КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (26), 2024
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2024.26.693
УДК 004.005(49)

Капелюшна Тетяна Вікторівна
к.е.н., доцент, професор кафедри управління кібербезпекою та захистом інформації
Державний університет інформаційно-комунікаційних технологій, Київ, Україна
ORCID ID: 0000-0001-7490-6751
e-skr@ukr.net

Легомінова Світлана Володимирівна
д.е.н., професор, завідувач кафедри управління кібербезпекою та захистом інформації
Державний університет інформаційно-комунікаційних технологій, Київ, Україна
ORCID ID: 0000-00002-4433-5123
chiarasvitlana77@gmail.com

Мужанова Тетяна Михайлівна
к.держ.упр., доцент, доцент кафедри управління кібербезпекою та захистом інформації
Державний університет інформаційно-комунікаційних технологій, Київ, Україна
ORCID ID: 0000-0002-7435-0287
muzanovat@gmail.com

Тищенко Віталій Сергійович
старший викладач кафедри управління кібербезпекою та захистом інформації
Державний університет інформаційно-комунікаційних технологій, Київ, Україна
ORCID ID: 0000-0003-3849-6243
tvs5vetal@gmail.com

РЕГУЛЯТОРНЕ ПОЛЕ ФОРМУВАННЯ ПОЛІТИКИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ОРГАНІЗАЦІЇ

Анотація. У статті розглянуто проблему недосконалості регуляторних документів у частині перегляду основних нормативно-правових актів, їх оновлення відповідно до змін та тенденцій щодо захисту інформаційних ресурсів. Наголошено на потребі удосконалення комплаєнсу організацій із урахуванням: динамічності оцифровізації послуг в Україні; інтегрованості у світовий діджиталізований простір, а також активного використання інформаційно-комунікаційних технологій; розширення спектру послуг у сфері електронних комунікацій, якими обумовлюються нові атаки на підприємства. Підкреслено, що перераховані тенденції вказують на потребу посилення захисту інформаційних потоків організацій (від несанкціонованого доступу, витоку конфіденційних даних, втрати інформаційних активів, розповсюдження результатів інтелектуальної діяльності, поширення інформації, що становлять комерційну таємницю) на основі формування надійного регуляторного підґрунтя. Наведено визначення понять: «політика інформаційної безпеки», «політика безпеки інформації», «політика інформаційної безпеки банку», а також представлено ресурси, які виступають об’єктами поширення політики інформаційної безпеки організації. Проведено моніторинг нормативно-правових документів та виокремлено основні регуляторні документи щодо забезпечення інформаційної безпеки організацій, а саме: закони, положення, постанови, міжнародні стандарти, укази Президента, що регулюють питання кібербезпеки та захисту інформації організацій, які функціонують у фінансовій сфері. Результати моніторингу документів та їх узагальнення розглядаються як підґрунтя формування посилення комплаєнсу та можливість їх імплементування у практичну діяльність банків при розробленні політики управління інформаційною безпекою фахівцями з кібербезпеки (головного комплаєнс-менеджера (CCO) та керівника, що загалом виступає гарантом забезпечення інформаційної безпеки — CISO)).

Ключові слова: кібербезпека; політика управління; управління інформаційною безпекою організацій; комплаєнс управління інформаційною безпекою підприємства.

ВСТУП

Простір функціонування підприємств огорнутий інформаційними потоками, які збільшуються у міру діджиталізації, активним оцифруванням послуг й переходом на онлайн платформи, використанням веб-додатків, популяризацією цифрових послуг. Інформація є невід'ємною складовою факторів виробництва, ресурсом, що використовується підприємствами для формування власного іміджу та позитивного сприйняття клієнтами продукту (послуги) на ринку, проте часто інформаційні технології використовуються як засіб маніпулювання інформацією. Тобто інформація одночасно є сильною та слабкою стороною організації в залежності від цілей її використання та інтерпретації, способів її отримання й оприлюднення. Безперечно, що інформатизація, онлайн доступ до інформації, поширення її через соціальні мережі, підвищують порушення принципів інформаційної безпеки (так звану тріаду: конфіденційність, цілісність, доступність). Потреба захисту інформації з боку організацій зростає ще й з причин гібридної війни, що провадиться тринаправлено у фізично-інформаційному просторі країни: безпосередньо бойові дії, маніпулювання й вплив на свідомість людей та сприйняття подій, дипломатичні відносини за використання інформаційних, військових, економічних, політичних та інших ресурсів, що порушують безпеку функціонування організацій, країн.

