УДК 342.951

ЖЕРЕБЕЦЬ О.М., начальник відділу Українського науково-дослідного інституту спеціальної техніки та судових експертиз Служби безпеки України
ORCID: https://orcid.org/0000-0002-2059-2045

ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ МЕТОДИКИ ІДЕНТИФІКАЦІЇ ТА ОЦІНКИ КІБЕРРИЗИКІВ НА НАЦІОНАЛЬНОМУ РІВНІ: СУЧАСНИЙ ДОСВІД СЛОВАЧЧИНИ ТА ЛАТВІЇ

DOI: https://doi.org/10.37750/2616-6798.2025.2(53).334163

Анотація. *Визначено поняття, зміст та складові проведення оцінки ризиків кібербезпеки. Узагальнено фактори, які доцільно враховувати під час проведення оцінки кіберризиків. Окреслено сучасні тенденції поширення кіберзагроз та кібератак. Деталізовано складові компоненти та елементи методики здійснення оцінки кіберризиків. Визначено класифікацію, види, мету та завдання оцінки кіберризиків. Акцентовано увагу на ініціативах України в контексті розробки та реалізації планових заходів у сфері посилення кібербезпеки держави в умовах правового режиму воєнного стану. Розглянуто позитивний досвід Словаччини та Латвії з нормативного забезпечення стратегічних засад кібербезпеки, методики ідентифікації та оцінки кіберризиків на національному рівні. Визначено роль та значення оцінки кіберризиків для єдиної інформаційної системи кібербезпеки цих країн. Окреслено подальші напрямки удосконалення національної системи забезпечення кібербезпеки в контексті необхідності прискорення розроблення та затвердження методики ідентифікації та оцінки кіберризиків на національному рівні, нормативного врегулювання питань щодо впровадження обов'язковості проведення періодичної оцінки кіберризиків.*

Ключові слова: *кібербезпека, кіберзахист, кіберризик, кіберінцидент, ландшафт кіберзагроз, критична інформаційна інфраструктура, оцінка, методологічне забезпечення, методика, управління вразливостями, ризик-орієнтований підхід, управління ризиками, збитки.*

Summary*. The concept, content and components of a cybersecurity risk assessment are defined. The factors that should be considered when conducting a cyber risk assessment are summarized. The current trends in the spread of cyber threats and cyber attacks are outlined. The components and elements of the methodology for conducting a cyber risk assessment are detailed. The classification, types, purpose and objectives of cyber risk assessment are defined. Attention is focused on Ukraine's initiatives in the context of developing and implementing planned measures to strengthen the state's cybersecurity under the legal regime of martial law. The positive experience of Slovakia and Latvia in regulatory support for strategic cybersecurity principles, methods for identifying and assessing cyber risks at the national level is considered. The role and significance of cyber risk assessment for the unified cybersecurity information system of these countries is defined. Further directions for improving the national cybersecurity system are outlined in the context of the need to accelerate the development and approval of a methodology for identifying and assessing cyber risks at the national level, and regulatory environment for the introduction of mandatory periodic cyber risk assessments.*

Keywords: *cybersecurity, cyber protection, cyber risk, cyber incident, cyber threat landscape, critical information infrastructure, assessment, methodological support, methodology, vulnerability management, risk-based approach, risk management, losses.*

Постановка проблеми. Як переконливо демонструє світовий досвід, будь-які інформаційно-комунікаційні системи або об'єкти критичної інфраструктури можуть бути уражені чи виведені з ладу внаслідок потужних кібератак. У свою чергу,

динамічне розширення ландшафту кіберзагроз, ускладнення інструментарію їх реалізації спонукає уряди провідних держав світу посилювати спроможності та розвивати архітектуру національних систем кібербезпеки, змінювати стратегію і тактику протидії таким кіберзагрозам. На перманентній основі вносяться зміни до існуючих стратегічних моделей протидії кіберзагрозам, які пов'язані із розумінням фактично недостатньої можливості побудувати абсолютно невразливі та удосконалені системи кіберзахисту. За таких умов актуалізується проблематика розробки сучасних механізмів швидкого виявлення вразливостей і кібератак, оперативного реагування та поширення інформації про них з метою мінімізації негативних наслідків та запобігання масштабним збиткам. Це стає можливим завдяки розробці та практичному запровадженню системи управління ризиками кібербезпеки, що являє собою процес виявлення, оцінки та пом'якшення ризиків для інформаційних систем та даних від кіберзагроз. У свою чергу, це передбачає розробку та впровадження стратегій з метою посилення захисту цифрових активів, забезпечуючи безперервність кіберзахисту. При цьому, основні принципи управління ризиками кібербезпеки включають: ідентифікацію, що передбачає розуміння потенційних кіберзагроз, вразливостей і активів; оцінку виявлених кіберризиків; пошук шляхів пом'якшення з метою впровадження заходів для мінімізації або усунення кіберризиків; системний моніторинг з метою постійного перегляду і оновлення стратегій для адаптації до нових кіберзагроз. Відповідно до звіту Всесвітнього економічного форуму (WEF) Global Cybersecurity Outlook 2025 [1], кібербезпека вступає в епоху безпрецедентної складності через посилення геополітичної напруженості, а швидкий технологічний прогрес і дедалі більш витончені загрози вимагають, на постійній основі, забезпечувати кіберстійкість. За таких умов набуває актуальності вивчення та опанування практик ризик-орієнтованого підходу щодо практичної реалізації заходів з метою забезпечення кібербезпеки об'єктів критичної інфраструктури та державних органів, здійснення нормативного врегулювання питань впровадження обов'язковості здійснення періодичної оцінки кіберризиків на підставі розроблених методик. Динамічний характер кіберзагроз вимагає здійснювати постійну оцінку ефективності управління ризиками кібербезпеки.

