УДК: 342.723
https://doi.org/10.32703/2663-6352/2025-1-17-298-306
https://orcid.org/0009-0000-4442-0275
Павло ГРИЦЕНКО
аспірант Національної академії Служби безпеки України

ІНФОРМАЦІЙНА БЕЗПЕКА НА ДЕРЖАВНОМУ ПІДПРИЄМСТВІ В УМОВАХ ВОЄННОГО СТАНУ ТА ОРГАНІЗАЦІЙНІ МЕТОДИ ЇЇ ВПРОВАДЖЕННЯ

Анотація. *Стаття присвячена дослідженню правових і організаційних засад забезпечення інформаційної безпеки підприємств у складних умовах сьогодення, а саме в умовах війни, коли постає необхідність збереження, захисту персональної та комерційної інформації та розвитку інформаційного суспільства. Метою статті є аналіз особливостей управління інформаційною безпекою підприємства. З'ясовано, що інформаційна безпека охоплює різноманітні напрями діяльності спрямована на створення умов для захисту інтересів підприємства, регіону та держави в інформаційному просторі. Розглянуто теоретичні підходи до визначення змісту понять «інформаційна безпека» і «національна безпека». Управління інформаційною безпекою ґрунтується на системному підході до захисту конфіденційної інформації підприємства, забезпечуючи його безпеку. Ця система включає персонал, бізнес-процеси та інформаційні системи. Сучасні інформаційні системи являють собою комплексні поєднання технологій — апаратного, програмного та мікропрограмного забезпечення, а також відповідних процесів і персоналу, які спільно забезпечують ефективну обробку, зберігання та передачу інформації. Їхня головна мета — підтримка господарської діяльності та забезпечення безперервності бізнес-процесів організацій.*

Ключові слова: *безпека, інформаційна безпека, інформаційний захист, технічні загрози, внутрішні і зовнішні джерела загрози*

Annotation. *The article is devoted to the study of legal and organizational foundations for ensuring information security of enterprises in today challenging conditions, particularly during wartime, when the need arises to preserve and protect personal and commercial information and to foster the development of the information society. The aim of the article is to analyze the specific features of enterprise information security management. It is established that information security encompasses various areas of activity aimed at creating conditions for protecting the interests of the enterprise, the region, and the state within the information space. Theoretical approaches to defining the concepts of "information security" and "national security" are examined. Information security management is based on a systematic approach to protecting the confidential information of an enterprise, thereby ensuring its safety. This system includes personnel, business processes, and information systems.*

Forms and methods of ensuring information security act as a tool, in addition to which security features are implemented for a full range of tasks for the protection of those important for the functioning of enterprises and organizations interests in the sphere of economics, business and finance. Connected with this is the need for clear legal regulation during the development of relevant legal acts that regulate the activities of information security agencies.

A key role in the management of government enterprises to ensure information security is the promotion of mechanisms for implementing existing legal norms in this area and the disaggregation and promotion of access control regulations to information systems of state enterprises. At the same time, the kernel of the state enterprise is responsible for recognizing the cause-and-hereditary connection between powerful administrative actions in this sphere and will become the protection of the enterprise from internal ones and external information threats.

Modern information systems are complex combinations of hardware, software, and firmware technologies, as well as the corresponding processes and personnel, which together ensure efficient

processing, storage, and transmission of information. Their main goal is to support business activities and ensure the continuity of organizational business processes.

***Key words**: security, information security, information protection, technical threats, internal and external sources of threat.*

Постановка проблеми. В умовах війни інформаційна безпека стає критичним елементом захисту державних і приватних підприємств. Кіберзагрози зростають у рази, оскільки атакують не лише військові об'єкти, а й стратегічно важливі підприємства, критичну інфраструктуру та державні установи. З огляду на зростаюче значення інформаційних ресурсів та наявність численних загроз, питання інформаційної безпеки підприємств і організацій в Україні набувають особливої актуальності та потребують ретельного аналізу. Ефективний захист інформаційного середовища є невід'ємною умовою забезпечення економічної стабільності та безпеки підприємства. У статті розглянуто та представлено покроковий алгоритм впровадження вимог українського законодавства та міжнародних стандартів в діяльність сучасного державного підприємства. Розроблено план впровадження інформаційної безпеки на державному підприємстві.

