ISSN 2519-2310 (Online)

КОМП'ЮТЕРНІ НАУКИ ТА КІБЕРБЕЗПЕКА, 2025, № 1 (27)

COMPUTER SCIENCE AND CYBERSECURITY, 2025, Iss. 1 (27)

DOI: https://doi.org/10.26565/2519-2310-2025-1-05
УДК 340.137

ДОСЛІДЖЕННЯ ТА ПОРІВНЯННЯ НОРМАТИВНИХ РЕГУЛЯТОРНИХ ДОКУМЕНТІВ ЄВРОПЕЙСЬКОГО СОЮЗУ У СФЕРІ КІБЕРБЕЗПЕКИ

Марина Єсіна[1,2], канд. техн. наук, доцент, в.о. завідувача кафедри кібербезпеки інформаційних систем, мереж і технологій, ННІ КШ та ШІ; науковий співробітник-консультант, e-mail: m.v.yesina@karazin.ua, ORCID: https://orcid.org/0000-0002-1137-2382

Єлизавета Логачова[1], студентка 5 курсу кафедри кібербезпеки інформаційних систем, мереж і технологій, ННІ КШ та ШІ, e-mail: lohachova2020kb11@student.karazin.ua, ORCID: https://orcid.org/0000-0002-9815-466X

Євгенія Колованова[1], канд. техн. наук, в.о. заступника директора з навчальної роботи, ННІ КШ та ШІ, e-mail: e.kolovanova@karazin.ua, ORCID: https://orcid.org/0000-0002-0326-2394

[1]Харківський національний університет імені В.Н. Каразіна, майдан Свободи, 4, Харків, 61022, Україна

[2]ПрАТ "Інститут Інформаційних Технологій", вул. Отамановського професора, 15, Харків, 61022, Україна

Рукопис надійшов 1 березня 2025 р. Отримано після рецензування 1 квітня 2025 р. Прийнято 2 травня 2025 р.

Анотація: У статті представлено ґрунтовне дослідження та порівняння основних нормативно-правових актів Європейського Союзу у сфері кібербезпеки, серед яких: Директива NIS2, Загальний регламент про захист даних (GDPR), Регламент про цифрову операційну стійкість (DORA) та стандарт PCI DSS. Ці документи розглядаються як основоположні елементи формування сучасної політики ЄС у сфері захисту цифрової інформації, що охоплює персональні дані, фінансову інформацію та критичну інфраструктуру. У роботі окреслено ключові завдання кожного з актів, проаналізовано їхню сферу застосування, вимоги до суб'єктів регулювання, механізми управління ризиками, звітування про інциденти, взаємодію з постачальниками, а також санкційні положення. Особливу увагу приділено порівнянню актів за впливом на бізнес та IT-інфраструктуру, а також виявленню взаємозв'язків між ними. Встановлено, що хоча кожен документ має власний фокус - захист персональних даних, стійкість фінансової інфраструктури, безпека цифрових мереж чи захист транзакцій з платіжними картками – всі вони спрямовані на створення цілісної екосистеми кіберзахисту в межах ЄС. Стаття також аналізує міжнародні аналоги згаданих актів, такі як GDPR-подібні закони у США та Бразилії, стандарти NIST та ISO, що свідчить про глобальний характер проблеми цифрової безпеки та пошук спільних підходів до її вирішення. У підсумку, робота підкреслює важливість комплексного та гармонізованого підходу до кібербезпеки як ключової умови сталого розвитку цифрового суспільства. З огляду на актуальні загрози, зокрема геополітичні конфлікти та зростання масштабів кіберзлочинності, ефективна імплементація європейських стандартів набуває особливого значення для країн-партнерів, зокрема України, яка потребує адаптації відповідних норм для підвищення національної кіберстійкості.

Ключові слова: *нормативні документи, європейський союз, регуляторні документи, кібербезпека, бізнес, захист інформації*

Як цитувати: Єсіна М., Логачова Є., Колованова Є. Дослідження та порівняння нормативних регуляторних документів європейського союзу у сфері кібербезпеки. *Комп'ютерні науки та кібербезпека.* 2025; № 1(27): С. 60–72. https://doi.org/10.26565/2519-2310- 2025-1-05

In cites: Yesina M., Lohachova Ye., Kolovanova Ye. (2025). Research and comparison of European Union regulatory documents in cybersecurity. *Computer Science and Cybersecurity. 1*(27): 60–72. https://doi.org/10.26565/2519-2310- 2025-1-05 (in Ukrainian)

1. Вступ

У сучасному світі цифрові технології стали невід'ємною складовою суспільного, економічного та політичного життя. Разом із безпрецедентними можливостями, які вони відкривають для розвитку економік та суспільств, вони також створюють нові загрози – від кібершахрайства до масових атак на критичну інфраструктуру. У цьому контексті питання кібербезпеки набуло особливої ваги як на національному, так і на міжнародному рівнях. Європейський Союз, як одне із провідних інтеграційних об'єднань у світі, визначає кібербезпеку як пріоритетний напрямок своєї політики, прагнучи створити високий рівень кіберзахисту для своїх громадян, бізнесу та державних інституцій.

