет, у % до кількості підприємств, які використовували комп'ютери, %	98,0	98,2	98,2
5	Кількість підприємств, які мали фахівців у сфері ІКТ, од.	8541	10436	10660
6	Кількість підприємств, що мали веб-сайт, який функціонував у мережі Інтернет, од.	18323	15608	16240
7	Кількість підприємств, які використовували соціальні медіа (соціальні мережі, блоги чи мікроблоги підприємства, веб-сайтн з мультимедійним вмістом, засоби обміну знаннями, од.	21722	22064	23849
8	Кількість підприємств, що купували послуги хмарних обчислень упродовж року, од., в т.ч.:	2673	3639	4135
	із загальних серверів постачальників послуг	967	1506	1832
	серверів постачальників послуг, зарезервованих виключно для обстежуваного підприємства	430	665	807
9	Кількість підприємств, які надавали рахункн - фактури в електронному/паперовому вигляді:			
	іншим підприємствам	26010	27919	29171
	державним органам	3465	6582	7238
	приватним споживачам	12869	14302	154733
10	Кількість підприємств, що отримували замовлення через комп'ютерні мережі на продаж товарів або послуг (за винятком замовлень, отриманих електронною поштою)	2489	2503	2596
II	Кількість підприємств, що здійснювали закупівлі через комп'ютерні мережі товарів або послуг (за винятком замовлень, отриманих електронною поштою)	5495	7147	8168

Примітка. Сформовано автором за даними [8].

Серед підприємств, які мали доступ до мережі Інтернет найбільша частка належить до сфери «оптова та роздрібна торгівля; ремонт автотранспортних засобів і мотоциклів», переробної промисловості та будівництва.

Серед напрямів використання мережі Інтернет слід відзначити:

– надсилання чи отримання повідомлень електронною поштою;

– здійснення телефонних дзвінків за допомогою Інтернет/VoIP-зв'язку або відео-конференцій;

– отримання інформації про товари та послуги;

– користування миттєвим обміном повідомленнями та електронною дошкою оголошень;

– отримання інформації від органів державної влади;

– здійснення різноманітних операцій з органами державної влади (за винятком отримання інформації);

– здійснення банківських операцій; доступ до інших фінансових послуг.

Зазначимо, що згідно очікувань українських респондентів, за критерієм суттєвості для організацій з точки зору фінансових збитків або інших наслідків у 2019-2020 рр., кіберзлочини не лише відзначені у топ 5 видів економічних злочинів та / або шахрайства, а й посіли друге місце, поступаючись лише хабарництву та корупції (рис.2.1).

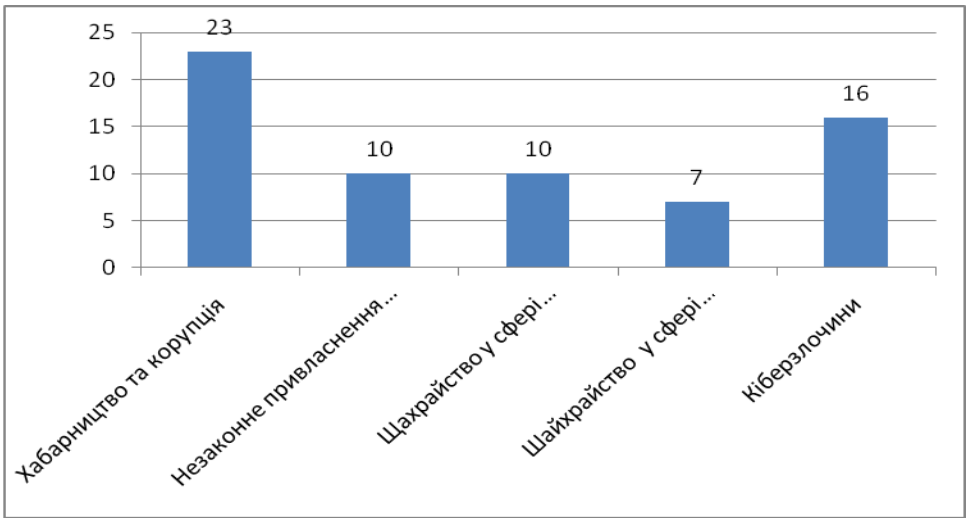

Рис. 2.1 Місце кіберзлочинів за критерієм суттєвості для організацій з точки зору фінансових збитків.

Примітка. Складено автором [8]

Наразі в Україні незадовільний стан захищеності державних електронних інформаційних ресурсів, реєстрів, баз даних та інших інформаційних масивів, і наголосив на важливості практичної співпраці між суб’єктами забезпечення кібербезпеки.

За останні п’ять років в Україні кількість інформаційних злочинів зросла щонайменше у 2,5 рази. Про це повідомляє прес-служба Opendatabot.

«Стрибок» кількості всіх кіберзлочинів відбувся у 2017 році, значною мірою він пов'язаний з вірусом Petya. Відтоді, кількість інформаційних злочинів не зменшується. В 2017 році було зафіксовано 1795 справ, в 2018 – 1023, за останні півроку – 1005. (Рис. 2.2). На даний момент в судовому реєстрі є 1500 справ.

Кількість справ, порушених проти кіберзлочинців, зростає не лише через те, що почастішали самі злочини. Друга причина – побільшало фахівців, здатних ці злочини виявити», – додають у прес-службі.

За перше півріччя 2020 року Держспецзвязок, зокрема система кіберзахисту державних інформаційних ресурсів та об’єктів критичної інфраструктури на об’єктах моніторингу зафіксував 26017752 підозрілих подій, що на 11% більше, ніж попереднього року.

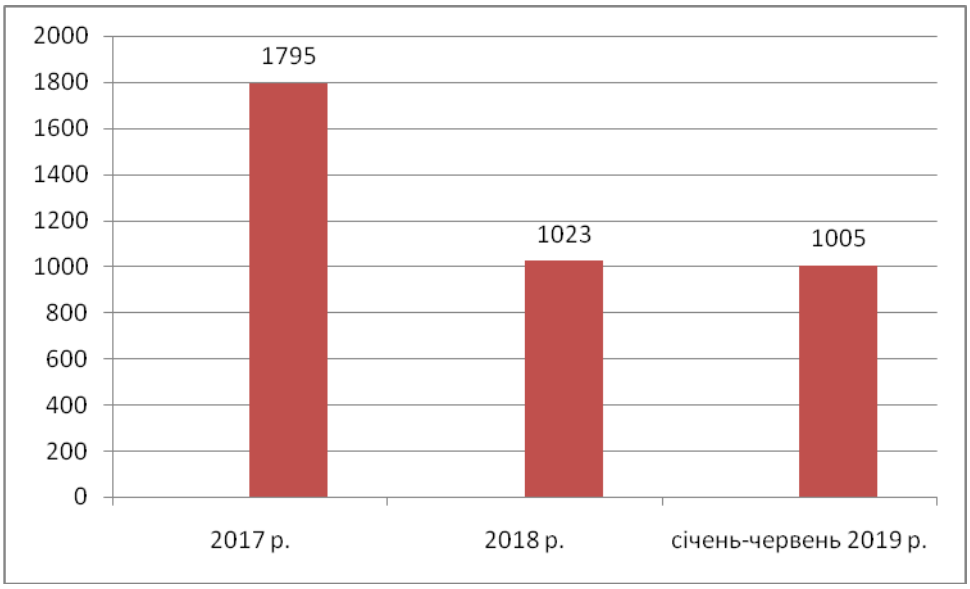

Рис. 2.2 Динаміка кількості інформаційних злочинів в Україні.

Примітка. Складено автором

Переважна більшість зафіксованих підозрілих подій стосується спроб мережевого сканування (91%), застосування нестандартних протоколів (7%) та виявлення мережевого ШПЗ (1%).Система захищеного доступу державних органів до мережі Інтернет заблокувала 1088712 атак різних видів, що на 22% більше, ніж попереднього року. Переважна більшість - це мережеві атаки

прикладного рівня (94%) та атаки типу «Harvest Attack» (4%). Також зафіксовано і заблоковано 6 DDoS-атак.

Урядова команда реагування на комп'ютерні надзвичайні події України CERT-UA у цей період зареєструвала та опрацювала 63888 кіберінцидентів, що на 4% менше, ніж за відповідний період 2019 р.

Переважна більшість опрацьованих інцидентів стосується недержавного сектору (близько 99%). Основна кількість інцидентів стосується розповсюдження ШПЗ (99%).

Проаналізувавши вірусну активності за 2019 рік в Україні експерти [1] відзначають зростання частоти використання відомих троянських програм, але в їх модернізованих варіантах (рис. 2.3).

Трояни – базовий інструмент кіберзлочинців.