Виклад основного матеріалу. В підтвердження існуючої позиції, що в сучасних військово-політичних реаліях важко і навіть недоречно заперечувати роль інформації як інструменту протистояння, фактично – зброї.[12] Інформація дає змогу перемагати у війнах і політичних конфліктах без застосування зброї, впливаючи на суспільство через загострення внутрішніх суперечностей.

Основними загрозами в умовах війни є:

1. Кібератаки з боку ворожих держав, такі як:
- DDoS-атаки на державні ресурси та сайти підприємств.
- Зломи баз даних та викрадення конфіденційної інформації.
- Впровадження шкідливого ПЗ для саботажу.
2. Дезінформація та психологічні операції:
- Фальсифікація даних з метою дестабілізації роботи підприємств.
- Фішингові атаки для отримання доступу до внутрішніх систем.
- Використання соцмереж для поширення паніки серед співробітників.

3. Фізичне знищення серверів та дата-центрів, відбуваються в наслідок ураження кіберінфраструктури під час бойових дій й відповідно втрачається доступу до важливих цифрових ресурсів через руйнування комунікаційних мереж.

Не треба забувати й про внутрішні загрози, такі як:

- Саботаж або зрада окремих співробітників.
- Недостатня обізнаність персоналу щодо правил інформаційної безпеки.

У цьому випадку фахівці у сфері інформаційних технологій виступають у ролі етичних хакерів: вони здійснюють спроби проникнення в систему за попередньою згодою її власника. Такий підхід передбачає аналіз і використання всіх наявних вразливостей для оцінки рівня захищеності.

Захист інформаційних даних необхідний для всіх компаній та підприємств, незалежно від форм власності чи від розміру, будь то невеличка фірма чи то велика корпорація. Захист потребують всі без виключення електронні технічні засоби, призначені для обробки, зберігання, передавання та відображення інформації, що взаємодіють з інформаційними даними. Будь-яка інформація, яка опинилася в руках зловмисників, становить загрозу. Тому необхідно докладати максимальних зусиль для забезпечення високого рівня конфіденційності ІТ-систем. У сучасних умовах не існує універсального способу захисту, що гарантував би абсолютну безпеку, отже, система інформаційної безпеки повинна постійно оновлюватися й удосконалюватися. Це зумовлено тим, що хакери та злочинні угруповання постійно покращують свої методи злому та несанкціонованого доступу.

Протягом довгого часу багато вчених займалися вивченням та дослідженням питань інформаційної безпеки. До цієї кагорти науковців можна віднести: Абрамчук М.,

Барановський О., Богуш В, Боярчук Р., Герасименко А., Горбатюк О., Кормич Б., Кравченко О., Ліпкан В., Максименко Ю., Маркіна І., Марущак А., Нашинець-Наумова А., Ортинськии В., Петрик В., Сороківська О., Скопа О., Черв'як А., Смотрич Д., Шилова Ю., Шевченко С. та ін. Однак досі залишаються відкритими питання сутності та змісту інформаційної безпеки підприємств; відсутні чітко визначені підходи до її складових, а також не сформульовано науково обґрунтовані принципи управління інформаційною безпекою в умовах сучасного господарювання. Проте, як слушно наголошують правники, «інформаційна безпека – це унікальний феномен сучасного суспільства, поява якого має глобальне значення для всього людства, а тому важливо сформулювати її об'єктивне, практичне визначення». [7] Ще одним підтвердженням важливості уваги до цих питань є позиція щодо пріоритетності кібербезпеки як частини національної безпеки держави особливо, [10] в умовах агресії рф.