Нормативно-правове регулювання кібербезпеки в ЄС є багаторівневим та динамічним процесом. Його розвиток відображає прагнення країн-членів забезпечити як надійний захист критичної інфраструктури та персональних даних, так і сталий розвиток цифрової економіки. З цією метою ЄС прийняв низку важливих нормативно-правових актів, серед яких особливе місце займають Директива NIS та її оновлена версія – NIS2, GDPR, DORA, а також PCI DSS [1-4]. Кожен із цих документів має свою сферу застосування, особливості та завдання, однак усі вони спрямовані на досягнення спільної мети – забезпечення кіберстійкості та цифрової довіри в Європейському Союзі.

Аналіз та порівняння цих нормативних актів дозволяє глибше зрозуміти, якими шляхами ЄС намагається врегулювати питання кібербезпеки, ураховуючи постійні технологічні зміни та еволюцію кіберзагроз. Особливої актуальності це набуває в умовах геополітичних викликів, зокрема в контексті агресії російської федерації проти України, що ще більше підкреслило важливість кібербезпеки для захисту державних інституцій та критичних сервісів.
Метою цієї статті є дослідження та порівняння основних нормативно-правових документів Європейського Союзу у сфері кібербезпеки, визначення їхніх спільних рис та відмінностей, а також аналіз впливу на держави-члени та бізнес.

2. Ключові нормативно-правові документи ЄС

Атаки на основі ШІ можна класифікувати за багатьма різними параметрами. Так, наприклад, кілька систем класифікації атак були представлені в роботах [7, 8]. Також NIST в своєму звіті щодо атак на машинне навчання ШІ представив різні типи класифікації [1, 25]. В цьому розділі будуть розглянуті деякі типи класифікацій.

2.1. Директива NIS2 та її особливості

CNIS2 Directive (Network and Information Security Directive 2) – це оновлена структура Європейського Союзу з кібербезпеки, яка замінює оригінальну Директиву NIS (2016) [1]. Вона розроблена для посилення кібербезпеки в Європейському Союзі шляхом встановлення високого загального рівня безпеки для мережевих та інформаційних систем. Її основною метою є

посилення кіберстійкості критичних секторів, а також забезпечення уніфікованих стандартів кіберзахисту для всіх суб’єктів цифрової економіки, незалежно від їхньої галузі та розміру.

Директива ставить за мету кілька ключових завдань, які разом утворюють системний підхід до кібербезпеки. Насамперед це зміцнення можливостей держав-членів у сфері кібербезпеки, що передбачає розвиток національних стратегій, створення компетентних органів та ефективних механізмів реагування на інциденти. Другим важливим завданням є покращення співпраці між державами-членами, що сприяє своєчасному обміну інформацією про кіберзагрози та координації дій у випадку масштабних атак. Ще одна мета – зменшення фрагментації на внутрішньому ринку ЄС, адже різні підходи до регулювання в окремих країнах створювали прогалини у захисті цифрової інфраструктури. Нарешті, Директива запроваджує обов’язкові вимоги з управління ризиками та звітування про кіберінциденти, що суттєво посилює відповідальність організацій за стан кібербезпеки [1].

Основні вимоги Директиви охоплюють кілька напрямків. Перш за все, це управління ризиками, яке передбачає впровадження суб’єктами (операторами основних послуг та постачальниками цифрових послуг) технічних, операційних та організаційних заходів. До таких заходів належать [1]: систематичний аналіз ризиків та розробка політики безпеки; ефективне реагування на інциденти; забезпечення безперервності бізнесу та планування відновлення після інцидентів; безпека закупівель та використання ІТ-систем; а також політика моніторингу, тестування та аудитів кібербезпеки.

Другим важливим компонентом є звітування про інциденти. Відповідно до Директиви, суттєві інциденти повинні бути повідомлені до відповідних компетентних органів протягом 24 годин з моменту їх виявлення. При цьому організація має надати повне повідомлення про інцидент не пізніше, ніж через 72 години, а остаточний звіт – не пізніше, ніж через один місяць після події. Такий підхід дозволяє державним органам оперативно реагувати на інциденти, координувати дії між суб’єктами ринку та зменшувати потенційний вплив на суспільство [1].

Окрему увагу Директива приділяє постачальникам ІКТ-послуг, встановлюючи обов’язок оцінки та контролю ланцюга постачання. Це означає, що організації повинні впроваджувати заходи безпеки для забезпечення надійності своїх партнерів та контрагентів, а також враховувати кіберризики у договірних відносинах із критичними постачальниками. Такий підхід допомагає створити більш стійку екосистему цифрових послуг у межах ЄС [1].

Важливою особливістю NIS2 є посилення ролі керівних органів. Відтепер вони несуть відповідальність за схвалення та нагляд за впровадженням заходів кібербезпеки у своїх організаціях. У разі недотримання вимог Директиви керівники можуть бути притягнуті до відповідальності, що підкреслює важливість кібербезпеки як стратегічного питання для кожної компанії [1].

Зрештою, кожна держава-член ЄС зобов’язана призначити національні компетентні органи, які здійснюють нагляд за виконанням вимог Директиви. Це сприяє уніфікації підходів до моніторингу та контролю в межах ЄС, а також створює механізми ефективної взаємодії між країнами у сфері кібербезпеки.

