

Міністерство освіти і науки України
Національний університет
«Полтавська політехніка імені Юрія Кондратюка»

Навчально-науковий інститут фінансів, економіки, управління та права
Кафедра публічного управління, адміністрування та права

Кваліфікаційна робота

на тему:

«КІБЕРБЕЗПЕКА ОРГАНІВ ДЕРЖАВНОЇ ВЛАДИ В УМОВАХ ЦИФРОВИХ ТРАНСФОРМАЦІЙ»

Виконала:

студентка академічної групи 401-ПУ
освітньо-професійної програми
«Публічне управління та адміністрування»
першого (бакалаврського) рівня вищої освіти
спеціальності 281
«Публічне управління та адміністрування»

_____ В. Ю. Костенко

Науковий керівник:

кандидат наук з державного управління,
доцент, завідувач кафедри публічного
управління, адміністрування та права

_____ І. О. Кульчій

Полтава – 2026 рік

завдання

Бібліографічний опис та анотація кваліфікаційної роботи

Бібліографічний опис: Костенко Валерія Юріївна. Кібербезпека органів державної влади в умовах цифрових трансформацій. Спеціальність: 281 «Публічне управління та адміністрування». Національний університет «Полтавська політехніка імені Юрія Кондратюка». Навчально-науковий інститут фінансів, управління та права. Кафедра публічного управління, адміністрування та права. Науковий керівник: кандидат наук з державного управління, доцент, завідувач кафедри публічного управління, адміністрування та права Національного університету «Полтавська політехніка імені Юрія Кондратюка» Кульчій Інна Олексіївна. Полтава. 2026 рік.

Зміст роботи: робота включає вступ, три розділи, висновки та пропозиції, перелік використаних джерел, додатки.

Анотація. У роботі розкрито зміст та природу системи кіберзахисту держави; досліджено нормативно-правове поле формування інформаційної безпеки країни; охарактеризовано актуальний стан забезпечення кібербезпеки; описано результативні заходи із захисту даних в інформаційно-телекомунікаційних системах на державному рівні; запропоновано рекомендації, спрямовані на посилення інформаційної безпеки держави.

Ключові слова: кібербезпека, інформаційні загрози, нормативно-правова база з кібербезпеки, національна стратегія з кібербезпеки, рекомендації з кіберзахисту.

ЗМІСТ

ВСТУП.....	5
РОЗДІЛ 1. НОРМАТИВНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В УКРАЇНІ	7
1.1. Поняття та принципи забезпечення кібербезпеки.....	7
1.2. Системи кіберзахисту та кіберзагроз у країнах ЄС	11
РОЗДІЛ 2. АНАЛІЗ ОСОБЛИВОСТЕЙ ТА СКЛАДОВИХ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ	19
2.1. Аналіз кіберзагроз та систем кіберзахисту в Україні	19
2.2. Аналіз рівня кібербезпеки України в порівнянні зі світовими практиками	26
РОЗДІЛ 3. НАПРЯМИ УДОСКОНАЛЕННЯ МЕХАНІЗМІВ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ.....	35
3.1. Удосконалення нормативно-правової бази в сфері забезпечення кібербезпеки в Україні	35
3.2. Забезпечення кібербезпеки органів державної влади України	37
ВИСНОВКИ ТА ПРОПОЗИЦІЇ	46
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ.....	52
ДОДАТКИ	59
Додаток А. Матеріали апробації результатів кваліфікаційної роботи	60

ВСТУП

Актуальність теми. Воєнний стан і стрімкий поступ ІТ-галузі перетворили кіберпростір на важливу частину життя кожного громадянина, а його захист на нагальну потребу держави. Україна вже впровадила низку міжнародних нормативних документів, створила інституції кіберзахисту, сформувала відповідну правову основу тощо. Проте простір для вдосконалення й нових ініціатив залишається значним. Євроінтеграційні процеси, які відбуваються в державі, забезпечують узгодженішу протидію кіберзлочинності - захист цілісності конфіденційних і державних електронних даних став спільною справою. Сьогодні питання кібербезпеки в Україні стоять поряд із захистом суверенітету, територіальної цілісності та економічної безпеки.

Комплексний характер проблем інформаційної сфери потребує ідентифікації загроз інформаційній безпеці, оцінювання їх ризиковості та розроблення теоретико-методологічних засад протидії, що враховуватимуть національні інтереси як України, так і держав, з якими вона підтримує співпрацю.

Об'єктом дослідження виступають суспільні відносини у сфері забезпечення кібербезпеки.

Предметом дослідження є державна політика щодо забезпечення кібербезпеки України на сучасному етапі державного будівництва.

Метою дослідження є з'ясування сутності, принципів і особливостей кіберзахисту та опрацювання механізмів забезпечення кібербезпеки в Україні.

Завдання дослідження:

- розкрити поняття та принципи забезпечення кібербезпеки;
- проаналізувати системи кіберзахисту та кіберзагроз у країнах ЄС;
- оцінити кіберзагрози та функціонування систем кіберзахисту в Україні;
- провести порівняння рівня кібербезпеки України із світовими практиками;
- запропонувати окремі напрями вдосконалення нормативно-правової бази у сфері кібербезпеки України;

- визначити шляхи забезпечення кібербезпеки органів державної влади України на сучасному етапі.

Методи дослідження. Під час вивчення проблематики кібербезпеки держави та формування пропозицій щодо вдосконалення державної політики у цій сфері застосовано аналіз, синтез, індукцію, дедукцію та аналогію. Окрім цього, у роботі використано кількісні методики оцінювання стану національної безпеки, що дали змогу досягти поставлених цілей.

Апробація результатів. Результати кваліфікаційної роботи оприлюднено на науково-практичній інтернет-конференції, опубліковано тези наведені в додатку А; матеріали роботи впроваджено в діяльність Головного управління Пенсійного фонду України в Полтавській області.

Структура роботи: робота складається зі вступу, трьох розділів, висновків і пропозицій, переліку використаних джерел та літератури.

РОЗДІЛ 1.

НОРМАТИВНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ

КІБЕРБЕЗПЕКИ В УКРАЇНІ

1.1. Поняття та принципи забезпечення кібербезпеки

Поява новітніх технологій та активне використання інформаційного простору породжують низку викликів для національної безпеки держави. Соціальні мережі, інтернет і електронна пошта стали майданчиком для ведення інформаційних війн, які набирають форми кібервоєн. Аналізуючи проблематику кібербезпеки, доцільно з'ясувати її ключові поняття та основні труднощі.

За даними моніторингу дослідницької групи McAfee Advanced Threat, у першому кварталі спостерігалися спроби мережових атак та використання віддалених ресурсів. Зібрані дані допомагають окреслити основні й унікальні вектори нападу, що застосовуються різними суб'єктами та кіберзлочинними угрупованнями. Вони відображають поточний ландшафт мережових загроз для компаній та приватних осіб у світовому масштабі [48; 52].

Брак фахівців із кібербезпеки гальмує впровадження новітніх захисних рішень у багатьох організаціях. Дефіцит персоналу залишається серйозною проблемою: без достатньо кваліфікованих спеціалістів неможливо ні розслідувати, ні нейтралізувати окремі види загроз, ні розгортати технології, здатні зміцнити систему безпеки (рис. 1.1). За результатами Порівняльного дослідження рішень безпеки, чимало респондентів зазначили, що ідеально було б автоматизувати або передати на аутсорсинг більшість рутинних операцій, щоб співробітники могли зосередитися на більш продуктивних завданнях [47].

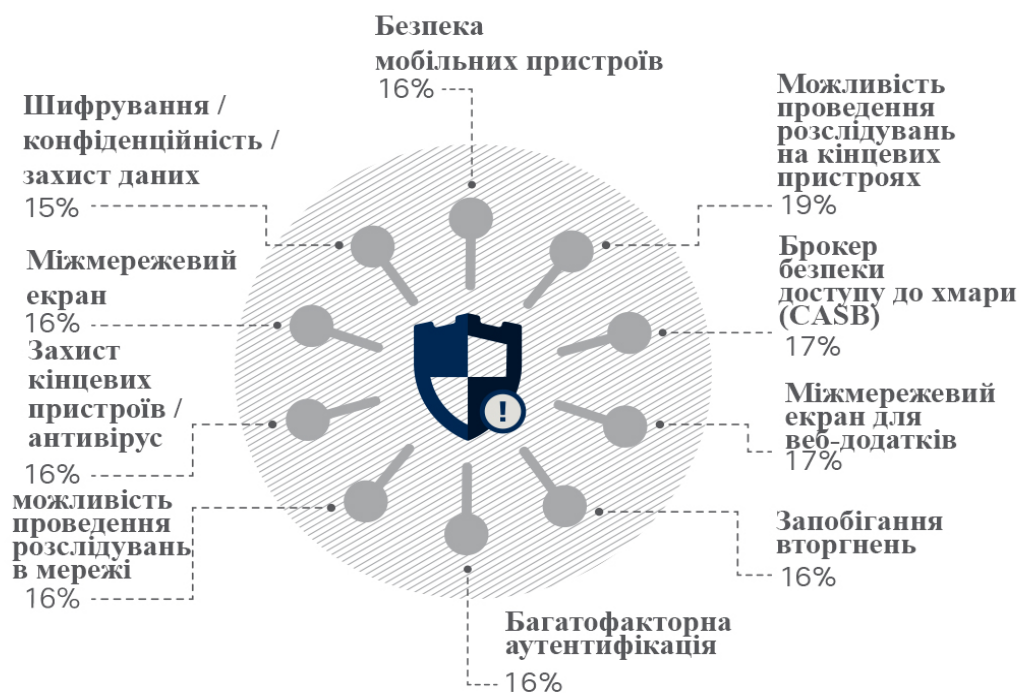


Рис. 1.1 – Можливості, які захисники додали б за умови наявності більшої кількості працівників (розроблено автором на основі [47])

Чимало зломів промислових систем управління починаються з порушення безпеки вразливих серверів і обчислювальних ресурсів корпоративної ІТ-мережі. Експерти TrarX радять застосовувати такі заходи для зниження ризиків та збереження цілісності виробничих процесів у різних підрозділах:

- перевіряти постачальників і системи, контролювати своєчасну установку всіх патчів та оновлень (якщо оновлення відсутні -варто обміркувати перехід на нову технологію);
- обмежити використання USB-носіїв та DVD-дисків;
- ізолювати промислові системи управління від ІТ-мереж, не допускаючи прямих з'єднань -ані мережевих, ані через ноутбуки чи карти пам'яті;
- запровадити політику, яка суворо обмежує використання промислових систем управління винятково необхідними операціями;
- знизити доступність відповідних робочих станцій і моніторів до зовнішнього Інтернету через браузер;

- передбачати ситуації, коли політика не діятиме, і мати плани реагування;
- змінити паролі за замовчуванням у виробничій мережі та запровадити двофакторну автентифікацію скрізь, де це можливо;
- перевіряти плани аварійного відновлення на випадок масштабної кібератаки.

Закон України «Про основні засади забезпечення кібербезпеки України» офіційно роз'яснив поняттєвий апарат цієї сфери [27]. Захист повинен ґрунтуватися на міжнародних стандартах і не порушувати прав громадян під час кіберагресії. Пріоритетом визнані заходи, що практикуються в розвинених країнах: міжнародне співробітництво, об'єднання зусиль у розслідуваннях тощо [27]. Через міжнародну взаємодію формуються спільні дії з протидії кіберінцидентам та узгоджуються єдині стандарти кіберзахисту. Першочергове значення має повага до нормативних актів європейської спільноти, а захист інтересів громадян у кіберпросторі виходить на міжнародний рівень.

Розвиток ІТ-технологій породжує потребу в послугах фахівців із кібербезпеки. Вони мають бути компетентними, відповідальними, своєчасно вживати спільних заходів проти кіберзагроз, ефективно реагувати, виявляти інциденти й співпрацювати з міжнародними організаціями у сфері виявлення та протидії.

Спеціалістам із кібербезпеки потрібно розробляти й упроваджувати засоби протидії, враховуючи появу нових і трансформацію наявних загроз. Якщо давати правову оцінку реалізованим в Україні системі кіберзахисту, варто наголосити: ця сфера переважно зорієнтована на вимоги євроатлантичної інтеграції держави й спирається на доктрини, стратегії та принципи НАТО і Європейського Союзу. Стратегія національної безпеки України визначила об'єкти критичної інфраструктури (державне управління фінансово-банківського сектору, енергетики й транспорту, внутрішні та міжнародні комунікації). Реалізація державної політики потребує розроблення та запровадження національних стандартів, побудованих на основі європейських стандартів та Конвенції про кіберзлочинність. Саме це є запорукою формування

глобальної системи протидії кіберзагрозам, як зазначено у відповідній резолюції Генеральної Асамблеї ООН [15].

Закон «Про національну безпеку України» зараховує до загроз в інформаційній сфері такі явища, як обмеження свободи слова та доступу громадян до інформації, поширення культу насильства, жорстокості та комп'ютерного тероризму, оприлюднення відомостей із державною або іншою таємницею, конфіденційної інформації, що належить державі або забезпечує національні інтереси, а також маніпуляцію свідомістю шляхом поширення хибної, неповної чи необ'єктивної інформації [20].

Це закріплено на стратегічному рівні, оскільки комп'ютерні злочини та кібертероризм не охоплюють усього спектра загроз. Увагу зосереджено саме на впровадженні новітніх та конкурентоспроможних інформаційних технологій, передусім сучасних програмних продуктів. Слід забезпечити безпеку інформаційно-телекомунікаційних систем, що функціонують в інтересах держави, відповідають потребам оборони, кредитно-банківського сектору, об'єктів критичної інфраструктури, а також створити національну систему кібербезпеки. До загроз віднесено інформаційну війну, що ведеться проти України, відсутність комунікативної політики в цьому напрямі, відсталий рівень медіакультури. Вразливими виявляються й об'єкти критичної інфраструктури: державні інформаційні ресурси відкриті для кібератак через фізичне зношення систем захисту державної таємниці тощо [20].

Закон України «Про основні засади забезпечення кібербезпеки України» закріпив терміни цієї сфери: індикатори кіберзагроз, інцидент кібербезпеки, кібератака, кібербезпека, кіберзагрози, кіберзахист, кіберзлочин, кібероборона, кіберпростір, кібертероризм тощо. Окреслено сферу дії закону - це і захист інформації, і державна таємниця, і соціальні мережі, приватні електронні інформаційні ресурси, комунікаційні системи тощо [27].

Правовою основою визнано Конституцію України, Конвенцію про кіберзлочинність, укази Президента України, постанови Кабінету Міністрів та інші нормативно-правові акти. Визначено об'єкти кібербезпеки й кіберзахисту,

об'єкти критичної інфраструктури, принципи забезпечення кібербезпеки та засади національної системи кібербезпеки [27]. Узагальнення основних дій держави у сфері кіберзахисту наведено в таблиці 1.1.