Як зазначається в науковій літературі «поняття інформаційної безпеки, в залежності від його використання, розглядається в декількох ракурсах. У загальному випадку інформаційна безпека – це стан захищеності інформаційного середовища суспільства, що забезпечує її формування, використання і розвиток в інтересах громадян, організацій, держави. Необхідно зазначити, що серед науковців відсутній єдиний погляд на сутність поняття «інформаційна безпека». Для одних це поняття відображає діяльність, стан; для інших – властивість, процес, функцію, систему гарантій, здатність. Також відсутня норма, яка б містила дефініцію поняття «інформаційна безпека», враховуючи різницю між поняттями інформаційної безпеки й безпеки інформації.»[8]

При цьому, науковцями наголошується, що відносно розуміння змісту інформаційної безпеки «основний наголос робиться не на захисті життєво важливих інтересів (категорії достатньо аморфної і суб'єктивної через відсутність чіткого законодавчого визначення), а на забезпеченні (збереженні) умов, необхідних для нормального існування, життєдіяльності, функціонування об'єкту захисту, причому загальноприйняті вимоги щодо цих умов визначаються та регулюються низкою документів, зокрема Загальною декларацією прав людини, Конституцією України, Господарським кодексом України тощо».[1]

Інформаційне середовище (англ. information environment) слід розглядати як сферу діяльності суб'єктів, що охоплює процеси створення, трансформації та використання інформації. Воно умовно поділяється на три основні функціональні компоненти:

- генерація та поширення первинної й обробленої інформації;
- формування інформаційних ресурсів, розробка інформаційних продуктів і надання відповідних послуг;
- використання інформації.

Окрім того, виділяють дві підтримувальні складові, такі як:

- впровадження й використання інформаційних систем, технологій та відповідних технічних засобів;
- розробка і застосування інструментів та механізмів забезпечення інформаційної безпеки.

В залежності від видів загроз фахівці розглядають інформаційну безпеку, «як забезпечення стану захищеності особистості, суспільства, держави від впливу неякісної інформації;

- інформації та інформаційних ресурсів від неправомірного впливу сторонніх осіб;
- інформаційних прав і свобод громадянина.

В інформаційному праві інформаційна безпека – це одна із сторін розгляду інформаційних відносин у рамках інформаційного законодавства з позицій захисту життєво важливих інтересів особистості, суспільства, держави і акцентування уваги на погрози, механізми усунення або запобігання таких загроз правовими методами.

Питання інформаційної безпеки, які наведені в юридичній та спеціальній літературі, і базуються на розумінні інформаційної безпеки як складової національної безпеки України.

По суті це є вірним, оскільки завданням заходів з інформаційної безпеки є мінімізація шкоди за неповноти, несвоєчасність або недостовірність інформації чи негативного інформаційного впливу через наслідки функціонування інформаційних технологій, а також несанкціоноване поширення інформації» [11]. Тому забезпечення інформаційної безпеки потребує існування відповідних державних інституцій та умов для існування її суб'єктів, визначених міжнародним та національним законодавством. В Україні існує ряд нормативно-правових актів, які регулюють питання інформаційної безпеки та встановлюють вимоги до підприємств щодо інформаційної безпеки, зокрема щодо зберігання даних, захисту від кіберзагроз та використання криптографічних засобів.

Укази Президента України:

1. Указ Президента України «Про рішення Ради національної безпеки і оборони України від 14.05.2021 «Про Стратегію кібербезпеки України» - основний документ, що встановлює основні принципи безпеки, зокрема інформаційні.
2. Указ Президента України «Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про доктрину інформаційної безпеки України».

Закони України:

1. Закон України «Про національну безпеку України» – визначає загальні засади безпеки, включаючи інформаційну.
2. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» – регулює питання захисту інформації, обробки та передачі даних.
3. Закон України «Про доступ до публічної інформації» – встановлює порядок доступу та захисту державної інформації.
4. Закон України «Про електронну ідентифікацію та електронні довірчі послуги» – регулює питання електронного цифрового підпису та безпечного документообігу.
5. Закон України «Про захист персональних даних» – встановлює вимоги до обробки, зберігання та передачі персональних даних.
6. Закон України «Про інформацію» – визначає правові основи отримання, зберігання, використання та поширення інформації.
7. Закон України «Про основні засади забезпечення кібербезпеки України» – встановлює основи захисту кіберпростору держави та підприємств.

Підзаконні акти та постанови

- Постанова Кабінету Міністрів України № 373 від 29 березня 2006 р. – «Про затвердження Правил забезпечення захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах».
- Постанова КМУ № 764 від 28 червня 202024 р. – «Деякі питання електронної ідентифікації та електронних довірчих послуг».

