УДК 340+35.078.3

ДОВГАНЬ О.Д., *доктор юридичних наук, професор*,
НДІ інформатики і права НАПрН України
ТАРАСЮК А.В., *кандидат юридичних наук,*
НДІ інформатики і права НАПрН України

ПРОТИДІЯ ЗАГРОЗАМ КІБЕРБЕЗПЕЦІ ДЕРЖАВИ НА ГЛОБАЛЬНОМУ РІВНІ

Анотація. *У статті проаналізовано основні тенденції розвитку кіберпростору, а також визначені пов'язані із цим актуальні проблеми забезпечення кібербезпеки на глобальному та національному рівнях, зокрема, у контексті забезпечення безпеки об'єктів критичної інфраструктури, становлення Інтернету речей тощо. За результатами дослідження визначені можливі шляхи вирішення відповідних проблем та підвищення ефективності забезпечення кібербезпеки.*

Ключові слова: *кібербезпека, інформаційна безпека, кіберпростір, кіберзагрози, кіберсистема, критична інфраструктура, інтернет речей.*

Summary: *The article analyzes the main trends in the development of cyberspace and identifies related cyber security issues at the global and national levels, in particular in the context of ensuring the security of critical infrastructure, the emergence of the Internet of Things and so on. According to the results of the study, the possible ways of solving the corresponding problems and improving the efficiency of providing cybersecurity were identified.*

Keywords: *cybersecurity, information security, cyberspace, cyber threats, cyber system, critical infrastructure, Internet of Things.*

Аннотация: *В статье проанализированы основные тенденции развития киберпространства, а также определены связанные с этим актуальные проблемы обеспечения кибербезопасности на глобальном и национальном уровнях, в частности, в контексте обеспечения безопасности объектов критической инфраструктуры, становление Интернета вещей и тому подобное. По результатам исследования определены возможные пути решения соответствующих проблем и повышения эффективности обеспечения кибербезопасности.*

Ключевые слова: *кибербезопасность, информационная безопасность, киберпространство, киберугрозы, киберсистемы, критическая инфраструктура, интернет вещей.*

Постановка проблеми. Перші десятиліття 21 століття можна охарактеризувати як справжній прорив інформаційної греблі, коли хвилі інформаційних мереж і технологій досягли практично кожної людини. Глобальне поширення інформаційних мереж, передовсім Інтернету, зумовлює актуалізацію проблематики доступу до інформації, сумісності мереж тощо. Але водночас заходи із забезпечення безпеки глобальних мереж у теперішній важко визнати адекватними. Значною мірою це зумовлено тим, що загальносвітова соціально-економічна вагомість Інтернету виявилася дещо пізніше, а спочатку він замислювався як засіб якнайбільшого накопичення наукових даних і якнайшвидшого обміну ними. Відтак, відповідні безпекові заходи і засоби поки що змушені постійно наздоганяти стрімке поширення й удосконалення як конструктивних, так і зловмисних Інтернет-технологій.

Як і будь-яке досягнення науково-технічного прогресу, розвиток кіберпростору має як переваги, так і недоліки. До переваг може бути віднесені оперативність та розмаїття інформаційної взаємодії для ефективності розвитку всіх сфер людської діяльності,

розширення можливостей використання всього обсягу накопичених людством знань, тоді як до недоліків – розширення можливостей несанкціонованого доступу з будь-якої точки до будь-якої іншої точки кіберпростору, в тому числі й з протиправними намірам (саме такі можливості і розглядаються як загрози порушення нормального режиму функціонування кіберпростору, тобто, кіберзагрози). Динамічний розвиток світового кіберпростору істотно підвищує небезпеку реалізації кіберзагрози, актуалізуючи значну кількість проблем забезпечення кібербезпеки на глобальному та національному рівнях.

Результати аналізу наукових публікацій. В основу написання даної статті покладено аналіз чинного інформаційного законодавства, законопроекти, які стосуються предмету дослідження, а також творчий доробок відомих вчених, зокрема В. Білоуса, В. Брижка, О. Довганя, І. Дороніна, В. Рубана, Т. Ткачука, В. Фурашева та ін.

Метою статті є визначення концептуальних засад правового співвідношення інформаційної та кібернетичної безпеки на сучасному етапі з урахуванням сучасних загроз та перспектив розвитку.

Виклад основного матеріалу. Сьогодні практично всі розвинені країни наразі розробили національні стратегії кібербезпеки, за якими здійснюватимуть захист своєї частини світового кіберпростору і участі в світовій кооперації вирішення виникаючих проблем. Розроблено та затверджено Міжнародний Стандарт ISO IEC 27032-2012 “Інформаціонние технології – технології безпеки – вимоги для кібербезпеки”, відповідно до якого поняття “кібербезпека” розглядається як узагальнююче і включає в себе питання забезпечення безпеки систем, комунікацій і об’єктів, що входять до складу кіберпростору (інформаційної безпеки, безпеки мережевих структур, безпеки Інтернету, захисту критичної інформаційної інфраструктури тощо). До найважливіших положень Стандарту, на які мають орієнтуватися національні стратегії, слід віднести міжнародне співробітництво в реалізації спільних рішень, а також тісний контакт суспільства, держави і бізнесу в забезпеченні кібербезпеки.

Визначення актуальних питань протидії кіберзагрозам передбачає виділення критичних сфер національного кіберпростору, які вимагають захисту, і їх специфіки. До таких критичних сфер мають бути віднесені: інформаційна безпека, яку слід розглядати у широкому сенсі; безпека інформаційно-телекомунікаційного середовища, яка передбачає забезпечення безпеки всіх каналів і спеціальних систем зв’язку, що реалізують інформаційні взаємозв'язку будь-яких автоматизованих систем (систем органів державної влади, оборони, правопорядку, соціальної сфери, органів місцевого самоврядування, виробництва і технологічних процесів, корпоративних, громадських тощо) між собою і з зовнішнім світом; безпека автоматизованих систем управління і інформаційного забезпечення життєво важливих елементів національної інфраструктури.