В цьому контексті проведення оцінки ризиків кібербезпеки має важливе значення для усіх інформаційних систем, організації та вжиття відповідних заходів для їх захисту. Цей процес передбачає системний підхід до виявлення, оцінки та пом'якшення потенційних кіберзагроз. Загальновідомо, що для ефективного пом'якшення кіберризиків державні органи та приватні структури повинні впроваджувати комбінацію технологічних рішень, стратегій управління. Використовуючи правильні інструменти та процеси, уповноважені суб'єкти можуть підвищити свою кіберстійкість до потенційних загроз. Це стає можливим завдяки проведенню оцінки ризиків кібербезпеки — процесу виявлення, кількісної оцінки та управління ризиками для систем та даних інформаційних технологій державних органів та приватних структур. Загалом кіберризик являє собою ризик фінансових втрат, збоїв у роботі або пошкодження у результаті відмови цифрових технологій, що використовуються для інформаційних та/або операційних функцій, впроваджених до промислової системи за допомогою електронних засобів, через несанкціонований доступ, використання, розкриття, порушення, модифікацію або пошкодження промислової системи.

Саме тому оцінка ризиків кібербезпеки допомагає краще зрозуміти вразливість інформаційних систем до кібератак, а також розставити пріоритети у ресурсному забезпеченні з урахуванням можливих витрат на кібербезпеку. Виявляючи конкретні загрози та роблячи кроки щодо їх усунення, стає можливим знизити загальний рівень

ризику та захиститися від несанкціонованого витоків даних. Оцінка ризиків кібербезпеки спрямована на виявлення вразливостей та підготовки рекомендаційних рішень з метою зниження або усунення будь-яких загроз. Окрім включення аналізу загроз і вразливостей, процес оцінки враховує пом'якшення наслідків за допомогою запланованих або наявних заходів безпеки. Оцінка ризиків кібербезпеки є лише частиною управління ризиками кібербезпеки, яка також включає дії з визначення ризику, реагування та моніторингу. Оцінка ризиків кібербезпеки зосереджена саме на ризиках кібербезпеки або втраті конфіденційності, цілісності або доступності інформації, даних або інформаційних систем, які існують у кіберпросторі або періодично присутні в ньому. Ризики кібербезпеки є підгрупою технологічних ризиків.

Основною метою оцінки ризиків у сфері кібербезпеки є захист цифрових активів держави та приватних структур шляхом виявлення вразливостей і впровадження відповідних заходів безпеки. Структура оцінки ризиків кібербезпеки забезпечує структурований підхід до проведення оцінки ризиків. Оскільки ризики кібербезпеки розвиваються, організації повинні постійно контролювати та оновлювати свої методики проведення оцінки ризиків. Це передбачає переоцінку загроз, уразливостей і засобів контролю безпеки з урахуванням зміни ІТ-середовища. Чинники та фактори, які доцільно враховувати під час проведення оцінки кіберризиків, включають: характер та масштаби уразливості комп'ютерних систем та даних організації; узагальнення наслідків успішної кібератаки на інформаційні системи; пошук оптимальних шляхів запобігання та протидії кіберзагрозам. Враховуючи актуальність та необхідність проведення комплексної оцінки управління ризиками кібербезпеки, набуває актуальності питання розробки та запровадження методологічної ідентифікації і оцінки кіберризиків на національному рівні, особливо для України в умовах правового режиму воєнного стану.