Абсолютним лідером використання в кількісному вираженні та в загальній частці від усього обсягу атак на ПК користувачів в Україні стали троянські програми різного функціоналу та спрямування.

За аналітичними даними за 2019 рік практично кожен другий випадок атаки на ПК українців був здійснений за допомогою троянської програми. На основі цих даних можна зазначити, що трояни використовувалися у 54% випадків від усіх атак на ПК українських користувачів, що на 7% більше ніж за аналогічний період 2018 року.

Лідерами серед троянських програм, які були активні в 2019 році,були так звані банківські троянці, що «спеціалізуються» на крадіжки банківської інформації, а також трояни-шифрувальники даних.

Варто зазначити що шифрувальники в цілому були видом шкідливого ПЗ, що найбільш динамічно розвивався в минулому році. Варто зазначити, що все частіше новими зірками категорії все частіше стають оновлені версії старих версій шифрувальників, яким надавалися нові сучасні функції і унікальні можливості для крадіжки особистих даних, а також проникнення на ПК жертв.

Рис. 2.3. Вірусна активність в Україні 2018-2019 рр.

Примітка. Джерело [1]

Серед найбільш знакових троянів 2019 року варто відмітити три наступні різновиди, які суттєво вплинули та статистику використання даного виду шкідливого ПЗ:

GandCrab - Декілька останніх років цей відносно новий вимагач набирав силу і у 2018 році увійшов у список найбільш розповсюджених та небезпечних програм-вимагачів. Правоохоронні органи, антивірусні та кіберсекьюріті компанії сфокусувалися на боротьбі з ним і вважалося, що епідемію зупинено. Однак, в 2019 році GandCrab знову потужно заявив про себе отримавши нові модифікації від своїх творців.

Найбільш поширеним шляхом розповсюдження GandCrab є СПАМ-розсилка. Однак варто зауважити, що кіберзлочинці провили в даному аспекті неабияку хитрість та винахідливість. По перше треба зазначити, що СПАМ розсилка GandCrab будується на принципах соціальної інженерії, якою власники шкідника досить вміло користуються задля своїх кримінальних цілей.

Sodinokibi - Новітній шифрувальник використовує вразливості сервера додатків OracleWebLogic та інші системні вразливості. Але для ініціації шкідливого коду на ПК до нього потрібно спочатку потрапити. Власне як і в багатьох відомих компаніях зараження, основним методом доставки

шифрувальника до ПК користувачів-жертв є СПАМ-розсилка. Зазвичай такі акції будуються на принципах соціальної інженерії.

Emotet - Банківський троян EMOTET отримав суттєві зміни, що вивели його в ТОП шкідливого програмного забезпечення 2019 та початку 2020 років. У 2019 році це шкідливе програмне забезпечення, було перетворено на багатофункціональний інструмент, що здатен саморозповсюджуватися та завантажувати на ПК інші види шкідливих програм без відома власника.

Adware не ТОП з 2016 року - asof 2016. Важливим інструментом кіберзлочинців залишається Adware, що продовжують входити в ТОП-3 по кількісному показнику виявлених вірусних погроз. Варто зазначити, що використання програм для несанкціонованого показу рекламної інформації втрачає свої позиції в загальній кількості атак на ПК в останні 3-4 роки.

Згідно даних [1] за 2019 рік, цей вид шкідливих програм залишається в межах 28% (ті ж самі 28% в 2018 році) від усіх виявлених заражень і атак на комп'ютери українців.

Від вірусу Petya, що був у 2017 р. постраждали тисячі компаній. Але тоді заяви в кіберполіцію про дані, втрачені через цей вірус, часто залишалися без відповідей. Нині ситуація змінилася, однак залишається складною.

Збільшення кількості таких злочинів в останні два роки значною мірою пов'язане з тим, що поступово штат співробітників кіберполіції все-таки розширюється і відповідно більше порушується кримінальних справ. Але, на жаль, левова частка таких справ або не доходить до суду, або розвалюється в суді через погане збирання доказів слідчими органами. У нашій країні зовсім небагато грамотних слідчих і експертів, які могли б кваліфіковано, з усіма необхідними доказами, довести до суду злочин цих категорій.

Інформаційні злочини (кіберзлочини) – це різні види злочинів, що здійснюються за допомогою комп'ютера та інтернету. Кіберзлочинці можуть полювати на персональні дані, банківські рахунки, паролі та іншу інформацію, яка існує в електронному вигляді. Потерпілими можуть стати як фізичні особи, так і бізнес та державний сектор.

Український Кримінальний кодекс передбачає 4 статті за інформаційні злочини. Ст. 361 передбачає притягнення до відповідальності за незаконне проникнення до комп'ютерів, систем чи мереж і втручання в їхню роботу (або її блокування). Ст. 361-1 передбачає санкції за написання та поширення вірусів, незалежно від того, робиться це безкорисливо чи за гроші. Ст. 361-2 покликана карати за зловживання правом доступу до інформації. Наприклад, співробітника компанії, який продав конкурентам базу даних клієнтів своєї компанії, доступ до якої мав через свої службові обов'язки. Ст. 362 передбачає покарання для тих, хто мав право доступу до комп'ютера чи мережі, але скористався ним для інших цілей. Якщо перед звільненням знищується на службовому комп'ютері важлива інформація, то такі дії підпадатимуть під цю статтю.

Таким чином, Державна служба спеціального зв'язку та захисту інформації України звертається до всіх: в разі будь-яких кіберінцидентів, кібератак або підозрілих дій щодо інформаційно-телекомунікаційних систем необхідно інформувати урядову команду реагування на комп'ютерні надзвичайні події України.

РОЗДІЛ 3
НАПРЯМИ УДОСКОНАЛЕННЯ ЗАХОДІВ ЗАХИСТУ ДЕРЖАВНИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ У СФЕРІ КІБЕРБЕЗПЕКИ

3.1. Методика експертного оцінювання функціональних профілів загроз державних інформаційних ресурсів

Методика експертного оцінювання функціональних профілів загроз державних інформаційних ресурсів методика призначена для уточнення функціональних профілів (ФП) загроз державним інформаційним ресурсам (ЗДІР), які були визначені в розрізі побудови класифікатора загроз у роботах [61; 62; 64]. Безпосередньо методологія побудови класифікатора ЗДІР була розглянута в праці [65].

Як зазначалося в роботах [61; 62; 64], авторами була розглянута класифікація ЗДІР нормативно-правового, організаційного та інженерно-технічного спрямування. Надалі кожна загроза була віднесена: за джерелом загрози (антропогенні, техногенні, стихійні); за відношенням до інформаційного об’єкта (внутрішні, зовнішні); за характером загрози (навмисні, ненавмисні); за структурою впливу (системні, структурні, елементні); за рівнем впливу (фізичні засоби, мережеве обладнання, мережеві додатки та сервіси, операційна система, системи управління базами даних). Загалом це складає ФП ЗДІР за відповідним спрямуванням.

Нижче наведена безпосередньо методика експертного оцінювання ФП ЗДІР, яка полягає в такому:

1. Складання таблиць опитування експертів, які відповідають будові класифікаторів загроз ДІР нормативно-правового, організаційного та інженерно-технічного спрямування (були наведені в роботах [61; 62; 64]).

2. Формування складу експертної групи.

3. Проведення експертизи (заповнення таблиць опитування).

4. Аналіз експертної інформації (аналіз узгодженості відповідей експертів).

5. Прийняття рішення щодо оцінювання ФП ЗДІР з урахуванням експертного оцінювання.

Розглянемо докладніше кожен із етапів методики.

1. *Складання таблиць опитування експертів.*

Для складання таблиць опитування експертів використаємо анкетування, що припускає письмову відповідь експерта на систему запитань [7]. Приклад таблиці опитування для одного експерта наведено в таблиці 3.1.

Таблиця 3.1

Таблиця опитування

Функціональний профыль загроз	Джерело загроз			Відносно до інформаційного об'єкта		Характер загроз		Загрози за структурою вплив			Рівні впливу загроз				
	Антропогенні	Техногенні	Стихійні	Внутрішні	Зовнішні	Навмисні	Ненавмисні	Системні	Структурні	Елементні	Фізичні засоби	Мережеве обладнання	Мережеві додатки	Операційна система	Системи управління базами даних
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

Примітка. Складено автором.

Пропонується використовувати закриті питання, а саме відповіді у формі «так» — експерт ставить 1, або «ні» — експерт ставить 0.

У даному випадку експерти добре розуміють питання, експертиза проводиться оперативно, експерти добре розуміють поставлене завдання та впевнено працюють.

Ця форма використовується у зв'язку з тим, що набір альтернатив достатньо очевидний.