У контексті загроз у кіберпросторі однією із основних проблем убачається здебільшого приватна належність інформаційно-комунікаційних мереж, тоді як на державу покладається значна частина відповідальності за їх безпеку. При цьому інтереси вказаних суб’єктів зазвичай різняться, що, звісно, не сприяє організації належного захисту інформаційної сфери з одночасним забезпеченням дотримання основних прав і свобод людини. Ситуація ускладнюється через глобальність як самої проблеми, так і методів і засобів її розв’язання.

На нашу думку, вагоме слово стосовно розробки міжнародно-правових норм щодо функціонування й захисту інформаційної сфери мають сказати міжнародні структури, створені для боротьби з кібернетичною злочинністю. З-поміж таких структур можна назвати, зокрема, підгрупу Великої вісімки з питань високотехнологічної (кібернетичної) злочинності, Конгрес ООН з питань профілактики злочинності та

кримінального судочинства, Конференція Ради Європи з питань співробітництва у сфері боротьби з кіберзлочинністю та ін. Вони здатні виступити координаторами оптимізації національних законодавств у частині регулювання питань притягнення до відповідальності (у тому числі кримінальної) за правопорушення у даній сфері, ведення слідчих дій та інших процесуальних моментів, гарантування недоторканності приватного життя та збереження особистих даних, забезпечення мережевої безпеки, адекватного реагування на кібератаки тощо. Убачається, що ці міжнародні структури можуть також посприяти виявленню прогалин у системі нагляду, формуванню дійових методів суспільного контролю над діяльністю суб'єктів боротьби з кібернетичними правопорушеннями.

Особливої уваги це питання потребує тому, що вказані міжнародні структури при розробці заходів протидії кіберзлочинності питання контролю відсувають на задній план, зосереджуючись переважно на дієвості. А тим часом, значні відмінності окремих національних законодавств, розрив у ресурсних і технічних потенціях різних країн ще більше актуалізують проблематику контролю й нагляду.

Приміром, величезні кошти у програми боротьби з кібернетичною злочинністю та вдосконалення відповідного законодавства вкладають уряди Великої Британії та США, тоді як чимало країн не мають не те що стратегій забезпечення кібербезпеки та боротьби з різновекторними кіберзагрозами, ба навіть базової інформаційної інфраструктури.

Брак технічних можливостей для ефективної боротьби з кібернетичними правопорушеннями, посилений слабким правовим забезпеченням, практично унеможливлює їх розкриття і притягнення винних до відповідальності. Звідси випливає потреба розробки нормативно-правової бази сфери кібербезпеки й боротьби з кіберзлочинністю, зокрема й дійового регулювання питань суспільного контролю. Крім того, відсутність спеціальних державних наглядових інституцій підвищує загрози порушення прав людини на недоторканність приватного життя, свободу думки, об'єднань тощо.

Серед чинних міжнародно-правових документів у цій сфері слід назвати резолюції Генасамблеї ООН "Боротьба із використанням інформаційних технологій зі злочинною метою" від 4 грудня 2000 року 55/63 і від 19 грудня 2001 року № 56/121, а також ухвалені Всесвітньою конференцією "Співробітництво проти кіберзлочинності", що відбулася 1 – 2 квітня 2008 року у Страсбурзі, "Головні принципи спільної роботи правоохоронних органів та Інтернет-провайдерів у сфері боротьби з кіберзлочинністю". З-поміж відповідних регіональних правових актів варто виокремити Рекомендацію Ради Європи "Про боротьбу з комп'ютерними злочинами" (№ R(89)9) та Європейську Конвенцію "Про боротьбу з кіберзлочинністю". Цей документ зобов'язує учасників Ради Європи передбачити в національних законодавствах повноваження відповідних органів, а також процедури для провадження розслідувань, зокрема для збирання електронних доказів у кримінальних злочинах, які вчинюються за допомогою комп'ютерних технологій.

Боротьби з кіберзлочинністю безпосередньо стосуються деякі правові акти щодо захисту прав людини міжнародного й регіонального характеру. Це, наприклад: ухвалений Генасамблеєю ООН у 1966 році Міжнародний пакт про громадянські й політичні права, де, зокрема, йдеться про права на недоторканність приватного життя (ст. 17), на свободу висловлення думки (ст. 19) та на свободу об'єднань (ст. 22); Європейська конвенція з прав людини, Американська конвенція з прав людини, Африканська хартія прав людини і народів та ін.

Захист електронних даних теж входить до функцій згаданих вище міжнародних і регіональних організацій. Так, положення щодо захисту прав на недоторканність приватного життя та свободу висловлення думки під час розміщення персональних даних в електронних мережах, електронного листування тощо містять ухвалені Генасамблеєю ООН "Принципи регулювання комп'ютеризованих баз персональних даних", прийнята Радою Європи Конвенція "Про захист фізичних осіб у зв'язку з автоматизованою обробкою персональних даних" та ін.

Уряди багатьох країн в своїх стратегіях кібербезпеки приділяють особливу увагу інфраструктурі, тісно пов'язаної з питаннями безпеки. Для оцінки масштабу проблеми кібербезпеки і можливих загроз важливо розуміти взаємозв'язок між кібербезпекою й критичною інфраструктурою. Критична інфраструктура складається як з матеріальних (наприклад, будівель і споруд), так і віртуальних елементів (наприклад, систем і даних). Кожна країна може мати своє розуміння терміна "найважливіший", проте зазвичай це поняття може включати в себе елементи інформаційно-комунікаційних технологій (включаючи електрозв'язок, енергетику, банківська справа, транспорт, суспільна охорона здоров'я, сільське господарство і продовольство, водопостачання, хімічну промисловість, судноплавство, а також найважливіші державні служби). Кожен з цих секторів економіки має свої власні матеріальні ресурси, наприклад будівлі банків, електростанції, поїзди, лікарні і урядові офіси. Разом з тим, всі ці найважливіші сектори національної економіки залежать від інформаційно-комунікаційних технологій. Відтак загальносвітові тенденції використання інформаційно-комунікаційних технологій роблять критичну інфраструктуру всіх секторів більш вразливою для кібератак.