Результати аналізу наукових публікацій. Методи комплексної оцінки ризиків кібербезпеки досліджували у своїх працях: Д. Палко та Л. Мирутенко [2], С. Гаврик, А.Шишацький, О. Сова, О. Троцько, Г. Ляшенко, С. Паламарчук [3]. Міжнародні стандарти оцінки кіберстійкості вивчали: О. Федієнко [4] та О. Панченко [5]. Оцінка стану кібербезпеки критичної інформаційної інфраструктури та її особливості перебували у фокусі уваги: І. Ткаченка, В. Козачка, С. Гахова та В. Дмітрієва [6], А.Положенцева та В. Сидоренка [7] та інших. Дослідження умов проведення оцінки ризиків кібербезпеки в інформаційних системах державного управління здійснювали Є. Живило та Д. Шевченко [8]. Проте жоден із вказаних фахівців не здійснював розгляд актуальних питань правового забезпечення методики ідентифікації та оцінки кіберризиків на національному рівні через призму законодавства окремих країн ЄС (Словаччини та Литви).

Метою статті є узагальнення кращих європейських практик і висвітлення правових засад впровадження методики здійснення оцінки кіберризиків, визначення подальших шляхів удосконалення національної системи кібербезпеки через призму впровадження ризик-орієнтованого підходу щодо практичної реалізації заходів з метою забезпечення кібербезпеки об'єктів критичної інфраструктури та державних органів.

Виклад основного матеріалу. Пункт 16 Плану заходів на 2025 рік з реалізації Стратегії кібербезпеки України, затвердженого розпорядженням Кабінету Міністрів України від 07.03.2025 року №204 [9], визначає, що важливим завданням держави залишається розроблення методики ідентифікації та оцінки кіберризиків на національному рівні, забезпечення нормативного врегулювання питань щодо

впровадження обов'язкового проведення періодичної оцінки кіберризиків на підставі розроблених методик.

Аналогічна вимога зафіксована у п.42 Плану реалізації Стратегії кібербезпеки України, затвердженого рішенням РНБО України від 30.12.2021 року "Про План реалізації Стратегії кібербезпеки України", уведеного в дію Указом Президента України від 01.02.2022 року №37/2022 [10]. Ця вимога обгрунтована тим, що Україна розробляє та реалізує дієві заходи з метою створення системи національної кіберготовності в інтересах забезпечення економічного добробуту та захисту прав і свобод кожного громадянина України, особливо в умовах правового режиму воєнного стану. За таких умов наша держава має суттєво посилити національну кіберготовність, яка полягатиме у здатності усіх суб'єктів сектору безпеки і оборони своєчасно й ефективно реагувати на кібератаки, забезпечувати режим постійної готовності до реальних та потенційних кіберзагроз, виявляти та усувати передумови до їх виникнення, забезпечивши тим самим кіберстійкість, передусім об'єктів критичної інформаційної інфраструктури, що потребує створення національної системи управління інцидентами.

На цьому фоні перший важливий крок на державному рівні зумовлював затвердження на підставі наказу Адміністрації Держспецзв'язку України від 14.01.2025 року №17 [11] Методики та критеріїв і показників оцінки стану захищенності об'єктів критичної інфраструктури. Відповідна методика спрямована на реалізацію заходів з метою визначення стану захищеності об'єктів критичної інфраструктури, а також заходів для забезпечення захисту, безпеки та стійкості критичної інфраструктури.

Кабінет Міністрів України своєю постановою "Про затвердження вимог щодо управління ризиками безпеки на об'єктах критичної інфраструктури І категорії критичності" від 01.04.2025 р. № 367 [12] визначив та унормував комплекс заходів, спрямованих на ефективне зниження і посилення контролю за ризиками безпеки, зниження ризиків реалізації можливих кіберзагроз, ліквідацію та мінімізацію наслідків реалізованих загроз, кризових ситуацій тощо. Дія цієї постанови поширюється на об'єкти критичної інфраструктури (ОКІ) І категорії критичності – особливо важливі об'єкти, які мають загальнодержавне значення, значний вплив на інші об'єкти критичної інфраструктури та потенційне порушення функціонування яких призведе до виникнення кризової ситуації державного значення. Ця постанова визначає, що оператор критичної інфраструктури (КІ) здійснює управління ризиками безпеки шляхом створення системи управління ризиками безпеки, яка повинна відповідати визначеним принципам, таким як інтегрованість, структурованість і комплексність, індивідуальність тощо. Нормативно визначено, що до основних кіберризиків відносяться: матеріальні кіберризики – ризики настання інциденту як для ОКІ, так і для його критичних елементів, що можуть призвести до заподіяння їм шкоди, а також шкоди життю та здоров'ю людей; ризики кібербезпеки та захисту інформації – ризики щодо забезпечення безпеки, функціональності, безперервності роботи, відновлюваності, цілісності і стійкості інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, електронних комунікаційних мереж; ризики людського фактору – ризики порушення штатного режиму функціонування об'єкта критичної інфраструктури, безпосередньо пов'язані з працівниками ОКІ, іншими особами, які перебувають на об'єкті, що можуть призвести до виникнення інциденту, порушення виконання життєво важливих функцій, надання послуг тощо. Одночасно цим нормативно-правовим актом затверджено вимоги як до операторів критичної інфраструктури, так і безпосередньо до їхніх окремих структурних підрозділів або працівників, відповідальних за організацію захисту критичної інфраструктури. Зокрема, на оператора КІ покладаються обов'язки