Таблиця 1.1.

Дії з боку держави в сфері кіберзахисту. Розроблено автором на основі [27].

Інформація	Деталі	Примітка
Термінологія	Кібербезпека, кібератака, кіберзагрози, кібероборона, кіберпростір, та інше	Запровадили
Основні суб'єкти забезпечення кібербезпеки, та їх завдання	Міністерство оборони України, РНБО, ДСЗІ, СБУ, CERT-UA, Національна поліція України, Національний банк, розвідувальні органи України	Сформовано
Відповідальність	Кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку (статті 361 - 362)	Запровадили
Відповідність до міжнародних стандартів	Україна ратифікувала конвенцію Ради Європи про кіберзлочинність, Стратегія кібербезпеки України	Впровадили

Тобто держава підготувала нормативно-правову базу для розбудови національної системи кіберзахисту, удосконалюючи її правову основу, поширює систему інформаційної безпеки на об'єкти критичної інфраструктури, створює галузеві центри реагування на атаки, активно діє у сфері міжнародного співробітництва, готує кадри з кібербезпеки, підвищує цифрову грамотність громадян та розвиває системи захисту інформації, формуючи довіру між державою і суспільством.

1.2. Системи кіберзахисту та кіберзагроз у країнах ЄС

Однією з проблем, спричинених кібератаками й загрозами, є негативний вплив на внутрішній ринок Європейського Союзу. Оскільки кіберпростір не має кордонів, одна серйозна загроза здатна позначитися на всьому Союзі. Якщо буде зламано чи відключено мережеву систему однієї з держав-членів (наприклад, систему управління аеропортами), це позначиться й на інших країнах. Транскордонні послуги в межах ЄС можуть бути перервані, зупинені

чи пошкоджені. У 2010 році eBay зазнав кібератак, які повністю або частково обмежили доступ до сайтів та призупинили електронну торгівлю - частину внутрішнього ринку [50, с. 12-13].

Голландська компанія DigiNotar, що випускала цифрові сертифікати для забезпечення безпеки інтернет-комунікацій, була зламана і не зупинила випуск фальшивих сертифікатів. У результаті в мережі поширилася значна кількість недійсних сертифікатів, а після виявлення шахрайства користувачі втратили довіру і до самої компанії, і до подібних організацій. Згодом охоронна компанія FOX-IT оприлюднила звіт, у якому констатувала відсутність належних заходів безпеки та активів управління ризиками. Уряд Нідерландів окремо наголосив на ризиках для внутрішнього ринку: порушення безпеки ускладнюють транскордонне обслуговування й постачання продукції [50, с. 12-13].

Згодом Нідерланди оголосили про впровадження системи, яка зобов'яже всі приватні компанії повідомляти про порушення безпеки та інформувати про критичну державну інфраструктуру в цій сфері [9]. Майже всі держави-члени готують аналогічні нормативні акти, аби обмінюватися інформацією з іншими компаніями та урядовими установами щодо інцидентів у кіберпросторі й тим самим запобігати дальшим збиткам для критичної інфраструктури та забезпечувати безпеку внутрішнього ринку. У Люксембурзі й Великобританії вже діють регуляції, що передбачають інформування про загрози для ключових секторів - енергетики, транспорту, фінансів, - аби уникнути негативного впливу кібератак на решту ЄС [50, с. 13].

Серед причин, що можуть викликати збої в роботі інформаційно-комунікаційних систем, є природні катаклізми. У 2002 році повінь на Ельбі пошкодила комунікаційні структури і порушила роботу всієї мережі. Сильні шторми легко руйнують наземну інфраструктуру, що призводить до призупинення інтернет-послуг [50, с.14]. Проте головною причиною подібних інцидентів залишається людський фактор - він присутній приблизно у 95 % випадків. У 2012 році випадково пошкоджений інтернет-кабель між Нідерландами та Великобританією вивів інтернет з ладу більш ніж на добу,

через що електронна комерція та інші приватні й державні компанії зазнали значних збитків [50, с. 14].

Водночас основні загрози й атаки виникають та поширюються самими користувачами Інтернету: жертви стають ключовою ланкою, що спричиняє поширення вірусів або шкідливого програмного забезпечення - через невідомі USB-накопичувачі, відкривання підозрілих електронних листів або доступ до файлів і сайтів. Загалом саме людський фактор залишається головним винуватцем цифрових атак і загроз [50, с. 14].

Інформаційно-комунікаційні технології (ІКТ) не лише стали частиною соціального життя, але й перетворилися на важливий компонент економіки та бізнес-процесів. ІКТ - один із чинників зростання Європейського Союзу. За оцінками Світового банку, підвищення швидкості Інтернету на 10 % дає 1,3 % економічного зростання. Загальний внесок ІКТ у ВВП ЄС становить близько 6 % . Усі користувачі - органи влади, приватний сектор, громадяни та постачальники соціальних послуг -використовують Інтернет для спілкування, ведення бізнесу й виконання повсякденних завдань. Тому будь-яка загроза має сприйматися як загальне питання безпеки, адже здатна заблокувати всю систему [50, с. 15-16].

Кібератаки можуть паралізувати державну інфраструктуру на кілька днів, як це сталося 2007 року в Естонії, де громадяни й уряд зіткнулися з серйозними збоями в електронному управлінні та інтернет-банкінгу, втратили доступ до мережі та зазнали фінансових втрат. Згодом, у 2011–2012 роках, об'єктами кібератак стали і інституції ЄС [50, с. 16].

Такі загрози фінансово коштовні, особливо для бізнесу, який працює переважно онлайн . У 2009 році, за звітами, близько 16 % приватних компаній у Союзі зазнали кібератак . У 2011 році втрати Sony від кібератак становили 175 млн дол. , BlackBerry - 50 млн дол. Наступного року великі американські банки зазнали атак, які призвели до фінансових збитків і - що особливо важливо - крадіжки конфіденційної фінансової інформації [47; 50, с. 16]. Маштаб фінансових наслідків кібератак ілюструє рис. 1.2.

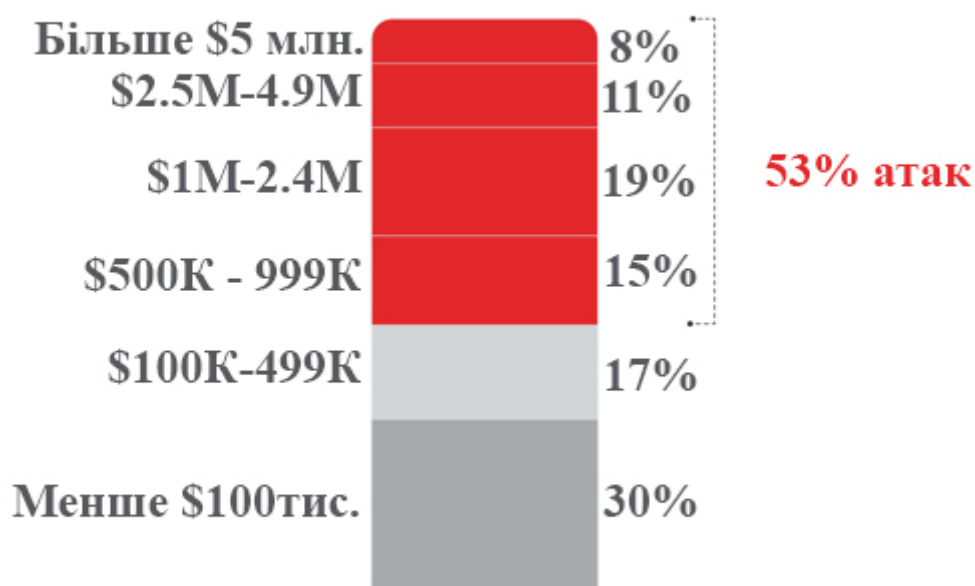


Рис. 1.2. – П'ятдесят три відсотки атак завдали шкоди в розмірі \$ 500 000 або більше (розроблено автором на основі [47])

Жертвами зрештою стають звичайні клієнти, від яких залежать державні й приватні підприємства, або які самі є основними суб'єктами бізнесу. У 2011 році тридобова кібератака на BlackBerry зачепила приблизно 70 млн користувачів (Кабінет міністрів Великобританії, 2012). У 2010 році клієнти німецьких банків не могли користуватися картками ані в Німеччині, ані за кордоном і не мали змоги зняти готівку в банкоматах через збій програмного забезпечення мікрочіпів [50, с. 16-17].

Подібні кіберзагрози потенційно небезпечні й можуть призводити до людських жертв. Так, в енергетичному секторі компанії, що управляють постачанням газу та нафти через трубопроводи й використовують ІТ для управління потоками та обміну інформацією, можуть стати об'єктами кібератак, що завдадуть шкоди довкіллю та працівникам станцій. Аналогічні ризики є й у залізничному та повітряному транспорті, де ІКТ -невід'ємна частина систем управління. Такі атаки можуть призупинити, затримати або навіть спричинити катастрофічні інциденти [50, с. 16].

Перед Європейським Союзом постає завдання координації та вдосконалення ІКТ-систем і підвищення рівня безпеки, оскільки рівень розвитку технологій і витрати на безпеку відрізняються між державами-членами. Щоб ефективно протидіяти кібератакам, країни -члени мають координувати дії та обмінюватися інформацією, що передбачає співпрацю державного й приватного секторів [50, с. 23-24].

Так, до групи країн із високим рівнем безпеки та можливостей ЄС належать Данія, Фінляндія, Нідерланди, Швеція й Великобританія. До другої групи зараховують Бельгію, Німеччину, Австрію, Францію, Ірландію, Люксембург. Сукупно ці країни забезпечують 82 % загальних витрат ЄС на безпеку та близько 69 % ВВП. Саме там зосереджені провідні компанії у сфері мережевої безпеки, що активно впливають на формування кіберполітики [50, с. 36-37].

Захист інформації існував задовго до появи комп'ютерів та Інтернету. Перші ініціативи цього напрямку застосовували ще під час Першої світової війни, коли радіохвилі використовувалися для надсилання повідомлень і отримання даних супротивника [25]. Британські радіооператори перехоплювали зашифровані повідомлення з Німеччини та передавали їх до радіорозвідки Королівського флоту, де їх дешифрували [25].

Наприкінці Першої світової війни німецький інженер Артур Шербіус створив машину «Енігма», що шифрувала бездротову інформацію та використовувалася до середини XX ст. для захисту економічного, військового та дипломатичного зв'язку. Вона була однією з ключових технологічних переваг нацистської Німеччини під час Другої світової війни, доки британський учений Алан Тюрінг не створив пристрій, здатний розшифровувати її сигнали [25].

Сьогодні змінилися лише методи й засоби: вони стали значно складнішими, але продовжують слугувати дієвою зброєю для злочинців і навіть деяких держав. Водночас низка організацій - Міжнародний союз

електрозв'язку, Організація економічного співробітництва та розвитку - формують адекватну сучасним викликам кіберполітику [54].

Особливо помітну роль відіграють НАТО та Європейський Союз: вони включають кібербезпеку до своїх безпекових стратегій і за рахунок співпраці й координації формують ефективну відповідь на кіберзагрози, які стрімко ускладнюються.

Більшість країн є членами обох цих організацій, тож співпраця між ними має критичне значення [37].

Окрім того, Європейський Союз спільно з Високим представником із закордонних справ і безпекової політики оприлюднив стратегію кібербезпеки [25]. Стратегія спрямована на ефективне запобігання загрозам у кіберпросторі та реагування на них. Її основна мета -захист європейських цінностей (свободи, демократії, безпечного зростання цифрової економіки) та приватності громадян ЄС. У документі пропонуються заходи з підвищення стійкості інформаційних систем, протидії кіберзлочинам і підтримки оборонної політики Союзу [25]. Комісія також запропонувала директиву щодо захисту мереж та інформації - спрямовану на високий рівень мережевої безпеки в усьому ЄС [50].

У контексті кібербезпеки інституції Союзу орієнтуються на боротьбу з кіберзлочинами, скоєними як у самому ЄС, так і проти нього з-за кордону. Стратегічний документ окреслює компетенцію та дії, потрібні для надійного захисту прав громадян , а також визначає основні принципи кіберполітики, що мають бути узгодженими в межах ЄС і у світі . Принципи кіберполітики Союзу повинні втілюватися в національних стратегіях відповідних держав-членів [25].

Директива ЄС охоплює такі принципи:

- захист даних, конфіденційності, свободи вираження поглядів та основоположних прав;
- доступ до Інтернету для всіх;
- цінності ЄС є життєво важливими у цифровому світі так само, як і у фізичному;

- ефективно й демократичне управління віртуальним простором за участі різних зацікавлених сторін;
- усвідомлене ставлення до відповідальності у питаннях кібербезпеки.

Стратегія ЄС визначає коротко- й довгострокові заходи для протидії загрозам зазначеним цінностям. Її ключовими пріоритетами, що передбачають участь інституцій ЄС, держав-членів і бізнесу, є :

- досягнення ефективної кіберстійкості;
- зменшення кіберзлочинів, скоєних у Союзі;
- формування політики й компетенцій у сфері кіберзахисту як частини Спільної політики безпеки та оборони;
- сприяння розвитку необхідних технологічних та промислових засобів для стратегії кібербезпеки;
- вироблення послідовної політики ЄС щодо кіберпростору та поширення основних цінностей Союзу [25].

Основна ініціатива полягає в налагодженні ефективної співпраці між приватним сектором і державою у сфері кібербезпеки, оскільки значна частина суб'єктів галузі -це приватні компанії. Їх залучення є визначальним, адже саме вони контролюють ключові процеси в кіберпросторі, а уряд самотужки не здатний забезпечити кібербезпеку; водночас формат участі приватного сектору ще остаточно не сформувався [50, с.36-37].

Приватний сектор не може чекати, доки держава покарає кіберзлочинців у суді: ідентифікувати їх і притягнути до відповідальності надзвичайно складно через брак необхідних технологічних і промислових ресурсів. Тому участь бізнесу в реалізації стратегії кібербезпеки є вирішальною -це його власний інтерес і запит на безпечну кібермережу [25].

Зменшення кіберзлочинів вимагає ухвалення дієвих і суворих законів. Конвенція про кіберзлочинність прийнята 2001 року: 47 держав-членів ратифікували її через парламент, проте близько 196 країн досі цього не зробили. Україна ухвалила закони щодо протидії кіберзлочинності, а ратифікація Конвенції є важливою з огляду на міжнародне співробітництво та

координацію дій [13]. Україна разом із ЄС прийняла стратегію національної безпеки, узгоджуючи визначення, аспекти й ключові загрози, серед яких - кібербезпека. Майже всі держави-члени визнають кіберзагрози та атаки одним із головних вразливих місць національної безпеки. Тому формування безпечного кіберпростору є нині ключовим завданням і для України.