Зазначене підкреслює актуалізацію питань щодо формування інформаційної безпеки господарюючих суб'єктів, розроблення політик управління інформаційною безпекою задля стійкого функціонування організацій.

Постановка проблеми. Важливим аспектом у формуванні політики інформаційної безпеки є специфіка діяльності організації та нормативно-правові документи регулювання його функціонування, що дозволяє підприємствам врегульовувати безпекові питання, ґрунтуючись на законах, постановах, стандартах й уникати спірних питань при розв'язанні проблем щодо її порушення за рахунок чіткого визначення вимог, зобов'язань, обов'язків та відповідальності дотримання інформаційної безпеки у межах правового поля. Аналіз нормативно-правових актів, на які посилаються організації при розробленні інформаційної власної політики безпеки, вказують на потребу перегляду, оскільки переважна більшість документів ґрунтується на застарілих стандартах та законодавчих документах. Тісна співпраця з європейськими країнами, посилення інтеграції у світову спільноту обумовлює потребу приведення регуляторних документів щодо управління інформаційною безпекою до світових вимог.

Аналіз останніх досліджень та публікацій. Дослідженням політики інформаційної безпеки присвячено чимало наукових робіт, але передусім розглядаються етапи її розроблення, складові, керування доступом, проте не досить глибоко розриваються питання регуляторного характеру, які, на нашу думку, є базисом формування її надійності та правомірності. Так, науковицею В. Тітовою досліджуються основні складові політики інформаційної безпеки підприємства, що охоплюють комплекс заходів із забезпечення захисту, які реалізуються через організаційні механізми, закладені в політиці безпеки організації. Окреслюються межі дії політики інформаційної безпеки, пропонуються критерії для оцінювання її ефективності [**Error! Reference source not found.**].

Конструктивно розглядається питання комплаєнсу в системі корпоративної інформаційної безпеки І. Чубаєвським. На думку автора, організації мають орієнтуватися на мінімізацію ризиків, пов'язаних із витоком конфіденційної інформації, як умисного розголошення даних співробітниками, так і ненавмисного порушення внутрішніх стандартів та регламентів, що регулюють зберігання й передачу інформації.

У банківському секторі, де застосування комплаєнсу регламентується відповідними законодавчими актами, використовують два основних підходи до його організації: rule-based approach (підхід, заснований на дотриманні норм), яким передбачається мінімальний рівень впровадження комплаєнсу, коли виконуються лише ті вимоги, які прямо передбачені законодавством та risk-based approach (підхід, заснований на управлінні ризиками), який орієнтований на оцінку й аналіз ризиків, що дозволяє побудувати систему комплаєнсу з урахуванням специфіки діяльності організації. Цей підхід рекомендований міжнародними структурами, такими як Вольфсберзька група та Базельський комітет з банківського нагляду й використовується в європейських країнах.[2]. А. Босак вважає, що інформаційна безпека містить дві складові: інформаційну атаку та захист інформації. Перша є комплексом дій, спрямованих на захист корпоративної інформації від зовнішніх загроз, які порушують її цілісність, несанкціонованому розголошенню конфіденційної інформації, а друга — охоплює безпеку інформаційних ресурсів підприємства, а також засобів, що забезпечують їх зберігання, передачу й обробку за рахунок заходів: для захисту автоматизованих процесів від зовнішніх впливів; визначення інформаційної політики підприємства; контролю і регулювання поширення інформації в межах та поза межами організації, що вказує на бачення автором захисту саме у політиці інформаційної безпеки [**Error! Reference source not found.**]. Н. Ржевська [**Error! Reference source not found.**], посилається на науковий доробок Брамана, який у термін «інформаційна політика» вкладає регуляторні смисли, а саме: сукупність законів, нормативно-правових актів та концептуальних положень, які регулюють сфери інформації, комунікації та культури.

Заслуговує уваги напрацювання І. Опірського, Ю. Курія [5], якими проаналізовано зміни стандарту ISO/IEC 27001, проведено його порівняння із попередньою редакцією та надано пропозиції щодо адаптації підприємств до виявлених змін.

Вищезгадані наукові результати вчених слугуватимуть базисом для дослідження управління інформаційною безпекою підприємств у частині аналізу регуляторного забезпечення за означеною нами проблематикою щодо розроблення політики інформаційної безпеки організацій на підґрунті виявлених нормативно-правових змін.

Мета статті. Проаналізувати регуляторні зміни щодо управління інформаційною безпекою підприємств для врахування їх при розробленні політики управління інформаційною безпекою організацій.

ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ

Розуміння сутності «політики» дозволяє окреслити основні аспекти та розстановку основних акцентів-вимог щодо її формування. Термін «політика» найчастіше зустрічається та вживається у політичній сфері та визначений, як особливий вид людської діяльності, пов’язаний з одержанням і здійсненням влади, насамперед державної [7, с. 11].

Основний акцент політики організації — спільність інтересів персоналу щодо усвідомлення значення безпеки у функціонуванні підприємств, забезпечення захисту інформації для гарантування безперебійної роботи організації й досягнення його цільових результатів. Влучно та ємно розкрито сутність поняття науковицею Г. Колбеч: «політика — це особливий спосіб структурування дій, який складається з визначення цілей, вибору способу дій, впровадження цього способу, оцінки результатів, зміни політики тощо, і має лідерів, виконавців, зацікавлених сторін, коен з яких є учасником суспільної системи» [8, с. 26, 20]. Можемо припустити, що розробка політики передбачає:

- визначення повноважень, затверджених уповноваженим органом, що надає легітимності політиці;
- використання глибинних (експертних) знань щодо розуміння проблем та способів її вирішення з метою зміцнення організації, ефективного розв'язання проблем;
- забезпечення порядку шляхом формування системності, узгодженості дій та визначення обмежень для регулювання поведінки відповідальних осіб, управлінців, персоналу з питань усунення виявлених загроз.

Активне використання інформаційно-комунікаційних технологій, розширення спектру послуг у сфері електронних комунікацій обумовлює появу нових та більш витончених атак на підприємства, тому захист підприємств від несанкціонованого доступу, витоку конфіденційних даних, втрати інформаційних активів, розповсюдження результатів інтелектуальної діяльності, поширення інформації, що становить комерційну таємницю є нагальними проблемами до вирішення.

Тож, сучасний цифровий ландшафт, одночасно формуючи широкі можливості, спричиняє появу нових загроз, примножує кількість кіберінцидентів та підвищує вразливість до них організацій й потребує надійного захисту організації.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Одним із шляхів упередження інформаційних загроз є формування політики інформаційної безпеки підприємства задля управління безпекою підприємства, на меті якої захист інформаційних ресурсів підприємства, як активу.

Політика безпеки інформації — документ або сукупність документів системного рівня, які містять набір вимог, правил, обмежень, рекомендацій, що регламентують порядок інформаційної діяльності в інформаційній системі і спрямовані на досягнення й підтримку стану інформаційної безпеки системи та організації в цілому [7].

Політика інформаційної безпеки — політика, що визначає підхід підприємства, установи та організації, які відповідно до законодавства віднесені до об'єктів критичної інфраструктури, до інформаційної безпеки, вимоги, правила, обмеження, рекомендації, що регламентують порядок дотримання та забезпечення інформаційної безпеки [6].

Згідно із «Положенням про здійснення контролю за дотриманням банками вимог законодавства з питань інформаційної безпеки, кіберзахисту та електронних довірчих послуг», Національний банк здійснює контроль з метою:

1) оцінювання ефективності функціонування системи управління інформаційною безпекою (СУІБ) банку;
2) оцінювання повноти виконання банком вимог нормативно-правових актів Національного банку з питань інформаційної безпеки, кіберзахисту;
3) оцінювання рівня управління ризиками інформаційної безпеки/кіберризиками банком і системи внутрішнього контролю, яка функціонує на всіх організаційних рівнях, за напрямами діяльності, що перевіряються;
4) прийняття засвідчувальним центром рішення про внесення відомостей про кваліфікованого надавача електронних довірчих послуг до довірчого списку;
5) перевірки виконання вимог нормативно-правових актів з питань надання кваліфікованих електронних довірчих послуг кваліфікованим надавачем електронних довірчих послуг, відомості про якого внесені до довірчого списку за поданням засвідчувального центру [14]. Варто зазначити, що із

вищеозначених п’яти пунктів два стосуються саме нормативно-правових актів, що доводить вагу комплаєнсу у розбудові ефективного управління інформаційною безпекою організацій.

Оскільки політикою передбачається набір певних правил та норм щодо її формування, регламентування дотримання господарюючими суб’єктами інформаційної безпеки, перед її формуванням слід проводити моніторинг нормативно-правових документів та стандартів щодо забезпечення інформаційної безпеки, які слугуватимуть базисом для формування загальної концепції дотримання порядку інформаційної безпеки та управління нею. Дослідження регуляторного поля має здійснюватися у межах специфіки діяльності суб’єкта господарювання, так, для установ, що функціонують у фінансовій сфері, зокрема банків, основними документами є: постанови Національного банку України та Кабінету Міністрів України, Закони України, укази Президента, ISO-стандарти [9] – [20] (їх перелік наведено в табл. 1).