розробляти та затверджувати документи (правила, політики тощо) щодо управління ризиками безпеки; забезпечувати підрозділи необхідними ресурсами; забезпечувати складення профілю ризиків безпеки ОКІ, розроблення проєктних загроз об'єктового рівня та інші. У свою чергу, структурні підрозділи забезпечують: своєчасне виявлення та оцінювання ризиків безпеки; організацію заходів, спрямованих на запобігання ризикам безпеки чи їх мінімізацію; моніторинг і контроль за ризиками безпеки та перегляд їхньої актуальності; обмін інформацією та взаємодію із суб'єктами національної системи захисту критичної інфраструктури; підготовку звітної та аналітичної інформації, інформування керівника ОКІ щодо ризиків безпеки та виконання інших завдань.

Враховуючи викладене, доцільним є висвітлення кращих практик зарубіжного досвіду на прикладі таких держав як Словаччина та Латвія, в контексті розроблення та впровадження національних методик ідентифікації та оцінки кіберризиків з метою запозичення європейського досвіду у цьому контексті.

Словаччина. Основним актом законодавства, який регламентує кібербезпекову сферу, є закон Словаччини "Про кібербезпеку" від 30 січня 2018 року [13]. Відповідно до його норм та положень кібербезпека розглядається як стан, в якому мережі та інформаційні системи здатні протистояти, з певним ступенем надійності, будь-яким діям та загрозам, які посягають на доступність, автентичність, цілісність або конфіденційність збережених, переданих або оброблених даних, доступ до яких здійснюється через ці мережі та інформаційні системи. Одночасно на рівні словацького законодавства кіберризик являє собою рівень кіберзагрози, виражений ймовірністю виникнення небажаної події та її негативних наслідків. З метою подолання кіберінцидентів, кіберризиків та кіберзагроз в Словаччині запроваджена єдина інформаційна система кібербезпеки, яка включає центральну систему раннього попередження. Єдина інформаційна система кібербезпеки – це інформаційна система, яка слугує задля ефективного управління, координації, обліку та контролю діяльності органів державного управління у сфері забезпечення кібербезпеки та підрозділів CSIRT. Єдина інформаційна система кібербезпеки також призначена для обробки та проведення оцінки даних та інформації про стан кібербезпеки та служить для кризового планування в мирний час, а також для проведення необхідних заходів під час запровадження воєнного стану.

Національна стратегія кібербезпеки на 2021-2025 роки, схвалена на підставі постанови Уряду Словаччини №5/2021 від 7 січня 2021 року [14], є базовим стратегічним документом, який регламентує порядок, умови та особливості забезпечення кібербезпеки у цій країні ЄС. Національна стратегія кібербезпеки є базовим стратегічним документом, який комплексно визначає стратегічний підхід Словаччини до забезпечення кібербезпеки. Частиною національної стратегії кібербезпеки є План дій з реалізації положень стратегії. Згідно положень стратегії, управління ризиками кібербезпеки є процесом, який мінімізує кіберризики на всіх етапах, починаючи від підготовки, проектування архітектури кібербезпеки, встановлення умов експлуатації та обслуговування складових кібербезпеки. Нормативно встановлено, що управління кібербезпекою має бути природною частиною управління інформаційними системами на загальнодержавному рівні. Кібербезпека являє собою складну систему, яка включає не лише нормативно-правове регулювання, але й практичну діяльність, таку як: управління кіберризиками, прогнозування та аналіз кіберризиків, виявлення кіберінцидентів, відновлення систем, кіберосвіта, розробка інструментів і механізмів управління кібербезпекою.

На підставі положень Стратегії кібербезпеки та закону “Про кібербезпеку” Словаччини була розроблена та затверджена Методологія аналізу ризиків кібербезпеки [15]. Відповідно до цього програмного документу, процес управління кіберризиками складається з циклічних та взаємопов’язаних процесів, зокрема включає: встановлення контексту кіберризику; проведення оцінки кіберризику; моніторинг та уточнення кіберризику. Оцінка кіберризиків являє собою комплексний процес, який складається з таких стадій: виявлення ризиків, аналіз ризиків, оцінювання ризиків. При цьому, для спрощення термінології замість терміну “оцінка ризиків” використовується лише узагальнюючий термін “аналіз ризиків”. Методологія стратегічного аналізу кіберризиків включає три різні взаємопов’язані підходи до такого аналізу з різними перевагами та складністю: 1) підхід, орієнтований виключно на кіберзагрози – передбачає визначення джерел кіберзагроз, завдяки якому розробляються ймовірні сценарії та аналізуються сучасні моделі кіберзагроз; 2) підхід, орієнтований на визначення поточного стану захищенності об’єктів критичної інформаційної інфраструктури, завдяки якому проводиться аналіз за наслідками кіберзагроз; 3) підхід, орієнтований на виявлення та деталізацію кібервразливостей.