Зокрема, актуальним для України є питання кіберзахисту цивільних ядерних об'єктів. Слід враховувати, що для цивільних ядерних об'єктів не існує універсальних стандартних рішень з інтеграції інформаційних технологій. Кожна атомна електростанція, її архітектури і топології є унікальним об'єктом, на якому реалізовані оригінальні рішення з такої інтеграції. Відповідно, в кожному випадку мереж та ІТ-системам такого об'єкта притаманний унікальний набір вразливостей кібербезпеки, що істотно обмежує можливості і практичний сенс застосування операторами цивільних ядерних об'єктів накопиченого досвіду і кращих іноземних практик. Існує проблема довіри до ІТ-постачальників і необхідність забезпечення цілісності ланцюжків поставок ІТ-продукції, більшість з яких – транснаціональні компанії. Відсутність конкурентоспроможних вітчизняних рішень на ринку змушує використовувати імпортні аналоги обладнання та програмного забезпечення. Таким чином, в даний момент ІТ-інфраструктура України (і це стосується не лише цивільних ядерних об'єктів) залежна від іноземних виробників і розробників, активно впроваджуючи їх вирішення (від бібліотек програмного забезпечення до апаратних платформ і систем управління). Фактично на кожній з ділянок ІТ-інфраструктури з високою часткою ймовірності використовуються закордонні рішення з невідомою "начинкою". Рішенням цієї проблеми видається популярна в світі аутсорсингова модель виробництва, згідно з якою розробка і виведення на ринок затребуваних продуктів можливі лише за умови тісної кооперації з зарубіжними та вітчизняними компаніями. Це дозволяє на етапі проектування сформувати концепцію нового продукту, пред'являючи йому затребувані ринком сучасні вимоги та передати стороннім спеціалізованим виробникам види робіт, які не є профільними для підприємства.

Системний підхід до питань кібербезпеки на рівні держави включає в себе не тільки підвищення обізнаності щодо існування ризиків в кіберпросторі, створення національних структур, що займаються питаннями кібербезпеки, а й встановлення

необхідних взаємин між різними групами учасників (держава, науково-дослідні інститути, розробники і виробники інфокомунікаційних рішень, замовники і споживачі), в тому числі між галузями економіки, для розвитку аутсорсингових моделі виробництва. Тож складність внутрішньої ІТ-інфраструктури і інтенсивність потоків даних на об'єктах критичної інфраструктури вимагають комплексного підходу до кібербезпеки, який принципово виходить за рамки тільки реагування на інциденти.

Слід зазначити кібератаки проти об'єктів критичної інфраструктури не підпадають під дію існуючих міжнародних механізмів протидії кіберзлочинів і їх розслідування. Найбільш відомим механізмом такого роду є Будапештська конвенція про боротьбу з комп'ютерними злочинами, прийнята Радою Європи в 2001 році і відкрита для підписання всіма країнами. Схожа ситуація має місце щодо регіональних угод у сфері кібербезпеки, а також двосторонніх угод. Кіберінциденти на цивільних ядерних об'єктах та інших об'єктах критичної інфраструктури також не підпадають під дію юридично необов'язкових транскордонних механізмів співпраці, таких як альянс Міжнародного союзу електрозв'язку (МСЕ) і міжнародного державно-приватного партнерства ІМПАКТ або FIRST (міжнародний Форум взаємодії між центрами реагування на інциденти кібербезпеки). Крім того, наразі не вироблена міжнародна система стандартизації щодо специфічних ІТ-продуктів і сервісів, які поставляються операторам об'єктів критичної інфраструктури, відсутні загальні критерії і стандарти аудиту кібербезпеки на таких об'єктах.

Збільшення числа користувачів інтернету і розширення послуг онлайн послуг (за даними Gemius, станом на червень 2019 року в Україні число користувачів Інтернету становило 24,8 млн. осіб) призвело до зростання кіберзлочинності, в основному у фінансовій сфері. До найбільш істотних особливостей цього виду злочинів зазвичай відносять особливу складність їх розкриття та розслідування, надзвичайно високу їх латентність, прозорість національних кордонів для злочинців і відсутність єдиної правової бази для боротьби з ними, нерідко особливо великий розмір збитку, високопрофесійний склад осіб, які вчиняють такі злочини.

Сьогодні активно оцифровується сфера внутрішньої безпеки: документи, що засвідчують особу, камери відеоспостереження, електронні запити у кримінальних справах, перехоплення повідомлень стільникового зв'язку, системи моніторингу і збору інформації і тощо. Все це не тільки актуалізує проблему захисту персональних даних, а й уможливлює використання ІТ-комунікацій в організації громадських протестів або терористичних актів, а також управлінні можливими конфліктами. Саме тому суспільство потребує твердих гарантій її стійкості до кібератак та інших критичних ситуацій, незалежно від того, чи спрямовані такі атаки проти державних органів, комерційних підприємств або фізичних осіб.

Активне використання кіберпростору впливає і на людську особистість, зумовлюючи, окрім залежності від Інтернету, також і інші проблеми, зокрема, використання зловмисниками методів соціальної інженерії та вразливостей, пов'язаних з використанням Інтернету речей.

