УДК 34:004.056(477)
DOI https://doi.org/10.32782/2524-0374/2024-4/97

ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ В СУЧАСНИХ РЕАЛІЯХ

ENSURING INFORMATION AND CYBER SECURITY IN MODERN REALITIES

Метелев О.П., д.філос. у галузі права,
завідувач спеціальної кафедри
Інститут підготовки юридичних кадрів для Служби безпеки України
Національного юридичного університету імені Ярослава Мудрого

Плетньов О.В., к.ю.н., доцент,
професор спеціальної кафедри № 2
Інститут підготовки юридичних кадрів для Служби безпеки України
Національного юридичного університету імені Ярослава Мудрого

Стаття присвячена виокремленню напрямів забезпечення інформаційної та кібернетичної безпеки в Україні в сучасних реаліях. Автори зазначають, що інформаційна безпека захищає конфіденційну інформацію від несанкціонованих дій, включаючи перевірку, модифікацію, записування та будь-яке порушення чи знищення. Автори виділяють наступні категорії загроз інформаційній безпеці: незахищені або погано захищені системи; атаки в соціальних мережах; соціальна інженерія; зловмисне програмне забезпечення на кінцевих точках; відсутність шифрування; неправильна конфігурація безпеки; активні та пасивні атаки. Основними принципами забезпечення інформаційної безпеки автори вважають конфіденційність, цілісність і доступність. Автори наголошують на тому, що створення ефективної політики безпеки та вжиття заходів для забезпечення її відповідності є важливим кроком до запобігання та пом'якшення загроз інформаційній безпеці. Щоб зробити свою політику безпеки дійсно ефективною, її потрібно систематично оновлювати на основі змін у компанії, нових загроз, висновків, зроблених із попередніх порушень, а також змін систем та інструментів безпеки. Автори підкреслюють, що інформаційна безпека відрізняється від кібербезпеки як за обсягом, так і за призначенням. Ці два терміни часто використовуються як синоніми, але точніше кажучи, кібербезпека є підкатегорією інформаційної безпеки. Інформаційна безпека – це широка сфера, яке охоплює багато напрямів, зокрема, таких як фізична безпека, безпека кінцевих точок, шифрування даних і безпека мережі. Це також тісно пов'язано із забезпеченням інформації, яке захищає інформацію від таких загроз, як стихійні лиха та збої серверів. Кібербезпека, в першу чергу, спрямована на вирішення проблем, пов'язаних із технологіями, за допомогою практик та інструментів, які можуть запобігти їм або пом'якшити їх. Іншою пов'язаною категорією є безпека даних, яка зосереджена на захисті даних організації від випадкового чи зловмисного доступу неавторизованих сторін. Автори пропонують комплексний підхід щодо захисту даних, який базується на кількох рівнях: брандмауер бази даних; керування правами користувачів; маскування та шифрування даних; запобігання втраті даних; аналітика поведінки користувачів; відкриття та класифікація даних; моніторинг активності бази даних; пріоритезація сповіщень.

Ключові слова: інформаційна безпека, кібербезпека, конфіденційна інформація, шифрування даних, політика безпеки.

The article is devoted to highlighting the areas of information and cyber security in Ukraine in modern realities. The authors note that information security protects confidential information from unauthorized actions, including inspection, modification, recording and any disruption or destruction. The authors distinguish the following categories of threats to information security: unprotected or poorly protected systems; attacks on social networks; social engineering; malware on endpoints; lack of encryption; wrong security configuration; active and passive attacks. The authors consider confidentiality, integrity and availability to be the main principles of ensuring information security. The authors emphasize that creating an effective security policy and taking measures to ensure its compliance is an important step towards preventing and mitigating threats to information security. To make the security policy truly effective, it is necessary to systematically update it based on changes in the company, new threats, lessons learned from previous breaches and changes in security systems and tools. The authors emphasize that information security differs from cyber security both in terms of scope and purpose. The two terms are often used interchangeably, but more specifically, cyber security is a subcategory of information security. Information security is a broad field that encompasses many areas, including physical security, endpoint security, data encryption, and network security. It is also closely related to information security, which protects information from threats such as natural disasters and server failures. Cybersecurity is primarily about addressing technology-related issues with practices and tools that can prevent or mitigate them. Another related category is data security, which focuses on protecting an organization's data from accidental or malicious access by unauthorized parties. The authors propose a comprehensive approach to data protection, which is based on several levels: a database firewall; user rights management; data masking and encryption; data loss prevention; analytics of user behavior; discovery and classification of data; database activity monitoring; prioritization of notifications.