2.2. Регламент GDPR та його особливості

General Data Protection Regulation (GDPR) – це Загальний регламент про захист даних, прийнятий Європейським Союзом і такий, що набув чинності 25 травня 2018 року [2]. Він є ключовим нормативним документом, який визначає правила обробки персональних даних громадян ЄС. Особливість цього документа полягає в його екстериторіальній дії: правила GDPR поширюються не лише на організації, що перебувають у межах Європейського Союзу, але й на будь-які компанії, що обробляють персональні дані громадян ЄС, незалежно від місця їхньої

реєстрації [2]. У такий спосіб GDPR суттєво підвищує рівень захисту персональних даних і гарантує громадянам ЄС контроль над тим, як їхні дані збираються та використовуються.

Основними принципами, на яких базується GDPR, є законність, справедливість і прозорість обробки даних [2]. Це означає, що персональні дані повинні оброблятися на законних підставах, чесно та прозоро для суб'єкта даних. Наприклад, компанія має чітко повідомити людині, які дані збираються, для чого вони потрібні та як довго їх планують зберігати. Це створює довіру між користувачем і організацією та забезпечує право особи знати, що відбувається з її персональними даними.

Іншим ключовим принципом є обмеження мети: персональні дані повинні збиратися лише для конкретних, явних і законних цілей та не можуть оброблятися далі у спосіб, несумісний з цими цілями. Наприклад, якщо компанія збирає електронні адреси для реєстрації в сервісі, вона не має права використовувати ці дані для нав'язливої реклами без додаткової згоди користувача [2].

Мінімізація даних означає, що організації повинні збирати лише ті дані, які справді необхідні для досягнення задекларованих цілей. Таким чином, збір надлишкових даних забороняється, що запобігає зловживанням та підвищує безпеку особистої інформації. Принцип точності вимагає від організацій забезпечити актуальність даних: інформація повинна бути точною й оновлюватися за потреби [2]. Це важливо, щоб уникнути помилок або використання застарілих даних, що можуть призвести до порушення прав особи.

Принцип обмеження зберігання вказує на те, що персональні дані не повинні зберігатися довше, ніж це необхідно для досягнення цілей обробки [2]. Організації мають визначати строки зберігання даних і знищувати або анонімізувати їх після завершення обробки. Це суттєво знижує ризики витоку інформації та зловживання.

Цілісність і конфіденційність є одними з найважливіших вимог GDPR, оскільки вони вимагають забезпечити належну безпеку персональних даних, у тому числі їх захист від несанкціонованої або незаконної обробки, випадкової втрати, знищення чи пошкодження. Організації повинні впроваджувати технічні та організаційні заходи безпеки, такі як шифрування, регулярне резервне копіювання та контроль доступу, щоб гарантувати безпеку даних [2].

GDPR застосовується до організацій, розташованих у межах ЄС, які обробляють персональні дані. Крім того, його вимоги поширюються й на організації, що перебувають за межами ЄС, якщо вони пропонують товари чи послуги громадянам ЄС або моніторять поведінку осіб у межах ЄС [2]. Таким чином, навіть компанії, що не мають фізичної присутності в ЄС, підпадають під дію GDPR, якщо вони працюють із громадянами ЄС.

Порушення вимог GDPR може призвести до накладення значних штрафів, які становлять до 20 мільйонів євро або до 4% річного світового обороту компанії – залежно від того, яка сума є більшою [2]. Такі фінансові санкції стимулюють компанії дотримуватися принципів прозорої, законної та безпечної обробки персональних даних, а також створюють новий рівень відповідальності для бізнесу в цифровому середовищі.

2.3. Регламент DORA та його особливості

Digital Operational Resilience Act (DORA) – це Регламент Європейського Союзу, спрямований на посилення цифрової стійкості фінансового сектору. Він набув чинності 16 січня 2023 року, а його застосування розпочалось 17 січня 2025 року [3]. Цей регламент є ключовим кроком ЄС у забезпеченні стійкості фінансових установ до ризиків, пов'язаних із інформаційними та комунікаційними технологіями (ІКТ), зокрема кіберінцидентами та технічними збоями. DORA створює єдиний стандарт цифрової операційної стійкості для всіх

фінансових організацій, щоб гарантувати їхню здатність витримувати, реагувати та відновлюватися після порушень у сфері ІКТ [3].

Однією з основних вимог DORA є управління ІКТ-ризиками, яке передбачає, що фінансові установи повинні впроваджувати комплексні рамки управління ризиками. Це включає ідентифікацію ризиків, їхню профілактику, своєчасне виявлення інцидентів, ефективне реагування та відновлення після подій [3]. Такий підхід дозволяє організаціям підготуватися до потенційних кіберзагроз та забезпечує безперервність надання фінансових послуг навіть під час кризових ситуацій.

Регламент також запроваджує обов’язкове звітування про інциденти: фінансові установи повинні повідомляти національні регуляторні органи про значні інциденти у сфері ІКТ. Це дозволяє державним органам оперативно реагувати на інциденти та координувати заходи для запобігання системним ризикам у фінансовому секторі [3]. Таким чином, DORA сприяє своєчасному обміну інформацією та знижує ризики поширення кіберзагроз.