Можливості Інтернету речей (далі – IoT) дозволять віддалено керувати автомобілями, персональними медичними системами або змусити "розумний" холодильник здійснювати покупки, які не входили в плани власника. Мобільний банкінг дозволяє претворити будь-який гаджет в пристрій з функцією оплати. Однак, ототожнюючи фінансові відносини з ІТ-технологіями, не варто забувати і про поширення розкрадань грошових коштів, збої в роботі систем електронного банкінгу і, як наслідок, зростання операційних і репутаційних ризиків кредитно-фінансових організацій. Наразі

найбільший потенціал підвищення безпеки систем електронного банкінгу за допомогою ІТ вбачається у використанні біометричних даннях (відбитки пальців або системи розпізнавання зовнішності) для посвідчення особи користувача.

Головна небезпека IoT полягає в тому, що ІТ-системи створюють нові точки доступу для зловмисників, які оперують у кіберпросторі – хакерів, кракерів тощо. Так, точкою входу до системи може стати мережевий принтер, який надає хакерам маршрут доступу до комп'ютерів в мережі фінансової організації, або мобільний пристрій, який має доступ до системи радіозв'язку високотехнологічного автомобілю тощо. При цьому кіберзлочинці йдуть завжди на крок попереду, вони нападають раптово і можуть використовувати нешаблонні способи атак, до яких не лише пересічні користувачі "розумної техніки", але й служби безпеки та правоохоронці. У зв'язку із цим розробники та виробники засобів захисту змушені шукати нові рішення в умовах жорсткого ліміту часу, оскільки найбільша шкода виходить саме від так званих атак "нульового дня" (коли засобів протидії "інноваційним" атакам у кіберпросторі ще не винайдено). У деяких випадках захищатися взагалі доводиться від того, про що є вкрай поверхове уявлення: відсутні дані про кількість подібних атак, про способи, за допомогою яких безпосередньо здійснюється "вірусна інвазія" до програмного забезпечення, про алгоритмах дій зловмисників в певних ситуаціях тощо.

Ці та ряд інших важливих проблем кібербезпеки IoT слугували підставою випуску Технічним комітетом Європейського інституту телекомунікаційних стандартів (ETSI) з кібербезпеки стандарту кібербезпеки в Інтернет речей TS 103 645.

Документ встановлює базовий рівень безпеки для споживчих товарів, підключених до Інтернету, і закладає основу для майбутніх схем сертифікації IoT.

Згаданий стандарт, у частині захисту персональних даних, крім іншого, передбачає:

Положення 4.8-1. Виробники пристроїв і постачальники послуг зобов'язані надавати споживачам чітку і прозору інформацію про те, як, ким і з якою метою використовуються їхні персональні дані. Це також відноситься до третіх сторін, які можуть бути залучені, включаючи рекламодавців.

Положення 4.8-2. Якщо особисті дані обробляються на основі згоди споживачів, ця згода має бути отримана належним чином.

Положення 4.8-3. Споживачам, які дали згоду на обробку своїх персональних даних, повинна бути надана можливість відкликати згоду в будь-який час.

Минулого року Каліфорнія стала першим штатом США, де був прийнятий закон про кібербезпеку щодо IP-пристроїв (Закон № SB-327). Цей нормативно-правовий акт має набрати чинності у 2020 р.

У законі викладені вимоги до виробників пристроїв, які напряму чи опосередковано підключаються до Інтернету. Такі пристрої повинні передбачати "розумні" функції безпеки для запобігання несанкціонованого доступу, знищення, зміни чи крадіжки інформації. Положення закону спрямовані на захист звичайних користувачів. Законодавчі ініціативи щодо більш масштабних корпоративних рішень ще попереду.

Уряд Великобританії в минулому році випустив Звід практичних правил для забезпечення безпеки IP. В цьому нормативному акті акцент робиться на тому, що потрібно забезпечити кібербезпеку пристроїв, а не працювати над оновленням програмного забезпечення для посилення безпеки.

Значну увагу питанню кібербезпеки IP-пристроїв приділяє уряд Японії. В лютому 2019 р. японські чиновники з Національного інституту інформаційних та комунікаційних технологій оголосили про перевірку ефективності безпеки 200 млн.

ІР-адрес у країні. Мета цього масштабного дослідження – виявити пристрої з низьким рівнем безпеки. Ця програма допоможе інтернет-провайдерам і телекомунікаційним компаніям краще зрозуміти вразливості в мережах та пристроях.

В ЄС Закон про кібербезпеку набрав чинності 27 червня 2019 р. Його положення закріплюють індивідуальні схеми сертифікації для певних категорій продуктів, процесів та послуг з ІР-сфери. У сертифікатах має позначатися рівень гарантії безпеки та довіри до продукту, процесу чи послуги. Передбачається три рівні довіри. Найвищий відзначає успішне проходження всіх тестувань щодо кібербезпеки та повну гарантію для користувачів від виробника. Поки що застосування схем сертифікації не є обов'язковою вимогою для виробників ІР-пристроїв. Це лише перші ініціативи, які намічають подальший напрямок законотворчості в цій сфері.

У даному контексті набуває загострення ще одна глобальна загроза – застосування штучного інтелекту виробниками зброї.

У звіті PAX зазначено, щонайменше 30 світових виробників зброї займаються розробкою подібних систем озброєнь, і, як виявилося, вони роблять це набагато швидше, ніж політики домовляються про регулювання цього питання. У число розробників входять американські оборонні фірми Lockheed Martin, Boeing і Raytheon, китайські державні конгломерати AVIC і CASC, ізраїльські фірми IAI, Elbit і Rafael, Ростех Росії і турецька STM.