На рівні словацького законодавства нормативно задекларовано, що існує два напрямки подолання кіберризиків, а саме: зменшення та уникнення. Так, зменшення кіберризиків є найпоширенішим методом, оскільки досягається шляхом вжиття відповідних заходів з метою мінімізації негативних наслідків або ліквідації будь-якої ймовірності реалізації сценарію кіберризику. У свою чергу, уникнення ризиків здійснюється у випадку, коли виявлений кіберризик вважається занадто високим або витрати на його обробку перевищують витрати захисту. Найпоширеніший спосіб уникнути ризику – це зміна кіберсередовища, в якому виникає той чи інший ризик. Ця зміна спрямована на те, щоб цей ризик не був варіантом (наприклад, у разі загрози конфіденційності даних під час їх передачі через ненадійний канал зв’язку, використовується інший канал). Відповідно до загальних принципів цієї методології, ризики слід розглядати в порядку від найвищого до найнижчого, а саме тому заходи безпеки повинні вживатися залежно від визначеного рівня кіберризику.

Важливим аспектом визначено процес проектування кібербезпеки, що включає сукупність заходів, спрямованих на потенційне зниження будь-яких кіберризиків. При цьому ці заходи поділяються на оперативні та системні. Оперативні заходи – це заходи, впровадження яких не вимагає багато часу та фінансових ресурсів, але їхня реалізація має моментальний позитивний ефект, що передбачає зниження негативного кіберризику. Системні заходи – це більш масштабні організаційно-технічні заходи з довгостроковим впливом на зниження кіберризику. Послідовність, у якій будуть реалізовані запропоновані заходи (так званий план впровадження) розробляється в рамках практичної реалізації базових положень стратегії кібербезпеки та залежить від таких факторів, які необхідно враховувати під час її розробки. Важливою є пріоритетність, що випливає з поточної та перспективної оцінки кіберризиків, наявних обсягів фінансових ресурсів та витрат, необхідних для впровадження відповідних заходів. Заслуговує на увагу оперативна кіберготовність та можливості впроваджувати такі заходи (технічні, організаційні, фінансові) тощо. Розділ 8 вказаної методології регламентує комплексне питання залишкового кіберризику, який являє собою ризик, значення якого настільки нівельовано, що є прийнятним для організації та відсутня нагальна потреба застосовувати подальші заходи для його зниження або ліквідації.

Латвія. Стратегія кібербезпеки Латвії на 2023-2026 роки [16], розроблена Міністерством оборони, визначає ключові напрямки розвитку національної політики

кібербезпеки, декларує майбутні виклики та загрози у кібердомені. Метою національної політики кібербезпеки, розробленої Міністерством оборони на період до 2026 року, визначено посилення безпеки кіберпростору шляхом розвитку можливостей та спроможностей у сфері кіберзахисту, підвищення кіберстійкості проти кібератак, сприяння обізнаності громадськості про реальні та потенційні загрози в кіберпросторі. Основними напрямами щодо розбудови кібербезпеки відповідно до стратегії визначено: удосконалення управління кібербезпекою, посилення кіберстійкості, інформування громадськості про загрози та виклики у кібердомені, міжнародне співробітництво у сфері забезпечення кібербезпеки, запобігання та боротьба з кіберзлочинністю, у тому числі й з міжнародною. Стратегія кібербезпеки Латвії була розроблена на вимогу адаптації цифрового законодавства Європейського Союзу, а також з урахуванням національних тенденцій, концептів та особливостей сучасного ІТ-розвитку, включених до стратегічних документів щодо планування та розбудови національної цифрової політики з метою забезпечення узгодженого розвитку кібербезпеки Латвії.