2. *Формування складу експертної групи.*

Є різні підходи до обирання кількості експертів у складі робочої групи. Розглянемо деякі загальноприйняті підходи [34; 60]:

− кількість експертів (m) повинна бути не менше числа факторів (n) або варіантів, які необхідно оцінити експертним шляхом ($\geq nm$). Даний підхід не підходить, оскільки кількість альтернативних відповідей, запропонованих експерту, всього дві: так чи ні;

− кількість експертів можна визначати за такою формулою:

$$m \geq b +)5/33,0(5,0 , \qquad (3.1)$$

де b — помилка результату експертного аналізу або допустимаймовірність помилки ($b << 10$) [34].

У праці [122] наведено іншу формулу:

$$m = \alpha + 0,5(3/ 5) , \qquad (3.2)$$

тут α — параметр, який задає мінімальний рівень помилки експертизи (допустима ймовірність помилки) та лежить у межах $0\ 1 < \alpha \leq$.

У формулах (3.1) та (3.2) параметр b та α визначають відсутність помилки (значення дорівнюються нулю), 100 % помилка (значення дорівнює одиниці).

При цьому повинна спостерігатися стабілізація середньої оцінки характеристики, що прогнозується.

Про досягнення цієї стабілізації свідчить той факт, що включення або виключення експерта із групи не змінює відносну оцінку вихідної величини більш ніж на або виключення експерта із групи не змінює відносну оцінку вихідної величини більш ніж на b (α) [26].

Як бачимо дані формули схожі, але дають різні результати (табл. 3.2, 3.3).

Так, за допустимої помилки експертного аналізу в 5 % (b = 05,0 або α = 0,05) до складу робочої групи має входити не менше шести осіб за формулою (3.1) і не менше 33 за формулою (3.2). Але під час перевірки посилання в праці [34] щодо правильності формули (3.1) виявляється, що була допущена помилка. Посилаючись на працю [26, С. 158], формула ідентична (3.2). Та сама помилка і в праці [60, С. 156], де також наведена формула (3.1), але посилання йде на працю [26].

Таблиця 3.2

Таблиця розрахунку кількості експертів за формулою (3.1)

Помилка	0,05	…	0,1	0,2	0,3	0,4	0,5	0,6	0,7	0,8	0,9	1
Кількыість експертів	5,8	…	4,15	3,33	3,05	2,91	2,83	2,78	2,74	2,71	2,69	2,67

Примітка. Складено автором.

Таблиця 3.3

Таблиця розрахунку кількості експертів за формулою (3.2)

Помилка	0,05	…	0,1	0,2	0,3	0,4	0,5	0,6	0,7	0,8	0,9	1
Кількыість експертів	32,5	…	17,5	10	7,5	6,25	5,5	5	4,64	4,38	4,17	4

Примітка. Складено автором.

Таким чином, кількість експертів необхідно визначати виходячи.

Надалі необхідно, знаючи категорію експертів, врахувати їх компетентність. Рівень компетентності експертів робочої групи *M* повинен відповідати таким вимогам [15]:

$$0{,}67 \leq M \leq 1{,}00 \qquad (3.3)$$

При цьому значення *M* розраховується за такою формулою:

$$\text{М}=\frac{1}{m}*\sum_{j=1}^{m} K_j, \qquad (3.4)$$

де m — кількість експертів у складі робочої групи; $K\ j$ — рівень компетентності j -го експерта.

Для проведення експертизи були задіяні експерти з державної установи. Отже, знаючи категорії задіяних експертів, можна їх компетентність визначити таким чином (табл. 3.4).

Отримаємо за формулою (3.4) значення рівня компетентності робочої групи. Виходячи із кількості експертів *(m* — 17), які розбиті за категоріями коефіцієнтів компетентності експертів (табл. 3.4) значення M — 0,76 , що відповідає умові (3.3).

Таблиця 3.4

Визначення коефіцієнта компетентності експертів з урахуванням їх категорії (рівня професійної підготовки та інформованості)

Номер з/п	Кваліфікація експертів	Значення коефіцієнта компетентності, к	Кількість задіяних експертів
1	Керівник	1	2
2	Заступник керівника	0,95	2
3	Начальник відділу	0,9	3
4	Спеціаліст	0,85	5
5	Інженер зі стажем роботи більше 20 років	0,8	1
6	Інженер зі стажем роботи від 15 до 20 років	0,7	1
7	Інженер зі стажем роботи від 10 до 15 років	0,6	1
8	Інженер зі стажем роботи від 5 до 10 років	0,5	2

Примітка. Складено автором.

Перевіримо кількість визначених експертів способом, наведеним в праці [34]. Відповідно до нього кількість експертів рекомендується визначати за формулою:

$$m \le \frac{3}{2 * Q_{\max}} * \sum_{i=1}^{m^*} Q_i \ , \qquad (3.5)$$

де Q_{max} — максимально можлива компетентність i -го експерта;

m^* — кількість експертів у попередньо сформованій групі; Q_i — компетентність i -го експерта, яка оцінюється в балах (рекомендується від 1 до 5).

Для цього значення коефіцієнтів компетентності, які наведені в табл. 3.4 нормуємо в межах від 1 до 5 (табл. 3.5).

Розраховуючи за формулою (3.5) отримаємо значення $m < 20{,}925$, тобто кількість експертів у нашому випадку може знаходитися в інтервалі від 17 до 21, що не суперечить раніше визначеній кількості.

У праці [34] наведено підхід з використанням теорії ймовірності та математичної статистики. Згідно з даним підходом склад експертної групи має бути в межах від 11 до 21 особи, що також не суперечить раніше визначеній кількості експертів.

Таблиця 3.5

Нормовані коефіцієнти компетентності експертів

Номер з/п	Кваліфікація експертів	Нормоване значення коефіцієнта компетентності, O_I	Кількість задіяних експертів
1	Керівник	5	2
2	Заступник керівника	4,75	2
3	Начальник відділу	4,5	3
4	Спеціаліст	4,25	5
5	Інженер зі стажем роботи більше 20 років	4	1
6	Інженер зі стажем роботи від 15 до 20 років	3,5	1
7	Інженер зі стажем роботи від 10 до 15 років	3	1
8	Інженер зі стажем роботи від 5 до 10 років	2,5	2

Примітка. Складено автором.

Необхідно зауважити, що підбір кількісного та якісного складу експертів здійснюється на основі масштабів проблеми, що вивчається, достовірності оцінок, характеристик експертів та витрат ресурсів. Отже, мінімальна кількість експертів визначається кількістю різних аспектів, спрямувань, які необхідно врахувати. У зв’язку із цим, не завжди є правильним судження, що як видно з табл. 3.5 при обиранні групи експертів з чотирьох осіб допустима ймовірність помилки буде становити 1. В разі призначення коефіцієнта компетентності всім чотирьом експертам, чи ще меншій кількості експертів значення 1 (найбільше значення), можна стверджувати, що допустима ймовірність помилки буде

прагнути до 0.

3. Проведення експертизи (заповнення таблиць опитування).

Під час заповнення таблиць опитування необхідно встановити рівень взаємодії між експертами. Відповідно до праці [7], виділяють три рівні взаємодії:

1. Експерти можуть вільно обмінюватися інформацією один з одним.
2. Обмін інформацією між експертами регламентований.
3. Експерти ізольовані один від одного.

Для проведення експертизи оцінювання функціональних профілів загроз державних інформаційних ресурсів з урахуванням категорій експертів, наведених в табл. 3.4, доцільно ізолювати експертів один від одного. Як уже зазначалося, таблиці заповнюються шляхом віднесення (1) чи невіднесення (0) вказаного параметра до визначеного функціонального профілю загроз ДІР (приклад заповнення для функціонального профілю ЗДІР нормативно-правового спрямування наведено в Додатку Б).

Категорія експерта вказується обов'язково. Для подальшого визначення коефіцієнта компетентності

4. *Аналіз експертної інформації.*

Є три основні групи методів обробки експертної інформації: статистичні методи, алгебричні методи та методи шкалірування [7].

Аналіз найбільш розповсюджених методів аналізу експертних оцінок наведено в праці [35]. Здійснюючи оцінювання ФП ЗДІР, доцільно використати статистичні методи. В даному випадку достатньо застосувати метод чисельної оцінки, результуючі оцінки, за яким визначаються за формулою методу середньозважених.

Оскільки результатами опитування експертів є декілька думок x_i, $i = 1, m$, то результуюча оцінка визначається за формулою:

$$\varphi\,(x_1,x_2,\ldots,x_m)=\frac{\sum_{i=1}^{m} x_i k_i}{\sum_{i=1}^{m} k_i}, \qquad (3.6)$$

де ф(x_1, x_2,..., $x_т$) — результуюча оцінка; m — кількість експертів

(визначено під час формування складу експертної групи); x_i — оцінка i -го експерта; κ_i — вага i -го експерта (визначено під час формування складу експертної групи).