У першому розділі проаналізовано такі дії держави щодо підвищення безпеки в кіберпросторі: закріплення понять у нормативно-правовому полі цієї сфери, визначення суб'єктів кіберзахисту та об'єктів (критичної інфраструктури), де впроваджуватимуться основні методи захисту. Це створює правове підґрунтя для реагування на кіберзлочини. Ключових напрямів значно більше, проте основні вже окреслені. Також систематизовано, що кібербезпека є пріоритетом і для інших країн: важливо інтегрувати міжнародні стандарти в українські, розвивати міжнародне співробітництво у сфері кіберзахисту, підвищувати грамотність користувачів і шукати кіберзлочинців.

РОЗДІЛ 2.

АНАЛІЗ ОСОБЛИВОСТЕЙ ТА СКЛАДОВИХ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

2.1. Аналіз кіберзагроз та систем кіберзахисту в Україні

Національна безпека є першочерговим завданням для України. Внутрішні чинники - реформи, обороноздатність, підтримка військових, недофінансування, складна економіка - створюють умови, за яких зовнішні загрози здатні завдати шкоди національній безпеці. Поточний її стан не дає змоги повною мірою нейтралізувати наявні виклики.

Безпека держави має охоплювати всі сфери життєдіяльності - економічну, організаційну, громадську, політичну - і захищати інтереси особи, держави та суспільства. Кібербезпека складається з багатьох компонентів, які забезпечують функціонування й розвиток системи в цілому. Її заходи спрямовані на захист національних інтересів суспільства та держави [14, с. 57]. Кібербезпека є невід'ємною частиною національної безпеки [5].

В епоху високих технологій сформувалося нове середовище кіберпростір - створене технічною, телекомунікаційною, інформаційною, мережевою та комп'ютерною складовими. Геополітика диктує сучасні умови, і держава повинна відігравати визначальну роль у кіберпросторі. Саме він використовується для досягнення політичних цілей, і саме тут розгортається війна. Її «правила» не обмежені міжнародно-правовими нормами, простір і час значення не мають, тому ефективність кіберсередовища надзвичайно висока.

Вирішальним у цьому протистоянні є міцна організація державної системи та військового управління в інформаційно-технічному вимірі, а також належний інформаційно-психологічний стан населення як складової оборонної сили. Кіберпростір є частиною інформаційного простору, тому й протидія має відбуватися через інформаційний чинник і бути керованою [45]. Потрібне правове поле - нормативні акти, що визначатимуть правила поведінки в кіберпросторі та сферу міжнародної інформаційної безпеки.

Внутрішня та зовнішня безпека держави спирається на власні збройні формування й органи державної безпеки. Намір України дотримуватися нейтралітету (не брати участі у військових блоках, дотримуватися трьох неядерних принципів - не приймати, не виробляти, не купувати ядерної зброї) пов'язаний саме з безпековим виміром. Для ефективного захисту національних інтересів Україна активно співпрацює з міжнародними організаціями, сприяє зміцненню глобальної безпеки [14]. Системи національної безпеки провідних держав ґрунтуються на нормативних документах, у яких закріплено роль і місце держави у світі, її цілі, цінності та засоби протидії внутрішнім і зовнішнім загрозам [14, с. 58]. Належний рівень кібербезпеки потребує високого рівня розвитку інформаційного суспільства [6].

Розвинені країни приділяють увагу створенню або вдосконаленню системи захисту критичної інфраструктури від внутрішніх і зовнішніх кіберзагроз, чого потребують глобалізаційні процеси в інформаційній сфері. Більшість країн готові поєднувати зусилля держави й приватного сектору для протидії загрозам. Україна перебуває на етапі становлення власної системи кібербезпеки. Ще 2011 року Кабінет Міністрів напрацював пропозиції щодо її побудови за участю Служби безпеки України [3; 43]. Система кібербезпеки - це сукупність спеціальних суб'єктів, що застосовують ресурси та методи, а також взаємопов'язані правові, організаційні й технічні заходи [44, с. 300].

Йдеться також про узгоджену сукупність елементів кібербезпеки, які розробляються та комплектуються відповідно до плану захисту інформаційно-телекомунікаційних систем [10]. Національна система кібербезпеки є невід'ємною частиною національної безпеки [6], тобто складовою життєдіяльності нації - народу та пов'язаної з ним суспільно-політичної діяльності. У цьому й полягає сутність держави, належність до неї громадян та їхнє ставлення до неї [2]. Кібербезпека характеризує стан захисту інтересів кожного громадянина й держави у кіберпросторі - там, де створюється, зберігається і поширюється інформація [6]. Формування національної системи кібербезпеки відбувається спільно з приватним сектором, що сприяє

коригуванню реформ системи національної безпеки в цілому [6]. Світ стрімко трансформується у сфері інформаційних технологій.

Кіберпростір розширює свободу й можливості громадян, з'являється новий глобальний ринок інноваційних ідей, формується ефективно державне управління, яке залучає громадян та забезпечує прозорість, зменшуючи корупцію. Цифрові технології впроваджуються в державне управління, проте водночас з'являються нові виклики національній та міжнародній безпеці.

Під час природних або соціальних інцидентів зростає кількість і потужність кібератак, націлених на державні, групові та індивідуальні інтереси. Йдеться про незаконні збір, зберігання, використання, видалення й поширення персональних даних, незаконні фінансові операції, крадіжки та інтернет-шахрайство. Кіберзлочинність набирає поширення і здатна шкодити не лише особі, а й суспільству та державі загалом.

Зміни в зовнішній і внутрішній оборонній безпеці України, тривала агресія РФ, запровадження безвізового режиму -це знакові події, що вимагають подальшого вдосконалення національної системи кібербезпеки як складової національної безпеки. Кіберпростір не має чітких меж, є динамічним та анонімним. Усвідомлюючи це, держава повинна на конституційному рівні гарантувати безпеку в кіберпросторі. Цими питаннями опікуються відповідні підрозділи СБУ, Державна служба спеціального зв'язку та захисту інформації, відділи боротьби з кіберзлочинністю та спеціальні підрозділи МВС.

Координацію здійснює відповідний підрозділ Ради національної безпеки і оборони [31]. Національна система кібербезпеки створюється та розвивається на основі Конституції України та інших нормативно-правових актів, що регулюють відносини у сфері національної безпеки, зокрема Закону України «Про основи національної безпеки України» [20], Концепції розвитку сектору безпеки та оборони [21], положення про Національний координаційний центр кібербезпеки [31], Стратегії кібербезпеки України [30], Воєнної доктрини [34], Доктрини інформаційної безпеки [22] та інших.

Членство в європейській спільноті вимагає від держави належного забезпечення кібербезпеки на національному рівні -таких стандартів дотримуються держави ЄС. Тематика кібербезпеки є пріоритетною при формуванні нормативної бази. Її розвитку сприяє координація з боку правоохоронних органів. Під час війни поява нових кіберзагроз -звична річ; вони підривають інтереси громадян і держави, тому остання має забезпечити належний рівень функціонування інформаційно-телекомунікаційних систем [11].

Реагування з боку держави має тривалий характер, бо самі загрози у кіберпросторі є протяжними, динамічними та глобальними. На рівень захисту впливають також інформаційна війна окремих країн проти України, відсутність цілісної комунікативної політики, низький рівень медіа, уразливість критичної інфраструктури та державних інформаційних ресурсів до атак, морально й фізично застарілі системи захисту державної таємниці та іншої інформації з обмеженим доступом [22].

Кіберзагрози активно виникають через людський фактор як у державному, так і в приватному секторі, у транспортній, фінансовій та інших сферах [7]. Щоб запобігти цьому, потрібно сформувати та задіяти національну систему кібербезпеки як складову національної безпеки України. Її розбудова є необхідною умовою безпечного користування кіберпростором в інтересах суспільства й держави. Потрібно чітко розуміти алгоритм дій і налагодити комунікації у сфері політики для сучасного реагування.

Потрібні фінансові ресурси та результативні засоби захисту. Для організаційного забезпечення системи кібербезпеки слід створити спеціалізовані структури, обізнані у сфері безпеки кіберпростору, та сприятливі умови для ухвалення й реалізації управлінських рішень. Ці підрозділи мусять координувати свою діяльність під час реалізації заходів захисту [44, с. 301]. Основні організаційні та ресурсні перешкоди забезпеченню кібербезпеки наведено на рис. 2.1.

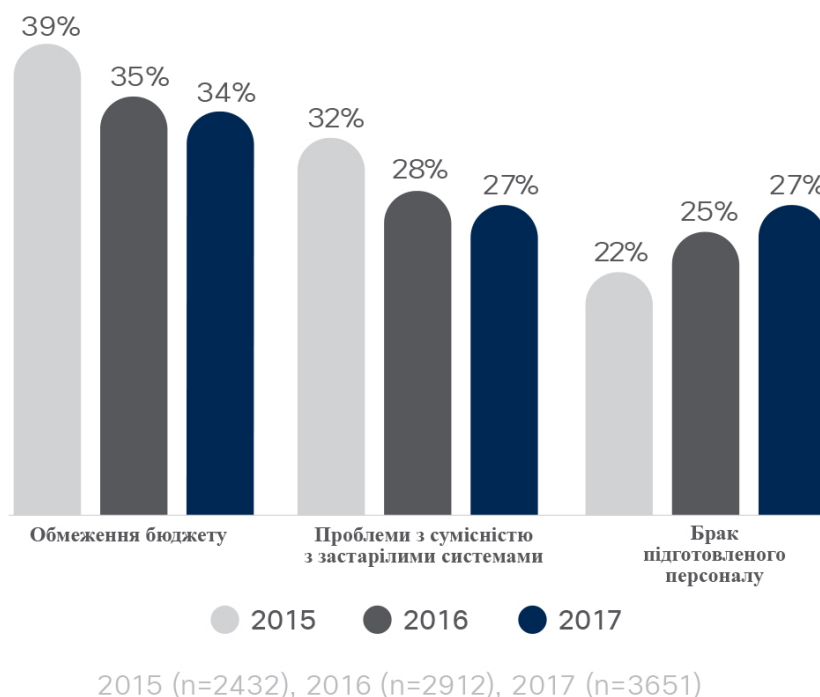


Рис. 2.1. – Найбільш серйозна перешкода забезпеченню безпеки: обмеження бюджету (розроблено автором на основі [47])

Система кібербезпеки повинна забезпечити взаємодію з питань кіберзахисту не тільки органів державної влади та місцевого самоврядування, а й військових формувань, правоохоронних органів, громадських об'єднань, підприємств, установ -освітніх і науково-дослідних. Основу національної системи становлять Міністерство оборони, Державна служба спеціального зв'язку та захисту інформації, Служба безпеки України, Національна поліція, Національний банк, спеціальні служби [27]. Регулярно проводяться наукові конференції, форуми, семінари національного та міжнародного рівня, виходять публікації з різних аспектів цієї тематики. Передові країни -Франція, Німеччина, США, Канада -також послідовно реалізують власні стратегії кібербезпеки [54].

Аналіз їхніх систем кібербезпеки показує, що єдиної моделі побудови національної системи не існує. При її формуванні слід запровадити, зокрема, відповідальність інтернет-провайдерів -зобов'язати їх надавати інформацію про кіберзлочини без рішення суду, на запит спеціальних підрозділів, як це зроблено в США [12].

Доречно визнати кібертероризм та ворожі дії інших держав у кіберпросторі різновидом кібершпигунства й окреслити основні загрози -за прикладом Канади. У деяких країнах створено спеціальні підрозділи кіберзахисту на базі правоохоронних органів, які реалізують національну стратегію. Окремі держави не лише захищаються, а й проводять відповідні наступальні кібероперації (активний кіберзахист). Аналізуючи нормативно-правову базу й системи кібербезпеки провідних держав, можна узагальнити: ключову роль варто надати розвідці, із наданням їй спеціальних повноважень, у тому числі контррозвідувальних.

В Україні таким органом є Служба безпеки України -вона наділена відповідними повноваженнями та цілеспрямовано протидіє кіберзлочинності й внутрішнім і зовнішнім загрозам в інформаційно-кібернетичній сфері. Спираючись на світову практику, доцільно створити національний центр кібербезпеки, повністю підпорядкований СБУ [12, с. 77]. Сьогодні існує Національний координаційний центр кібербезпеки -робочий орган РНБО, який координує діяльність органів національної безпеки і оборони у реалізації Стратегії кібербезпеки України та підвищує ефективність державного управління у цій сфері [31].

Основні завдання центру: аудит стану кібербезпеки; оцінка готовності суб'єктів до протидії загрозам; контроль виконання законодавчих вимог щодо захисту державних електронних ресурсів та інформації; збір даних про кіберінциденти в інформаційно-телекомунікаційних системах тощо [31]. Національний координаційний центр кібербезпеки має бути системоутворюючим елементом усієї системи кібербезпеки та кіберзахисту держави [41].

У національній системі діє також команда комп'ютерного реагування CERT-UA - спеціалізований підрозділ управління інформаційно-телекомунікаційних систем Державної служби спеціального зв'язку та захисту інформації України. Її створено 2007 року для захисту державних інформаційних ресурсів та інформаційно-телекомунікаційних систем від

несанкціонованого доступу, неправомірного використання або порушення конфіденційності [27]. Діяльність CERT-UA регулюється законами України «Про Державну службу спеціального зв'язку та захисту інформації» [23], «Про телекомунікації» [24] та підзаконними актами. Важливе значення для функціонування національної системи кібербезпеки має взаємодія між уповноваженими державними органами та координація їхньої діяльності [27]. Потрібно не лише захищатися, а й проводити дослідження, експерименти й операції в інформаційних війнах, фінансуючи цю діяльність. Рекомендації:

- створити умови для формування індустрії програмного забезпечення в Україні;
- розбудовувати та вдосконалювати мережу суперкомп'ютерних комплексів на базі великих обсягів і високошвидкісного волоконно-оптичного зв'язку;
- сприяти просуванню вітчизняних ІТ-компаній на міжнародних ринках;
- готувати ІТ-фахівців з кіберзахисту у вітчизняних закладах вищої освіти;
- розробляти не лише вітчизняну операційну систему, а й національне програмне забезпечення, у тому числі антивірусне;
- формувати умови для створення матеріально-технічної та інформаційно-аналітичної бази, автоматизації робочих місць за рахунок вітчизняних виробників;
- забезпечити системний підхід до кібербезпеки на основі ефективного державного управління; запровадити комплекс нормативних, організаційних, функціональних, фінансових, технічних і навчальних заходів;
- підвищувати самосвідомість громадян у сфері інформаційної безпеки та усвідомлення особистої відповідальності перед державою [11].