Національний план розвитку Латвії на 2021-2027 роки, затверджений Сеймом від 02.07.2020 року [17], регламентує, що на загальнодержавному рівні має бути запроваджена запланована процедура проведення оцінки відповідності усіх державних інформаційних систем визначеному рівню безпеки на етапі планування та розробки. Таким чином, міністерство оборони Латвії має забезпечити впровадження вимог, що відповідають заданому рівню безпеки, до усіх інформаційних та інформаційно-комунікаційних систем. Іншими словами, заплановано проведення комплексної оцінки ризиків кібербезпеки для кожної електронної послуги та щодо усіх об’єктів критичної інфраструктури. Розпорядженням Кабінету Міністрів Латвії від 7 липня 2021 року № 490, були затверджені рекомендації цифрової трансформації 2021-2027 роки [18]. В контексті аналізу цих рекомендацій важливе місце посідають питання політики цифрової безпеки (розділ 4.2.1). Органи державного управління та приватний сектор мають на постійній основі розвивати стійкість до кіберзагроз і вдосконалювати її у відповідь на нові технологічні можливості. Державні адміністрації та приватний сектор співпрацюють не лише у розробці політики кібербезпеки та виявленні та запобіганні інцидентам безпеки, але й у забезпеченні безперервності ІКТ-рішень, важливих для національної економіки в кризових ситуаціях.

У Латвії у сфері цифрової безпеки реалізується загальнодержавний підхід, у якому всі установи та організації державного сектору беруть активну участь у розробці та реалізації політики цифрової безпеки. Нормативно встановлено, що аналіз ризиків цифрової безпеки має здійснюватися на початковому етапі створення кожного цифрового рішення, а безпека має контролюватися протягом усього життєвого циклу. При цьому вагоме місце у цих процесах відводиться саме розробці та запровадженню методики ідентифікації та оцінки кіберризиків на загальнодержавному рівні. У Латвії використовуються різні методології для виявлення потенційних кіберризиків, включаючи сканування вразливостей, тестування на проникнення та аналіз кіберзагроз тощо. Використання цих інструментів може значно покращити та сприяти розумінню змісту та природи кіберризиків, надає сприятливі можливості щодо розробки планових кібербезпекових стратегій. За законодавством, першочергово оцінка кіберризиків спрямована на виявлення потенційних кіберзагроз та вразливостей, та у подальшому – на перспективну розробку плану щодо зниження цих ризиків та їхніх негативних наслідків. Однією із ключових переваг використання інструментів аналізу кіберризиків є те, що вони можуть допомогти сектору безпеки і оборони, державним та приватним організаціям розставити пріоритети у своїх інвестиціях в кібербезпеку, визначити слабкі

місця та вірогідні вразливості. Виявляючи найбільш критичні вразливості та кіберризики, можливий ефективний розподіл ресурсів та визначення успішного алгоритму ліквідації кіберзагроз.

Оцінка кіберризиків спрямована на надання пріоритетного списку ризиків у порядку ранжиру, таким чином це надає змогу розподілити ресурси таким чином, щоб якнайкраще організувати захист найважливіших систем. Адже існує безліч різних методів розрахунку ризику, але всі вони, як правило, ґрунтуються на таких факторах, як: виявлення та оцінка кіберзагроз; оцінка вразливості; предметна оцінка кожної загрози-вразливості. Загрози можуть виходити із внутрішніх або зовнішніх джерел і бути навмисними (наприклад, кібератаки) або випадковими. Оптимальним методом оцінки загроз є метод експертних оцінок, у якому експертам пропонується оцінити можливість реалізації певного переліку загроз. Після оцінки загроз необхідно оцінити вразливості – це слабкі місця в системі безпеки, якими можуть скористатися зловмисники або хакери. Вразливість системи – це причини та передумови, які призводять до порушення безпеки системи та її функціонування чи безпеки інформації, що у ній обробляється. У якості критеріїв оцінки небезпеки вразливості можна визначити: фатальність наявності в системі вразливості, доступність вразливості для джерел загроз, а також кількість вразливостей певного типу для системи або частота їх появи. Виявлення та усунення вразливостей важливі для зниження ризику, особливо найбільш критичні з них. Нарешті, як тільки вся відповідна інформація зібрана, її необхідно узагальнити в кількісну оцінку кожної пари “загроза-вразливість”. У подальшому ця оцінка може бути використана для визначення пріоритетності ризиків та загроз. Для оцінки ризиків кібербезпеки інформаційно-комунікаційних систем необхідно насамперед виділяти її активи. Сукупність активів інформаційно-комунікаційних систем – усі засоби та технічні рішення, які необхідні для її штатного функціонування і які знаходяться в її розпорядженні (апаратні засоби, програмне забезпечення, службова інформація, що зберігається тощо). Процес оцінки кіберризиків для кожного з активів повинен враховувати вартість самого активу та характеристику можливостей порушення його штатного функціонування (роботи). При цьому важливо враховувати, як усі види кіберзагроз, так і усю сукупність уразливостей, які є взаємопов’язаними в контексті здійснення оцінки кіберризиків. В реальних умовах одна і та ж загроза для інформаційно-комунікаційних систем може реалізуватися через декілька вразливостей. Саме виявлення вразливостей в технічних та організаційних контролях є важливим та актуальним завданням, яке у свою чергу, впливає на конфіденційність, цілісність та доступність продуктів інформаційних технологій (наприклад, систем, обладнання, програмного забезпечення та послуг). За статистичними даними у 2023 році в Латвії було зафіксовано 2378 кіберінцидентів, найбільша кількість з яких мала місце в інфраструктурі хостінг-провайдерів, секторі державного управління та об’єктах критичної інфраструктури [19].