Ступенем узгодженості думок експертів є дисперсія результуючої оцінки, яка визначається згідно з виразом:

$$\sigma_x^2 = \frac{\sum_{i=1}^{m} \left(\varphi(\chi_1, \chi_2, ..., \chi_m) - \chi_i\right)^2 k_i}{\sum_{i=1}^{m} k_i}. \qquad (3.7)$$

Визначимо статистичну значимість отриманих результатів. Якщо задатись імовірністю помилки $P_{\text{пом}}$, то інтервал, у який оцінювана величина потрапить з імовірністю 1 -$P_{\text{пом}}$, становитиме:

$$\varphi(x_1, x_2, ..., x_m) - \Delta \le \varphi(x_1, x_2, ..., x_m) \le \varphi(x_1, x_2, ..., xm) + \Delta, \qquad (3.8)$$

рахується, що величина $\varphi(x_1, x_2, ..., x_m)$ розподілена нормально з центром $\varphi(x_1, x_2, ..., x_m)$ та дисперсією (3. 6).

Тоді

$$\Delta = t\sqrt{\sigma^2/m}, \qquad (3.9)$$

де величина t має розподіл Стьюдента з $m-1$ степенями вільності.

Її визначають за таблицею, задавши величину $P_{\text{пом}}$.

Розглянемо приклад розрахунку за одним із показників елементу функціонального профілю.

Нехай експерти провели оцінювання ФП ЗДІР НПС за відношенням до антропогенного джерела загрози (табл. 3.7). Результуюча оцінка, яка розрахована за формулою (3.6) становить $\phi = (x_1, x_2, ..., x_m) = 0{,}83$, з дисперсією $\sigma = 2 \times 0{,}14$. Задавши ймовірність помилки $P_{\text{пом}} = 0{,}01$, за таблицями розподілу Стьюдента визначимо величину t : кількість степенів вільності дорівнює 16;

$t = 1{,}7458837$. За формулою (3.9) $\Delta = 16{,}0$. Отже, з імовірністю 0,9 величина $\phi(x_1, x_2, ..., x_m)$ знаходиться в інтервалі [0,67; 0,99], що характеризує ймовірність результату.

Таблиця 3.7

Приклад узагальнення оцінок, отриманих від експертів

Номер з/п	Категорія експерта (за табл. Д4.4)	Коефіцієнт компетентності (за табл. 3.4)	Оцінка відношення ФП до антропогенного джерела загроз
1	Керівник	1	1
2	Керівник	1	1
3	Заступник керівника	0,95	1
4	Заступник керівника	0,95	1
5	Начальник відділу	0,9	1
6	Начальник відділу	0,9	1
7	Начальник відділу	0,9	1
8	Спеціаліст	0,85	1
9	Спеціаліст	0,85	1
10	Спеціаліст	0,85	0
11	Спеціаліст	0,85	1
12	Спеціаліст	0,85	1
13	Інженер зі стажем роботи більше 20 років	0,8	0
14	Інженер зі стажем роботи від 15 до 20 років	0,7	0
15	Інженер зі стажем роботи від 10 до 15 років	0,6	1
16	Інженер зі стажем роботи від 5 до 10 років	0,5	1
17	Інженер зі стажем роботи від 5 до 10 років	0,5	1

Примітка.

5. *Прийняття рішення щодо оцінювання ФП ЗДІР з урахуванням експертного оцінювання.*

Для прийняття рішення використаємо ступінь узгодженості думок експертів — дисперсію, величина якої не повинна перевищувати 0,3 та мінімальне значення граничної інтервальної оцінки, величина якої повинна

відповідати $\varphi(x_1,x_2,...,x_m)-\Delta\geq 0,5$.

Отже, повертаючись до розглянутого вище прикладу, можна стверджувати, що оцінку відношення ФП до антропогенного джерела загроз буде визначено 1, оскільки $\sigma^2_x \leq 0{,}14$ та $\varphi(x_1, x_2,..., x_m)-\Delta = 0{,}67$ більше ніж 0,5.

3.2. Рекомендації щодо підвищення рівня захищеності інформаційних ресурсів при віддаленій роботі співробітників установи

В сьогоднішніх змінах і умовах необхідність соціального дистанціювання сприяє масовому переходу до віддаленої роботи. 85 % компаній, опитаних каналом CNBC, заявили, що більше половини їх співробітників тепер працюють віддалено. Однак є свідчення того, що віддалена робота відкриває нові унікальні можливості для кіберзлочинців.

З переходом до віддалених операцій існує ряд ризиків і загроз безпеці центральних та місцевих органів, інших державних органів, органів місцевого самоврядування, підприємств, установ, організацій та їх конфіденційної інформації. В результаті, хоча установи працюють над розширенням і підвищенням ефективності віддаленої роботи в реальному часі через Інтернет, вони також повинні зосередитися на поліпшенні кібербезпеки в цілому і віддалено працюючого кожного співробітника.

Однак така форма роботи піддає інформаційні та телекомунікаційні системи і державні інформаційні ресурси, оброблювані в них, до підвищеного ризику і, в крайній мірі, збільшує ризик кібербезпеки:

1. відключення цих систем або неможливість їх нормальної роботи; несанкціонований витік, зміна і знищення державних інформаційних ресурсів;

2. несанкціоноване вторгнення третіх осіб і установка виконавчих модулів для шкідливого ПО і т. д.

Ми вважаємо, що терміново потрібні додаткові заходи кібербезпеки, щоб запобігти реалізації цих ризиків кібербезпеки щодо державних інформаційних ресурсів і систем, де вони обробляються при організації віддаленої роботи співробітників.

Далі на рис. 3.1 ми представимо ряд рекомендацій щодо додаткових заходів по забезпеченню кіберзахисту інформаційних і телекомунікаційних систем підприємств, установ, організацій і т. д.

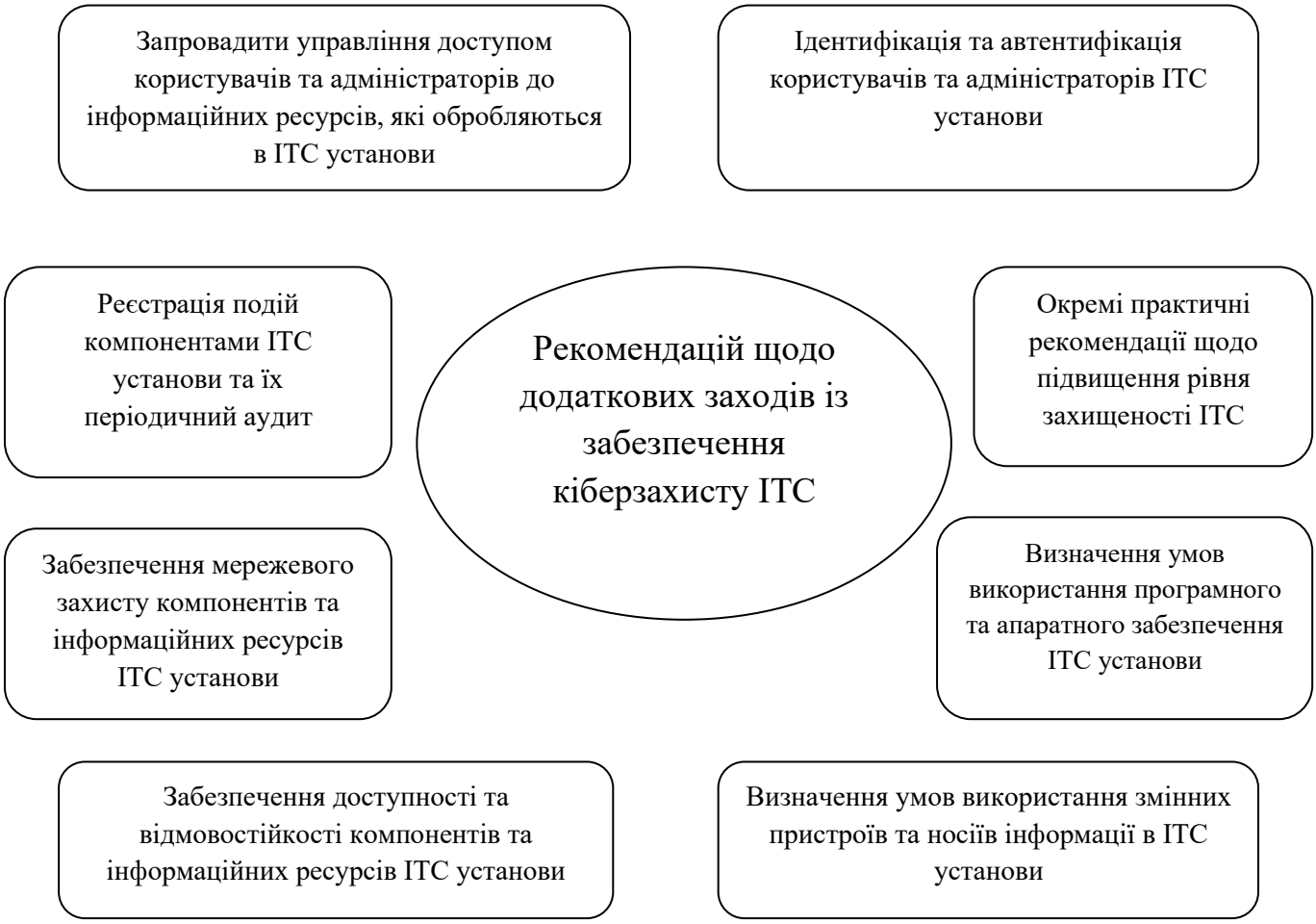

Рис. 3.1. Рекомендацій щодо додаткових заходів із забезпечення кіберзахисту ІТС.