Держава повинна сформувати належну нормативно-правову базу, аби кібербезпека стала повноцінною складовою державного управління. Національна система кібербезпеки має функціонувати у форматі співпраці державних органів з установами, приватним сектором, науково-дослідними інститутами, професійними асоціаціями. Базисом є державні органи, які безпосередньо реалізують функції кіберзахисту, а решта інституцій залучається

до виявлення, запобігання та нейтралізації кіберзагроз [27]. Роботу всіх підрозділів координує Рада національної безпеки і оборони України, у якій діє координаційний орган з питань кібербезпеки [31]. Національна система кібербезпеки є складовою національної безпеки, її мета -забезпечення функціонування й розвитку всієї системи. У сучасних умовах рівень кібербезпеки має бути максимально високим. Подекуди систему кібербезпеки розглядають як сукупність специфічних для конкретної країни суб'єктів, що взаємодіють для захисту особи, суспільства й держави. Потрібно створити єдину методологію або модель побудови національної системи, а також налагодити взаємодію між державами та їхніми спеціалізованими органами у форматі співпраці й координації заради ефективнішого захисту від інцидентів.

2.2. Аналіз рівня кібербезпеки України в порівнянні зі світовими практиками

Сполучені Штати одними з перших усвідомили стратегічне значення безпеки кіберпростору. Розвиток інформаційної сфери, її зростаюча роль у житті суспільства й держави, посилення залежності економіки від ІКТ, а також теракти 2001 року спричинили ухвалення Національної стратегії безпеки кіберпростору 2003 року. Розглянемо корисні практики США в контексті можливого впровадження в Україні.

За цією стратегією відповідальність за безпеку кіберпростору розподілили між федеральними відомствами й міністерствами, а координаційний орган створили роком раніше при Міністерстві внутрішньої безпеки. Одночасно запустили понад 50 пунктів інформаційної мережі для запобігання кіберзагрозам.

У 2009 році оприлюднили «Огляд політики в кіберпросторі», який на основі аналізу наявної системи запропонував план її вдосконалення. Документ ґрунтувався на всеосяжній Національній ініціативі з кібербезпеки 2008 року. Ключовими нововведеннями стали запровадження посади координатора

державної політики кібербезпеки, відповідального за міжвідомчу взаємодію та спільне формування політики, а також послаблення ролі держави в захисті інфраструктури: відтепер приватні компанії мали забезпечувати власну безпеку, а держава зберігала функції загального керівництва та стандартизації.

Розширення міжнародної співпраці у сфері кіберзахисту призвело до ухвалення міжнародної стратегії «Процвітання, безпека й відкритість у мережевому світі 2011 року» [16].

Цей документ став першим політико-стратегічним актом, що закріпив комплексний підхід до регулювання широкого кола питань кіберпростору й визначив його як самостійну сферу регулювання, що потребує міжнародної співпраці. Стратегія мала створити єдину платформу для міжнародної взаємодії в кіберпросторі на основі американських підходів. Для її реалізації заснували посаду координатора з кіберпросторових питань у Держдепартаменті США.

Важливим напрямом міжнародної стратегії є нарощування потенціалу країн, що розвиваються, шляхом надання знань, ресурсів і фахівців, у тому числі для розробки національних стратегій кібербезпеки [16].

Прикладом співпраці США з іншими державами стало підписання 2013 року Спільної заяви президентів США та РФ про нову сферу взаємодії в зміцненні довіри, що передбачала співпрацю в захисті критичних інформаційних систем і зниженні ризиків у кіберпросторі. Сьогодні ці домовленості припинено через російську агресію проти України.

У вересні 2018 року нова адміністрація США представила своє бачення в Національній кіберстратегії США (далі - Кіберстратегія США). Документ ґрунтується на Указі Президента «Про зміцнення федеральних мереж і критичної інфраструктури» та Стратегії національної безпеки США 2017 р. [17; 36]. Структурно Кіберстратегія складається з тез: «I: захист американського народу, Батьківщини та американського способу життя», «II: сприяння американському процвітання», «III: збереження миру через силу», «IV: просування американського впливу». Кожен компонент визначає окремі цілі та пріоритетні дії [16].

Названі тези Кіберстратегії США корелюють із завданнями адміністрації Президента у сфері кіберзахисту, а саме:

- захищати країну через забезпечення мереж, систем, функцій і даних;
- сприяти процвітанню Америки шляхом розбудови безпечної цифрової економіки та стимулювання інновацій;
- зберігати мир і безпеку, посилюючи спроможність США (спільно із союзниками й партнерами) стримувати й, за потреби, карати тих, хто використовує кіберінструменти у зловмисних цілях;
- розширювати американський вплив за кордоном задля поширення принципів відкритого, сумісного, надійного й безпечного Інтернету [18, с. 14].

Будь-яка стратегія базується на оцінці ризиків, загроз, тенденцій і потенціалу -тобто на аналізі ситуації. У Кіберстратегії США такий аналіз представлено за такими напрямками:

- констатація зростаючого впливу кіберпростору на всі сфери сучасного світу й, зокрема, на політичне, соціальне, економічне та суспільне життя США;
- підтримка й просування американського бачення відкритого, сумісного, надійного й безпечного Інтернету;
- визнання того, що противники та конкуренти використовують переваги вільного Інтернету на шкоду економічним, військовим і політичним інтересам США, їхніх партнерів та союзників.

Доцільно докладніше розглянути ключові компоненти Кіберстратегії США, цілі та змістові блоки, що визначають пріоритетні дії.

Компонент I: захист американського народу, Батьківщини й американського способу життя формулює головну мету -управління ризиками кібербезпеки задля підвищення безпеки й стабільності національних та інформаційних систем. Цей компонент складається з трьох блоків.

Блок 1. Захист федеральної мережі та інформації передбачає такі пріоритетні дії: подальша централізація управління та нагляду за федеральною цивільною кібербезпекою; узгодження діяльності з управлінням ризиками й інформаційних технологій; вдосконалення управління ризиками федеральних

ланцюжків постачання; зміцнення кібербезпеки федеральних підрядників; забезпечення лідерства держави у розвитку інноваційних практик.

Новою тенденцією є розвиток системи управління ризиками федеральних ланцюжків постачання, яка передбачає, зокрема, виключення окремих ризикованих постачальників із процесу закупівель. Такі заходи поєднуються з ризик-менеджментом ланцюжків, пов'язаних із національною інфраструктурою [18]. Ступінь ризику від продукції конкретного постачальника має визначатися індивідуально.

Прикладом захисту в цій галузі стала кампанія проти китайського виробника обладнання Supermicro. Розслідування Bloomberg Businessweek повідомляло про впровадження апаратних закладок китайським урядом у серверні плати, що використовувалися багатьма американськими компаніями, зокрема Amazon і Apple [46].

За цими повідомленнями, чіпи додавали на заводах Supermicro оперативні агенти Народно-визвольної армії Китаю.

Блок 2. Забезпечення безпеки критичної інфраструктури охоплює: уточнення ролей і відповідальності; пріоритизацію дій відповідно до національних ризиків; використання постачальників ІКТ як засобу забезпечення кібербезпеки; захист демократії; стимулювання інвестицій у кібербезпеку; пріоритетне інвестування в дослідження й розробки; покращення транспортної, морської та космічної кібербезпеки. США розглядають безперешкодний доступ і свободу дій у космосі як життєво важливі для безпеки й економічного процвітання. Космічні активи мають критичне значення для позиціонування, навігації, хронометражу, розвідки, спостереження, супутникового зв'язку та моніторингу погоди. Тому адміністрація планує посилити захист поточних і майбутніх космічних активів від кіберзагроз у взаємодії з промисловістю та міжнародними партнерами [18, с. 10].

Космічні війська в США вже формуються, головними противниками вважають Китай і Російську Федерацію.

Блок 3. Боротьба з кіберзлочинністю та поліпшення звітності про інциденти охоплює: покращення повідомлень про інциденти й реагування на них; модернізацію електронного спостереження та комп'ютерної техніки; зменшення транснаціональних кіберзагроз; вдосконалення механізмів затримання злочинців, які перебувають за кордоном; зміцнення правоохоронних можливостей країн-партнерів у протидії злочинній кібердіяльності.

Удосконалення законодавства про комп'ютерні злочини розширює можливості правоохоронних органів щодо законного збору доказів та проведення слідчих і судових дій. Збирання інформації може відбуватися й за межами США. Якщо раніше для цього використовували угоди про взаємну правову допомогу (зокрема, в межах Будапештської конвенції про кіберзлочинність), то прийнятий цьогогоріч «хмарний закон» дає правоохоронцям широкі повноваження отримувати інформацію, що зберігається на серверах американських компаній за кордоном [8]. Укласти угоди з відповідними державами вже не потрібно.

Передбачено, що для зниження загроз із боку транснаціональних кіберзлочинних організацій федеральні міністерства й відомства матимуть необхідні юридичні повноваження та ресурси, включно з виявленням і ліквідацією ботнетів, темних ринків та інфраструктури, що уможлиблює кіберзлочинність, а також боротьбою з економічним шпигунством. Для ефективного стримування правоохоронці співпрацюватимуть із приватним сектором, аби долати технологічні бар'єри -анонімізацію, шифрування -і отримувати важливі докази вчасно. Правоохоронні заходи слугують інструментом національної влади, зокрема як механізм стримування [18, с. 10].

Компонент II: сприяння американському процвітанню формулює мету: збереження впливу США в технологічній екосистемі та розвиток кіберпростору як відкритого двигуна економічного зростання, інновацій та ефективності. Компонент складається з трьох блоків.

Блок 1. Сприяння динамічній і стійкій цифровій економіці охоплює: стимулювання адаптивного й безпечного ринку технологій; пріоритетність інновацій; інвестиції в інфраструктуру нового покоління; вільний потік даних через кордони; збереження лідерства США в нових технологіях; кібербезпеку повного життєвого циклу.

Захист американських інновацій є критичним для збереження стратегічної переваги США в кіберпросторі. Уряд розвиватиме інститути й програми, що підвищують конкурентоспроможність країни, протидіятиме хижим злиттям та крадіжкам інтелектуальної власності. Він стимулюватиме лідерство США в нових технологіях - штучному інтелекті, квантовій інформації, телекомунікаційній інфраструктурі наступного покоління [18, с. 16].

Підтримка лідерства США в передових технологіях включає глобальне просування інновацій у сфері кібербезпеки через:

- торговельні операції;
- підвищення обізнаності про інноваційні інструменти та послуги американського походження у сфері кібербезпеки;
- викриття та протидію репресивним режимам, які використовують такі інструменти для порушення прав людини;
- усунення бар'єрів для формування єдиного глобального ринку кібербезпеки.

Блок 2. Заохочення й захист винахідливості США охоплює: оновлення механізмів огляду іноземних інвестицій; підтримку збалансованої системи захисту інтелектуальної власності; захист конфіденційності й цілісності американських ідей.

Блок 3. Розвиток висококваліфікованої робочої сили у сфері кібербезпеки: створення «конвеєра талантів»; розширення можливостей перепідготовки та навчання працівників; зміцнення федеральної робочої сили у сфері кібербезпеки; використання виконавчої влади для виявлення й заохочення талантів.

Компонент III: збереження миру через силу -мета полягає в тому, щоб виявляти, протидіяти, руйнувати, ослаблювати та стримувати поведінку в кіберпросторі, яка дестабілізує ситуацію й суперечить національним інтересам, водночас зберігаючи перевагу США в кіберпросторі. Компонент складається з двох блоків.

Блок 1. Підвищення кіберстійкості через норми відповідальної поведінки держави передбачає пріоритетні дії щодо стимулювання дотримання норм у кіберпросторі.

Блок 2. Атрибуція й стримування неприйнятної поведінки в кіберпросторі: формування об'єктивної спільної розвідки; накладення наслідків; розбудова ініціативи кіберстримування; протидія шкідливому кібервпливу та інформаційним операціям.

Компонент IV: просування американського впливу формулює мету: збереження довгострокової відкритості, інтероперабельності, безпеки й надійності Інтернету, що відповідає інтересам США.

Блок 1. Сприяння відкритому, сумісному, надійному та безпечному Інтернету охоплює: захист і заохочення свободи Інтернету; співпрацю з країнами-однодумцями, бізнесом, академічними колами та громадянським суспільством; сприяння багатосторонній моделі управління Інтернетом; розбудову сумісної та надійної комунікаційної інфраструктури; підтримку ринків інновацій США в усьому світі.

Принцип свободи Інтернету є основою Кіберстратегії США. Сполучені Штати декларують намір просувати його як міжнародний стандарт. Водночас будь-які спроби інших держав обмежити цю свободу - навіть під приводом боротьби з тероризмом і забезпечення безпеки -визначаються політичною загрозою та ознакою авторитаризму.

Україна виробляє спільні підходи до протидії кіберінцидентам, всіляко сприяє об'єднанню зусиль у розслідуванні та запобіганні кіберзлочинам, а також не допускає використання кіберпростору в незаконних і військових цілях [30]. З цією метою держава бере участь у міжнародних проєктах, що

нарощують кіберпотенціал, упроваджує європейські та світові надбання у сфері кібербезпеки, сприяє розвитку відповідних органів, які ефективно взаємодіють із ЄС і НАТО. Таким чином Україна стає й джерелом нових знань для міжнародної спільноти [19; 26; 37, с. 12-13].

Зважаючи на важливість теми, організаціям необхідно відповідальніше підходити до кібербезпеки. Можливість інвестицій у цей напрям перетворюється на невід'ємну частину національної стратегії.

Сучасність вимагає посилення реагування на кіберінциденти -це сприяє реалізації Стратегії кібербезпеки України, особливо у виборчих системах та об'єктах критичної інфраструктури. Для цього важливо залучати приватний сектор, запроваджувати механізм обміну інформацією між державними органами, бізнесом і громадянами. Для своєчасного реагування на кіберзлочини посилюють підготовку через тренінги, які проводять висококваліфіковані фахівці у сфері кібербезпеки та цифрової криміналістики за участі міжнародних експертів [30; 37]. Координація й переорієнтація науково-дослідних і дослідно-конструкторських робіт у галузі комп'ютерної безпеки передбачає вдосконалення інформаційних технологій, застосування математичних методів багатовимірного аналізу даних, розробку технологій комплексного захисту апаратних і програмних платформ, виявлення ознак кібератаки за допомогою активних і пасивних сенсорів, створення систем управління, що дають змогу зафіксувати масштабну скоординовану атаку та формувати ранні попередження про можливе джерело загрози [40, с. 5-7].

Користування онлайн-сервісами створює умови для інтеграції України у світовий електронний інформаційний простір. Тому посилення заходів щодо недопущення доступу зловмисників до конфіденційних даних є першочерговим завданням під час упровадження новітніх технологій та електронних транзакцій. Аби зменшити вразливість і ризик крадіжки під час кібератак, персональні дані мають бути ретельно захищені - це стосується електронних виробів, смарт-карток, криптовалют, хмарних сховищ тощо [38]. Найскладніші для захисту складові цифрової інфраструктури наведено на рис. 2.2.