Key words: information security, cyber security, confidential information, data encryption, security policy.

Постановка проблеми. Інформація стала надзвичайно важливою для допомоги організаціям у досягненні їхніх бізнес-цілей і наданні онлайн-послуг в інформаційно-центричному суспільстві. Незважаючи на конструктивну роль інформації в успіху організації, вона також може завдати шкоди репутації компанії та призвести до значних невдач, якщо її не захистити. Крім того, більшість підприємств покладаються на кіберпростір для управління своїми бізнес-процесами, передачі інформації та надання послуг. Чим більше організації залежать від Інтернету для надання послуг, тим більше виникають кіберризики, а також зростає потреба в захисті від них. Вищезазначене обумовлює актуальність обраної теми дослідження.

Аналіз останніх досліджень. Питання забезпечення інформаційної та кібернетичної безпеки є об'єктом принципового інтересу для вітчизняних і зарубіжних вчених і практиків, зокрема, таких, як: А. В. Бєгун, А. М. Гребенюк, Л. В. Рибальченко, Ю. П. Лісовська, А. І. Марущак та ін. Проте надзвичайно актуальним залишається дослідження процесів забещпечення інформаційної та кібернетичної безпеки України в умовах повномасштабного російського вторгнення.

Відповідно, **метою статті** є виокремлення напрямів забезпечення інформаційної та кібернетичної безпеки в Україні в сучасних реаліях.

Виклад основного матеріалу. Інформаційна безпека охоплює інструменти та процеси, які організації використовують для захисту інформації. Це включає параметри політики, які запобігають доступу неавторизованих осіб до ділової чи особистої інформації. Інформаційна безпека – це галузь, що розвивається, й охоплює широкий

спектр сфер, від безпеки мережі та інфраструктури до тестування та аудиту [1; 5].

Інформаційна безпека захищає конфіденційну інформацію від несанкціонованих дій, включаючи перевірку, модифікацію, записування та будь-яке порушення чи знищення. Мета полягає в тому, щоб забезпечити безпеку та конфіденційність важливих даних [6; 9].

Наслідки інцидентів безпеки включають крадіжку особистої інформації, підробку і видалення даних. Атаки можуть порушити робочі процеси та завдати шкоди репутації компанії, а також спричинити відчутні збитки.

Основними принципами забезпечення інформаційної безпеки є конфіденційність, цілісність і доступність.

Зокрема, заходи конфіденційності призначені для запобігання несанкціонованому розголошенню інформації. Метою принципу конфіденційності є збереження особистої інформації та забезпечення її видимості й доступу лише для тих осіб, які нею володіють або потребують її для виконання своїх організаційних функцій.

Цілісність включає захист від несанкціонованих змін (додавання, видалення, зміни тощо) даних. Принцип цілісності гарантує, що дані є точними і надійними та не змінюються неправильно, випадково чи зловмисно.

Доступність – це захист здатності системи робити програмні дані повністю доступними, коли це потрібно користувачеві (або у визначений час). Метадоступність – це можливість зробити технологічну інфраструктуру, програми та дані доступними, коли вони потрібні для організаційного процесу або для клієнтів організації [5; 7].

Існує велика кількість категорій загроз інформаційній безпеці.

1. Незахищені або погано захищені системи. Швидкість і технологічний розвиток часто призводять до компромісів у заходах безпеки. В інших випадках системи розробляються без урахування безпеки та залишаються в експлуатації в організації як застарілі. Організації повинні ідентифікувати ці погано захищені системи та пом'якшити загрози для їх функціонування шляхом їх модернізації, виведення з експлуатації або ізоляції [1; 6].

2. Атаки в соціальних мережах. Багато людей мають облікові записи в соціальних мережах, де вони часто ненавмисно діляться великою кількістю інформації про себе. Нападники можуть запускати атаки безпосередньо через соціальні мережі, наприклад, розповсюджуючи зловмисне програмне забезпечення через повідомлення соціальних мереж, або опосередковано, використовуючи інформацію, отриману з цих сайтів, для аналізу користувачів і організацій, та використовувати її для планування атаки [2; 8].

3. Соціальна інженерія. Соціальна інженерія включає зловмисників, які надсилають електронні листи та повідомлення, що обманом змушують користувачів виконувати дії, які можуть поставити під загрозу їхню безпеку або розкрити особисту інформацію. Зловмисники маніпулюють користувачами за допомогою психологічних тригерів, таких як цікавість, терміновість або страх [5; 9].