Примітка. Складено автором.

Опишемо більш детально деякі рекомендації щодо заходів захисту інформаційних і телекомунікаційних систем підприємств, установ, організацій і т. д. в мережі Інтернет:

1. Введення контролю доступу користувачів і адміністраторів до інформаційних ресурсів, оброблюваних в інформаційно-телекомунікаційних системах установи.

1.1 Механізми призначення прав доступу до інформаційних ресурсів повинні:

- охоплювати всі інформаційні ресурси інформаційних і телекомунікаційних систем установи (інформація, що зберігається і обробляється в інформаційних і телекомунікаційних системах, технологічна інформація програмного і апаратного забезпечення інформаційно-телекомунікаційних систем, журнали подій і т. д.);

- визначення прав на виконання операцій для всіх користувачів і адміністраторів (при необхідності також активних процесів) над інформаційними ресурсами інформаційних і телекомунікаційних систем об'єкта (читання, зміна, створення, видалення і т. д.);

- при необхідності визначити права доступу користувачів і адміністраторів до сервісів (функцій) інформаційно-телекомунікаційних систем об'єкту.

1.2 Інформаційні та телекомунікаційні системи повинні по можливості віддавати пріоритет централізованому поширенню інформації про налаштування прав доступу і атрибутів, параметрів реєстрації подій, інших параметрів безпеки і системних настройок компонентів системи.

2. Ідентифікація та аутентифікація користувачів і адміністраторів інформаційних і телекомунікаційних систем на об'єкті.

2.1 Учасники та адміністратори інформаційних і телекомунікаційних систем об'єкта (можливо, також активні процеси) повинні отримувати доступ до послуг (функцій), інформації та компонентів систем тільки після успішного проходження процесу аутентифікації на основі унікального персоналізованого ідентифікатора в рамках зазначених ними прав доступу і деяка інформація, введена користувачем (пароль) і/або фізичний ідентифікатор (ключ, сертифікат, токен і т. д.), наданий користувачем. Користувачі та адміністратори повинні використовувати надійні паролі, які містять не менше 8 символів, цифр і букв в різних регістрах. Змінювати паролі не рідше одного разу в тиждень.

2.2 Інформаційні ресурси та телекомунікаційні системи об'єкта повинні дозволяти визначати роботу користувачів і адміністраторів інформаційних і телекомунікаційних систем і їх реєстрацію в журналах подій.

2.3 Для забезпечення доступу до послуг (функцій) і інформації з інформаційних та телекомунікаційних систем об'єкту користувачі і адміністратори повинні віддавати перевагу використанню багатофакторної аутентифікації.

2.4 У інформаційних і телекомунікаційних системах об'єкта облікові записи адміністраторів за замовчуванням і їх паролі повинні бути заблоковані або змінені у всіх компонентах систем. Заборонено використання стандартних облікових записи і паролів в програмних і апаратних інформаційних і телекомунікаційних системах.

2.5 У інформаційних і телекомунікаційних системах неперсоналізовані і гостьові облікові записи користувачів і адміністраторів повинні бути видалені або заблоковані, і тільки персоналізовані облікові записи користувачів і адміністраторів можуть використовуватися у всіх компонентах системи. У разі звільнення, переведення і т. д. обліковий запис співробітника повинен бути негайно заблокований, видалений або його права доступу змінені відповідно до нової посади в усіх компонентах інформаційно-телекомунікаційних систем.

3. Реєстрація подій компонентами інформаційно-телекомунікаційних систем інституту і їх регулярна перевірка.

3.1 Журнали подій (логи) компонентів інформаційної та телекомунікаційної системи повинні містити інформацію про дату, час, місце розташування, тип і успішності або невдачі кожної зареєстрованої події. Журнали повинні містити достатньо інформації для ідентифікації користувача, процесу і мережевого об'єкта, які мали відношення до кожної зареєстрованої події.

3.2 Системні адміністратори повинні регулярно переглядати журнали подій (логів) компонентів інформаційної та телекомунікаційної системи Інституту для виявлення можливих атак або сканування, а також інших подій, які можуть бути пов'язані з інформаційною безпекою.

3.3 Журнали подій (логи) компонентів інформаційних і телекомунікаційних систем об'єкта повинні архівуватися і зберігатися не менше одного року з моменту їх архівування.

4. Забезпечення мережевого захисту компонентів та інформаційних ресурсів інформаційних і телекомунікаційних систем об'єкту.

4.1 Інформаційні та телекомунікаційні системи об'єкта, включаючи віддалені робочі станції користувачів і системних адміністраторів, повинні використовувати засоби захисту від шкідливого коду, шкідливого програмного забезпечення і вірусів (антивірусне програмне забезпечення або інші засоби, які містять такі функції з останніми оновленнями).

4.2 Адміністратори і користувачі зі своїх робочих станцій, які хочуть отримати доступ до компонентів інформаційних і телекомунікаційних систем, повинні отримувати доступ тільки з певних IP-адрес.

4.3 На кордоні (області) інформаційних і телекомунікаційних систем об'єкту між Інтернетом, зовнішніми мережами і системами об'єкта повинні бути встановлені Інструменти мережевої безпеки (IDS, IPS, міжмережевий екран і т. д.), які виконують як мінімум наступні функції безпеки :

- захист від атак нульового дня (уразливості програмного забезпечення, які ще не відомі користувачам або розробникам програмного забезпечення і проти яких ще не розроблені механізми захисту), виявлення шкідливого коду і шкідливих програм;

- фільтрація трафіку і розмежування доступу між Інтернетом, зовнішніми мережами і системами об'єктів на основі критеріїв дозволених і заборонених послуг, протоколів, портів, мережевих адрес, здійснювати підключення до мережі, небажаних веб-сайтів і т. д. Блокування трафіку і підключення, що не відповідають певним критеріям.

- захист від атак типу «відмова в обслуговуванні» та інших відомих мережевих атак;

- фільтрація і аналіз трафіку відповідно до критеріїв, визначених у відповідності до Директиви про інформаційну безпеку;

- моніторинг трафіку даних на наявність шкідливого коду, шкідливих програм, вірусів і інших критеріїв, що визначаються відповідно до рекомендацій з інформаційної безпеки;

- виявлення та запобігання атак і втручань в програмні і апаратні компоненти, а також інформацію про інформаційних - телекомунікаційних системах об'єкта;

- захист від несанкціонованого доступу через Інтернет;

- балансування навантаження;

- маскування структури і мережевих адрес мережі;

- припинення підключення до вузла в разі атаки;

- реєстрація подій, пов'язаних з безпекою;

- інші функції, визначені в політиці безпеки установи.

4.4. Для захисту інформаційних і телекомунікаційних систем об'єкта слід використовувати програмне і апаратне забезпечення, пропускна здатність якого визначається виходячи з наявної пропускної здатності мережі з урахуванням їх потенційного збільшення.

4.5 У інформаційних і телекомунікаційних системах об'єкта необхідно розподілити системи об'єкта на фізичному і / або логічному рівні (сегментація мережі) і обмежити доступ між сегментами мережі за допомогою міжмережевих екранів або аналогічних функцій захисту мережі.

4.6 Реалізована архітектура інформаційних і телекомунікаційних систем об'єкта повинна дозволяти розділяти мережі об'єкта на наступні частини / зони (віртуальні підмережі):

зовнішня зона (DMZ zone): зона з адресними зонами зовнішньої мережі для розміщення зовнішніх (загальнодоступних) інформаційних ресурсів і сервісів інформаційних і телекомунікаційних систем;

область застосування інформаційних і телекомунікаційних систем (зона APP): захищена внутрішня область з внутрішньої адресацією для розміщення серверів додатків, доступна для задоволення функціональних вимог користувачів інформаційних послуг;

зона зберігання даних інформаційно-телекомунікаційних систем (БВ-zone): захищена внутрішня зона з внутрішньої адресацією, призначена для розміщення баз даних, для доступу до запитів з прикладних програм зони (APP-zone);

область застосування безпеки (8esigiyu-gope): захищена внутрішня область з внутрішньої адресацією, в якій розташовуються служби та служби захисту інформації;

тестова зона: захищена внутрішня зона з внутрішньої адресацією, яка призначена для тестування нових компонентів і / або оновлення програмного і апаратного забезпечення інформаційних і телекомунікаційних систем перед їх комерційною експлуатацією в інформаційних і телекомунікаційних системах.