На рівні законодавства Латвії активно використовується факторний аналіз кіберризиків під назвою “FAIR”. Методика FAIR забезпечує структурований спосіб оцінки та кількісної оцінки кіберризиків шляхом аналізу впливу та ймовірності потенційних загроз. На відміну від інших методик, “FAIR” використовує ймовірнісний підхід, при цьому визнаючи випадковість даних для більш точного аналізу кіберризиків. Він зосереджений на критично важливих активах і ймовірних сценаріях кіберризику, що дозволяє здійснювати оцінку фінансових наслідків та визначати пріоритетність заходів у сфері забезпечення кібербезпеки. Ця модель передбачає прийняття обґрунтованих управлінських рішень, перекладаючи складні кіберризики на чіткі фінансові умови.

Методика “FAIR” кількісно визначає ризик кібербезпеки, розбиваючи його на окремі фактори за допомогою статистичного аналізу та теорії ймовірностей. Оцінка кіберризику відбувається за допомогою розроблених сценаріїв, з урахуванням частоти подій збитків (частота збитків) і потенційного впливу цих збитків (величина збитків). Поєднуючи ці компоненти, методика “FAIR” забезпечує комплексне та кількісне розуміння ризику в грошовому еквіваленті, що дозволяє організаціям приймати обґрунтовані рішення щодо заходів безпеки на основі здобутих даних. Методика “FAIR” прив’язує частоту та величину потенційних збитків до конкретних активів в тієї чи іншої організації або державного органу. Ідентифікація та оцінка цих активів має вирішальне значення для визначення та вимірювання кіберризику. Інвестицією може бути будь-який пристрій, дані або компонент із внутрішньою вартістю, які можуть бути втрачені. Таким чином, методика “FAIR” поділяє ризик на кілька компонентів, включаючи частоту подій кіберзагроз, вразливість і величину завданих збитків. Основна концепція FAIR полягає в тому, щоб обчислити ймовірні фінансові втрати, що допомагає державі та її уповноваженим органам детально зрозуміти потенційний економічний вплив від кіберзагроз. Це полегшує передачу інформації про ризики зацікавленим сторонам і визначає пріоритетність стратегій пом’якшення. “FAIR” надає комплексну структуру для оцінки та кількісного визначення кіберризиків, пропонуючи численні переваги для державних органів та організацій, які прагнуть зміцнити свою позицію в галузі кібербезпеки та приймати обґрунтовані бізнес-рішення. Зосереджуючись на фінансовій кількісній оцінці, “FAIR” надає змогу здійснювати оцінку впливу окремих подій-загроз або сукупних кіберризиків за кількома сценаріями, забезпечуючи глибше розуміння того, як ці загрози можуть мати вплив на зацікавлені сторони. По суті, ця здатність переводити складні сценарії ризиків у грошові вирази може бути корисною для державних органів або організацій, які прагнуть визначити пріоритетність інвестицій у кібербезпеку. У сучасному нормативному середовищі демонстрація повного розуміння кіберризиків і вжитих заходів для їх пом’якшення є надзвичайно важливою для відповідності. Методика “FAIR” сприяє дотриманню нормативних вимог, надаючи структурований метод оцінки та документування кіберризиків.

Паралельно застосовується методика OCTAVE (оцінка критичної загрози, активів і вразливості). Таким чином, OCTAVE — це методологія оцінки ризиків, яка акцентує увагу на організаційному контексті, який включає три етапи: створення профілів кіберзагроз на основі активів, виявлення вразливостей критичної інфраструктури та розробка стратегій і планів кібербезпеки. Оцінки ризику виводяться на основі аналізу кіберзагроз, вразливостей і вірогідності впливу на критичні активи. Особливість цієї методики полягає в тому, що увесь процес аналізу проводиться силами співробітників організації, без залучення зовнішніх консультантів. Для цього створюється змішана група, що включає як технічних фахівців, так і керівників різного рівня, що дозволяє всебічно оцінити наслідки для бізнесу можливих інцидентів в області безпеки і розробити контрзаходи.