Оскільки джерело повідомлення соціальної інженерії виглядає надійним, люди, швидше за все, погодяться, наприклад, натиснути посилання, яке встановить зловмисне програмне забезпечення на їхній пристрій, або нададуть особисту інформацію, облікові дані чи фінансову інформацію.

Організації можуть пом'якшити соціальну інженерію, поінформувавши користувачів про її небезпеку та навчивши їх виявляти та уникати підозрілих повідомлень соціальної інженерії. Крім того, технологічні системи можна використовувати для блокування соціальної інженерії в її джерелі або запобігання користувачам від виконання небезпечних дій, таких як натискання невідомих посилань або завантаження невідомих застосунків.

4. Зловмисне програмне забезпечення на кінцевих точках. Організаційні користувачі працюють із великою різноманітністю кінцевих пристроїв, включаючи настільні комп'ютери, ноутбуки, планшети та мобільні телефони, багато з яких є приватною власністю, та не контролюються організацією, і всі вони регулярно підключаються до Інтернету [1; 5].

Основною загрозою для всіх цих кінцевих точок є зловмисне програмне забезпечення, яке може передаватися різними способами, та може призвести до компрометації самої кінцевої точки, а також до ескалації привілеїв для інших організаційних систем.

Традиційного антивірусного програмного забезпечення недостатньо, щоб заблокувати всі сучасні форми зловмисного програмного забезпечення, відповідно, розробляються більш просунуті підходи до захисту кінцевих точок, наприклад виявлення кінцевих точок і дотичних елементів (EDR).

5. Відсутність шифрування. Процеси шифрування кодують дані таким чином, що їх можуть декодувати лише користувачі з секретними ключами. Це дуже ефективно відносно запобігання втрати даних або пошкодження у разі втрати чи крадіжки обладнання, або якщо організаційні системи скомпрометовані зловмисниками.

На жаль, цей захід часто ігнорується через його складність і відсутність юридичних зобов'язань, пов'язаних із належним виконанням. Організації все частіше використовують шифрування, купуючи пристрої зберігання даних або використовуючи хмарні служби, які підтримують шифрування, або використовуючи спеціальні інструменти забезпечення безпеки [6; 7].

6. Неправильна конфігурація безпеки. Сучасні організації використовують величезну кількість технологічних платформ й інструментів, зокрема web-додатки, бази даних і програми «Програмне забезпечення як послуга» (SaaS) або «Інфраструктура як послуга» (IaaS) від таких постачальників, як Amazon Web Services.

Платформи корпоративного рівня та хмарні служби мають функції безпеки, але їх повинна налаштувати організація. Неправильне налаштування безпеки через недбалість або людську помилку може призвести до порушення безпеки. Іншою проблемою є «зміщення конфігурації», коли правильна конфігурація безпеки може швидко застаріти та зробити систему вразливою.

Організації можуть пом'якшити помилки конфігурації безпеки за допомогою технологічних платформ, які постійно відстежують системи, виявляють прогалини в конфігурації та попереджають або навіть автоматично усувають проблеми конфігурації, які роблять системи вразливими [1; 5].

7. Активні та пасивні атаки. Інформаційна безпека призначена для захисту організацій від зловмисних атак. Існує два основних типи атак: активні та пасивні. Активні атаки вважаються складнішими для запобігання, і основна увага приділяється їх виявленню, пом'якшенню та відновленню після них. Пасивних атак легше запобігти за допомогою суворих заходів безпеки [8; 9].

Активна атака передбачає перехоплення комунікації або повідомлення та зміну їх для зловмисного ефекту. Розрізняють три поширених варіанти активної атаки:

– переривання – зловмисник перериває первинне спілкування та створює нові шкідливі повідомлення, видаючи себе за одну зі сторін, що спілкуються;

– модифікація – зловмисник використовує існуючі комунікації та або відтворює їх, щоб обдурити одну зі сторін, що спілкуються, або модифікує їх, щоб отримати перевагу;

– виготовлення – зловмисник створює фальшиві або синтетичні повідомлення, як правило, з метою досягнення відмови в обслуговуванні. Це перешкоджає користувачам отримати доступ до систем або виконувати звичайні операції [6; 7].

Під час пасивної атаки зловмисник стежить за системою та незаконно копіює інформацію, не змінюючи

її. Потім зловмисник використовує цю інформацію, щоб порушити роботу мереж або зламати цільові системи.