Список частин / зон мережі, в яких вони розподілені, може відрізнятися від наведеного розподілу, в залежності від функцій і структури мережі установи.

5. Забезпечення доступності та відмовостійкості компонентів та інформаційних ресурсів інформаційно-телекомунікаційних систем об'єкту.

5.1 Використання флеш і інших типів знімних носіїв на робочих станціях користувачами і адміністраторами інформаційних і телекомунікаційних систем на об'єкті повинно бути заборонено або, в крайньому разі, зведено до мінімуму.

5.2 Робочі місця користувачів і адміністраторів інформаційних і телекомунікаційних систем об'єкта не повинні бути доступні для членів сімей персоналу об'єкта.

6. Визначення умов використання змінних (зовнішніх) пристроїв і носіїв інформації в інформаційно-телекомунікаційній системі об'єкта.

6.1 У інформаційних і телекомунікаційних системах об'єкта, включаючи віддалені робочі станції користувачів і системних адміністраторів, все знімні (зовнішні) пристрої і носії інформації повинні бути перевірені на наявність зловмисного коду, шкідливих програм і вірусів (антивірусне програмне забезпечення або інші інструменти), які мають такі функції, перед будь-яким використанням з останніми оновленнями своїх антивірусних баз).

6.2 У інформаційних і телекомунікаційних системах об'єкта, в тому числі на віддалених робочих місцях користувачів і системних адміністраторів, слід відключити автоматичний запуск програм зі змінних (зовнішніх) пристроїв і носіїв інформації.

6.3 Порти компонентів мережевих пристроїв, робочих станцій і серверів, які не використовуються, повинні бути заблоковані адміністраторами цих систем.

7. Визначення умов використання програмно-технічних засобів інформаційно-телекомунікаційних систем об'єкту.

7.1 Цілісність та справжність оновлень компонентів інформаційних і телекомунікаційних систем інституту повинні перевірятися в інформаційних і телекомунікаційних системах інституту. У разі порушення цілісності або неможливості підтвердити справжність поновлення, воно буде відхилено і не буде застосовуватися.

7.2 Інформаційні та телекомунікаційні системи підприємства, включаючи робочі станції віддалених користувачів і адміністраторів, використовують програмне, програмно апаратне забезпечення та обладнання, підтримка яких не припинена виробником. Необхідно використовувати офіційні стабільні версії прикладного програмного забезпечення та драйверів. Все програмне забезпечення повинно регулярно оновлюватися, щоб включати останні оновлення та виправлення, в тому числі останні критичні оновлення та оновлення безпеки, від виробників цього програмного забезпечення та мікропрограм.

7.3 Програмне і апаратне забезпечення, яке використовується в інформаційних і телекомунікаційних системах об'єкта, включаючи віддалені робочі станції користувачів і адміністраторів, не повинно відбуватися або розроблятися в іноземній державі, щодо якої були накладені санкції відповідно до Закону України «Про санкції», чи були зроблені юридичною особою - резидентом такої іноземної держави або юридичною особою, частка статутного капіталу якого належить вказаному іноземній державі, або юридичній особі, яка перебуває під контролем юридичної особи цієї іноземної держави.

8. Деякі практичні рекомендації щодо підвищення безпеки інформаційних і телекомунікаційних систем на об'єкті.

8.1 Організація процесу моніторингу наявності вразливостей безпеки в активних мережах, серверних пристроях і робочих станціях користувачів інформаційно-телекомунікаційних систем об'єкту.

8.2 Впровадження системи моніторингу працездатності мережі, серверного обладнання інформаційно-телекомунікаційних систем об'єкта і каналів зв'язку; як варіант використовувати функції протоколу SNMP.

8.3 Для запобігання атак типу Man-in-the-Middle з використанням методів ARP- spoofmg приймати заходи по налаштуванню статичних значень ARP-таблиць робочих станцій і серверного обладнання інформаційно-телекомунікаційних систем установи.

8.4 Вжити заходів для запобігання використанню стороннього програмного забезпечення в інформаційних і телекомунікаційних системах.

8.5 Зв'язати MAC-адреси комп'ютерів співробітників з конкретним інтерфейсом комутатора і тим самим уникнути підключення сторонніх комп'ютерів.

Ще одна рекомендація - зробити пріоритетними зовнішні служби управління кібербезпекою. Професійний постачальник – провайдер пропонує якісні послуги, яка забезпечується Угодою про рівень обслуговування, і у клієнта є можливість змінити конфігурацію послуги або тимчасово розширити обсяг послуг кібербезпеки.

Отже, визначення боротьби із загрозами безпеці в інформаційних системах є складним завданням, що вимагає поєднання заходів на правовому, адміністративному, процедурному та програмному рівнях ІБ.

Розробка і прийняття нормативних актів в області захисту інформації спрямоване на регулювання безпечного використання інформаційних та комунікаційних технологій, доступу до інформації, захисту інформації від несанкціонованого доступу і передачі по технічних каналах.

ІБ повинна враховувати поточний стан і найближчі перспективи розвитку інформаційних технологій, мета, завдання, правову основу для роботи інтелектуальної власності, функціонування об'єктів, аналіз загроз безпеки і способи їх реалізації. Програмно-технічний рівень боротьби з загрозами ІБ

включає механізми безпеки, такі як ідентифікація і аутентифікація користувачів, управління доступом по ІС, ведення журналів і тестування, криптографія, захист каналів зв'язку, забезпечення високої доступності і т. д.

ВИСНОВКИ

У магістерській роботі наведено вирішення важливого науково-практичного завдання, що полягає в аналізі та обґрунтуванні напрямів удосконалення заходів захисту державних інформаційних ресурсів у сфері кібербезпеки. Отримані в процесі дослідження результати дають змогу сформулювати такі висновки:

Розкрито суть поняття "інформаційна безпека", яке набагато ширше за поняття безпеки інформації і аж ніяк не зводиться до нього. Наразі тема щодо безпеки у кіберпросторі є найпоширенішою і найбільш затребуваною суспільством, оскільки це стосується кожного, хто стикається зі світом інформаційних технологій.

Визначено, що законодавче регулювання кібербезпеки в Україні знаходиться на початку свого створення, але найскладніший етап - визначення стратегії, меж і напрямів державної політики кібербезпеки пройдено. Ще є багато проблем, але є і досягнення. Невирішені питання державно-приватного співробітництва, ще не сформульовані списки об’єктів критичної інфраструктури та інші, розробка підходів до кіберзахисту, попереду великий пласт проблем і обсяг роботи спрямованої на нормативно-правове врегулювання в сфері кібербезпеки.

Охарактеризовано діяльності суб’єктів національної системи кібербезпеки і виявили, що переваги сучасного цифрового світу і розвиток інформаційних технологій привели до появи нових загроз національній і міжнародній безпеці. Тому для її захисту крім відповідних підрозділів збройних сил, повинні бути включені збройні сили і ресурси державної спеціальної служби, служба безпеки, служба охорони державного кордону, національна гвардія, національна поліція і спецслужби, яким доручено забезпечувати державну оборону.

Аналіз сучасного стану кіберзлочинів в Україні показав, що за останні п’ять років в Україні кількість інформаційних злочинів зросла щонайменше у 2,5 рази. За перше півріччя 2020 року Держспецзвязок, зокрема система кіберзахисту державних інформаційних ресурсів та об’єктів критичної

інфраструктури на об’єктах моніторингу зафіксував 26017752 підозрілих подій, що на 11% більше, ніж попереднього року. Переважна більшість зафіксованих підозрілих подій стосується спроб мережевого сканування (91%), застосування нестандартних протоколів (7%) та виявлення мережевого ШПЗ (1%).Система захищеного доступу державних органів до мережі Інтернет заблокувала 1088712 атак різних видів, що на 22% більше, ніж попереднього року.

Запропоновано ряд рекомендацій щодо додаткових заходів по забезпеченню кіберзахисту інформаційних і телекомунікаційних систем підприємств, установ, організацій і т. д. Розробка і прийняття нормативних актів в області захисту інформації спрямоване на регулювання безпечного використання інформаційних та комунікаційних технологій, доступу до інформації, захисту інформації від несанкціонованого доступу і передачі по технічних каналах.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Антивірус український. URL: https://zillya.ua/

2. Бакалинський О.О. «Інформаційний бліцкриг». Правова інформатика, № 2(42)/2014, UPL.: http://ippi.org.ua/sites/default/files/14booib.pdf. (дата звернення 02.09.2019).