Ще однією важливою вимогою є регулярне тестування цифрової операційної стійкості, яке передбачає проведення як базових, так і передових тестувань для певних установ [3]. Це допомагає визначити слабкі місця у системах та процесах організацій, а також забезпечити їхню готовність до реагування на кіберінциденти. Регулярні тренування та симуляції атак підвищують загальну кіберстійкість фінансової екосистеми ЄС.

Крім того, DORA передбачає управління ризиками третіх сторін. Фінансові установи зобов’язані встановлювати вимоги до ІКТ-постачальників, укладати відповідні контракти та забезпечувати належний моніторинг їхньої діяльності [3]. Це положення має на меті зменшити ризики, пов’язані із зовнішніми підрядниками, та гарантувати, що всі учасники цифрового ланцюга відповідають високим стандартам кібербезпеки.

Особливе значення в DORA приділяється обміну інформацією між фінансовими установами. Регламент заохочує обмін знаннями про кіберзагрози та вразливості, щоб підвищити колективну стійкість фінансової системи ЄС [3]. Такий підхід дозволяє швидко ідентифікувати нові загрози та ефективно реагувати на них у партнерстві з іншими учасниками ринку.

DORA поширюється на широкий спектр фінансових установ, серед яких: банки, страхові та перестрахові компанії, інвестиційні фірми, платіжні установи, електронні грошові установи, постачальники послуг з обміну криптовалют, центральні контрагенти, центральні депозитарії цінних паперів, управляючі компанії інвестиційних фондів, а також постачальники ІКТ-послуг, що обслуговують фінансові організації [3]. Така широка сфера застосування забезпечує комплексний підхід до захисту фінансової інфраструктури від кіберзагроз.

У разі порушення вимог DORA до фінансових установ можуть бути застосовані серйозні санкції. Це можуть бути адміністративні штрафи, розмір яких визначається національними регуляторами, а також обмеження або заборона на надання певних послуг [3]. Крім того, регулятори можуть вимагати усунення порушень у встановлені терміни. Такі заходи спрямовані на забезпечення високого рівня відповідальності фінансових установ та стимулювання їхнього дотримання єдиних правил цифрової операційної стійкості.

2.4. Атака отруєння даних

Атаки на етапі навчання ML називаються атаками отруєння [1, 9]. Під час атаки отруєння даних [5, 9] зловмисник контролює підмножину навчальних даних, вставляючи або змінюючи навчальні зразки. У атаці отруєння моделі [10] зловмисник контролює модель та її параметри. Атаки з отруєнням даних можуть застосовуватися до всіх парадигм навчання, тоді як атаки з отруєнням моделі є найбільш поширеними у федеративному навчанні [11], де клієнти

надсилають локальні оновлення моделі на сервер, що обробляє вхідні дані, і в атаках на ланцюг поставок, де шкідливий код може бути доданий до моделі постачальниками технології моделі. Під федеративним навчанням тут мається на увазі метод машинного навчання, орієнтований на умови, в яких кілька суб'єктів (часто званих клієнтами) спільно навчають модель, при цьому дані, які використовуються для навчання, розподіляються децентралізовано. Це відрізняє його від машинного навчання, в якому дані зберігаються централізовано.

Перші атаки отруєння, виявлені в додатках кібербезпеки, були атаками на доступність проти генерації профілів хробака та класифікаторів спаму, які невибірково впливають на всю модель машинного навчання та, по суті, спричиняють атаку типу «відмова в обслуговуванні» для користувачів системи ШІ.

Атаки отруєння вважаються одними з найнебезпечніших серед атак на ШІ та можуть спричинити або порушення доступності, або порушення цілісності. Зокрема, атаки з порушенням доступності спричиняють деградацію моделі машинного навчання на всіх етапах, тоді як цільові та бекдорні атаки з отруєнням є більш прихованими та викликають порушення цілісності на невеликому наборі даних. Атаки отруєння використовують широкий спектр конкурентних можливостей, таких як отруєння даних, отруєння моделі, контроль міток, контроль вихідного коду та контроль тестових даних, що призводить до кількох підкатегорій атак отруєння. За моделлю загрози вони можуть використовуватись як у сценаріях білої скриньки, так і чорної скриньки [18], що були розглянуті в розділі 1.3 цієї статті.

Серед методів запобігання атакам отруєння даних виділяють два найефективніші [1]:

• Очищення навчальних даних. Ці методи використовують той факт, що отруєні набори зазвичай відрізняються від звичайних навчальних наборів, які не контролюються зловмисниками. Таким чином, методи очищення даних призначені для очищення навчального набору та видалення отруєних наборів перед виконанням навчання машинного навчання.

• Надійне навчання. Альтернативним підходом до пом'якшення атак з порушенням доступності є модифікація алгоритму навчання ML і проведення надійного навчання замість звичайного навчання. У кількох статтях визначено методи надійної оптимізації, такі як використання функції скорочених втрат [20] або випадкове згладжування для додавання шуму під час навчання [21].

2.5. Стандарти PCI DSS та їх особливості

Payment Card Industry Data Security Standard (PCI DSS) – це міжнародний стандарт безпеки, розроблений для захисту даних власників платіжних карток [4]. Його головною метою є забезпечення безпечного середовища для обробки, зберігання та передавання даних про кредитні картки. Всі організації, які приймають, обробляють або зберігають дані платіжних карток, повинні дотримуватися вимог цього стандарту, щоб зменшити ризик несанкціонованого доступу, шахрайства та витоку конфіденційної інформації.