Зловмисники не вносять жодних змін у комунікаційні чи цільові системи. Це ускладнює виявлення пасивних атак. Однак шифрування може допомогти запобігти пасивним атакам, оскільки воно заплутує дані, ускладнюючи їх використання для зловмисників [1; 8].

Політика інформаційної безпеки – це набір правил, якими керуються особи під час використання ІТ-активів. Компанії можуть створювати політики безпеки інформації, щоб забезпечити дотримання протоколів і процедур забезпечення безпеки співробітниками та іншими користувачами. Політики безпеки призначені для того, щоб лише авторизовані користувачі мали доступ до конфіденційних систем і інформації.

Створення ефективної політики безпеки та вжиття заходів для забезпечення її відповідності є важливим кроком до запобігання та пом'якшення загроз інформаційній безпеці. Щоб зробити свою політику безпеки дійсно ефективною, її потрібно систематично оновлювати на основі змін у компанії, нових загроз, висновків, зроблених із попередніх порушень, а також змін систем та інструментів безпеки [2; 9].

В Україні до законодавчих та підзаконних нормативних актів, що містять норми забезпчення інформаційної безпеки, належать наступні:

– Закон України «Про інформацію» від 02.10.1992 № 2657-XII [13];

– Закон України «Про державну таємницю» від 21.01.1994 № 3855-XII [10];

– Закон України «Про захист персональних даних» від 01.06.2010 № 2297-VI [12];

– Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 № 2163-VIII [14];

– Постанова Кабінету міністрів України «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» від 29.03.2006 № 373 [11];

– Постанова Кабінету міністрів України «Деякі питання забезпечення функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки» від 23 грудня 2020 р. № 1295 [4];

– Указ Президента України «Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки» від 28 грудня 2021 року № 685/2021 [15].

Для прикладу динаміку активності проросійських хакерських угруповань за типами протягом І та ІІ кварталів 2023 року наведено на рисунку 1 [3].

Інформаційна безпека постійно взаємодіє із законами та правилами тих місць, де організація веде бізнес. Норми

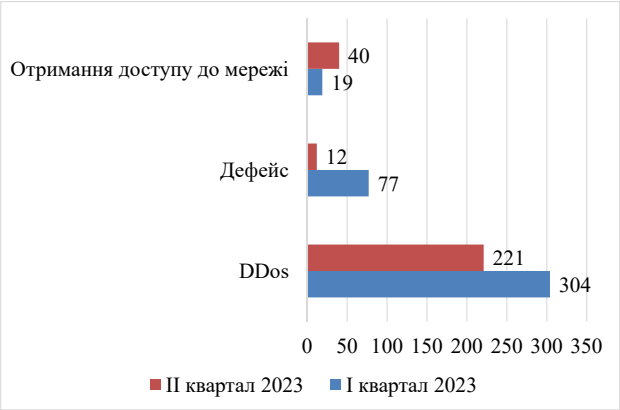

Рис. 1. Динаміка активності проросійських хакерських угруповань за типами протягом І та ІІ кварталів 2023 року

захисту даних у всьому світі зосереджені на підвищенні конфіденційності персональних даних і накладають обмеження на те, як організації можуть збирати, зберігати та використовувати дані клієнтів.

Конфіденційність даних фокусується на особисту інформацію, і, в першу чергу, стосується того, як дані зберігаються та використовуються.

Найвідомішим законом про конфіденційність в ЄС є Загальний регламент захисту даних (GDPR). Цей регламент охоплює збір, використання, зберігання, безпеку та передачу даних, пов'язаних із резидентами ЄС [2; 5].

GDPR поширюється на будь-яку організацію, яка веде бізнес з громадянами ЄС, незалежно від того, чи знаходиться сама компанія в Європейському Союзі, чи за його межами. Порушення вказівок може призвести до штрафів у розмірі до 4% світових продажів або 20 мільйонів євро.

Основними цілями GDPR є:

– встановлення конфіденційності персональних даних основним правом людини;

– впровадження вимог до критеріїв конфіденційності;

– стандартизація застосування правил конфіденційності.

GDPR передбачає захист таких типів даних:

– особиста інформація, зокрема, ім'я, прізвище, ідентифікаційний номер, дата народження або адреса;

– web-дані, такі як IP-адреса, файли cookie, місцезнаходження тощо;

– інформація про здоров'я, включаючи діагноз і прогноз;

– біометричні дані, включаючи голосові дані, ДНК і відбитки пальців;

– приватні комунікації;

– фото та відео;

– культурні, соціальні чи економічні дані [1; 6].