У Постанові Національного Банку України ризик інформаційної безпеки (складова операційного ризику) визначається, як імовірність виникнення збитків або додаткових втрат, або недоотримання запланованих доходів унаслідок порушення конфіденційності, цілісності, доступності даних в інформаційних системах банку, недоліків або помилок в організації внутрішніх процесів або настання зовнішніх подій, уключаючи кібератаки або неадекватну фізичну безпеку. Ризик інформаційної безпеки включає кіберризик [11].

Політика інформаційної безпеки банку — сукупність правових і морально-етичних норм, правил, адміністративних, організаційних заходів, а також технічних, програмних і криптографічних засобів, направлених на захист інформаційної інфраструктури банку від випадкового і навмисного втручання в процес її функціонування. Можемо дійти висновку, що інформаційна безпека в банках не точиться суто навколо технічного захисту інформації, а включає весь спектр засобів захисту інформаційної інфраструктури банку. Тобто об’єктами, на які поширюється дія політики інформаційної безпеки банку, є наступні ресурси: інформаційні ресурси, програмні ресурси, фізичні ресурси, сервісні ресурси, людські ресурси (рис. 1).

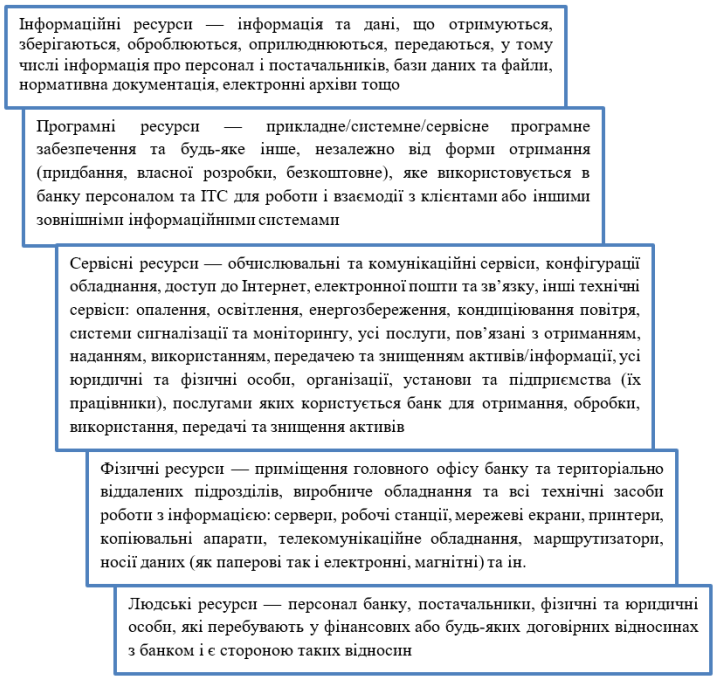

Рис. 1. Ресурси-об’єкти поширення політики інформаційної безпеки

Слід зазначити недосконаліть перегляду законодавчих документів у частині змістовного наповнення, зокрема у положенні «Про організацію заходів із забезпечення інформаційної безпеки в банківській системі України» вказано, що при його складанні базою слугували стандарти з питань інформаційної безпеки ДСТУ ISO/IEC 27000:2015 «Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Огляд і словник», ДСТУ ISO/IEC 27001:2015 «Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги», ДСТУ ISO/IEC 27002:2015 «Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки», тобто потребує оновлення зміст документу, зважаючи на перегляд стандартів, прийнятих у міжнародній практиці забезпечення інформаційної безпеки та кіберзахисту в банківській сфері та управління ризиками, а саме до: ISO/IEC 27002:2022 «Інформаційна безпека, кібербезпека та захист конфіденційності. Засоби контролю інформаційної безпеки» [20] та ISO/IEC 27001:2022 «Інформаційна безпека, кібербезпека та захист конфіденційності. Система керування інформаційною безпекою. Вимоги» [19], оскільки стандарти 2015 року були скасовані і не діють, що вказує на недосконаліть законодавства, а передусім — моніторингу нормативно-правових документів. Із метою посилення значущості дослідження, можливості використання їх на практиці, нами було проаналізовано нормативно-правові документи, що регулюють діяльність організацій у фінансові сфері та виокремлено основні із них, які варто використовувати при формуванні ІБ банківських установ (табл. 1).