Більше занепокоєння у противників роботів-вбивць викликає розгортання штучного інтелекту в наступальних системах, які будуть вибирати і атакувати цілі самостійно, без людського контролю. Досі незрозуміло, як ця зброя буде відрізняти комбатантів від цивільного населення, або оцінювати пропорційність удару у відповідь. Юридичні експерти також не знають, хто буде нести відповідальність, якщо така автоматична зброя порушить міжнародне право. Без контролю людини ця зброя могла б полегшити розв’язання війни, зробивши її механічно жорстокою. В результаті застосування роботів-вбивць порушить основні правові та етичні принципи і дестабілізує міжнародний мир і безпеку, – зазначає автор звіту Рах Френк Слайпер.

Окрім зазначеного, особливо актуально знову постає проблема “іноземної залежності”. Як пересічні громадяни, так і оператори об’єктів критичної інфраструктури, державні органи та електронний уряд користуються іноземними операційними системами та антивірусними продуктами, що не сприяє забезпеченню кібербезпеки. В країні також використовується імпортне мережеве обладнання, яке може обслуговуватись зарубіжними розробниками дистанційно, а відтак – в “потрібний” момент виведено з ладу.

Крім того, існують і інші фундаментальні проблеми, що виникають внаслідок розвитку інформаційно-комунікаційних технологій та Інтернету речей. Так, психологи попереджають про загрози інтелектуальної деградації особистості через надмірно тривалого перебування в мережі, ігроманії, манії переслідування, острах втратити свой комунікатор, порушеннях пам’яті (здатності запам’ятовувати числа і факти), виснаження інтуїції, що в цілому може привести до ослаблення інтелектуального потенціалу людини. До того ж постійне використання зовнішніх пристроїв знижує рівень щастя (умовне значення міжнародного індексу щастя, Happy Planet Index) населення. Інтернет-залежність сприяє також на імплементацію населенню сторонніх культурних кодів, нав’язування вигідної іноземним державам світоглядної картини.

Відтак розвиток заходів щодо зміцнення кібербезпеки має здійснюватися на відмінній від інших держав базі, а в ідеалі слід формувати власну програмну платформу. Крім того, слід розробляти власні криптографічні программи. Зокрема, партнерські

відносини з вітчизняними розробниками ІТ-технологій, криптографічних засобів захисту тощо дають державі не лише безпосередньо технології, знання, фахівців, мале й ожливість створення власних, контрольованих рішень. Відповідно, в усіх розвинених країнах існують компанії з розробки антивірусів та інших рішень у сфері кібербезпеки.

Цілком зрозуміло, що без участі пересічних користувачів мережі боротьба з кіберзлочинністю навряд чи буде достатньо ефективною. Відтак, убачається необхідним залучати їх до заходів із роз'яснення прав користувачів всесвітньої мережі Інтернет, етичних аспектів її функціонування, варіантів і механізмів комп'ютерних шахрайств, викрадення особистих реквізитів та інших Інтернет-злочинів.

Таблиця 2.1. Джерела кібернетичних загроз[1]

Джерело загрози	Зміст загрози
Держава	Спеціальні (розвідувальні) служби держави застосовують для збирання відкритої інформації та шпигунства стосовно інших держав (не тільки ворожих, а й союзних) або недержавних суб'єктів кібернетичних атак комп'ютерні технології. Проти ворожих держав (суб'єктів) з метою дезінформації, залякування, дестабілізації, аж до кібернетичної війни, можуть здійснюватися кібератаки. Можуть також здійснюватися перехоплення персональних даних та їх використання. Подеколи це відбувається без передбаченого законом санкціонування та належного демократичного контролю, що порушує права людини.
Корпорації	Приватні корпорації чи підприємства займаються промисловим шпигунством, диверсіями тощо, нерідко залучаючи для цього хакерів, організовані злочинні угруповання і т.п.). Як і в разі державних спецслужб, корпорації, збираючи, аналізуючи й використовуючи значні обсяги персональних даних, обмінюючись ними з іншими суб'єктами (як приватними, так і державними), можуть порушувати права людини.
Хакери	У теперішній час хакерство, яке розпочиналось зі зламування комп'ютерних мереж для професійного вихваляння або ж із хуліганською метою, все більше набуває кримінального характеру. Усе більш витонченими й доступними стають засоби для здійснення кібератак, інструкції щодо застосування яких не важко знайти в Інтернеті. Тому сьогодні для проникнення у віддалені мережі вже не треба, як раніше, глибокі знання й віртуозне володіння комп'ютерними технологіями.
Хактивісти	Хактивізм (англ. *hack* – прорубуватися, проникати та *acktivism* – активність, діяльнісність) – соціальне явище, соціальних протестний рух за допомогою хакерства – незаконного проникнення у певні веб-сайти чи поштові сервери з метою їх пошкодження, викривлення, спотворення чи руйнації для досягнення певних політичних цілей.

[1] За матеріалами United States Government Accountability Office, Information Security: Cyber Threats and Vulnerabilities Place Federal Systems at Risk (Washington DC: US GAO, 2009); William A. Wulf and Anita K. Jones, "Reflections on Cybersecurity," *Science* 326 (13 November 2009): 943-4; см. Martin Charles Golumbic, *Fighting Terror Online: The Convergence of Security, Technology, and the Law* (New York: Springer, 2007).