Інформаційна безпека відрізняється від кібербезпеки як за обсягом, так і за призначенням. Ці два терміни часто використовуються як синоніми, але точніше кажучи, кібербезпека є підкатегорією інформаційної безпеки. Інформаційна безпека – це широка сфера, яке охоплює багато напрямів, зокрема, таких як фізична безпека, безпека кінцевих точок, шифрування даних і безпека мережі. Це також тісно пов'язано із забезпеченням інформації, яке захищає інформацію від таких загроз, як стихійні лиха та збої серверів [8; 9].

Інформаційна безпека включає кібербезпеку як один із своїх компонентів. З іншого боку, кібербезпека відповідає за забезпечення безпеки інформації від кіберзагроз і кібератак під час її обробки, зберігання або транспортування. Контроль доступу, процедурний контроль, контроль відповідності та технічний контроль є прикладами забезпечення інформаційної безпеки, тоді як безпека застосунків, мережева безпека, хмарна безпека та захист критичної інфраструктури є прикладами кібербезпеки.

Кібербезпека, в першу чергу, спрямована на вирішення проблем, пов'язаних із технологіями, за допомогою практик та інструментів, які можуть запобігти їм або пом'якшити їх. Іншою пов'язаною категорією є безпека даних, яка зосереджена на захисті даних організації від випадкового чи зловмисного доступу неавторизованих сторін [1; 6].

Зокрема, на рисунку 2 показано порівняльну характеристику кількості зареєстровних кіберінцидентів та критичних кіберінцидентів протягом 2022–2023 років [3].

З рисунку 2 можна побачити, що кількість кіберінцидентів у 2023 році збільшилися вдвічі порівняно з попереднім 2022 роком. Що ж до критичних кіберінцидентів, то у 2023 році їх кількість зменшилася майже в 12 разів, що є позитивною тенденцією.

Компанії з кібербезпеки допомагають організаціям будь-якого розміру та форми власності впроваджувати програми інформаційної безпеки та захищати конфіденційні дані та активи.

Рис. 2. Порівняльна характеристика кількості зареєстровних кіберінцидентів та критичних кіберінцидентів протягом 2022–2023 років

Традиційно такі компанії забезпечують багаторівневий захист, щоб web-сайти та програми були доступними та безпечними. Подібні рішення щодо забезпечення багаторівневого захисту традиційно передбачають:

– захист від DDoS – підтримувати безвідмовну роботу в будь-яких ситуаціях. Запобігати будь-якому типу DDoS-атак будь-якого розміру, щоб запобігти доступу до web-сайту та мережевої інфраструктури;

– CDN (англ. – Content Delivery Network) – підвищити продуктивність web-сайту та зменшити витрати на пропускну здатність за допомогою CDN. При цьому здійснюється кешування статичних ресурсів на межі, одночасно прискорюючи API (англ. – Application Programming Interface) та динамічні веб-сайти;

– WAF (англ. – Web Application Firewall) – хмарне рішення, що дозволяє легітимний трафік і запобігає поганому трафіку, захищаючи програми на межі. Шлюз WAF забезпечує безпеку програм і API у мережі;

– управління ботом – аналізує трафік бота, щоб виявити аномалії; виявляє погану поведінку бота та перевіряє її за допомогою механізмів перевірки, які не впливають на трафік користувачів;

– безпека API – захищає API, забезпечуючи доступ лише бажаного трафіку до кінцевої точки API, а також виявляючи та блокуючи використання вразливостей;

– захист від захоплення облікового запису – використовує процес виявлення на основі намірів для ідентифікації та захисту від спроб захоплення облікових записів користувачів із зловмисною метою;

– аналітика атак – ефективно й точно пом'якшуйте реальні загрози безпеці та реагуйте на них за допомогою оперативної розвідки на всіх рівнях захисту [2; 7].

Подібні рішення захищає дані, де б вони не знаходилися – на фізичній території, у хмарі та в гібридних середовищах.