3. Біла книга. Пропозиції до політики щодо реформування сфери кібербезпеки в Україні. Матеріал для обговорення (Policy Paper) - UPL: parlament.org.ua › 2017/12 › au_White-book-on-cybersecurity-draft_5. (дата звернення 02.09.2019).

4. Бебик В.М. Інформаційно-комунікаційний менеджмент у глобальному суспільстві: психологія, технології, техніка паблік рилейшнз: монографія. К.: МАУП, 2005

5. Бородакий Ю.В., Добродеев А.Ю., Бутусов И.В. Кибербезопасность как основной фактор национальной и международной безопасности XXI века (часть 2). Вопросы кибербезопасности №1(2). 2014 . С. 5-12.

6. Бучик С. С., Кондратенко С. О., Писарчук О. О. Системи підтримки прийняття рішень : конспект лекцій / С. С. Бучик,. Житомир : ЖВІРЕ, 2006. 168 с.

7. Використання інформаційно-комунікаційних технологій на підприємствах України. Статистичний бюлетень за 2019 р. Київ. Державна служба статистики в Україні, 2020. 39 с.

8. Вимоги до незалежного тестування інформаційної безпеки на об’єктах критичної інфраструктури та процедура для незалежного тестування інформаційної безпеки на об'єктах критичної інфраструктури

9. Всесвітнє дослідження економічних злочинів та шахрайства 2018: результати опитування українських організацій. Виведення шахрайства з тіні. URL: https://www.pwc.com/ua/uk/survey/2018/economic-crime-survey.html

10. ДСТУ ISO/IEC 27032:2016 (ISO/IEC 27032:2012, IDT) «Інформаційні технології. Методи захисту. Настанови щодо кібербезпеки». 27.12.2016. № 448 http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=69128 (дата звернення 02.09.2019).

11. Дубов Д.В. Державно-приватне партнерство у сфері кібербезпеки: міжнародний досвід та можливості для України : аналіт. доп. / за заг. ред. Д. Дубова. – К. : НІСД, 2018. – 84 с.

12. Ибрагимова Г. Стратегия КНР в киберпространстве: вопросы управления интернетом и обеспечение информационной безопасности. *Индекс безопасности.* 2013. № 1 (104). С. 169 -184.

13. Інформаційна кібербезпека: соціотехнічний аспект: підручник / В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа. Київ: ДУТ, 2015. 288с.

14. Каратанов А. В. Информационные технологии экспертного оценивания проектных решений при формировании единого информационного пространства. *Збірник наукових праць Харківського університету повітряних сил*. 2014. №3(40). С. 155–160.

15. Кібербезпека: віртуальна зброя держави. URL: https://biz.nv.ua/ukr/experts/kutsenko1/kiberbezpeka-zbroja-derzhavi-u-virtualnijploshchini-2014774.html. (дата доступу – 10.01.2018).

16. Клименко А. Правовые аспекты кибербезопасности бизнеса - URL: https://cpk.ua/publications/articles/full/pravovyye-aspekty-kiberbezopasnosti-biznesa-2/ (дата звернення 02.09.2019).

17. Коваленко Н. В. Про правовий режим кібербезпеки в Україні. Актуальні проблеми вітчизняної юриспруденції. 2016. № 3. С. 96–100.

18. Коломієць О. В. Проблеми національного законодавства в сфері боротьби з кіберзлочинністю та шляхи їх вирішення. Гілея. 2012. Вип. 57 (№ 2). С. 546–551.

19. Конституція України: закон України від 28.06.1996 № 254к/96-ВР *Відомості Верховної Ради України (ВВР*), 1996, № 30, ст. 141.

20. Кормич Б. А. Інформаційне право. Х.: БУРУН і К, 2011. 334 с.

21. Кормич Б. А. Організаційно-правові засади політики інформаційної безпеки України. *Одеська національна юридична академія*. О.: Юридична література, 2003. – 471 с.

22. Кузьменко Б. В. Інформаційна диверсія та інформаційний саботаж інструменти кібертероризму. Роль правоохоронних органів у формуванні

правової держави в умовах євроінтеграції України: матеріали Всеукр. підсумк. наук.-практ. конф. (м. Київ, 12 березня 2015 р.). Київ: Нац. акад. внутр. справ, 2015. Ч. 1. С. 20–22.

23. Ліпкан В. А. Правові засади розвитку інформаційного суспільства в Україні: [монографія] / за заг. ред. В. А. Ліпкана. К. : ФОП О. С. Ліпкан, 2015. – 664 с.

24. Лук'янчук Р. В. Державна політика у сфері забезпечення кібернетичної безпеки в умовах проведення антитерористичної операції. *Вісник Національної академії державного управління при Президентові України.* 2015. № 3. С. 110–117.

25. Лукичева Л. И. Управленческие решения : учеб. по спец. «Менеджмент организации» / под ред. Ю. П. Анискина. М. : «Омега-Л», 2009. 383 с.

26. Малик Я. Інформаційна війна і Україна. Демократичне врядування. 2015. - Вип. 15. URL: http://nbuv.gov.ua/UJRN/DeVr_2015_15_3

27. Марков В. В. Поняття та види форм адміністративно-правової протидії кіберзлочинності в Україні. Європейські перспективи. 2015. Вип. 7. С. 43–47.

28. Марущак А. І. Інформаційне право: регулювання інформаційної діяльності: Навчальний посібник. К.: Дакор, 2011. 344 с

29. Орлов Ю. Ю. Реалізація вимог Міжнародної конвенції про кіберзлочинність у законодавстві України. Наук. вісн. Нац. акад. внутріш. справ. 2011. № 6. С. 3–9.

30. Паршин С.А., Горбачев Ю.Е., Кожанов Ю.А. Кибервойны - реальная угроза национальной безопасности? М.: КРАС АНД, 2011. 96 с.

31. Петрик В. М. Забезпечення інформаційної безпеки держави: підручник / за заг. ред. О. А. Семченка та В. М. Петрика. Київ: ДНУ «Книжкова палата України», 2015. 672 с.

32. Порядок створення переліку критично важливих об'єктів інформаційної інфраструктури: Постанова Кабінету Міністрів України від 23.

08. 2016 р. №563. URL: https://zakon.rada.gov.ua/laws/show/563-2016-%D0%BF#Text

33. Постников В. М. Анализ подходов к формированию состава экспертной группы, ориентированной на подготовку и принятие. *Наука и образование.* 2012. № 5 URL: http://technomag.bmstu.ru/doc/360728.html.

34. Постников В. М. Подход к расчёту весовых коэффициентов ранговых оценок экспертов при выборе варианта развития информационной системы. *Наука и образование*. 2013. № 8 URL:http://technomag.edu.ru/doc/580272.html.

35. Приймак Ю. Ю. Національні інформаційні ресурси джерело державних інформаційних продуктів та послуг. Державне управління: теорія та практика. 2009. № 2. С.15–25.

36. Про Державну службу спеціального зв'язку та захисту інформації України: Закон України від 07.11.2018, № 2155-VIII. Відомості Верховної Ради України (ВВР), 2006, № 30, ст.258

37. Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури. Постанови Кабінету Міністрів України № 518 від 19 червня 2019 року.Офіційний вісник України від 02.07.2019. 2019, № 50, стор. 53, стаття 1697, код акту 94896/2019.

38. Про затвердження Концепції створення Єдиної державної автоматизованої паспортної системи, Постанова Кабінету Міністрів України; Концепція від 20.01.1997 № 40. URL: https://zakon.rada.gov.ua/laws/term/40-97-%D0%BF. (дата звернення 02.09.2019).

39. Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах: Постанова Кабінету Міністрів України від 29.03.2006 № 373 URL:https://zakon.rada.gov.ua/laws/show/373-2006-%D0%BF#Text

40. Про затвердження протоколу спільних дій основних суб'єктів кібербезпеки, питання кіберзахисту та власників (менеджерів) об'єктів критичної інформаційної інфраструктури під час запобігання, виявлення та припинення кібератак та кіберінцидентів та усунення їх наслідків: Постанова

Кабінету Міністрів України від 2019 р. URL: http://www.drs.gov.ua/wp-content/uploads/2019/06/5606.pdf

41. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 05.07.1994 № 80/94-ВР. Відомості Верховної Ради України (ВВР), 1994, № 31, ст.286

42. Про захист прав людини і основних свобод. Європейська конвенція. від 04.11.1950. *Офіційний вісник України* від 16.04.1998., № 13, / № 32 від 23.08.2006 / стор. 270.