PCI DSS є універсальним набором вимог, обов'язковим для компаній різного масштабу: від невеликих Інтернет-магазинів до великих фінансових установ. Він сприяє зміцненню кіберстійкості компаній, які працюють у сфері електронних платежів, та формує довіру споживачів до цифрових транзакцій. Стандарт включає дванадцять головних умов, які разом забезпечують комплексний захист платіжної інформації [4].

Першою вимогою є захист систем, що обробляють платіжні дані, включаючи фізичний захист обладнання та програмного забезпечення. Це передбачає використання фаєрволів, сегментації мережі та інших заходів для запобігання несанкціонованому доступу. Друга вимога стосується захисту даних власників карток від стороннього доступу, зокрема шляхом шифрування даних як під час передавання, так і під час зберігання [4].

Також PCI DSS передбачає обов’язковий захист мереж, які обробляють дані про картки, від несанкціонованого доступу [4]. Це означає, що компанії повинні впроваджувати сучасні методи контролю доступу, моніторинг мережевого трафіку та системи виявлення вторгнень. Додатково стандарт вимагає захисту від шкідливого програмного забезпечення, яке може призвести до компрометації платіжних даних.

Суттєвою вимогою є обмеження доступу до платіжних даних: він має надаватися лише авторизованим користувачам, що мінімізує ризики внутрішніх загроз. PCI DSS також акцентує увагу на необхідності постійного тестування та розвитку безпеки систем, щоб своєчасно виявляти вразливості та запобігати можливим атакам [4].

Крім цього, компанії повинні впроваджувати та підтримувати діяльність ефективних політик безпеки, які встановлюють правила обробки платіжних даних та обов’язки працівників. Стандарт вимагає обмеження фізичного доступу до приміщень, де розміщене обладнання для обробки платіжних даних, а також постійного моніторингу інцидентів, які можуть свідчити про спроби несанкціонованого доступу [4].

PCI DSS наголошує на необхідності захисту від зовнішніх атак шляхом впровадження сучасних механізмів кіберзахисту, таких як системи виявлення вторгнень, міжмережеві екрани та антивірусні рішення [4]. Важливим є також управління підтримкою та обслуговуванням обладнання й програмного забезпечення, що передбачає регулярні оновлення систем та патч-менеджмент. Остання, але не менш важлива вимога – розробка та впровадження політик і процедур безпеки, які гарантують відповідність усім вимогам стандарту.

PCI DSS також запроваджує систему класифікації компаній за рівнями залежно від кількості оброблюваних транзакцій на рік [4]. Це дозволяє встановлювати різний рівень вимог до сертифікації залежно від обсягів діяльності. До першого рівня належать компанії, що обробляють понад 6 мільйонів транзакцій на рік, для яких передбачено найжорсткіші вимоги до безпеки. До другого рівня входять організації, що обробляють від 1 до 6 мільйонів транзакцій, а до третього – компанії з обсягом від 20 тисяч до 1 мільйона транзакцій на рік. Нарешті, до четвертого рівня належать компанії, які обробляють до 20 тисяч транзакцій щороку [4]. Такий підхід дозволяє гнучко адаптувати вимоги до різних бізнесів, одночасно забезпечуючи високий рівень захисту даних платіжних карток у всьому фінансовому ланцюгу.

3. Порівняння документів

3.1. Порівняння нормативно-правових документів ЄС

Для порівняльного аналізу нормативно-правових документів ЄС було обрано наступні критерії:

- мета регулювання;
- категорії суб’єктів регулювання;
- обов’язки організацій;
- вимоги до кібербезпеки;
- санкції за порушення;
- взаємозв’язки між документами.

Результати порівняння наведено у таблиці 1.

Таблиця 1 – Порівняння нормативно-правових документів ЄС за критеріями

Table 1 – Comparison of EU Regulatory Documents Based on Criteria

Критерій Criteria	**GDPR**	**DORA**	**NIS2**	**PCI DSS**
Мета регулювання **The purpose of regulation**	Захист персональних даних фізичних осіб у межах ЄС Protection of personal data of individuals within the EU	Забезпечення цифрової стійкості фінансових установ до ІКТ-ризиків Ensuring the digital resilience of financial institutions to ICT risks	Підвищення рівня кібербезпеки мережевих та інформаційних систем в ЄС Enhancing the cybersecurity level of network and information systems in the EU	Забезпечення безпеки даних платіжних карток Ensuring the security of payment card data
Категорії суб'єктів **Categories of subjects**	Усі організації, що обробляють персональні дані громадян ЄС All organizations that process personal data of EU citizens	Фінансові установи та ІКТ-постачальники, що працюють з ними Financial institutions and ICT providers working with them	Суб'єкти з «високим ступенем критичності», включаючи цифрові, енергетичні, медичні, транспортні сектори Entities with a high degree of criticality, including the digital, energy, healthcare, and transport sectors	Організації, які обробляють, передають або зберігають платіжні карткові дані Organizations that process, transmit, or store payment card data
Обов'язки організацій **Responsibilities of organizations**	Законна обробка даних, обмеження мети, мінімізація, точність, захист Lawful data processing, purpose limitation, data minimization, accuracy, protection	Управління ІКТ-ризиками, інцидент-репортинг, тестування, управління ризиками третіх сторін ICT risk management, incident reporting, testing, third-party risk management	Управління ризиками, звітування про інциденти, оцінка постачальників, відповідальність керівництва Risk management, incident reporting, supplier assessment, management accountability	Забезпечення 12 основних умов безпеки, включаючи шифрування, контроль доступу, моніторинг Ensuring 12 core security requirements, including encryption, access control, and monitoring
Вимоги до кібербезпеки **Cybersecurity requirements**	Забезпечення конфіденційності, цілісності й доступності даних Ensuring the confidentiality, integrity, and availability of data	Впровадження ІКТ-безпеки: виявлення, захист, реагування, відновлення, аудит Implementation of ICT security: detection, protection, response, recovery, audit	Впровадження технічних, організаційних заходів, тестування, безперервність бізнесу Implementation of technical and organizational measures, testing, and business continuity	Технічні та організаційні заходи для захисту даних платіжних карт та систем, що їх обробляють Technical and organizational measures to protect payment card data and the systems that process them