Кібер-диверсанти із числа невдоволених користувачів	Цей контингент являє собою неабияку загрозу, позаяк це зазвичай люди, котрі непогано обізнані з принципами функціонування мережі й можуть скористатися цим для пошкодження системи, викрадення конфіденційної інформації чи з іншою протиправною метою. Як з'ясували фахівці ФБР США, ймовірність організації кібернетичних атак користувачами системи вдвічі вища ніж зовнішніми суб'єктами.
Терористи	З метою досягнення своєї мети терористі намагаються спричинити масові людські жертви, вивести з ладу чи знищити об'єкти критичної інфраструктури, створити загрози національній безпеці, дестабілізувати економіку, порушити моральний стан суспільства, підірвати авторитет державної влади тощо. У теперішній час ті терористичні угруповання, які ще не мають технічних можливостей і фахівців для проведення кібератак, усе частіше звертаються до "послуг" організованих злочинних структур або ж намагаються отримати відповідні знання та фахівців, що сьогодні цілком реально.
Ботнет	Бот – програма у складі ботнету, яка приховано впроваджується у пристрій зловмисної зацікавленості й дає хакерові змогу, використовуючи ресурси комп'ютера жертви, провадити певні дії. Заражаючи такими програмами значну кількість пристроїв, хакери користаються ними для здійснення й координування кібератак, фішингу, перебору паролів на віддалених системах, розсилання спаму та інших шкідливих незаконних операцій. На рику нелегальної торгівлі широкий асортимент подібних "послуг" користується неабияким попитом.
Фішери	Фішинг (англ. *phishing* – виуджування) – незаконний спосіб отримання персональної інформації – паролів, номерів банківських рахунків чи кредитних карт тощо шляхом розсилання від імені банку електронних листів з посиланнями на підроблені сайти, які імітують роботу справжніх, або створення точної копії існуючої банківської веб-сторінки, аби змусити користувача ввести свої особисті фінансові дані; використовуються також шпигунські та інші шкідливі програми, спами). Фішери – окремі особи чи групи, котрі використовують вказаний вид інтернет-шахрайства у власних протиправних цілях чи з метою перепродажу добутих даних.
Спамери	Спамери – це фізичні чи юридичні особи, котрі з метою реклами займаються розповсюдженням незатребуваної електронної пошти – спаму, який нерідко містить недостовірну або приховану інформацію. Розсиланням спаму може також приховуватися фішинг, поширення шпигунського чи шкідливого програмного забезпечення, кібератаки тощо.
Виробники шпигунського чи шкідливого ПЗ	До цієї категорії належать фізичні чи юридичні особи, котрі виробляють шпигунське чи шкідливе програмне забезпечення і шляхом його розповсюдження здійснюють кібератаки.
Педофіли	Можливості всесвітньої мережі – електронна пошта, спеціалізовані файлообмінні сервіси, пірингове програмне забезпечення, соціальні мережі, чати тощо – все частіше використовується педофілами з метою обміну дитячою порнографією та задля пошуку потенційних жертв і знайомства з ними.

Таблиця 2.2. Види кібернетичних загроз

Вид загрози	Підвид загрози	Зміст та приклади
Цілісність даних Для викривлення, спотворення, знищення даних чи порушення їхньої цілісності в інший спосіб можуть застосовуватися хакерські методики.	Пропаганда, дезінформація	Зміна (викривлення) даних чи впровадження хибних даних для впливу на суспільно-політичні процеси, результати економічної, бізнесової діяльності або ж з метою дестабілізації обстановки (правлячих режимів) в іноземній країні.
	Залякування	Кібератаки здійснюються з метою примусити приватних чи державних власників веб-сайтів змінити (видалити) їх зміст або ж усю політику ресурсу.
	Знищення	Систематичне цілеспрямоване нищення певних даних іноземної держави чи конкурента. Зазвичай здійснюється в комплексі з іншими підривними заходами у процесі відповідних операцій.
Доступ Створення умов, коли законні (легітимні) користувачі не в змозі отримати доступ (або цей доступ ускладнений) до певних серверів (ресурсів), що їх надає система (атаки на відмову в обслуговуванні).	Зовнішня інформація	Подібні й інші атаки на на державні та приватні ресурси відкритого доступу (інформаційні сайти державних структур, ЗМІ та ін.).
	Внутрішня інформація	Кібератаки на локальні мережі державних чи приватних структур – управління об’єктами критичної інфраструктури, транспорту, аварійно-рятувальних служб, кредитно-банківських установ, системи оперативного управління, корпоративні сервіси електронної пошти тощо.
Конфіденційність Кібернетичні атаки зі злочинним умислом спрямовані на різноманітні джерела (ресурси) конфіденційної інформації.	Шпигунство	Шпигунська діяльність держав щодо іноземних держав, фізичних та юридичних осіб; здобуття конкурентними суб’єктами інформації про своїх опонентів.
	Викрадення персональних даних	Фішинг та подібні кібератаки з метою у шахрайський спосіб з’ясувати персональні дані користувачів, зокрема номери їхніх банківських рахунків, а також упровадження вірусів для зняття даних з комп’ютера жертви тощо

	“Крадіжка особистості” (викрадення персональних даних)	З метою викрадення персональних даних особи та використання їх для вчинення протизаконних дій застосовуються вірусні троянські й аналогічні програми
	Пошук інформації в Інтернеті	Технології пошуку інформації з відкритих джерел застосовуються з метою здобуття різноманітної інформації, зокрема персональних даних.
	Шахрайство	Цей злочин нерідко вчинюється за допомогою спаму, який розповсюджується через електронну пошту. Славнозвісними у цьому сенсі стали так звані “нігерійські листи 419”. З-поміж поширених подібних шахрайських схем – пропозиції щодо передоплати фіктивних товарів чи послуг.

Шкідливі дії в кіберпросторі з погляду порушення властивостей інформації та інформаційних мереж вчиняються з метою:

- порушення конфіденційності шляхом несанкціонованого доступу до наявних в інформаційній системі даних;
- порушення цілісності шляхом несанкціонованих змін чи модифікації інформаційних систем і даних, що в них зберігаються;
- порушення доступності шляхом зловмисного перешкоджання доступу до інформаційних систем і даних, що в них зберігаються.