Таблиця 1

Основні регуляторні документи щодо забезпечення інформаційної безпеки організацій

Закони	«Про Національний банк України» «Про банки і банківську діяльність» «Про захист персональних даних» «Про захист інформації в інформаційно-телекомунікаційних системах» «Про електронні документи та електронний документообіг» «Про національну безпеку України» «Про основні засади забезпечення кібербезпеки України» «Про електронні довірчі послуги» «Про хмарні послуги» Закон «Datenschutz-Grundverordnung» (DS-GVO) Закон «General Data Protection Regulation» (GDPR)
Положення	«Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України» «Положення про кваліфікованих надавачів електронних довірчих послуг» «Положення про здійснення контролю за дотриманням банками вимог законодавства з питань інформаційної безпеки, кіберзахисту та електронних довірчих послуг» «Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України»
Укази Президента України	від 13 лютого 2017 року № 32/2017 «Про рішення Ради національної безпеки і оборони України» від 29 грудня 2016 року «Про загрози кібербезпеки держави та невідкладні заходи з їх нейтралізації» від 15 березня 2016 року № 96/2016 «Про рішення Ради національної безпеки і оборони України» від 27 січня 2016 року «Про Стратегію кібербезпеки України»

Стандарти з питань інформаційної безпеки	ДСТУ ISO/IEC 27001:2023 (ISO/IEC 27001:2022, IDT) «Інформаційна безпека, кібербезпека та захист конфіденційності. Системи керування інформаційною безпекою. Вимоги»; ДСТУ ISO/IEC 27002:2023 (ISO/IEC 27002:2022, IDT) «Інформаційна безпека, кібербезпека та захист конфіденційності. Засоби контролювання інформаційної безпеки» Стандарт «Payment Card Industry Data Security Standard» (PCI DSS) Загальні принципи банківського нагляду (стандарти) «Основні Базельські принципи»
Рекомендації НБУ	«Про діяльність Правління Національного банку України щодо вдосконалення платіжної системи та проблеми цифрових валют центробанків та платіжних систем на блокчейні»

Стандарт 27002 слугує фундаментом для підприємств, які вибудовують надійний захист власних інформаційних активів. Стандарт узагальнює найкращі практики щодо контролю доступу, криптографії, безпеки людського ресурсу та реагування на кіберінциденти.

Розгляд та впровадження практик регулювання питань управління кібербезпекою та захисту інформації дозволив, зважаючи на євроінтеграційний вектор України, окрім стандартів ISO, виділити наступні, які вартують уваги при формуванні політики управління інформаційною безпекою підприємства:

1. Загальні принципи банківського нагляду «Основні Базельські принципи», в яких відображено, окрім основних положень щодо контролю за функціонуючими банками, банківськими ризиками, питання дотримання конфіденційності інформації.
2. Закон GDPR щодо регулювання захисту даних фізичних осіб в ЄС (GDPR — General Data Protection Regulation). Даний закон регламентує захист даних та застосовується у європейському регіоні з 25 травня 2018 року в усіх державах-членах для гармонізації законів про конфіденційність даних у всій Європі, наразі на перегляді задля приведення до умов сьогодення (розгляд пропозицій до 20 листопада 2024 року) [17].
3. Сукупність вимог щодо забезпечення безпеки даних про власників платіжних карток, які зберігаються, передаються та обробляються в інформаційних інфраструктурах. Дотримання стандарту PCI DSS (Payment Card Industry Data Security Standard) вимагається від усіх організацій, які зберігають, обробляють або передають дані власників карток Visa, включаючи фінансові установи, продавців і постачальників послуг [15], [16].
4. Німецький основний закон про захист даних — DS-GVO (Datenschutz-Grundverordnung). У документі описано інформаційні зобов'язання відповідальних осіб за інформаційні потоки клієнтів, співробітників, відвідувачів веб-сайту та ін., тобто стейкхолдерів, котрі, в свою чергу, мають бути поінформовані про правила використання їх особистих даних (деталізовано у ст. 13 та 14) [18].

Дедалі частіше організації стикаються з комплаєнс — ризиками — ймовірністю виникнення збитків/санкцій, додаткових втрат або недоотримання запланованих доходів або втрати репутації внаслідок невиконання банком вимог законодавства, нормативно-правових актів, ринкових стандартів, правил добросовісної конкуренції, правил корпоративної етики, виникнення конфлікту інтересів, а також внутрішньобанківських/внутрішньогрупових документів банку [12], [21]. При чому у «Положенні про організацію системи управління ризиками в банках України та

банківських групах» обов'язки відслідковувати та контролювати норми (комплаєнс) та їх дотримання покладено на головного комплаєнс-менеджера (CCO), а цілковито гарантом забезпечення інформаційної безпеки — CISO.