Санкції за порушення **Sanctions for violations**	До 20 млн. євро або до 4% світового обороту Up to €20 million or up to 4% of global turnover	Залежно від рішення національного регулятора: штрафи, обмеження діяльності, вимога усунення порушень Depending on the decision of the national regulator: fines, activity restrictions, requirement to eliminate violations	Адміністративні санкції, потенційна відповідальність керівників організації Administrative sanctions, potential liability of the organization's executives	Санкції від платіжних систем, відключення від обробки платежів, фінансові штрафи Sanctions from payment systems, disconnection from payment processing, financial penalties
Взаємозв’язки між документами **Interrelationships between documents**	GDPR фокусується на персональних даних, може доповнювати NIS2 або DORA GDPR focuses on personal data and can complement NIS2 or DORA	Може перетинатися з NIS2 (особливо в аспектах кібербезпеки) і з GDPR (якщо йдеться про персональні дані) May overlap with NIS2 (especially in cybersecurity aspects) and with GDPR (when personal data is involved)	Поширюється на ті самі галузі, що й DORA, та взаємодіє з GDPR у частині інцидентів і даних Applies to the same sectors as DORA and interacts with GDPR in terms of incidents and data	Може доповнювати GDPR щодо захисту фінансових персональних даних; має спільні цілі з DORA/NIS2 May complement GDPR in protecting financial personal data; shares common goals with DORA/NIS2

3.2. Порівняння нормативно-правових документів за впливом на бізнес та IT-інфраструктуру

GDPR в першу чергу впливає на організаційні процеси, змушуючи компанії переглянути політики конфіденційності, налагодити механізми для обробки запитів суб’єктів даних, наприклад: запити на доступ, виправлення чи видалення даних. Та призначити відповідального за захист даних. В IT-інфраструктурі це означає необхідність впровадження інструментів шифрування, анонімності, контролю доступу та логування. GDPR значно підвищує рівень захисту персональних даних, але майже не стосується фінансових транзакцій безпосередньо [2].

На відміну від GDPR, DORA зосереджується на цифровій стійкості фінансових організацій. Він впливає на бізнес через потребу в управлінні ІКТ-ризиками, регулярному тестуванні готовності до інцидентів, а також у створенні механізмів реагування та відновлення. Компанії повинні укладати чіткі контракти з IT-постачальниками, забезпечувати безперервність бізнесу навіть у разі кібератак або технічних збоїв. З технічного боку, це означає впровадження систем моніторингу, автоматизованих тестів безпеки, резервного копіювання, сегментації мереж тощо. DORA опосередковано посилює захист і персональних, і фінансових даних завдяки покращенню стійкості систем [2, 3].

Директива NIS2 також має значний вплив на організаційну структуру компаній, особливо тих, що належать до критично важливих секторів. Вона вимагає системного підходу до управління кіберризиками, створення інцидент-менеджменту, безпеки ланцюгів постачання, а також прямої відповідальності керівництва за впровадження кіберзахисту. В

IT-інфраструктурі це призводить до запровадження засобів моніторингу, журналювання, тестування безпеки, а також процедур забезпечення безперервності бізнесу. Як результат, посилюється захист як персональних, так і фінансових даних у рамках загальної кібербезпеки [1].

PCI DSS безпосередньо впливає на компанії, які працюють із платіжними картками. Він вимагає стандартизації процедур обробки платіжних даних, впровадження політик безпеки, обмеження доступу, фізичного захисту обладнання, а також регулярного тестування безпеки. В IT-сфері компанії повинні забезпечити шифрування даних карток, встановлення брандмауерів, систем виявлення вторгнень, обмеження доступу до систем. PCI DSS безпосередньо націлений на захист фінансових транзакцій та даних власників карток, забезпечуючи надійність платіжної інфраструктури [1].

4. Міжнародні аналоги нормативно-правових актів ЄС

Регуляторна система Європейського Союзу у сфері цифрової безпеки вважається однією з найрозвиненіших у світі. Водночас важливо зазначити, що багато інших країн та міжнародних організацій створили власні нормативні документи, які за своєю метою, структурою та принципами є подібними до європейських.