За походженням можна виокремити природні й антропогенні (рукотворні) загрози. До перших належать загрози, пов’язані з явищами природи, стихійними катаклізмами – буревії, повені, пожежі, землетруси, цунамі тощо, а також загрози техногенні, пов’язані з технічними проблемами. Натомість антропогенні загрози випливають із дій людини стосовно інформації, комп’ютерних систем і мереж. Вони поділяються на неумисні й умисні. З-поміж останніх загроз можна виокремити адресні атаки, ціллю яких є певна інформаційна система або ж об’єкт критичної інфраструктури, а також безадресні атаки, котрі не мають конкретної цілі (приміром, розповсюдження шкідливих програм).

Слід зауважити, що саме рукотворні загрози є головними викликами інформаційній безпеці, про що свідчить зростання й урізноманітнення методів і засобів зловмисних дій у кібернетичному просторі. Джерелом таких дій і відповідних загроз стають численні суб’єкти, котрі мають достатні знання й можливості для вчинення шкідливих дій в інформаційному середовищі.

Серед основних суб’єктів (джерел) кіберзагроз можна виокремити такі:

- держави, які використовують відповідні кіберзасоби для збирання інформації та розвідувальної діяльності (зокрема, економічне шпигунство задля отримання переваг в економічній, політичній, військовій та інших сферах); деякі держави вдаються до засобів інформаційної війни з метою обмеження противної сторони у прийнятті рішень, отримання стратегічних і тактичних переваг, руйнації окремих об’єктів (критичної інфраструктури, в тому числі пов’язаних з оборонною сферою);

- бізнесові структури: приватні компанії-конкуренти, котрі прагнуть здобути важливі дані щодо опонентів задля отримання ринкових переваг – виробництво, ціни, розробки, асортимент тощо;

- кримінальні угруповання, котрі вдаються до кібернетичних атак з метою грошового зиску; засоби, що при цьому застосовуються, найрізноманітніші: фішинг, спам, шкідливі програми для Інтернет-крадіжок, комп'ютерного вимагання, викрадення персональних даних тощо;

- міжнародне корпоративне шпигунство, метою якого є економічне, промислове шпигунство, викрадення значних коштів; нерідко користуються послугами хакерів, надаючи їм відповідні засоби;

- мережеві оператори, котрі використовують ботнет (мережу) дистанційно керованих зламаних систем задля розповсюдження спаму, фішингу, провадження узгоджених атак та ін.;

- розробники шкідливих програм і програм стеження – окремі особи чи організації, котрі створюють і застосовують вказаний продукт з протиправною метою;

- розробники фішингових схем, котрі створюють і застосовують їх для викрадення коштів, персональних даних тощо;

- працівники підприємств (компаній, установ), які мають доступ до внутрішньої конфіденційної інформації (інсайдери), у тому числі до комп'ютерних систем, а тому можуть викрадати дані або завдавати шкоди. До цих суб'єктів належать також некваліфіковані чи халатні співробітники, тимчасово наймані працівники, котрі можуть неумисно зашкодити системі через необережність;

- спамери, котрі використовують схеми фішингу, поширюють у мережі повідомлення, які містять приховані або хибні дані, а також шпигунські й вірусні програми, здійснюють кібератаки (приміром, "відмова в обслуговуванні" – DDoS);

- терористи, котрі ставлять за мету виведення з ладу чи руйнацію об'єктів критичної інфраструктури або ж втручання у їх функціонування, що може призвести до значних людських жертв, становить серйозну загрозу національній безпеці через підрив економіки країни, морально-психологічного стану суспільства. Ця категорія для отримання грошового зиску та важливої інформації також вдається до шпигунських та інших шкідливих програм, фішингу та ін.;

- хакери, котрі зламують закриті інформаційні системи й мережі з різних мотивів. Це може бути перевірка фахових здібностей, самоствердження, демонстрація певної громадянської позиції, отримання незаконного фінансового зиску;

- хактивісти, котрі з метою розміщення матеріалів політичного характеру атакують поштові сервери та веб-сторінки.

Усе наведене вище переконливо свідчить, що для забезпечення інформаційної безпеки необхідні здійснення комплексу заходів, скоординовані зусилля державних органів, бізнесових структур та окремих громадян. Особливо це стосується злагодженої взаємодії державного й приватного секторів, позаяк в останньому перебуває значна частина мереж і критичної інфраструктури. Відтак, неабиякого значення набуває підвищення загальної відповідальності за безпекову сферу, налагодження дійової міжрівневої взаємодії та ефективного зворотного зв'язку.

Висновки.

В цілому розвиток інформаційних технологій – процес з потужним потенціалом та надприбутковий бізнес. Наприклад, в Кореї обсяг системи E-learning (навчання за допомогою Інтернет і мультимедіа) щорічно зростає на 8,2 %, і вже працює близько 20 віртуальних університетів. Разом з тим, існує дуже мало систематизованої інформації

про безпеку в кіберпросторі, поданої в доступній формі. В Україні також існує гостра необхідність запуску програми навчання населення. Вона повинна бути розрахована не тільки на вузькоспеціалізовані структури, а й на вивчення основ кібербезпеки в школах і інститутах, а також навчання людей, що вийшли з шкільного та студентського віку. Для інформування та навчання необхідно, в тому числі, створити інформаційно-консультаційний центр, де користувачі зможуть отримувати відповіді на питання, пов'язані з кіберзагрозами і кіберзахистом. Одним з перших кроків в цьому напрямку може вважатися, наприклад, створення у 2017 році інформаційної площадки (Antivirus.ua), місією якої є створення умов для обміну кваліфікованою інформацією між рядовими користувачами, експертами, представниками ЗМІ, навчальних закладів тощо.