Зважаючи на зростаючу потребу підприємств у комплаєнсі задля успішного проходження зовнішнього аудиту компанії, відповідності міжнародним вимогам та правилам безпеки, можна із впевненістю стверджувати, що грунтовно сформоване регуляторне поле щодо правил функціонування підприємств слугуватиме базисом для забезпечення стійкої інформаційної безпеки та гарантування правомірності, легітимності політик інформаційної безпеки організації.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Підсумовуючи можемо стверджувати, що комплаєнс убезпечує підприємства від спірних питань щодо надійності та правомірності інформаційної безпеки підприємства, оскільки врахування регуляторних вимог чітко окреслює правила, вимоги, відповідальність щодо забезпечення безпеки організацій. Окрім того, дозволяє підприємствам спрямовати діяльність на запобігання порушенням законодавства у сфері інформації, які можуть завдати підприємству фінансових збитків, призводити до репутаційних ризиків. Управління кібербезпекою представляє собою сукупність принципів спрямованих регулювати процес прийняття рішень та забезпечувати досягнення визначених цілей, які у інформаційній безпеці представляються формуванням надійної політики безпеки, яка ґрунтується на регуляторних, законодавчих, нормативних вимогах до ІБ. Належна увага має приділятися дослідженню питань змін у стандартах та їх врахування при розробленні політики управління з чіткою відповідністю регуляторним міжнародним вимогам до ІБ.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Тітова, В., Кльоц, Ю., Волинець, В., Петляк, Н., & Огородник, М. (2024). Розроблення політики інформаційної безпеки приватного підприємства. *Measuring and computing devices in technological processes*, (3), 79–83. https://doi.org/10.31891/2219-9365-2024-79-10 Вип.3. 2024. С.79-83.
2. Чубаєвський, В. (2022). Методи управління корпоративною інформаційною безпекою. *Економіка та суспільство*, (43). https://doi.org/10.32782/2524-0072/2022-43-49
3. Bosak, A., Verzhykovskyi, V., Kalinin, I., Maksymiv, I., Prystupa, D., & Ryvak, O. (2023). Principles of formation of enterprise information security. *International scientific journal «Internauka». Series: «Economic Sciences»*, (11(79)). https://doi.org/10.25313/2520-2294-2023-11-9157
4. Rzhevska, N., & Feshchenko, A. (2022). The Peculiarities of Space State Information Policy. *Language-Cultura-Politics. International Jornal*, *1*, 247−264. https://doi.org/ 10.54515/lcp.2022.1.247-264
5. Kurii, Y., & Opirskyy, I. (2023). ISO 27001: analysis of changes and peculiarities of compliance with the new version of the standard. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 3(19)*, 46–55. https://doi.org/10.28925/2663-4023.2023.19.4655
6. Chmutova, I. M., Bezrodna, O. S., & Nechyporenko, D. I. (2020). The Methodological Instrumentarium for Assessing Compliance Risks Of Financial Monitoring of Banks. *Business Inform*, *11(514)*, 296–309. https://doi.org/10.32983/2222-4459-2020-11-296-309
7. Герасимчук, Т. Ф., Киридон, А. М., & Троян, С. С. (2017). *Загальна теорія політики: Навчальний посібник.* «Кондор».
8. Колбеч, Г. К. (2024). *Політика: Основні концепції в суспільних науках.* «КМ Академія».
9. Про затвердження Методичних рекомендацій щодо забезпечення кіберзахисту автоматизованих систем управління технологічними процесами, Наказ, № 463 (2023) (Україна). https://ips.ligazakon.net/document/fn077605?an=37&ed=&dtm=&le=