Рис. 2.2. – Найбільш складні для захисту області: мобільні пристрої і дані в хмарі (розроблено автором на основі [47])

Процес має бути автоматизованим: складний інтелектуальний аналіз і алгоритми поведінки дають змогу виявляти нетипову активність і потенційні загрози в реальному часі -саме ті, що реалізує зловмисник. Автоматична ідентифікація підозрілих втручань підвищує ефективність захисту й зменшує потребу в ручній праці. Будь-які інвестиції в цю галузь є виправданими: вони унеможливають втручання в інформацію та запобігають наслідкам, що можуть поставити під загрозу національну безпеку [47, с. 11-12].

Постійний моніторинг рівня кібербезпеки України у світових рейтингах і порівняння його зі світовими практиками свідчить, що проблема потребує комплексного підходу: координації дій на національному, регіональному й міжнародному рівнях, залучення громадян і приватного сектору. Ефективна протидія загрозам потребує співпраці між державами, дієвих розслідувань і переслідування зловмисників. Тому міжнародні зв'язки із зміцнення безпеки кіберпростору та критичної інфраструктури мають бути повністю скоординованими й відповідати глобальним технологічним тенденціям руху до цифрового інформаційного суспільства [51; 53].

РОЗДІЛ 3.

НАПРЯМИ УДОСКОНАЛЕННЯ МЕХАНІЗМІВ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

3.1. Удосконалення нормативно-правової бази в сфері забезпечення кібербезпеки в Україні

Останнім часом Україна активно впроваджує кіберзахист і реагує на кіберінциденти, кібероперації та кібератаки. Привести вітчизняну нормативну базу у відповідність до сучасних потреб і забезпечити протидію кіберзлочинам будь-якого рівня складності - першочергове завдання. Чинна законодавча база у сфері протидії кіберзлочинності лише частково відповідає вимогам часу й не охоплює всіх ключових елементів.

До переліку нормативних документів цієї галузі належать закони України «Про Державну службу спеціального зв'язку та захисту інформації» [23], «Про захист інформації в інформаційно-телекомунікаційних системах», «Про основи національної безпеки України» [20]. Україна має й стратегічні документи: Стратегію національної безпеки та Доктрину інформаційної безпеки [22], а Верховна Рада ратифікувала Конвенцію про кіберзлочинність [39, с. 55-56].

Чинний Кримінальний кодекс в розділі XVI встановлює відповідальність за «злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем і комп'ютерних мереж та мереж електрозв'язку» передбачені статтями 361-363 [1]. У Законі України «Про основні засади забезпечення кібербезпеки України» [27] закріплено терміни та концепції - кібербезпеку, кіберзахист тощо - які ефективно застосовуються у правоохоронній практиці.

Сформовано перелік суб'єктів національної системи кібербезпеки: Державна служба спеціального зв'язку та захисту інформації, Національна поліція, Служба безпеки України, Міністерство оборони, Збройні сили, розвідувальні органи й Національний банк України стаття 8 Закону України «Про основні засади забезпечення кібербезпеки України» [27]. Передбачено

розмежування їхніх функцій. Це принципово нові елементи, яких раніше не існувало: концепції у сфері кібербезпеки та національної системи кіберзахисту. До Закону України «Про оборону України» [28] внесено зміни щодо заходів кіберзахисту - питань державного суверенітету, оборони та запобігання конфліктам у сфері кіберрозвідки.

Кабінет Міністрів України визначив, що Міністерство оборони вживає заходів із забезпечення інформаційної безпеки, кібербезпеки й кіберзахисту, а також готує державу до відсічі військовій агресії в кіберпросторі [32] (підпункт 21 пункту 3). У 2019 році затверджено Положення про Генеральний штаб ЗСУ [33], відповідно до якого військове відомство бере участь у: забезпеченні функціонування єдиної системи кіберзахисту, її розгортанні та управлінні (підпункт 71 пункту 4); періодичному перегляді та формуванні національної системи кібербезпеки (підпункт 73 пункту 4); протидії військовій агресії в кіберпросторі; координації заходів кіберзахисту в органах місцевого самоврядування та виконавчої влади (підпункт 74 пункту 4); забезпеченні безпеки у кіберпросторі за умов використання іншими державами інформаційного простору проти України спеціальними засобами (підпункт 77 пункту 4). Раніше такого не було - бракувало чіткого розподілу відповідальності й узгодженого трактування понять у сфері кібербезпеки [29; 33].

Створено Командування Сил зв'язку та кібербезпеки ЗСУ [42], проте Закон про кібербезпеку не містить його чіткого опису: йдеться про кіберзахист, але не про безпеку. У березні внесли зміни до цих повноважень. Кіберзахист набуває особливого значення в системі національної безпеки, тому доцільно об'єднати всі сили оборони у сфері кібербезпеки (Держспецзв'язок, СБУ та інші) під керівництвом Головнокомандувача ЗСУ. Розробляючи оборонні плани, важливо визначати завдання та заходи з кібербезпеки [4; 35].

Слід зазначити, що під час саміту НАТО у Варшаві кіберпростір визнано сферою операцій [56]. Тому одразу було сформовано План кіберзахисту та дорожню карту [55]. Україна має створити правові умови для потужного кіберзахисту. Враховуючи превентивні й кібернаступальні дії, варто розробити

проект стратегії кіберзахисту України. Слід чітко визначити завдання та заходи у сфері кібербезпеки для формування Плану кіберзахисту: окреслити об'єкти кіберзахисту, структуру системи, її склад, функції й завдання, нарощувати спроможності тощо.

Потрібно встановити правила посилення кібербезпеки для державних установ та об'єктів критичної інфраструктури, визначити організацію, відповідальну за ці норми. Вона повинна щоквартально вносити коригування та проводити аудит. Слід створити умови для вітчизняного виробництва процесорів для виготовлення комп'ютерів, а також українських програм, передусім антивірусів та операційних систем.

3.2. Забезпечення кібербезпеки органів державної влади України

Під час виконання службових обов'язків державні службовці використовують кіберпростір як невід'ємний елемент роботи: листування з державними органами та громадянами, висвітлення діяльності на вебсайтах, електронний документообіг. Це вимагає від держави створення безпечних умов праці в кіберпросторі.

1. Зв'язок між суб'єктом загрози (або просто суб'єктом), його мотивами та способом дії варіюється залежно від галузі. Проте викрадені облікові дані залишаються кращим вектором атаки для фінансово вмотивованих злочинців та організованої злочинності.

Ці дані надважливі - вони показують, що зловмисники полюють саме за обліковими записами користувачів. Тому необхідно приділяти максимум уваги автентифікації, авторизації та правам доступу. Особистість користувача - це новий периметр, який потребує заходів безпеки, спеціально розроблених для перевірки осіб з огляду на їхні робочі функції та потребу в конкретних даних. Крадіжка облікових даних може стати лише першим кроком: маючи робочий обліковий запис у мережі, кіберзлочинець здатний поширити доступ і врешті підвищити привілеї до облікового запису адміністратора домену [47].

Тому концепція «глибокого захисту» залишається доброю стратегією забезпечення особистої безпеки користувачів за рахунок багатфакторної автентифікації. Поширення набуває функція зворотного виклику: користувач спершу автентифікується за обліковими даними (іменем і паролем), а потім отримує запит на введення PIN-коду. Лише за умови проходження обох факторів дозволяється доступ до системи.

Тому пропонується запровадити в державних органах такі заходи:

- паролі системних облікових записів (адміністратора домену, локального адміністратора, root тощо) змінювати щокварталу;
- усі паролі системних облікових записів, а також паролі додатків та активного обладнання зберігати в зашифрованій базі даних з обмеженим доступом;
- термін дії паролів облікових записів домену - не більше 9 місяців, рекомендований інтервал зміни - 6 місяців;
- пароль користувача з адміністративними привілеями, наданими через членство в групі або інструменти на кшталт sudo, повинен бути унікальним щодо інших паролів цього користувача [47, с. 34-36];
- передавати паролі електронною поштою чи іншими відкритими каналами та зберігати їх на комп'ютері заборонено;
- пароль, отриманий користувачем, потрібно змінити при першому вході. Адміністратор домену Active Directory має налаштувати політику паролів, яка забезпечує достатню складність, довжину та частоту зміни - для користувацьких і сервісних облікових записів [47, с. 38];
- для протоколу SNMP використовувати відмінні від стандартних значення рядків підключення (Community Name) - не «public», «private», «system» - і не такі, що збігаються з паролем входу;
- усі користувацькі та системні паролі повинні відповідати цій політиці.

2. Програми є точкою входу для користувача, який передає, обробляє чи зберігає в системі інформацію. Програмне забезпечення стрімко розвивається - питання його безпеки актуальне.

Тому пропонується запровадити в державному органі такі заходи (вони були застосовані під час практики):

- використовувати тільки санкціоновані та ліцензійні програми;
- завантажувати програми лише з офіційних джерел - усі інші є потенційно небезпечними;
- на кожному робочому комп'ютері застосовувати ліцензійний антивірус.

3. Файли та інформація державного значення. Ці дані можуть зберігатися на пристрої користувача, передаватися між хостами, перебувати на жорсткому диску локального сервера або у хмарному сховищі. Здійснено такі заходи:

- шифрування даних у стані спокою - на рівні файлів або диска;
- шифрування даних під час передавання - за допомогою протоколів SSL/TLS;
- регулярне резервне копіювання на сторонній знімний носій.

4. Фішинг як метод зовнішньої розвідки використовується для отримання даних від користувачів організації; він класифікований як інструмент розвідки в межах соціальної інженерії.

Однак фішинг має дві іпостасі: він може бути попередником атаки або самою атакою. Як розвідувальний інструмент хакери здобувають інформацію, видаючи себе за довіреним стороннім орган - наприклад, банк - і змушуючи користувача надати секретну інформацію. Вони можуть експлуатувати жадібність, емоції, страхи, нав'язливі ідеї та недбалість [47, с. 18-20].

Коли ж фішинг застосовується як справжня атака, що компрометує систему, фішингові листи містять корисне навантаження. Зловмисники використовують вкладення або посилання, аби скомпрометувати комп'ютер користувача. У випадку вкладень користувача можуть переконати завантажити прикріплений файл - нерідко це звичайний Word- або PDF-документ, який, утім, може містити шкідливий код. Найпоширеніші типи файлів, які використовуються для поширення шкідливого програмного забезпечення, наведено на рис. 3.1.

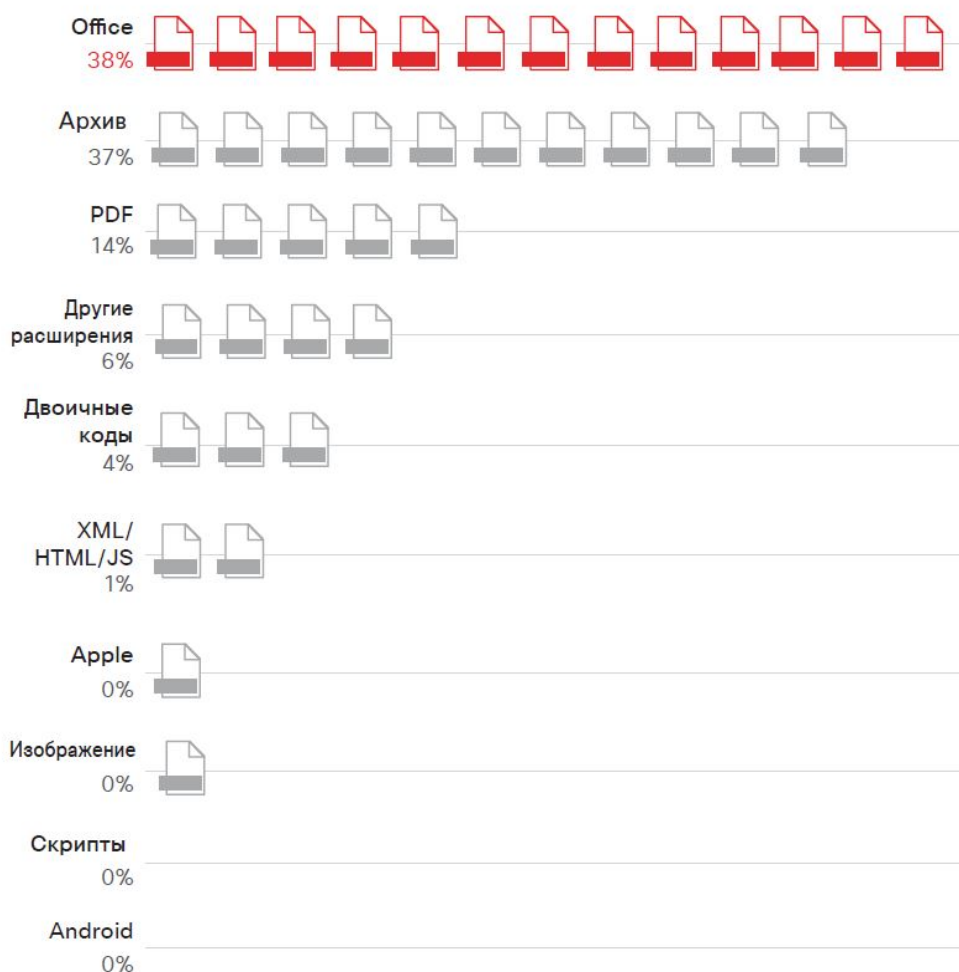


Рис. 3.1. – Основные 10 расширений шкідливих файлів (розроблено автором на основі [47])

Хакери також створюють підроблені сайти й вставляють посилання на них у фішингові листи. Наприклад, користувача можуть повідомити про «помилку безпеки» в банківському рахунку, після чого він змінить пароль через підставне посилання. Сайт-клон вкраде всі введені дані. Інший варіант - посилання спершу веде на шкідливий сайт, де встановлюється шкідливе ПЗ, а потім користувача перенаправляють на реальний сайт. У всіх таких випадках викрадаються автентифікаційні дані, які потім шахраї використовують для переказу коштів або крадіжки файлів. Набирають популярності й повідомлення в соцмережах, які спонукають користувачів натискати на посилання [47, с. 18-20; 49, с. 32-33]. Пропоную запровадити такі заходи:

- у разі надходження таких електронних листів адміністратори безпеки мають уникати запуску вкладень;
- проводити роз'яснення з користувачами, які працюють із поштою у службових справах - інформувати їх про правила безпеки при отриманні кореспонденції;
- проводити аудит мережі на предмет відкритості та наявності проблем у системі захисту;
- забороняти читати листи від незнайомих компаній і людей, особливо коли в темі або тексті є нетипові елементи, посилання на завантаження файлів exe, архівів тощо;
- роз'яснювати необхідність повідомляти безпекову службу про підозрілі дії;
- у жодному разі не вести службове листування через особисті поштові сервіси;
- у службовій діяльності використовувати домени GOV.UA, листи з інших - не відкривати.