43. Про заходи щодо розвитку національної складової глобальної інформаційної мережі Інтернет та забезпечення широкого доступу до цієї мережі в Україні: від 31.07.2000 № 928/2000. Офіційний вісник України. 2000. № 31. Ст. 11.

44. Про інформацію: Закон України від 02.10.1992 № 2657-XII. Відомості Верховної Ради України (ВВР), 1992, № 48, ст.650

45. Про кіберзлочинність. Конвенція Ради Європи від 21.11.2001. *Офіційний вісник України* від 10.09.2007р., № 65, стор. 107, стаття 2535, код акту 40846/2007.

46. Про критичну інфраструктуру та її захист: проект закону України від 27.05.2019. 10328. URL:http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=65996

47. Про Національний банк України. Закон України від 20.5.1999 № 679 – XIV. *Відомості Верховної Ради України (ВВР*), 1999, № 29, ст.238.

48. Про Національний банк України: закон від 11.10.2017 № 679 XIV. Відомості Верховної Ради України. 1999. № 29. Ст. 238.

49. Про національну безпеку України: закон України від 21.06.2018 № 2469-VIII. URL: http://zakon2.rada.gov.ua/laws/show/2469-19/conv. (дата доступу – 23.07.2018).

50. Про основні засади забезпечення кібербезпеки України: Закон України № № 2163-VIII від 05.10.2017 р. Відомості Верховної Ради (ВВР), 2017, № 45, ст.403

51. Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки: Закон України від 09.01.2007 р. № 537-V. Відомості Верховної Ради України (ВВР), 2007, № 12, ст.102 ISO/IEC 27032:2012 Information technology -- Security techniques -- Guidelines for cybersecurity - URL: www.iso.org/standard/44375.html. (дата звернення 02.09.2019).

52. Про Службу безпеки України: закон від 25.03.1992 №2229-XI. Відомості Верховної ради України. 1992. № 27. Ст. 382.

53. Про Стратегію кібербезпеки України: Указ Президента №96/2016 від 15.03.2016. UPL: https://zakon.rada.gov.ua/laws/show/96/2016 (дата звернення 02.09.2019).

54. Спасибо І. А. Щодо історії виникнення глобальної мережі інтернет. Право та інновації. 2014. № 3 (7). С. 15–25.

55. Стандарти ISO/IEC захистять від кіберзагроз. 31.08.2016. URL: http://csm.kiev.ua. (дата звернення 02.09.2019). ISO/IEC 27000. URL: https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en (дата звернення 02.09.2019).

56. Створення глобальної культури кібербезпеки: резолюція Генеральної Асамблеї ООН від 20.12.2002 №57/239. URL: https://documentsdds-ny.un.org/doc/UNDOC/GEN/N02/555/24/PDF/N0255524.pdf?OpenElement. (дата доступу – 13.03.2018).

57. Тихомиров О. О., Тугарова О. К. Юридична відповідальність за правопорушення в інформаційній сфері: навч. посіб. Київ: Нац. акад. СБУ, 2015. 172 с.

58. Угода про Асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони від 27.06.2014./*Офіційний вісник України* від 26.09.2014 — 2014, № 75, том 1, стор. 83, стаття 2125.

59. Чернышева Т. Ю. Иерархическая модель оценки и отбора экспертов. *Доклады ТУСУР. Управления, вычислительная техника и информатика*. 2009. № 1(19). Часть 1. С. 168–173. URL: http://tusur.ru/filearchive/reports-magazine/2009-1-1/168-173.pdf.

60. Юдін О. К. Бучик С. С. Класифікація загроз державним інформаційним ресурсам нормативно-правового спрямування. Методологія по будови класифікатора. *Захист інформації*. 2015. Т. 18 (2). С. 108–118.

61. Юдін О. К. Бучик С. С. Класифікація загроз державним інформаційним ресурсам організаційного спрямування. Методологія побудови класифікатора. *Спеціальні телекомунікаційні системи та захист інформації.* 2014. № 2(26). С. 43– 49.

62. Юдін О. К. Державні інформаційні ресурси. Методологія побудови класифікатора загроз : монографія / Юдін О. К., Бучик С. С. К. : НАУ, 2015. 214 с.

63. Юдін О. К. Класифікація загроз державним інформаційним ресурсам інженерно-технічного спрямування. Методологія побудови класифікатора. *Наукоємні технології*. 2015. № 2 (26). С. 188–195.

64. Юдін О. К., Бучик С. С., Чунарьова А. В., Варченко О. І. Методологія побудови класифікатора загроз державним інформаційним ресурсам. *Наукоємні технології*. 2014. № 2 (22). С. 200–210. URL: http://jrnl.nau.edu.ua/index.php/SBT/article/view/6820.

65. Digital in 2018: звіт. URL: https://www.slideshare.net/DataReportal/digital-2018-ukraine-january-2018

66. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance) OJ L 119, 4.5.2016, p. 1–88

67. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. OJ L 194, 19.7.2016, p. 1–30

68. Regulation (EU) 2019/881 of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act). Official Journal of the European Union. L 151/15, 7.6.2019

ДОДАТКИ

Додаток А

Термін	визначення
кібератака	спрямовані (навмисні) дії в кіберпросторі, які здійснюються за допомогою засобів електронних комунікацій (включаючи інформаційно
комунікаційні технології, програмні, програмно	апаратні засоби, інші технічні та технологічні засоби і обладнання) та спрямовані на досягнення однієї або сукупності таких цілей: порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, що обробляються (передаються, зберігаються) в комунікаційних та/або технологічних системах, отримання несанкціонованого доступу до таких ресурсів; порушення безпеки, сталого, надійного та штатного режиму функціонування комунікаційних та/або технологічних систем; використання комунікаційної системи, її ресурсів та засобів електронних комунікацій для здійснення кібератак на інші об’єкти кіберзахисту;
кібербезпека	захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі;
кіберзагроза	наявні та потенційно можливі явища і чинники, що створюють небезпеку життєво важливим національним інтересам України у кіберпросторі, справляють негативний вплив на стан кібербезпеки держави, кібербезпеку та кіберзахист її об’єктів;
кіберзахист	сукупність організаційних, правових, інженерно технічних заходів, а також заходів криптографічного та технічного захисту інформації, спрямованих на запобігання кіберінцидентам, виявлення та захист від кібератак, ліквідацію їх наслідків, відновлення сталості і надійності функціонування комунікаційних, технологічних систем;
кіберзлочин (комп’ютерний злочин)	суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України;
кіберзлочинність	сукупність кіберзлочинів;
кібероборона	сукупність політичних, економічних, соціальних, військових, наукових, науково технічних, інформаційних, правових, організаційних та інших заходів, які здійснюються в кіберпросторі та спрямовані на забезпечення захисту суверенітету та обороноздатності держави, запобігання виникненню збройного конфлікту та відсіч збройній агресії;
кіберпростір	середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене в результаті функціонування сумісних (з’єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет

	та/або інших глобальних мереж передачі даних;
кіберрозвідка	діяльність, що здійснюється розвідувальними органами у кіберпросторі або з його використанням;
кібертероризм	терористична діяльність, що здійснюється у кіберпросторі або з його використанням;
кібершпигунство	шпигунство, що здійснюється у кіберпросторі або з його використанням;
критична інформаційна інфраструктура	сукупність об’єктів критичної інформаційної інфраструктури;

Додаток Б

Таблиця опитування експерта (вказується категорія експерта) ФПЗ ДІР НПС

Функціональний профіль загроз	Джерело загроз			Відносно до інформаційного об’єкта		Характер загроз		Загрози за структурою впливу			Рівні впливу загроз				
	Антропогенні	Техногенні	Стихійні	Внутрішні	Зовнішні	Навмисні	Ненавмисні	Системні	Структурні	Елементні	Фізичні засоби (лінії зв’ язку, апаратні засоби)	Мережеві додатки та сервіси	Мережеві додатки та сервіси	Операційна система	Системи управління базами даних
	і	2	3	4	5	6	7	8	9	10	11	12	13	14	15
01_1.1_2_3.2 діяльність іноземних політичних, економічних і військових розвідувальних та інформаційних структур, спрямована проти інтересів України в інформаційній	1	0	0	1	1	1	0	1	0	0	1	1	1	1	1

Примітка. Складено автором.

Виконав: студент магістратури за спеціальністю 281 Публічне управління та адміністрування заочної форми навчання _____ _____В.Б. Витвицький

Науковий керівник:
доцент кафедри публічного управління та адміністрування, к.держ.упр. _____ _____Л.П. Требик

Робота допущена до захисту:
завідувач кафедри публічного управління та адміністрування, д.держ.упр., доцент _____ _____Е.В. Щепанський