Зокрема, регламент GDPR, що встановлює єдині правила захисту персональних даних у межах ЄС, має численні відповідники у законодавствах інших країн. У США діють кілька галузевих актів, таких як HIPAA – закон про захист персональних медичних даних, який містить вимоги щодо безпеки інформаційних систем у сфері охорони здоров'я [5]. Для освітнього сектору розроблено FERPA, що гарантує студентам і їхнім батькам право на доступ до освітніх записів та їхнє коригування [6]. Водночас в окремих штатах запроваджуються ширші закони про конфіденційність, зокрема CCPA у Каліфорнії, що дає споживачам право знати, які персональні дані збираються про них, і вимагати їх видалення [7]. У Південній Америці Бразилія прийняла закон LGPD, який вважається майже повним аналогом GDPR – як за принципами обробки даних, так і за правами користувачів [8]. Окрему роль відіграє Конвенція № 108 Ради Європи, до якої приєдналася і Україна, – вона є першою міжнародною угодою, що встановила обов'язкові правила щодо захисту персональних даних як у державному, так і приватному секторах [9].

Регламент DORA, спрямований на забезпечення цифрової стійкості фінансового сектору ЄС, також має функціональні аналоги. У США Міжбанківська координаційна рада розробила FFIEC Cybersecurity Assessment Tool – інструмент для оцінювання рівня кіберзахищеності фінансових установ [10]. Структурно близькою до DORA є і модель NIST Cybersecurity Framework, яка охоплює повний життєвий цикл безпеки: від ідентифікації загроз до відновлення після інцидентів [11].

Директива NIS2, яка зобов'язує операторів критичної інфраструктури впроваджувати кіберзахист, має численні відображення у регулюваннях інших країн і сфер. Найбільш очевидною паралеллю є NIST Cybersecurity Framework у США, який є універсальним інструментом для підвищення кіберстійкості організацій [10]. У галузі енергетики в США та Канаді застосовуються стандарти NERC CIP – обов'язкові норми безпеки для енергетичних компаній [12]. Велика Британія після виходу з ЄС ухвалила UK NIS Regulations – документ, що фактично є національною адаптацією європейської директиви NIS [13]. До найближчих до NIS2 за ініціативами документів також можна віднести міжнародний стандарт ISO/IEC 27001, який стосуються управління інформаційною безпекою та забезпечення безперервності діяльності [14].

У сфері платіжних систем міжнародний стандарт PCI DSS знаходить чіткі відповідники у низці документів. Зокрема, ISO/IEC 27001 як базовий стандарт управління інформаційною

безпекою часто використовується у фінансовому секторі [14]. У США подібну функцію виконують рекомендації NIST SP 800-53 та 800-171 – це комплексні каталоги технічних, фізичних і адміністративних заходів захисту інформаційних систем [15, 16]. У галузі електронної комерції та хмарних послуг активно використовується стандарт SOC 2, що дозволяє оцінити рівень безпеки, конфіденційності та моніторингу в компаніях, які обробляють дані клієнтів [17].

Загалом, міжнародна практика демонструє, що ключові принципи цифрової безпеки – управління ризиками, прозорість, захист персональних даних, відповідальність організацій – стали універсальними.

5. Висновки

1. У дослідженні проаналізовано основні нормативно-правові документи ЄС у сфері кібербезпеки: Директиву NIS2, Регламент GDPR, Регламент DORA та стандарт PCI DSS.

2. Усі ці документи спрямовані на посилення кіберстійкості та цифрової довіри в ЄС, але мають різні акценти:

- NIS2 фокусується на безпеці мережевих та інформаційних систем, зокрема для критичної інфраструктури.
- GDPR створює систему захисту персональних даних, встановлює права громадян і правила обробки інформації.
- DORA регулює цифрову стійкість фінансового сектору, зокрема управління ІКТ-ризиками.
- PCI DSS встановлює вимоги до безпеки обробки платіжної інформації, особливо для e-commerce компаній.

3. Також документи мають багато точок перетину:

- GDPR доповнює NIS2 і DORA у питаннях захисту персональних даних під час кіберінцидентів.
- DORA і NIS2 мають спільні вимоги щодо управління ризиками та кіберстійкості.
- PCI DSS виступає як практичний інструмент реалізації вимог з безпеки платіжних даних, що підкріплює цифрову безпеку загалом.

4. Ефективне впровадження цих документів у країнах-членах ЄС сприятиме: підвищенню кіберстійкості; зміцненню довіри до цифрових технологій; сталому розвитку цифрової економіки; закріпленню позицій ЄС як глобального лідера у сфері цифрової безпеки.

Конфлікт інтересів

Автори повідомляють про відсутність конфлікту інтересів.