5. Державні органи користуються вебсайтами; рівень довіри користувачів до часто відвідуваних ресурсів -інтерактивних форумів, сервісів обміну валют - досить високий. На таких сайтах користувачі схильні до недбалих дій: навіть найобережніші, які не клацають по посиланнях у листах, легко роблять це на знайомих сайтах. Такі ресурси називають «водопоями» (watering holes) -хакери чатують на жертв, як хижаки на тваринах біля водопою. Зловмисники експлуатують уразливості сайту, перехоплюють контроль над ним і впроваджують код, що заражає відвідувачів шкідливим ПЗ або переадресовує їх на шкідливі сторінки.

Через ретельне планування такі атаки зорієнтовані на конкретну мету - операційну систему, додаток або тип користувача. Вони застосовуються навіть проти просунутих ІТ-фахівців, зокрема системних адміністраторів. Прикладом «водопою» є експлуатація вразливостей на сайті StackOverflow.com, який часто відвідують ІТ-співробітники: коли на сайті є вразливість, хакер може впровадити шкідливе ПЗ у комп'ютери відвідувачів.

Тому в державних установах реалізовано такі заходи:

- використовувати SSL-сертифікат для захисту сайту - це шифрує дані під час передавання між користувачем і сервером;

Сторінки з протоколом https забезпечують безпеку на трьох рівнях:

1 рівень - шифрування даних: зловмисники не зможуть прочитати інформацію, якою обмінюються користувач і сайт;

2 рівень - цілісність даних: будь-які зміни під час передавання будуть зафіксовані;

3 рівень - автентифікація: користувач упевнений, що потрапив саме на потрібний, а не на шахрайський сайт.

Щоб задіяти цей протокол, необхідно отримати сертифікат безпеки: проводиться зіставлення даних, які підтверджують власника сайту. Це захищає відвідувачів від атак з перехопленням даних. Після отримання сертифіката його встановлюють на сайт -самостійно або через службу підтримки хостингу. Це підвищує довіру користувачів і ускладнює для зловмисників крадіжку паролів.

- оновлювати програмне забезпечення сайту - CMS, PHP, Apache тощо;

- використовувати захищені канали зв'язку.

Лише за тиждень на початку літа система реагування на кіберінциденти на державних інформаційних ресурсах та об'єктах критичної інфраструктури зафіксувала понад 100 тис. підозрілих подій. Це ще раз підтверджує важливість процесу та значущість заходів протидії кібернетичній агресії для підвищення кібербезпеки держави.

6. Для автоматизації роботи з документами впроваджено електронний документообіг. Це не лише поліпшує роботу з документами, а й вимагає особливої уваги до безпеки. По-перше, варто застосовувати електронний цифровий підпис - він зберігає цілісність та автентичність документа. По-друге, доцільно мати кілька рівнів автентифікації - це забезпечує безпечний вхід та розмежування прав. Для збереження даних потрібен технічний захист сервера, де зберігаються документи й бази даних. По-третє, адміністратори документообігу мають створювати облікові записи з відповідними правами (діловод, користувач, керівник). У Полтавській облдержадміністрації

впроваджено систему АСКОД, на сервері встановлено КСЗІ, права визначає адміністратор, проводиться аудит. Втім, входу з автентифікацією за КЕП наразі немає -варто запровадити кілька рівнів автентифікації.

Проаналізовано поточний ландшафт загроз і способи їх використання для компрометації даних, включно з обліковими, та додатків. Часто застосовуються старі методи (як-от фішинг), але вже у складніших формах. Я ознайомився з реаліями загальнонаціональних загроз і урядових атак. Для захисту організації від нових загроз варто враховувати ключові фактори, що допоможуть державі підвищити рівень безпеки.

Цю роботу можна спрямувати на запобігання несанкціонованому втручанню в державні електронні інформаційні ресурси. Зокрема, адміністраторам безпеки варто:

- уникати запуску вкладень у підозрілих повідомленнях та файлів виконуваних форматів;
- фільтрувати вхідні й вихідні інформаційні потоки, насамперед поштовий і вебтрафік, налаштовувати захист від спаму та підробки адреси відправника через DKIM, SPF, DMARC;
- регулярно перевіряти журнальні файли на наявність зазначених індикаторів;
- забороняти запуск файлів з розширеннями *.exe, *.js, *.com, *.bs на комп'ютерах користувачів з каталогів %TEMP%, %APPDATA%;
- регулярно оновлювати антивірусну базу й сканувати потенційно заражені системи;
- періодично проводити повну перевірку «чутливих» комп'ютерів на наявність шкідливого ПЗ;
- регулярно оновлювати програмне забезпечення та компоненти системи;
- відключати макроси;
- налаштувати Microsoft Word на обмеження мережевого трафіку, дозволяючи лише оновлення.

Ці заходи дієві та цілком безкоштовні. Вони здатні підвищити рівень безпеки приблизно на 70 %. Решта залежить від людського фактора, який

зачіпає психологічні аспекти роботи службовця. Однак постійна роз'яснювальна робота може довести цей показник до 90 %.

Ухвалюють закони та приводять законодавство у відповідність до міжнародних стандартів щодо захисту інформації в країнах ЄС.

Запровадження стандартів системи управління інформаційною безпекою (СУІБ) дозволяє Україні не лише посилити захист, а й наблизитися до норм і стандартів ЄС.

Робота попереду кропітка й важлива: тепер державні інформаційні ресурси та інформація з обмеженим доступом (окрім державної таємниці) за певних умов можуть оброблятися в системі без застосування Комплексної системи захисту інформації (КСЗІ) - запроваджується альтернативний спосіб підтвердження відповідності інформаційної системи вимогам із захисту інформації.

Серед основних напрямів -удосконалення правової основи кіберзахисту об'єктів критичної інфраструктури; впровадження системи незалежного аудиту інформаційної безпеки таких об'єктів; створення галузевих центрів реагування на кіберінциденти; розвиток міжнародного співробітництва; розвиток підготовки кадрів; підвищення цифрової грамотності (правил кібергігієни) громадян і культури безпекової поведінки в кіберпросторі. Сьогодення цього вимагає -держава має бути надійно захищена в кіберпросторі.

Після розвідки зловмисники мають достатньо інформації, аби продовжити або скасувати атаку. Внаслідок зовнішньої розвідки вони знатимуть про поведінку користувачів і використовуватимуть ці знання на шкоду організації. Мета - знайти вразливість, яку можна експлуатувати для доступу до мереж або систем. Внутрішня розвідка натомість дає змогу детальніше вивчити цільову мережу. Деякі з обговорюваних заходів - надзвичайно потужні й здатні запобігти витoku. Зловмисники з'ясовують вразливості, які експлуатуватимуть. У підсумку вони можуть зламати організацію двома шляхами - через користувачів або через вразливості мережі.

Отже варто:

- реформувати правову базу для державних установ із протидії кіберзлочинам;
- проводити незалежний аудит на наявність вразливостей у державних установах;
- створити спеціалізовані центри реагування на кіберзлочини;
- використовувати міжнародні технології для підвищення кібербезпеки;
- готувати фахівців із кібербезпеки;
- навчати та підвищувати кваліфікацію звичайних користувачів, розробляючи правила кіберзахисту, щоб вони почувалися безпечно в кіберпросторі.

Тож, у нормативно-правовому полі необхідно визначити методологію кіберзаходів і запровадити її на об'єктах критичної інфраструктури. Окреслені дієві правила відбиття кібератак і посилення кіберзахисту в державних органах. Їх упровадження на всіх об'єктах підвищить захист приблизно на 70 %.

ВИСНОВКИ ТА ПРОПОЗИЦІЇ

У роботі, відповідно до поставлених завдань, проаналізовано нормативно-правову базу держави, проведено оцінку стану кіберзахисту, а також на основі особистого досвіду надано рекомендації у сфері кібербезпеки. У законодавстві України поняття цієї сфери раніше широко вживалися без юридичного закріплення. Закон України «Про основні засади забезпечення кібербезпеки України» нарешті визначив ключові терміни. Завдяки цьому Україна долучилася до міжнародних і національних стандартів інших держав. Поширення комп'ютерних технологій посилює увагу до негативного інформаційного впливу в кіберпросторі -відповідна протидія належить до заходів кібербезпеки. Усе це зумовило потребу негайного втручання, ухвалення відповідних нормативних документів і встановлення відповідальності за кіберзлочини. Законом окреслено також принципи держави у сфері кібербезпеки, повноваження певних державних органів, відповідальність осіб і громадян, а також основні засади. Ці дії мають на меті захист життєво важливих інтересів людини й громадянина. До принципів забезпечення кібербезпеки включено верховенство права, національні інтереси України, доступність, відкритість і захищеність кіберпростору, розвиток мережі Інтернет. Це дає змогу застосувати комплексний підхід у тісній співпраці з приватним сектором і громадянським суспільством та створити умови для кіберзахисту критично важливих об'єктів і захисту інтересів громадян у правовому полі.

Під час вивчення правового регулювання кібербезпеки в Україні встановлено, що в законодавстві закріплено основні поняття цієї сфери, визначено суб'єкти забезпечення кібербезпеки та їхні завдання. Запроваджено відповідальність за правопорушення в кіберпросторі. Триває гармонізація законодавства зі стандартами міжнародних держав. Тобто держава посилює регулювання на національному й міжнародному рівнях, нарощує свою роль у

цій сфері, дає можливість і приватному сектору, і громадянам усвідомити свою причетність до захисту як власних, так і державних інтересів. Упроваджуються інновації у сфері кіберзахисту, вдосконалюється освіта, готуються фахівці.

Аналіз систем кіберзахисту та кіберзагроз у країнах ЄС засвідчив, що кіберпростір не має кордонів -одна серйозна загроза може зачепити національні інтереси багатьох держав. Розглянуто підхід інших країн до цієї сфери: що вони визначають пріоритетом і яких дій вживають. Доведено, що міжнародна співпраця з цими країнами має бути першочерговим та невід'ємним елементом створення національної системи кіберзахисту. Україні потрібно використовувати міжнародний досвід для захисту інтересів власних громадян у кіберпросторі, а також брати участь в обміні досвідом -у протидії кібератакам, виявленні й покаранні зловмисників тощо.

Аналіз кіберзагроз і систем кіберзахисту в Україні показав, що держава ще має над чим працювати. Слід приділити увагу підготовці й підвищенню кваліфікації фахівців із кіберзахисту, створенню власних операційних систем і програмних продуктів, а також техніки, мікросхем і процесорів. Залучати до цього процесу слід і приватний бізнес, і пересічних громадян. Держава повинна розуміти: вдосконалюючи кіберзахист, вона бере на себе відповідальність за створення належних умов захисту інтересів громадянина та власних. Необхідно сформувати єдину систему кібероборони, окреслити відповідальність і повноваження кожного, хто відповідатиме за кіберзахист, а також створити модель заходів кіберзахисту для впровадження спершу в державній сфері, а згодом -у приватній.

Порівняння рівня кібербезпеки України зі світовими практиками привело до висновку: щоб Україна не перетворилася на полігон сучасної кібервійни, вона має впроваджувати досвід країн, що мають ефективні системи протидії кіберзагрозам. Литва, наприклад, посідає 4 місце, Естонія - 5, Грузія - 18, Україна - 54 місце [51]. Очевидно, з ким варто співпрацювати. Кібератаки з несанкційним доступом та маніпуляційними елементами знищують електронну інформацію та фізичну інфраструктуру обробки даних. Рівень кібербезпеки

можна оцінити за обсягом завданої шкоди. Тому проведення міжнародних і національних форумів, конференцій, семінарів і впровадження наукових напрацювань дасть державі шанс побудувати надійну протидію кібератакам.

Питання кібербезпеки гостро стоїть перед українським суспільством. Пріоритет європейської інтеграції вимагає вдосконалення нормативно-правової бази з кібербезпеки. Вона має відповідати не лише міжнародним стандартам, а й передусім національним інтересам у сфері кіберзахисту. Тому потрібно закріпити в законодавстві правила посилення кібербезпеки об'єктів критичної інфраструктури й державних установ; визначити суб'єкта, відповідального за ці правила, їх коригування, аналіз та модернізацію; створити умови для виробництва вітчизняних процесорів і комп'ютерів, а також українських антивірусних програм.

Формуючи основні напрями державної політики із забезпечення та вдосконалення кібербезпеки, доцільно створити систему, що аналізуватиме й оцінюватиме загрози, оперативно реагуватиме, моніторитиме кіберпростір для своєчасного запобігання та нейтралізації наслідків кібератак. Ці питання мають розглядатися у Стратегії кібербезпеки України, законодавство якої треба гармонізувати з вимогами НАТО і ЄС. Слід розробити методологію боротьби з кіберзлочинністю, а потім втілити ці напрями на практиці.

Розвиток ІТ-сфери за останні десятиліття породжує якісно нові загрози національній і міжнародній безпеці. Протидія таким загрозам є пріоритетом у сфері національної безпеки й оборони. У воєнний час інформаційна сфера створює нові виклики, тому належна підготовка фахівців, здатних розробити механізми і правила дотримання кібербезпеки, дасть змогу вивести її на якісно новий рівень.

У дипломній роботі систематизовано особливості вдосконалення технологій забезпечення кібербезпеки, зокрема:

- визначено поняття «кібербезпека»;
- вивчено досвід упровадження технологій протидії інформаційним загрозам у державно-управлінській практиці провідних країн світу;

- проаналізовано нормативно-правове забезпечення розвитку кібербезпеки в державному управлінні України;
- досліджено систему захисту інформаційно-телекомунікаційного забезпечення органів державної влади;
- проаналізовано технології протидії інформаційним загрозам на державному рівні;
- сформовано практичні рекомендації щодо розвитку.

Слід зазначити, що вивчення системи кібербезпеки України виявило низку невирішених проблем, які істотно знижують захищеність держави. До основних із них належать:

- недостатня нормативно-правова база у сфері інформаційних відносин, у тому числі у сфері забезпечення кібербезпеки;
- слабе державне регулювання процесів функціонування й розвитку ринку засобів інформатизації, інформаційних продуктів і послуг;
- поширене використання у сфері державного управління та кредитно-фінансовій сфері імпортованих технічних і програмних засобів, не захищених від витоку інформації, для зберігання, обробки й передавання даних;
- зростання обсягів інформації, що передається відкритими каналами зв'язку;
- загострення криміногенної ситуації та зростання кількості комп'ютерних злочинів, особливо в кредитно-фінансовій сфері.