Державні стандарти (ДСТУ)

- ДСТУ 3396.1-96 – «Захист інформації. Технічний захист інформації. Порядок проведення робіт»
- ДСТУ ISO/IEC 27001:2023 – «Інформаційна безпека, кібербезпека та захист конфіденційності. Системи керування інформаційною безпекою. Вимоги» (На заміну ДСТУ ISO/IEC 27001:2015 (ISO/IEC 27001:2013; Cor 1:2014, IDT); (ISO/IEC 27001:2022, IDT).
- ДСТУ ГОСТ 28147:2009 – «Системи обробки інформації. Захист криптографічний. Алгоритми криптографічного перетворення» – алгоритми шифрування даних.

Побудова моделі управління інформаційною безпекою має дотримуватися загальноприйнятих концептуальних принципів, закладених при побудові будь-якої системи захисту інформації . Враховуючи основні тенденції в сфері забезпечення захисту інформації при управлінні інформаційною безпекою, пропонуємо підтримуватися таких концептуальних принципів:

– цілісність;

– доступність;

– конфіденційність;

– достовірність.

В науковій літературі представлено детальний опис-розшифровка кожного з наведених принципів «цілісність інформаційних відомостей – це ніщо інше, як властивість інформації залишатися незмінною, в її первісному вигляді, структурі, під час її зберігання або багаторазової передачі. Змінити, видалити, внести корективи має право тільки людина-користувач, якому належать права доступу. Також це дозволено особам із законним доступом до цієї інформації.

Доступність. Інформаційні дані, що знаходяться у вільному доступі, повинні оперативно надаватися легальним користувачам, без будь-яких зволікань і перешкод.

Конфіденційність інформації базується на понятті створення обмеженого доступу до інформаційних ресурсів третіх, сторонніх осіб. Відомості можуть надаватися виключно користувачам, які мають право взаємодіяти з даними системами, були ідентифіковані та отримали право доступу

Достовірність відомостей свідчить про те, що інформаційні дані належать довіреній особі або законному власнику, який також є першоджерелом відомостей».[4]

Інформаційна безпека є комплексом різнопланових ефективних заходів, спрямованих на запобігання, виявлення та усунення несанкціонованих спроб доступу до системи з боку сторонніх осіб. Вона також забезпечує захист системи від можливого ушкодження, викривлення, блокування чи несанкціонованого копіювання даних.

Її важливість зростає в умовах, коли проникнення до системи та викрадення інформації можуть мати серйозні наслідки — зокрема, спричинити значні фінансові втрати або суттєве погіршення репутації фізичної чи юридичної особи тощо.

Насьогодні існує щонайменше сто типів загроз інформаційної системи. Саме тому необхідно постійно з певною періодичністю проводити аналіз усіх наявних вразливостей, використовуючи різноманітні діагностичні прийоми-способи.

Лише за умови ретельного й грамотного аналізу показників можна визначити найбільш ефективний набір заходів для захисту системи від проникнення та атак зловмисників.

До причин вразливостей систем безпеки державного підприємства можна віднести:

- недосконале програмне забезпечення, інша техніка;
- деякі процеси роботи системи неповноцінні;
- робота з інформаційною системою відбувається в складних експлуатаційних умовах.

Вразливості не завжди з’являються навмисно. Їх класифікація передбачає вразливості, які можуть бути випадкового або об’єктивного характеру. Щоб звести загрози втрати, крадіжки, зміни інформаційних даних до мінімуму, потрібно ліквідувати або мінімізувати вплив слабких місць в системі безпеки.

Як приклади випадкових – ненавмисних загроз, це можуть бути:

– неполадки в роботі апаратури;

– помилки, збої в ПЗ;

– помилки в діях персоналу або працівників, які працюють в системі;

– форс-мажори, викликані діями стихій, природними факторами;

– проблеми через постійні перебої електроенергії. [5].

Несанкціоноване проникнення в систему може мати різноманітні причини. Зловмисниками нерідко виступають співробітники компанії, користувачі ресурсу, конкуренти або найняті спеціалісти з недобросовісними намірами. Основним мотивом часто є прагнення отримати вигоду за рахунок інших. Конкуренти можуть намагатися завдати шкоди, викрадаючи конфіденційні дані, а колишні працівники — мститися роботодавцю за звільнення.