Комплексний підхід щодо захисту даних базується на кількох рівнях:

– брандмауер бази даних – блокує впровадження SQL (англ. – Structured Query Language) та інші загрози, одночасно оцінюючи відомі вразливості;

– керування правами користувачів – відстежує доступ до даних і діяльність привілейованих користувачів, щоб виявити надмірні, невідповідні та невикористані привілеї;

– маскування та шифрування даних – заплутує конфіденційні дані, щоб вони були марними для зловмисника, навіть якщо їх якимось чином вилучити;

– запобігання втраті даних (DLP, англ. – Data Leak Prevention) – перевіряє дані в русі й у спокої на серверах, у хмарному сховищі або на кінцевих пристроях;

– аналітика поведінки користувачів – встановлює базові лінії поведінки доступу до даних, використовує машинне навчання для виявлення ненормальної та потенційно ризикованої діяльності та сповіщення про неї;

– відкриття та класифікація даних – розкриває розташування, обсяг і контекст даних у приміщеннях і в хмарі;

– моніторинг активності бази даних – здійснює моніторинг реляційних баз даних, сховища даних, великих даних та мейнфреймів, щоб генерувати сповіщення в реальному часі про порушення політики;

– пріоритезація сповіщень – використання штучного інтелекту і технології машинного навчання, щоб переглядати потік подій безпеки та визначати пріоритети для найважливіших із них [6; 8].

Висновки. У цілому, враховуючи відмінності між кібербезпекою та інформаційною безпекою з різних аспектів, кібербезпека захищає кіберпростір від кібератак, тоді як інформаційна безпека розглядає захист інформації від будь-якої форми загрози, незалежно від того, цифрова це інформація чи фізична. Таким чином, сфера кібербезпеки обмежена кіберпростором, а інформаційна безпека стосується захисту даних у більш широкій сфері. Що стосується загроз, то кібербезпека забезпечує захист від небезпек у цифровому середовищі, тоді як інформаційна безпека має справу із загрозами, які загрожують інформації незалежно від її типу. Атаки, які загрожують інформації в кіберпросторі, включають кібершахрайство та кіберзлочинність; однак будь-який тип несанкціонованого доступу до інформації, порушення або розголошення інформації розглядається як атака. Крім того, встановлено професійні стандарти для захисту інформації від загроз у кіберреалі, зокрема, щодо особистої інформації в соціальних мережах, проте професійні стандарти інформаційної безпеки розглядають безпеку інформаційних активів для забезпечення конфіденційності, доступності та цілісності інформації.

Існуючі моделі кібербезпеки та інформаційної безпеки зазвичай базуються на поточному стані безпеки даних та кіберпростору, однак кіберпростір постійно розширюється. Таким чином, слід розробляти відповідні моделі захисту інформації.

ЛІТЕРАТУРА

1. Бєгун А. В. Інформаційна безпека : навч. посібник. Київ : КНЕУ, 2008. 280 с.
2. Гребенюк А. М., Рибальченко Л. В. Основи управління інформаційною безпекою : навч. посібник. Дніпро : Дніпроп. держ. унт внутріш. справ, 2020. 144 с.
3. Державний центр кіберзахисту Державної служби спеціального зв'язку та захисту інформації України. URL: https://scpc.gov.ua/uk/articles/318.
4. Деякі питання забезпечення функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки: Постанова Кабінету міністрів України від 23 грудня 2020 р. № 1295. URL: https://zakon.rada.gov.ua/laws/show/1295-2020-%D0%BF#Text.
5. Когут Ю. І. Цифрова трансформація економіки та проблеми кібербезпеки : практич. посіб. Київ : «СІДКОН», 2021. 368 с.
6. Кормич Б. А. Організаційно-правові засади політики інформаційної безпеки України : монографія. Одеса: Юридична література, 2003. 472 с.
7. Лісовська Ю. П. Кібербезпека: ризики та заходи: навч. посібник. К.: Видавничий дім «Кондор», 2019. 272 с.
8. Марущак А. І. Інформаційне право. Доступ до інформації : навч. посіб. Київ : КНТ, 2007. 280 с.
9. Нашинець-Наумова А. Ю. Організаційно-правові методи забезпечення інформаційної безпеки корпорацій. *Підприємництво, господарство і право*. 2015. № 11. С. 21–24.
10. Про державну таємницю: Закон України від 21.01.1994 № 3855-XII. URL: https://zakon.rada.gov.ua/laws/show/3855-12#Text.

11. Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах: Постанова Кабінету міністрів України від 29.03.2006 № 373. URL: https://ips.ligazakon.net/document/KP060373.
12. Про захист персональних даних: Закон України від 01.06.2010 № 2297-VI. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text.
13. Про інформацію: Закон України від 02.10.1992 № 2657-XII. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text.
14. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text.
15. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки»: Указ Президента України «від 28 грудня 2021 року № 685/2021. URL: https://ips.ligazakon.net/document/U685_21?an=4&ed=2021_12_28.