Відповідно до зазначеного пропонується:

- запобігти витоку, розкраданню, втраті, перекручуванню, підробці інформації;
- запобігти загрозам державній безпеці, безпеці особи та суспільства в цілому;
- запобігти несанкціонованим діям зі знищення, модифікації, копіювання, блокування інформації;
- запобігти іншим формам незаконного втручання в інформаційні ресурси, бази даних і системи;
- забезпечити правовий режим документованої інформації як об'єкта власності;

- захистити конституційні права громадян на збереження особистої таємниці та конфіденційності персональних даних, що містяться в інформаційних системах і ресурсах суб'єктів та об'єктів різних форм власності;
- забезпечити права суб'єктів в інформаційних процесах при розробленні, виробництві й застосуванні інформаційних систем, технологій та засобів їх забезпечення.

Вивчення досвіду впровадження технологій електронного урядування в державно-управлінській практиці провідних країн світу зосереджено саме на процесі імплементації системи протидії інформаційним загрозам. З'ясовано, що для досягнення стовідсоткового рівня впровадження такої системи в державне управління необхідно:

- максимально ефективного забезпечення національних інтересів;
- побудова розвиненої економіки;
- формування недержавної підсистеми забезпечення національної безпеки;
- формування дієздатних сил національної безпеки;
- інформатизація суспільства;
- регіональне лідерство - одним із його механізмів має стати ініціювання створення систем безпеки різних рівнів, де Україна виступатиме лідером;
- побудова соціально-правової, демократичної держави та громадянського суспільства;
- формування позитивного іміджу України у світі;
- збалансоване функціонування систем безпеки регіонального та вищих рівнів з урахуванням життєво важливих інтересів країн-учасниць.

Дослідження нормативно-правового забезпечення інформаційної безпеки України показало, що відповідна база перебуває у стадії формування й постійного доопрацювання, що негативно позначається на інформаційному суверенітеті держави в цілому.

Становлення системи інформаційного законодавства висуває проблему його гармонізації на міждержавному рівні з урахуванням міжнародного права (публічного й приватного). Сьогодні в міжнародному праві активно формується

нова інституція -міжнародне інформаційне право світової інформаційної цивілізації. У різних регіонах світу з'являються міжнародні правові стандарти у формі типових законів, багатосторонніх конвенцій, угод тощо.

Міжнародне інформаційне законодавство має йти шляхом систематизації через кодифікацію -створення системоутворюючого Кодексу. Він повинен розвивати визначені в Конституції України положення про інформаційні відносини, зокрема щодо інформаційної безпеки людини, суспільства, нації, держави; об'єднувати, вдосконалювати й розвивати норми та принципи суспільних відносин, закріплені у вітчизняному законодавстві; враховувати ратифіковані Україною акти міжнародного права (угоди, конвенції); легалізувати позитивні звичаї в інформаційній сфері та норми суспільної моралі, загальнолюдські цінності, визначені ООН у її Статуті, Декларації прав людини, рішеннях Європейського Союзу та інших загальноприйнятих міждержавних актах -нинішніх стандартах цивілізованості як окремої країни, так і світового співтовариства.

У процесі забезпечення інформаційної безпеки важливо розуміти характер, природу, сутність і зміст загроз та небезпек, своєчасно ідентифікувати джерело загрози.

Ще однією проблемою впровадження системи інформаційної безпеки є недостатнє фінансування. Нехтування цим питанням ставить під загрозу успішне впровадження та модернізацію системи захисту інформації в органах державної влади.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Амелін О. Визначення кіберзлочинів у національному законодавстві. Науковий часопис Національної академії прокуратури України. 2024. С. 1–10. URL: <http://www.chasopysnapu.gp.gov.ua/ua/pdf/11-2024/amelin.pdf> (дата звернення: 01.06.2026).
2. Великий тлумачний словник сучасної української мови / гол. ред. В. Т. Бусел; редактори-лексикографи: В. Т. Бусел, М. Д. Василега-Дерибас, О. В. Дмитрієв та ін. Київ; Ірпінь: ВТФ «Перун», 2005. 1728 с.
3. В Україні створена Національна система кібербезпеки. URL: http://zaxid.net/news/showNews.do?v_ukrayini_bude_stvorena_natsionalna_sistem_kiberbezpeki&objectId=1380648 (дата звернення: 01.06.2026).
4. Військовий стандарт ВСТ 01.004.002. Воєнна безпека. Стратегічне планування. Терміни та визначення. Видання 2. Міністерство оборони України. URL: https://nuou.org.ua/assets/documents/VST_%2001-004-002_2019.pdf (дата звернення: 01.06.2026).
5. Демченко П. Кібернетична безпека як новітній напрям інформаційної складової національної безпеки України: конституційно-правовий аспект. Вісник Львівського університету. Серія юридична. 2024. Вип. 67. С. 170–179.
6. Діордіца І. В. Поняття та зміст національної системи кібербезпеки. URL: <https://goal-int.org/ponyattya-ta-zmist-nacionalnoi-sistemi-kiberbezpeki/> (дата звернення: 01.06.2026).
7. Діордіца І. Поняття і зміст кіберзагроз на сучасному етапі. Адміністративне право і процес. 2024. № 4. С. 99–107.
8. Закон про роз'яснення законного закордонного використання даних. URL: <https://www.congress.gov/bill/115th-congress/senate-bill/2383/all-info> (дата звернення: 01.06.2026).

9. Звіт Голови Національної поліції України про результати роботи відомства. URL: https://www.kmu.gov.ua/storage/app/sites/1/17-civik_2025/zvit_2025/zvit-npu-25pdf (дата звернення: 01.06.2026).
10. Куцаєв В. В., Живило Є. О., Срібний С. П., Черниш Ю. О. Розширення термінології сучасного кіберпростору. URL: mino.esrae.ru/pdf/2024/3Sm/1387.doc (дата звернення: 01.06.2026).
11. Коваль З. В. Динаміка світової управлінської реакції на кіберзагрози: уроки для України. Демократичне врядування. 2024. Вип. 14. URL: http://nbuv.gov.ua/UJRN/DeVr_2024_14_5 (дата звернення: 01.06.2026).
12. Климчук О. О. Роль і місце спецслужб та правоохоронних органів провідних країн світу в національних системах кібербезпеки. Інформаційна безпека людини, суспільства, держави. 2025. № 3. С. 75–83.
13. Камінська Н., Бондар І. Протидія кіберзлочинності: міжнародний досвід та національне законодавство. Правові реформи в Україні: реалії сучасності: матеріали Міжнародної науково-практичної конференції. Київ: НАВС, 2024. С. 34–38.
14. Ліпкан В. А. Поняття системи забезпечення національної безпеки України. Право і Безпека. 2003. Т. 2. № 4. С. 57–60.
15. Можливості боротьби з інформаційною злочинністю в державах «Восточного партнерства»: резолюція наради Ради Європи від 12–14 листопада 2024 р. URL: <http://conventions.coe.int/Treaty/RUS/Treaties/Html/185.htm> (дата звернення: 01.06.2026).
16. Міжнародна стратегія для кіберпростору «Процвітання, безпека, відкритість у мережевому світі». URL: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/international_strategy_for_cyberspace_US.pdf (дата звернення: 01.06.2026).
17. Національна кібер-стратегія Сполучених Штатів Америки. URL: <https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf> (дата звернення: 01.06.2026).

18. Національна кібер-стратегія Сполучених Штатів Америки. 2018. URL: <https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf> (дата звернення: 01.06.2026).
19. Президент: Ми домовилися про оновлений пакет проектів і практичних заходів допомоги для України. Сайт Президента України. URL: <https://www.president.gov.ua/news/prezident-mi-domovilisy-pro-onovlenij-paket-proektiv-i-prak-58149> (дата звернення: 01.06.2026).
20. Про національну безпеку України: Закон України від 21.06.2018 № 2469-VIII. База даних «Законодавство України» / Верховна Рада України. URL: <https://zakon.rada.gov.ua/laws/show/964-15#Text> (дата звернення: 01.06.2026).
21. Про рішення Ради національної безпеки і оборони України від 4 березня 2016 року «Про Концепцію розвитку сектору безпеки і оборони України»: Указ Президента України від 14.03.2016 № 92/2016. URL: <http://zakon3.rada.gov.ua/laws/show/92/2016> (дата звернення: 01.06.2026).
22. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України». URL: <http://www.president.gov.ua/documents/472017-21374> (дата звернення: 01.06.2026).
23. Про Державну службу спеціального зв'язку та захисту інформації України: Закон України від 16.10.2020 № 3475-IV. URL: <https://zakon.rada.gov.ua/laws/show/3475-15#Text> (дата звернення: 01.06.2026).
24. Про телекомунікації: Закон України від 18.11.2003 р. URL: <https://tax.gov.ua/zakonodavstvo/podatkove-zakonodavstvo/zakoni-ukraini/arhiv-zakoniv-ukraini/zakoni-ukraini-za-2003-rik/30850.html> (дата звернення: 01.06.2026).
25. Піскорська Г. А., Яковенко Н. Л. Сучасні виклики і загрози в кіберпросторі: формування механізму міжнародної інформаційної безпеки. Міжнародні відносини. Серія «Політичні науки». 2024. № 18–19. URL: http://journals.iir.kiev.ua/index.php/pol_n/article/view/3389 (дата звернення: 01.06.2026).

26. Про «священну корову» української кібербезпеки: наскільки дієва міжнародна кібердопомога? URL: <https://www.ukrinform.ua/rubric-technology/2567808-pro-svasennu-korovu-ukrainskoi-kiberbezpeki-naskilki-dieva-miznarodna-kiberdopomoga.html> (дата звернення: 01.06.2026).
27. Про основні засади забезпечення кібербезпеки України: Закон України від 24.10.2020 № 2163-VIII. База даних «Законодавство України» / Верховна Рада України. URL: <https://zakon.rada.gov.ua/laws/show/2163-19#Text> (дата звернення: 01.06.2026).
28. Про оборону України: Закон України від 27.03.2020 № 1932-XII. URL: <https://zakon.help/law/1932-XII> (дата звернення: 01.06.2026).
29. Про внесення змін до Положення про Генеральний штаб Збройних Сил України: Указ Президента України від 27.03.2020 № 122/2020. URL: <https://zakon.rada.gov.ua/laws/show/122/2020#Text> (дата звернення: 01.06.2026).
30. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України»: Указ Президента України від 15.03.2016 № 96/2016. URL: <https://zakon.rada.gov.ua/laws/show/96/2016#n11> (дата звернення: 01.06.2026).
31. Положення про Національний координаційний центр кібербезпеки: Указ Президента України від 07.06.2016 № 242. URL: <https://zakon.rada.gov.ua/laws/show/242/2016#n9> (дата звернення: 01.06.2026).
32. Про внесення змін до Положення про Міністерство оборони України: Постанова Кабінету Міністрів України від 10.01.2019 № 1. URL: <https://zakon.rada.gov.ua/laws/show/1-2019-%D0%BF#n55> (дата звернення: 01.06.2026).
33. Положення про Генеральний штаб Збройних Сил України: Указ Президента України від 30.01.2019 № 23. URL: <https://zakon.rada.gov.ua/laws/show/23/2019> (дата звернення: 01.06.2026).
34. Про рішення Ради національної безпеки і оборони України від 2 вересня 2015 року «Про нову редакцію Воєнної доктрини України»: Указ Президента

України від 24.09.2015 № 555. URL: <https://zakon.rada.gov.ua/laws/show/555/2015> (дата звернення: 01.06.2026).

35. Про рішення Ради національної безпеки і оборони України від 20 травня 2016 року «Про Стратегічний оборонний бюлетень України»: Указ Президента України від 06.06.2016 № 240. URL: <https://zakon.rada.gov.ua/laws/show/240/2016#n10> (дата звернення: 01.06.2026).

36. Розпорядження Президента 13800 «Зміцнення федеральних мереж та критичної інфраструктури». URL: <https://www.dhs.gov/executive-order-strengthening-cybersecurity-federal-networks-and-critical-infrastructure> (дата звернення: 01.06.2026).

37. Співробітництво Україна – ЄС – НАТО з протидії загрозам у кіберсфері / Центр глобалістики «Стратегія XXI». URL: <https://ukraine-office.eu/eu-nato-ukraine-cooperation-to-counter-hybrid-threats-in-the-cyber-field/> (дата звернення: 01.06.2026).

38. Трофименко О. Г. Моніторинг стану кібербезпеки в Україні. Правове життя сучасної України: матеріали міжнародної науково-практичної конференції: у 2 т. Т. 1. Одеса: Видавничий дім «Гельветика», 2019. С. 642–646.

39. Трофименко О. Г. Законодавча база забезпечення кібербезпеки держави. Кібербезпека в Україні: правові та організаційні питання: матеріали II Всеукраїнської науково-практичної конференції, 17 листопада 2024 р. Одеса: ОДУВС, 2024. С. 55–56.

40. Трофименко О. Г., Дубовой Я. В. Щодо правового потенціалу безпечного функціонування кіберпростору. Кібербезпека в Україні: правові та організаційні питання: матеріали III Всеукраїнської науково-практичної конференції, 30 листопада 2025 р. Одеса: ОДУВС, 2025. С. 5–7.

41. Заявив про нові кіберзагрози з боку Росії, 11 липня 2024 р. URL: <https://www.ukrinform.ua/rubric-polytics/2048633-turcinov-zaaviv-pro-novi-kiberzagrozi-z-boku-rosii.html> (дата звернення: 01.06.2026).

42. У Збройних Силах України створено нові командування: Управління зв'язків з громадськістю Збройних Сил України. URL:

<http://www.mil.gov.ua/news/2024/02/07/u-zbrojnih-silah-ukraini-stvoreno-novi-komanduvannya/> (дата звернення: 01.06.2026).

43. Шеломенцев В. П. Правове забезпечення системи кібернетичної безпеки України та основні напрями її удосконалення. Боротьба з організованою злочинністю і корупцією: теорія і практика. 2012. Вип. 1. С. 312–320.

44. Шеломенцев В. П. Сутність організаційного забезпечення системи кібернетичної безпеки України та напрями його удосконалення. Боротьба з організованою злочинністю і корупцією: теорія і практика. Київ: Міжвідомчий науково-дослідний центр з проблем боротьби з організованою злочинністю, 2012. № 2 (28). С. 299–309.

45. Шемчук В. В. Інформаційна безпека та інформаційна оборона в контексті розвитку інформаційної безпеки та захисту інформації в контексті розвитку національної доктрини та законодавчої бази. Вчені записки ТНУ імені В. І. Вернадського. 2019. № 4. С. 31–37. URL:

http://www.juris.vernadskyjournals.in.ua/journals/2019/4_2019/8.pdf (дата звернення: 01.06.2026).

46. Як Китай використовував крихітний чіп для проникнення на сайт США «Bloomberg». URL: <https://www.bloomberg.com/news/features/2025-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies> (дата звернення: 01.06.2026).

47. Cisco annual cybersecurity report 2018. URL: https://www.cisco.com/c/dam/m/hu_hu/campaigns/security-hub/pdf/acr-2025.pdf (дата звернення: 01.06.2026).