Отже, джерел загроз багато, і завдання інформаційної безпеки полягає в тому, щоб виявляти та блокувати зловмисні дії ще на ранньому етапі. Для досягнення високого рівня

захисту варто звертатися до перевірених фахівців із бездоганною репутацією. Саме тоді інформаційні системи будуть надійно захищені.

Наразі, в науковій літературі пропонуються здійснити досить масштабні кроки по удосконаленню законодавства, зокрема, прийняття окремих нормативно-правових актів рівня закону та підзаконних актів, які б регулювали обіг та захист інформації з обмеженим доступом.[6] І це тільки в окремій частині інформаційної безпеки державних підприємств. Але вже сьогодні, в реаліях сьогодення пріоритетним завданням кожного підприємства має стати захист, збереження наявної інформації та запобігання її витоку на зовні, аби не допустити використання інформації, яка належить підприємству, з метою нанесення шкоди його господарській діяльності та існуванню підприємства вцілому.

Задля убезпечення збереження і захисту інформації існує ряд методів, які можуть бути впровадженні на підприємстві, які пропонуються фахівцями. [3]

Нижче представлено покроковий алгоритм впровадження інформаційної безпеки на державному підприємстві, а також політики та заходи відповідно до законодавчих норм України, а саме регламент управління доступом до інформаційних систем:

1. Аналіз ризиків та аудит безпеки

• Перший етап – це визначення вразливостей та оцінка можливих загроз.

• Проведення аудиту інформаційної безпеки відповідно до ДСТУ ISO/IEC 27001:2015.

• Аналіз можливих загроз і ризиків (зовнішні та внутрішні атаки, витік даних, саботаж).

• Визначення рівня критичності інформації та можливих наслідків її втрати, розголошення, крадіжки, несанкціонованого копіювання тощо (компрометації).

2. Організаційні заходи

2.1. Створення підрозділу або відповідального за інформаційну безпеку

• Призначення відповідального за інформаційну безпеку (CISO – керівник відділу IT-безпеки, директор з IT-безпеки, головний менеджер з IT-безпеки).

• Формування комісії або служби з кібербезпеки.

2.2. Розробка нормативних документів

Згідно із Законами України «Про захист персональних даних», «Про інформацію», «Про кібербезпеку», підприємство повинне мати внутрішні регламенти:

• Положення про інформаційну безпеку підприємства (це основний документ, який регламентує правила захисту даних та кібербезпеки).

• Інструкцію доступу до інформації (включаючи розподіл прав доступу, облік користувачів, багаторівневу аутентифікацію).

• План реагування на інциденти (алгоритм дій у разі витоку, зламу системи).

• Регламент резервного копіювання та відновлення даних (опис частоти, методів та способів відновлення даних).

• Журнали обліку доступу та змін у системах (згідно з ISO 27001).

2.3. Проведення навчання персоналу

• Навчальні курси та тренінги з основ інформаційної безпеки (фішинг, соціальна інженерія, робота з конфіденційними даними).

• Перевірка співробітників при прийомі на роботу (згідно із Законом України "Про захист персональних даних").

• Запровадження угоди про нерозголошення (NDA) з метою захисту конфіденційної інформації.

3. Технічні заходи:

3.1. Контроль та розподіл прав доступу

• Впровадження методу підтвердження особи для доступу до комп'ютерної системи або онлайн-обліковки, іншими словами - двофакторної аутентифікації (2FA) для всіх критичних систем.

• Використання електронних цифрових підписів (ЕЦП, КЕП) для авторизації.

• Використання системи контролю доступу на за допомогою ролевої моделі (RBAC) – це спосіб контролювати, хто і до чого може отримати *доступ*.

• Адміністративний доступ надається лише спеціально уповноваженим особам.

• Доступ до інформаційних систем надається відповідно до посадових обов'язків.

• Користувачам заборонено передавати свої облікові дані третім особам.

3.2. Захист мережі та даних

• Встановлення апаратного та програмного брандмауера (Firewall) та систем виявлення вторгнень (IDS/IPS).