10. Про затвердження Загальних вимог до кіберзахисту об`єктів критичної інфраструктури, Постанова Кабінету Міністрів України № 518 (2022) (Україна). https://zakon.rada.gov.ua/laws/show/518-2019-п#Text
11. Про внесення змін до деяких нормативно-правових актів Національного банку України, Постанова Національного банку України № 40 (2023) (Україна). https://zakon.rada.gov.ua/laws/show/v0040500-23#Text
12. Про затвердження Положення про організацію системи управління ризиками в банках України та банківських групах, Постанова Національного банку України № 64 (2024) (Україна). https://zakon.rada.gov.ua/laws/show/v0064500-18#Text
13. Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України, Постанова Національного банку України № 95 (2017) (Україна). https://zakon.rada.gov.ua/laws/show/v0095500-17#Text
14. Про затвердження Положення про здійснення контролю за дотриманням банками вимог законодавства з питань інформаційної безпеки, кіберзахисту та електронних довірчих послуг, Постанова Правління Національного банку України № 4 (2021). Національний банк України. https://bank.gov.ua/ua/legislation/Resolution_16012021_4
15. PCI COUNCIL LLC. (2024). *Standart (PCI DSS/ v.4.0.1.).* https://east.pcisecuritystandards.org/document_library?category=pcidss&document=pci_dss
16. *What are the 12 requirements of PCI DSS Compliance?* (б. д.). ControlCase. https://www.controlcase.com/what-are-the-12-requirements-of-pci-dss-compliance/
17. Regulation (eu) 2016/679 of the European Parliament and of the Council (б. д.). EUR-Lex repealing Directive 95/46/EC (General Data Protection Regulation. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679
18. *EU Datenschutz Grundverordnung (EU-DSGVO)*. (б. д.). EU Datenschutz Grundverordnung (EU-DSGVO). https://www.privacy-regulation.eu/
19. INFORMATION SECURITY CONTROLS. (2022). *ISO/IEC 27001:2022*. IT Governance Publishing. https://doi.org/10.2307/j.ctv30qq13d.8
20. International Standart. (2022). *Information security, cybersecurity and privacy protection — Information security controls* (ISO/IEC 27002:2022).
21. Гулак, Г. М., Жильцов, О. Б., Киричок, Р. В., Коршун, Н. В., & Складанний, П. М. (2024). *Інформаційна та кібернетична безпека підприємства.* Підручник. Львів: Видавець Марченко Т. В.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (26), 2024
ISSN 2663 - 4023

Tetiana Kapeliushna
PhD in Economics, Associate Professor,
Professor of the Department of Cybersecurity and Information Protection Management
State University of Information and Communication Technologies, Kyiv, Ukraine
ORCID ID: 0000-0001-7490-6751
e-skr@ukr.net

Svitlana Lehominova
Doctor of Economics, Professor,
Head of the Department of Cybersecurity and Information Protection Management
State University of Information and Communication Technologies, Kyiv, Ukraine
ORCID ID: 0000-0002-4433-5123
chiarasvitlana77@gmail.com

Tetiana Muzhanova
PhD in Public Administration, Associate Professor, Associate Professor of the
Department of Cybersecurity and Information Protection Management
State University of Information and Communication Technologies, Kyiv, Ukraine
ORCID ID: 0000-0002-7435-0287
muzanovat@gmail.com

Vitalii Tyshchenko
Senior Lecture of the Department of Cybersecurity and Information Protection Management
State University of Information and Communication Technologies, Kyiv, Ukraine
ORCID ID: 0000-0003-3849-6243
tvs5vetal@gmail.com

REGULATORY FRAMEWORK FOR THE DEVELOPMENT OF AN ORGANISATION'S INFORMATION SECURITY MANAGEMENT POLICY

Abstract. The article deals with the problem of imperfection of regulatory documents in terms of revision of the main regulatory legal acts, their updating in accordance with changes and trends in the protection of information resources. The author emphasises the need to improve the compliance of organisations with due regard for the active digitisation of services in Ukraine, integration into the global digitalised space, as well as the active use of information and communication technologies, and expansion of the range of services in the field of electronic communications, which are the reasons for new attacks on enterprises. The author emphasises that these trends necessitate strengthening the protection of information flows of organisations (against unauthorised access, leakage of confidential data, loss of information assets, dissemination of intellectual property, dissemination of information constituting a trade secret) on the basis of a reliable regulatory framework. The article provides definitions of the following concepts: "information security policy", "information security policy", "bank information security policy", and the resources that are the objects of dissemination of the organisation's information security policy are presented. The authors have thoroughly monitored the regulatory and legal documents and identified the main regulatory documents on ensuring information security of organisations, namely: laws, regulations, resolutions, international standards, presidential decrees regulating cybersecurity and information protection of organisations operating in the financial sector. The results of the monitoring of documents and their summary are considered as the basis for the formation of compliance enhancements and the possibility of their implementation in the practical activities of banks in the development of information security management policies by cybersecurity specialists (chief compliance officer (CCO) and chief information security officer (CISO)).