References

1. Directive (EU) 2022/2555 of the European Parliament and of the Council (2022) On measures for a high common level of cybersecurity across the Union (NIS 2 Directive). Official Journal of the European Union. – URL: https://surl.li/xpktzi
2. Regulation (EU) 2016/679 of the European Parliament and of the Council (2016) On the protection of natural persons with regard to the processing of personal data (GDPR). Official Journal of the European Union. – URL: https://surl.lt/zdilhe
3. Regulation (EU) 2022/2554 of the European Parliament and of the Council (2022) On digital operational resilience for the financial sector (DORA). Official Journal of the European Union. – URL: https://surl.li/lvfsva

4. PCI DSS Certification (n.d.) Payment Card Industry Data Security Standard. PCI Security Standards Council. – URL: https://getpci.com/
5. Centers for Medicare & Medicaid Services (n.d.) HIPAA – Health Insurance Portability and Accountability Act. – URL: https://www.cms.gov/priorities/key-initiatives/burden-reduction/administrative-simplification/hipaa
6. U.S. Department of Education (n.d.) What is FERPA? – URL: https://surl.lu/oizpnq
7. Office of the Attorney General of California (n.d.) California Consumer Privacy Act (CCPA). – URL: https://oag.ca.gov/privacy/ccpa
8. Brazilian Government (n.d.) General Personal Data Protection Act (LGPD). – URL: https://lgpd-brazil.info/
9. Council of Europe (1981) Convention No. 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data. – URL: https://ippi.org.ua/vid-redaktsiinoi-kolegii-konventsiya-%E2%84%96-108-radi-%D1%94vropi-%E2%80%9Cpro-zakhist-osib-u-zv%E2%80%99yazku-z-avtomatizovano
10. Federal Financial Institutions Examination Council (FFIEC) (n.d.) Cybersecurity Assessment Tool. – URL: https://www.ffiec.gov/resources/cat
11. Federal Trade Commission (n.d.) What is the NIST Cybersecurity Framework? – URL: https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/nist-framework
12. North American Electric Reliability Corporation (n.d.) Critical Infrastructure Protection (NERC CIP). – URL: https://www.techtarget.com/searchsecurity/definition/North-American-Electric-Reliability-Corporation-Critical-Infrastructure-Protection-NERC-CIP
13. UK Government (2018) The Network and Information Systems Regulations 2018 (NIS Regulations 2018). – URL: https://surl.li/zahavi
14. ISO/IEC (2022) ISO/IEC 27001:2022 – Information Security, Cybersecurity and Privacy Protection. – URL: https://www.iso.org/standard/27001
15. National Institute of Standards and Technology (2020) NIST Special Publication 800-53 Rev. 5: Security and Privacy Controls for Information Systems and Organizations. – URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf
16. National Institute of Standards and Technology (2020) NIST Special Publication 800-171 Rev. 2: Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations. – URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf
17. Palo Alto Networks (n.d.) What is SOC 2 Compliance? – URL: https://www.paloaltonetworks.com/cyberpedia/soc-2

RESEARCH AND COMPARISON OF EUROPEAN UNION REGULATORY DOCUMENTS IN CYBERSECURITY

Maryna Yesina[1,2], Candidate of Technical Sciences, Associate Professor, Acting Head of the Department of Cybersecurity of Information Systems, Networks and Technologies, Institute of Cyber Security and Artificial Intelligence, Research Associate-Consultant, JSC «Institute of Information Technologies»; e-mail: m.v.yesina@karazin.ua; ORCID: https://orcid.org/0000-0002-1137-2382
Yelyzaveta Lohachova[1], 5th year student at the Department of Cybersecurity of Information Systems, Networks and Technologies, Institute of Cyber Security and Artificial Intelligencer; e-mail: lohachova2020kb11@student.karazin.ua; ORCID: https://orcid.org/0000-0002-9815-466X
Ievgeniia Kolovanova[1], Candidate of Technical Sciences, Acting Deputy Director of Educational Work, Institute of Cyber Security and Artificial Intelligence; e-mail: e.kolovanova@karazin.ua; ORCID: https://orcid.org/0000-0002-0326-2394
[1] *V. N. Karazin Kharkiv National University, Ukraine*
[2] *JSC "IIT", Ukraine*
Manuscript was received March 1, 2025; Received after review April 1, 2025;
Accepted May 2, 2025

Abstract. The article presents a thorough study and comparison of the main regulatory acts of the European Union in the field of cybersecurity, including: NIS2 Directive, General Data Protection Regulation (GDPR), Digital Operational Resilience Regulation (DORA) and PCI DSS standard. These documents are considered fundamental elements in shaping the EU's current policy on digital information protection, covering personal data, financial information and critical infrastructure. The paper outlines the key objectives of each of the acts, analyses their scope of application, requirements for regulated entities, risk management mechanisms, incident reporting, interaction with suppliers, and sanction provisions. Particular attention is paid to comparing the acts in terms of their impact on business and IT infrastructure, as well as identifying the interrelationships between them. It has been established that although each document has its own focus - personal data protection, financial infrastructure resilience, digital network security, or payment card transaction protection - they are all aimed at creating a comprehensive cyber security ecosystem within the EU. The article also analyses international analogues of these acts, such as GDPR-like laws in the United States and Brazil, NIST and ISO standards, which demonstrates the global nature of the digital security problem and the search for common approaches to solving it. In conclusion, the paper emphasises the importance of a comprehensive and harmonised approach to cybersecurity as a key condition for the sustainable development of a digital society. Given the current threats, in particular geopolitical conflicts and the growing scale of cybercrime, the effective implementation of European standards is of particular importance for partner countries, in particular Ukraine, which needs to adapt the relevant standards to enhance national cyber resilience.

Keywords: *regulatory documents, European Union, cybersecurity, business, information protection*

Conflicts of Interest: the authors declare no conflict of interest.