• Використання антивірусного ПЗ та SIEM-систем для моніторингу загроз.

• Регулярне оновлення ОС, програмного забезпечення та патчів безпеки.

• Шифрування баз даних та важливих документів (наприклад, ДСТУ ГОСТ 28147:2009).

3.3. Резервне копіювання

• Щоденне автоматичне створення резервних копій критично важливих даних та їх зберігання в захищених сховищах (офлайн та у хмарних рішеннях).

• Контроль USB-накопичувачів та знімних носіїв для запобігання несанкціонованому копіюванню.

4. Контроль та аудит

4.1. Регулярний аудит інформаційної безпеки

• Щоквартальні перевірки відповідності нормам ISO/IEC 27001.

• Проведення тестування на проникнення (penetration testing).

• Усі спроби входу та зміни прав доступу логуються.

4.2. Реагування на інциденти

• Автоматизована система фіксації та аналізу інцидентів (SIEM).

• Регулярні навчання щодо реагування на кіберзагрози.

5. Дотримання нормативних вимог та сертифікація

• Відповідність вимогам Закону України "Про захист інформації в інформаційно-телекомунікаційних системах".

• Сертифікація програмного забезпечення та криптографічних засобів відповідно до вимог Держспецзв'язку.

Цей регламент визначає порядок управління доступом до інформаційних систем державного підприємства з метою забезпечення конфіденційності, цілісності та доступності інформації.

Висновки. Проведені дослідження дають підстави стверджувати, що кожне підприємство незалежно від форм власності, буть то приватне, чи державне, чи величезні корпорації мають потребу у впровадженні комплексного плану захисту інформації. Імплементація норм інформаційної безпеки на підприємстві залежить від його масштабу, сфери діяльності та рівня чутливості оброблюваних даних. Комплексний підхід до імплементації норм інформаційної безпеки включає юридичні, організаційні та технічні заходи.

В умовах війни інформація – це зброя, і її захист має пріоритетне значення. Надійна система кібербезпеки допоможе:

- Запобігти витокам даних, що можуть зашкодити обороноздатності країни.
- Захистити фінансові та адміністративні ресурси підприємств.
- Підтримувати стабільну роботу стратегічних галузей навіть під час атак.

Інформаційна безпека у воєнний час – це не просто технічний аспект, а частина загальної національної безпеки. Її нехтування може призвести до серйозних наслідків як для підприємств, так і для держави загалом.

Форми та методи забезпечення інформаційної безпеки виступають інструментом, за допомогою якого реалізуються засоби захисту для вирішення повного спектру завдань із охорони важливих для функціонування підприємств і організацій інтересів у сфері економіки, бізнесу та фінансів. У зв'язку з цим виникає потреба в чіткому юридичному врегулюванні під

час розробки відповідних нормативно-правових актів, що регламентують діяльність органів інформаційної безпеки.

Ключову роль в управлінні державним підприємством для забезпечення інформаційної безпеки є впровадження механізмів реалізації діючих правових норм в цій сфері та розроблення та впровадження регламенту управління доступом до інформаційних систем державного підприємства. У свою чергу, кожен керівник державного підприємства повинен усвідомлювати причинно-наслідковий зв'язок між власними управлінськими діями в цій сфері та стану захищеності підприємства від внутрішніх і зовнішніх інформаційних загроз.