Keywords: cybersecurity; management policy; information security management of organisations; compliance management of enterprise information security.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Titova, V., Kliots, Yu., Volynets, V., Petliak, N., & Ohorodnyk, M. (2024). Development of an information security policy for a private enterprise Rozroblennia polityky informatsiinoi bezpeky pryvatnoho pidpryiemstva. *Measuring and Computing Devices in Technological Processes, 3*, 79–83. https://doi.org/10.31891/2219-9365-2024-79-10
2. Chubaievskyi, V. (2022). Methods of corporate information security management. *Ekonomika ta suspilstvo, 43*. https://doi.org/10.32782/2524-0072/2022-43-49
3. Bosak, A., Verzhykovskyi, V., Kalinin, I., Maksymiv, I., Prystupa, D., & Ryvak, O. (2023). Principles of formation of enterprise information security. *International Scientific Journal «Internauka». Series: Economic Sciences, 11(79)*. https://doi.org/10.25313/2520-2294-2023-11-9157
4. Rzhevska, N., & Feshchenko, A. (2022). The peculiarities of space state information policy. *Language-Cultura-Politics. International Journal, 1*, 247–264. https://doi.org/ 10.54515/lcp.2022.1.247-264
5. Kurii, Y., & Opirskyy, I. (2023). ISO 27001: Analysis of changes and compliance features of the new version of the standard. *Electronic Professional Scientific Journal «Cybersecurity: Education, Science, Technique», 3(19)*, 46–55. https://doi.org/10.28925/2663-4023.2023.19.4655
6. Chmutova, I. M., Bezrodna, O. S., & Nechyporenko, D. I. (2020). The methodological instrumentarium for assessing compliance risks of financial monitoring of banks. *Business Inform, 11(514)*, 296–309. https://doi.org/10.32983/2222-4459-2020-11-296-309
7. Herasymchuk, T. F., Kyrydon, A. M., & Troian, S. S. (2017). *Zahalna teoriia polityky: Navchalnyi posibnyk [General theory of politics: A study guide]*, Kondor.
8. Kolbech, H. K. (2004). *Polityka: Osnovni kontseptsii v suspil`nykh naukakh [Politics: Basic concepts in the social sciences]*. Vydav. dim «KM Akademiia».
9. On Approval of the Methodological Recommendations for Ensuring Cyber Security of Automated Process Control Systems, Order, № 463 (2023) (Ukraine). https://ips.ligazakon.net/document/fn077605?an=37&ed=&dtm=&le=
10. On Approval of the General Requirements for the Cyber Defence of Critical Infrastructure Objects, Resolution of the Cabinet of Ministers of Ukraine No. 518 (2022) (Ukraine). https://zakon.rada.gov.ua/laws/show/518-2019-п#Text
11. On Amendments to Certain Regulatory Acts of the National Bank of Ukraine, Resolution of the National Bank of Ukraine № 40 (2023) (Ukraine). https://zakon.rada.gov.ua/laws/show/v0040500-23#Text
12. On Approval of the Regulation on the Organisation of the Risk Management System in Banks of Ukraine and Banking Groups, Resolution of the National Bank of Ukraine № 64 (2024) (Ukraine). https://zakon.rada.gov.ua/laws/show/v0064500-18#Text
13. On Approval of the Regulation on the Organisation of Measures to Ensure Information Security in the Banking System of Ukraine, Resolution of the National Bank of Ukraine № 95 (2017) (Ukraine). https://zakon.rada.gov.ua/laws/show/v0095500-17#Text
14. On Approval of the Regulation on Monitoring of Banks' Compliance with Legislative Requirements on Information Security, Cyber Security and Electronic Trust Services, Resolution of the Board of the National Bank of Ukraine № 4 (2021). https://bank.gov.ua/ua/legislation/Resolution_16012021_4
15. PCI COUNCIL LLC. (2024). *Standart (PCI DSS/ v.4.0.1.)*. https://east.pcisecuritystandards.org/document_library?category=pcidss&document=pci_dss
16. *What are the 12 requirements of PCI DSS Compliance?* (б. д.). ControlCase. https://www.controlcase.com/what-are-the-12-requirements-of-pci-dss-compliance/
17. Regulation (eu) 2016/679 of the European Parliament and of the Council (б. д.). EUR-Lex repealing Directive 95/46/EC (General Data Protection Regulation. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679
18. *EU Datenschutz Grundverordnung (EU-DSGVO)*. (б. д.). EU Datenschutz Grundverordnung (EU-DSGVO). https://www.privacy-regulation.eu/
19. INFORMATION SECURITY CONTROLS. (2022). *ISO/IEC 27001:2022*. IT Governance Publishing. https://doi.org/10.2307/j.ctv30qq13d.8
20. International Standart. (2022). *Information security, cybersecurity and privacy protection — Information security controls* (ISO/IEC 27002:2022).
21. Hulak, H. M., Zhiltsov, O. B., Kyrychok, R. V., Korshun, N. V., & Skladannyi, P. M. (2024). *Information and cyber security of the enterprise.* Textbook. Lviv: Publisher Marchenko T. V.