Таким чином, швидка інформатизація, масштаби потенційних наслідків злочинів у кіберпросторі, недостатня кіберзахищеність об’єктів критичної інфраструктури та ризики, пов’язані з розвитком психологічної Інтернет-залежності вимагають від національних урядів та міжнародної спільноти серйозної уваги до розвитку систем кібербезпеки на національному та глобальному рівнях. Першочергові кроки в цьому напрямку повинні передбачати розробку необхідної нормативно-правової бази і підвищення ефективності роботи відповідних інституційних структур з урахуванням зарубіжного досвіду в цій сфері. Зокрема, перспективний підхід до забезпечення кібербезпеки об’єктів критичної інфраструктури має передбачати: забезпечення кібербезпеки на етапі проектування об’єктів критичної інфратсруктури; виявлення мережевих подій, реагування на них, а також моніторинг мережевого трафіку в режимі реального часу для всіх ІТ-контурів об’єктів критичної інфраструктури; введення нових вимог до постачальників критично важливих ІТ-комплектуючих об’єктів критичної інфраструктури (наприклад, зобов’язання постачальника розкривати оператору цивільних ядерних об’єктів вихідний код прошивки програмних логічних контролерів після підписання контракту на постачання); впровадження рішень з криптографічного захисту інформації, а також цифрових підписів і захищених міток часу на всіх мережевих рівнях об’єктів критичної інфраструктури для більш надійного захисту цілісності та конфіденційності даних.

Розробка та впровадження рішень з криптографічного захисту інформації, так само, як і розробка васних операційних систем, мережевих платформ, комунікаторів тощо, на сучасному етапі є необхідними заходами для забезпечення кібербезпеки (як кібербезпеки об’єктів критичної інфраструктури та інших технічних об’єктів, так і інформаційно-психологічної безпеки людини у кіберпросторі) на національному рівні.

На глобальному рівні, зважаючи на те, що не всі кібератаки підпадають під дію існуючих міжнародних механізмів протидії кіберзлочинам, для забезпечення кібербезпеки важливим є передбачити зобов'язання держав не вдаватися у кіберпросторі до дій, метою яких є завдання збитків інформаційним системам, процесам і ресурсам іншої держави, критичній інфраструктурі тощо, заради здійснення підриву політичної, економічної й соціальної систем, масованої психологічної обробки населення, що здатні дестабілізувати життєдіяльність суспільства й держави, відповідно до підходів, окреслених у Резолюції 60/45 Генеральної Асамблеї ООН “Досягнення в сфері інформатизації і телекомунікацій в контексті міжнародної безпеки”.

Використана література

1. ISO/IEC 27032:2012. Information technology – Security techniques – Guidelines for cybersecurity. URL: https://www.iso.org/standard/44375.html

2. Кибербезопасность гражданских ядерных объектов: оценка угрозы и пути ее преодоления. URL: http://pircenter.org/media/content/files/13/14875347670.pdf

3. Кибербезопасность объектов критической ядерной инфраструкутры. URL: http://pircenter.org/projects/46-cybersecurity-of-critical-nuclear-infrastructure

4. Державно-приватне партнерство у сфері кібербезпеки: міжнародний досвід та можливості для України (аналітична доповідь). URL: http://old2.niss.gov.ua/content/articles/files/AD_Dubov_206x301_pp1-84_press-b44d7.pdf

5. Ревенков П.В. Финансовый мониторинг в условиях интернет-платежей. Москва: КноРус, 2016. С. 64-67.

6. Ревенков П.В., Бердюгин А.А. ДБО: Интернет создает новых клиентов и расширяет профили рисков. *Банковское дело*. 2013. № 12. С. 64-67.

7. CYBER; Cyber Security for Consumer Internet of Things. ETSI TS 103 645 V1.1.1 (2019-02). URL: https://www.etsi.org/deliver/etsi_ts/103600_103699/103645/01.01.01_60/ts_103645v010101p.pdf

8. Slippery Slope. PAX. URL: https://www.paxforpeace.nl/publications/all-publications/slippery-slope

9. Ткачук Т. Сучасні загрози інформаційній безпеці держави: теоретико-правовий аналіз. *Підприємництво, господарство і право.* 2017. № 10. С. 182-186.

10. Скиннер К. Цифровой банк: как создать цифровой банк или стать им. Москва: Манн, Иванов и Фербер, 2015. 320 с.

11. Крупенникова Л.Ш., Курбатов В.И. Виртуальная личность: Net-мышление, сетевой психотип, и Интернет-фобии. URL: https://cyberleninka.ru/article/n/virtualnaya-lichnost-net-myshlenie-setevoy-psihotip-i-internet-fobii/viewer

12. Ситнова И.В., Поляков А.А. Информационно-психодогическое воздействие как практика ведения войн четвертого поколения. URL: https://cyberleninka.ru/article/n/informatsionno-psihologicheskoe-vozdeystvie-kak-praktika-vedeniya-voyn-chetvertogo-pokoleniya

13. За матеріалами United States Government Accountability Office, Information Security: Cyber Threats and Vulnerabilities Place Federal Systems at Risk (Washington DC: US GAO, 2009); William A. Wulf and Anita K. Jones, “Reflections on Cybersecurity”. *Science* 326 (13 November 2009): 943-4; см. Martin Charles Golumbic. *Fighting Terror Online: The Convergence of Security, Technology, and the Law* (New York: Springer, 2007).

14. Critical Infrastructure Protection: Multiple Efforts to Secure Control Systems Are Under Way, but Challenges Remain. United States Government Accountability Office. September 10, 2007. P. 12. URL: http://www.gao.gov/assets/270/268137.pdf

15. Wilshusen, Gregory C. Information Security: Cyber Threats and Vulnerabilities Place Federal Systems at Risk. Testimony Before the Subcommittee on Government Management, Organization, and Procurement; House Committee on Oversight and Government Reform United States Government Accountability Office. May 5, 2009. P. 3. URL: http://www.gao.gov/assets/130/122454.pdf

16. Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности: Резолюция 60/45, принятая Генеральной Ассамблеей Организации Объединенных Наций. URL: https://zakon.rada.gov.ua/laws/show/995_e45

~~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~~
~~~~~~~~~~~~~~