ЛІТЕРАТУРА

1. Архипов О.Є., Архипова Є.О. Особливості розуміння понять «інформаційна безпека» та «безпека інформації» / О.Є. Архипов, Є.О. Архипова // Информационные технологии и безопасность: основы обеспечения информационной безопасности (ИТБ-2014): Материалы XIV международной научнопрактической конференции. – К.: ИПРИ НАН Украины, 2014. – С.18-30. https://ktpu.kpi.ua/wp-content/uploads/2016/02/st-14_AA_Osoblivosti-rozuminnya-IB_BI.pdf
2. Волот О.І. Інформаційна та кібернетична безпека сучасного підприємства: забезпечення та моделювання// Центральний науковий вісник. Економічні науки – вип. 3(36)., Чернігів, Україна – 2019. – С. 238-244 // https://economics.kntu.kr.ua/pdf/3(36)/25.pdf
3. Габрук Юлія Охорона конфіденційної інформації та комерційної таємниці: як? що? навіщо? Юридична газета. https://yur-gazeta.com/publications/practice/informaciyne-pravo-telekomunikaciyi/ohorona-konfidenciynoyi-informaciyi-ta-komerciynoyi-taemnici-yak-shcho-navishcho.html
4. Інформаційна безпека та види можливих загроз / системний інтегратор// https://itbiz.ua/statti-ta-obzori/informacijna-bezpeka-ta-vidi-mozhlivih-zagroz/
5. Інформаційна безпека: види загроз і методи їх усунення// https://datami.ee/ua/blog/informatsijna-bezpeka-vidi-zagroz-i-metodi-yih-usunennya/
6. Кравченко, О. М. (2024). Розмежування понять «конфіденційна інформація» та «комерційна таємниця» у стратегії інформаційної доктрини України. Правовий часопис Донбасу, 1(4), 98–104. https://doi.org/10.32782/2523-4269-2022-81-4-1-98-104
7. М.О. Шевчук До питання генези поняття інформаційної безпеки як складової національної безпеки. Том 2 № 78 (2023): Науковий вісник Ужгородського національного університету. Серія: Право. http://visnyk-pravo.uzhnu.edu.ua/article/view/285994
8. Маркіна І.А. Інформаційна безпека підприємства та організаційні заходи її забезпечення. (Текст) / Український журнал прикладної економіки. – 2019. – Том 4. – С. 209-215. // http://ujae.org.ua/informatsijna-bezpeka-pidpryyemstva-ta-organizatsijni-zahody-yiyi-zabezpechennya/
9. Перун Т.С. Інформаційна безпека суб'єктів господарювання: нові загрози та перспективи розвитку// вчені записки ТНУ імені В.І. Вернадського, Серія: юридичні науки. – 2020. – Т.31(70) № 3 2020. – С. 138-142 // https://juris.vernadskyjournals.in.ua/journals/2020/3_2020/26.pdf
10. Пінкас Я. Нормативно-правове забезпечення інформаційної безпеки в Україні в умовах російсько-української війни (2014-2022 рр.). Збірник матеріалів Міжнародної наукову-практичної конференції «Інформаційна безпека: сучасний стан, проблеми та перспективи», електронне видання, Кам'янець-Подільський, 2023 – С. 10, 42. // https://politkaf.kpnu.edu.ua/wp-content/uploads/2023/04/zbirnyk-material-konfer.-inf_bezp_2023.pdf
11. Скопа О.О. звіт про науково-дослідну роботу «Удосконалення принципів та методів інформаційного забезпечення, інформаційної та фінансово-економічної безпеки підприємств та організацій сфери економіки, бізнесу та фінансів» (проміжний), Одеса, 2013 – С. 16-18 // http://dspace.oneu.edu.ua/jspui/bitstream/.pdf

12. Смотрич Д.В. Інформаційна безпека в умовах воєнного стану. (Текст) / Науковий вісник Ужгородського Національного Університету / Серія ПРАВО. Випуск 77: частина 2. – 2023. – С.121-126 // https://visnyk-juris-uzhnu.com/wp-content/uploads/2023/06/22-2.pdf
13. Черв'як А.В., Буряк А.А., Циганенко К.Д. Особливості формування безпекоорієнтованого інформаційного середовища національної економіки. (Текст) / Науковий вісник Херсонського державного університету. / Серія Економічні науки / Випуск 52, - 2024. – С. 19-23 // file:///C:/Users/varvarova/Downloads/849-%D0%A2%D0%B5%D0%BA%D1%81%D1%82%20%D1%81%D1%82%D0%B0%D1%82%D1%82%D1%96-1797-1-10-20241115.pdf
14. Шипілова Ю. Правова база української кібербезпеки: загальний огляд і аналіз / Юлія Шипілова // Міжнародна фундація виборчих систем в Україні, 2019. //https://ifesukraine.org/wp-content/uploads/2019/10/IFES-Ukraine-Ukrainian-Cybersecurity-Legal-Framework-Overview-and-Analysis-2019-10-07-Ukr.pdf