48. CrowdStrike Global Threat Report 2025. URL: <https://go.crowdstrike.com/rs/281-OBQ-266/images/CrowdStrikeGlobalThreatReport2025.pdf?version=0> (дата звернення: 01.06.2026).

49. Cyber Attack Trends: 2025 Mid-Year Report. URL: <https://www.checkpoint.com/downloads/resources/cyber-attack-trends-report-mid-year-2025.pdf> (дата звернення: 01.06.2026).

50. European Commission. Commission Staff Working Document: Impact Assessment accompanying the document Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high level of network and information security across the Union. SWD(2013) 32 final. Strasbourg, 7 February 2013. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52013SC0032> (дата звернення: 01.06.2026).
51. Global Cybersecurity Index (GCI) 2018. URL: https://www.itu-ibrary.org/science-and-technology/global-cybersecurity-index-2018_pub/813559ed-en (дата звернення: 01.06.2026).
52. McAfee Labs Threats Report August 2019. URL: <https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-aug-2019.pdf> (дата звернення: 01.06.2026).
53. National Cyber Security Index (NCSI) 2018. URL: https://ega.ee/wp-content/uploads/2018/05/ncsi_digital_smaller.pdf (дата звернення: 01.06.2026).
54. National Strategies. URL: <https://www.itu.int/en/ITU-D/Cybersecurity/Pages/cybersecurity-national-strategies.aspx> (дата звернення: 01.06.2026).
55. Press conference by NATO Secretary General Jens Stoltenberg following the meeting of the North Atlantic Council at the level of Defense Ministers, 16 February 2017. URL: https://www.nato.int/cps/ru/natohq/opinions_141340.htm. (дата звернення: 01.06.2026).
56. Warsaw Summit Communiqué: Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw, 8–9 July 2025. URL: https://www.nato.int/cps/ru/natohq/official_texts_133169.htm?selectedLocale=en (дата звернення: 01.06.2026).

ДОДАТКИ

ДОДАТОК А

Матеріали апробації результатів кваліфікаційної роботи



Міністерство освіти і науки України
 Національний університет
 «Полтавська політехніка імені Юрія Кондратюка»
 Ghent University (Бельгія)
 «1 DECEMBRIE 1918» University of Alba Iulia (Румунія)
 UNIVERSITY ISMA (Латвійська республіка)
 VARNA FREE UNIVERSITY «CHERNORIZETS HRABAR» (Болгарія)
 Академія праці, соціальних відносин та туризму
 Київський національний економічний університет імені Вадима Гетьмана
 Національний технічний університет «Дніпропетровська політехніка»
 Національний університет «Чернігівська політехніка»
 Тернопільський національний технічний університет імені Івана Пулюя
 Хмельницький університет управління та права імені Леоніда Юзькова

**Матеріали XIII Міжнародної
 науково-практичної Інтернет-конференції
 ОРГАНІЗАЦІЙНО-ПРАВОВІ АСПЕКТИ ПУБЛІЧНОГО
 УПРАВЛІННЯ В УКРАЇНІ**

23 квітня 2026 року



Полтава – 2026

ЗМІСТ

СЕКЦІЯ 1. ТЕОРЕТИКО-ПРАКТИЧНІ АСПЕКТИ РЕФОРМУВАННЯ ДЕРЖАВНОЇ СЛУЖБИ В УМОВАХ ЄВРОІНТЕГРАЦІЇ.....	12
<i>Адамович Віталій Романович</i> РЕГЛАМЕНТАЦІЯ КАДРОВОЇ РОБОТИ ЯК СКЛАДОВА ОРГАНІЗАЦІЙНОГО МЕХАНІЗМУ УПРАВЛІННЯ ПЕРСОНАЛОМ У ПУБЛІЧНІЙ СЛУЖБІ.....	12
<i>Александрович Андрій Олександрович</i> ЦИФРОВІ ІНСТРУМЕНТИ АДВОКАЦІЇ В ПУБЛІЧНОМУ УПРАВЛІННІ В УМОВАХ ВОЄННОГО СТАНУ.....	14
<i>Арабаджийський Ніколай Запрінов</i> УДОСКОНАЛЕННЯ СИСТЕМИ АДМІНІСТРАТИВНИХ ПОСЛУГ ПУБЛІЧНОЇ АДМІНІСТРАЦІЇ В РЕСПУБЛІЦІ БОЛГАРІЯ.....	16
<i>Білоусов Петро Сергійович</i> ЗАРУБІЖНИЙ ДОСВІД ЗАБЕЗПЕЧЕННЯ ДЕРЖАВНОЇ СЛУЖБИ У ПРАВООХОРОННІЙ СФЕРІ: ПЕРСПЕКТИВИ ДЛЯ УКРАЇНИ.....	18
<i>Гончарук Наталія Трохимівна,</i> РЕФОРМУВАННЯ ДЕРЖАВНОГО УПРАВЛІННЯ В УКРАЇНІ: СУЧАСНИЙ СТАН ТА СТРАТЕГІЧНІ ПРІОРИТЕТИ.....	20
<i>Гошовська Єлизавета Євгенівна,</i> КОРУПЦІЯ ЯК НЕГАТИВНЕ СОЦІАЛЬНО-ПРАВОВЕ ЯВИЩЕ В ОРГАНАХ ПУБЛІЧНОГО УПРАВЛІННЯ.....	24
<i>Діденко Софія Валентинівна</i> ДЕРЖАВНА ПОЛІТИКА У СФЕРІ КУЛЬТУРИ В КРАЇНАХ ЄВРОПЕЙСЬКОГО СОЮЗУ.....	26
<i>Задорожний Володимир Петрович,</i> <i>Шевченко Наталія Миколаївна</i> СУЧАСНІ ТЕНДЕНЦІЇ ДЕРЖАВНОЇ ПОДАТКОВОЇ ПОЛІТИКИ.....	28
<i>Качан Яна Віталіївна</i> ФУНКЦІОНУВАННЯ ТЕРИТОРІАЛЬНИХ ОРГАНІВ ВИКОНАВЧОЇ ВЛАДИ В УМОВАХ ВОЄННОГО СТАНУ: ОРГАНІЗАЦІЙНО-ПРАВОВІ ТА УПРАВЛІНСЬКІ АСПЕКТИ.....	30
<i>Казакова Олександра Дмитрівна,</i> ФОРМУВАННЯ ПОЗИТИВНОГО ІМІДЖУ ОРГАНІВ ПУБЛІЧНОЇ ВЛАДИ: ЕТИЧНІ АСПЕКТИ.....	33
<i>Костенко Валерія Юрійвна</i> СИСТЕМИ КІБЕРЗАХИСТУ ТА КІБЕРЗАГРОЗ У КРАЇНАХ ЄС.....	36

Костенко Валерія Юріївна

Національний університет

«Полтавська політехніка імені Юрія Кондратюка»,

здобувачка першого (бакалаврського) рівня вищої освіти,

спеціальність 281 «Публічне управління та адміністрування»

СИСТЕМИ КІБЕРЗАХИСТУ ТА КІБЕРЗАГРОЗ У КРАЇНАХ ЄС

Кіберзагрози можуть суттєво впливати на внутрішній ринок Європейського Союзу, оскільки кіберпростір не має кордонів і навіть одна атака здатна порушити функціонування кількох держав. Злам мережесистем, зокрема транспортної інфраструктури, може призвести до зупинки транскордонних сервісів і негативних економічних наслідків. Наприклад, у 2010 році атаки на eBay обмежили доступ до веб-сайтів і призвели до призупинення електронної комерції [4].

Важливим прикладом є інцидент із компанією DigiNotar, яка після зламу видала фальшиві сертифікати, що підірвало довіру до цифрової безпеки. У відповідь країни ЄС почали впроваджувати механізми обов'язкового повідомлення про кіберінциденти та обміну інформацією між державними органами і приватним сектором [3; 6].

Серед причин загроз для інформаційно-комунікаційних систем важливу роль відіграють природні фактори та технічні збої. Наприклад, затоплення річки Ельби у 2002 році пошкодило комунікаційну інфраструктуру і спричинило збої в роботі мереж, а аварії кабельних мереж можуть призводити до тривалого відключення Інтернету та значних економічних втрат [4; 6]. Водночас ключовим чинником більшості кіберінцидентів залишається людський фактор. Користувачі часто стають причиною поширення шкідливого програмного забезпечення через необережні дії, зокрема відкриття підозрілих файлів або використання ненадійних носіїв інформації.

Інформаційно-комунікаційні технології є важливою складовою сучасного суспільства та економіки, забезпечуючи функціонування державного управління, бізнесу і соціальних сервісів. Зростання використання Інтернету сприяє економічному розвитку, однак водночас підвищує вразливість до кіберзагроз, які можуть дестабілізувати систему. Кібератаки здатні суттєво впливати на державну інфраструктуру. Так, у 2007 році Естонія зазнала масштабних атак, які порушили роботу електронного управління та банківських систем, а в подальшому подібні інциденти спостерігалися і в установах ЄС [6].

Кіберзагрози завдають значних фінансових збитків, особливо бізнесу, що функціонує в Інтернеті. За даними звітів, близько 16% компаній у ЄС зазнавали кібератак. Зокрема, у 2011 році атаки на Sony та BlackBerry спричинили мільйонні збитки, а банківські установи зазнали втрат і витоку конфіденційних даних [7].

Водночас найбільше страждають користувачі, оскільки вони залежать від стабільної роботи цифрових сервісів. Наприклад, збій у

роботі BlackBerry вплинув на десятки мільйонів користувачів, а технічні проблеми банківських систем обмежили доступ до фінансових послуг [7].

Кіберзагрози є особливо небезпечними для критичної інфраструктури, зокрема енергетики та транспорту. Порушення роботи таких систем може призвести не лише до економічних втрат, а й до екологічних наслідків та загрози життю людей.

Європейський Союз стикається з проблемами координації кібербезпеки, оскільки держави-члени мають різний рівень розвитку ІКТ та витрат на безпеку. Для ефективної протидії загрозам необхідна співпраця між державними органами та приватним сектором, а також обмін інформацією між країнами.

За рівнем розвитку кібербезпеки країни ЄС умовно поділяються на групи. До лідерів належать Данія, Фінляндія, Нідерланди, Швеція та Велика Британія, які активно інвестують у цю сферу. Інші країни також розвивають свої можливості, однак їхній рівень є нижчим [3].

Історично захист інформації існував ще до появи сучасних технологій. Під час світових воєн застосовувалися методи шифрування та радіоперехоплення. Важливим етапом розвитку криптографії стало використання машини «Enigma» та її дешифрування британськими науковцями [1].

У сучасних умовах кіберзагрози залишаються ефективним інструментом як для злочинців, так і для держав, хоча методи їх реалізації значно ускладнилися. Для протидії цим загрозам діють міжнародні організації, зокрема Міжнародний союз телекомунікацій та Організація економічного співробітництва та розвитку, які сприяють розвитку кіберполітики. Особливу роль відіграють НАТО та Європейський Союз, які інтегрують кібербезпеку у свої стратегії безпеки та розвивають співпрацю для ефективного реагування на загрози. Європейський Союз сформував стратегію кібербезпеки, спрямовану на попередження та реагування на кіберзагрози, захист основних прав громадян і забезпечення стабільного розвитку цифрової економіки. Також була розроблена директива щодо захисту мереж та інформаційних систем, яка встановлює високий рівень безпеки в межах Союзу [4].

Політика ЄС у сфері кібербезпеки передбачає боротьбу з кіберзлочинністю, у тому числі транскордонною, а також узгодження національних стратегій держав-членів із загальноєвропейськими принципами. Основні принципи цієї політики включають захист даних і прав людини, забезпечення доступу до Інтернету, демократичне управління кіберпростором та відповідальність за безпеку.

Важливою умовою ефективної протидії кіберзагрозам є співпраця між державними структурами та приватним сектором, оскільки значна частина інфраструктури кіберпростору належить саме приватним компаніям. Держава самотійно не може забезпечити повний рівень кібербезпеки, тому участь бізнесу є необхідною. Водночас притягнення кіберзлочинців до відповідальності ускладнюється недостатністю тех-

нічних ресурсів і складністю їх ідентифікації. Це підсилює необхідність активної участі приватного сектору у формуванні системи кіберзахисту [4].

Для зниження рівня кіберзлочинності важливим є вдосконалення законодавства та міжнародна співпраця. Ключову роль у цьому відіграє Конвенція про кіберзлочинність, яка забезпечує координацію дій держав у боротьбі з кіберзагрозами. Україна також інтегрує європейські підходи до забезпечення національної безпеки, визнаючи кіберзагрози однією з основних проблем[2].

У результаті проведеного аналізу встановлено, що державна політика у сфері кібербезпеки передбачає визначення основних понять, суб'єктів і об'єктів кіберзахисту, зокрема критичної інфраструктури. Це створює правову основу для реагування на кіберзлочини та підвищення рівня безпеки.

Важливим напрямом є впровадження міжнародних стандартів і розвиток співробітництва у сфері кібербезпеки, що сприяє ефективній протидії кіберзагрозам та підвищенню рівня кіберграмотності.

Література

1. Кримінологічний довідник / О.М. Бандурка, В.С. Батиргарєєва, О.М. Литвинов та ін. / за наук. ред. О.М. Бандурки. Харків: Золота миля, 2023. 412 с.
2. Коваль З.В. Динаміка світової управлінської реакції на кіберзагрози: уроки для України // Демократичне врядування. 2024. Вип. 14 URL: http://nbuv.gov.ua/UJRN/DeVr_2024_14_5
3. Камінська Н. та Бондар І. Протидія кіберзлочинності: міжнародний досвід та національне законодавство. Правові реформи в Україні: реалії сучасності, Правові реформи в Україні: реалії сьогодення: Матеріали Міжнародної науково-практичної конференції. Київ: НАВС, 2024, С. 34-38.
4. Міжнародна стратегія для кіберпростору «Процвітання, безпека, відкритість у мережевому світі». URL: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/international_strategy_for_cyberspace_US.pdf
5. Марков В.В. Статистичне дослідження показників кіберзлочинності: методологічний аспект. Право і Безпека. 2025. № 2. С. 136 - 139
6. Піскорська Г. А. Сучасні виклики і загрози в кіберпросторі: формування механізму міжнародної інформаційної безпеки / Г. А. Піскорська, Н. Л. Яковенко // Міжнародні відносини. Серія «Політичні науки». 24. № 18–19 URL: http://journals.iir.kiev.ua/index.php/pol_n/article/view/3389
7. Cyber crime costs global economy \$445 billion a year: report URL: <https://www.reuters.com/article/us-cybersecurity-mcafee-csis/cyber-crime-costs-global-economy-445-billion-a-year-report-idUSKBN0EK0SV20140609>