Оскільки цифровий ландшафт кіберзагроз динамічно розвивається і змінюється, це потребує удосконалення методології та інструментів здійснення оцінки кіберризиків. Нові тенденції провокують періодичний перегляд методики оцінки кіберризиків на національному рівні та включають удосконалені алгоритми та інтеграцію штучного інтелекту й машинного навчання в моделі оцінки ризиків, щоб забезпечити більш точні та динамічні оцінки. Ці технології можуть аналізувати величезні обсяги даних у режимі реального часу, визначаючи закономірності та прогнозуючи потенційні загрози

ефективніше, ніж традиційні методи. Окрім того, важливим є моніторинг ризиків у реальному часі: перехід до постійного моніторингу та оцінки ризиків у реальному часі дозволяє організаціям оперативно реагувати на нові загрози, у зв'язку з чим цей проактивний підхід підвищує здатність організації зменшувати ризики до того, як вони матеріалізуються у значні проблеми. Людський фактор також є важливим під час проведення оцінки кіберризиків, таких як поведінка співробітників і внутрішні загрози, забезпечує більш повне уявлення про організаційний ризик. Розуміння людського фактора може допомогти в розробці цільових програм навчання та підвищення обізнаності для зменшення цих ризиків.

Висновки. Узагальнюючи кращі практики позитивного досвіду Словаччини та Латвії, можна констатувати, що першочерговим та важливим кроком під час проведення оцінки ризиків кібербезпеки є визначення систем та даних, які потребують захисту. У зв'язку з цим необхідно визначити загрози, які потенційно можуть завдати шкоди цим системам та даним. Останнім кроком є розробка плану зниження цих ризиків. Це може включати впровадження таких заходів безпеки як: брандмауери, антивірусне програмне забезпечення або резервне копіювання. Це також може передбачати навчання співробітників захисту від онлайн-загроз або розробку політик для боротьби з несанкціонованими витоками даних.

Оцінка ризиків кібербезпеки допомогає краще розуміти вразливість систем до кібератак, а також розставити пріоритети у витратах на забезпечення безпеки. Виявляючи конкретні загрози та здійснюючи кроки щодо їх усунення, проведення оцінки сприяє зниженню загального рівня кіберризику та надає змогу налагодити кіберзахист від будь-яких витоків даних. Також оцінка кіберризиків спрямована на виявлення вразливостей та розробку рекомендаційних рішень задля їхнього зниження або усунення. Фактори, які доцільно враховувати під час проведення оцінки кіберризиків, включають: характер та кількість комп'ютерних систем та даних; види та профіль кіберзагроз; вразливість тієї чи іншої системи до кібератак; аналіз за наслідками кібератаки на систему. Одночасно важливим в контексті здійснення оцінки ризиків кібербезпеки є проведення рейтингу кіберризиків, що надає можливість якісно оцінити та кількісно визначати той чи інший ризик або його ознаки.

За таких умов важливою складовою забезпечення кібербезпеки є методологічне забезпечення проведення оцінки кіберризиків на національному рівні. Загалом оцінка кіберризиків – це процес вивчення результатів застосування заходів з кіберзахисту систем, об'єктів критичної інформаційної інфраструктури, державних інформаційних ресурсів з метою визначення стану захищеності таких об'єктів та проведення огляду та ефективності вжитих у цій площині заходів. Оцінка кіберризиків – це процес виявлення, кількісної оцінки та управління ризиками, які можуть загрожувати системам та інформаційно-комунікаційним технологіям. Інструменти аналізу кіберризиків покликані допомогти реально оцінити поточний стан кібербезпеки, виявити вразливості, які можуть використовувати зловмисники, хакери або кіберзлочинці.

Узагальнюючи викладене, можна констатувати, що кожна країна ЄС обирає власну методику ідентифікації та оцінки кіберризиків на національному рівні. Так, наприклад, у Словаччині та Латвії отримали поширення на загальнодержавному рівні методики "FAIR" та "OCTAVE", які активно використовуються в діяльності державних органів та у приватному секторі. На виконання п.16 Плану заходів на 2025 рік з реалізації Стратегії кібербезпеки України, наприкінці цього року має бути розроблена та затверджена методика ідентифікації та оцінки кіберризиків на національному рівні, а на урядовому рівні — нормативно врегульовані питання впровадження обов'язковості проведення

періодичної оцінки кіберризиків, що є важливим та стратегічним завданням держави в контексті посилення та розбудови національної системи забезпечення кібербезпеки.

Використана література

1. Global Cybersecurity Outlook 2025. URL: https://www.weforum.org/publications/global-cybersecurity-outlook-2025/digest/

2. Палко Д.В., Мирутенко Л.В. Метод комплексної оцінки ризиків кібербезпеки в розподілених інформаційних системах. *Кібербезпека: освіта, наука, техніка.* 2024. № 2(26). С. 487-502.

3. Гаврик С., Шишацький А., Сова О., Троцько О., Ляшенко Г., Паламарчук С., Нерознак Є., Величко В. Методика оцінювання кібербезпекив інформаційно-телекомунікаційній системі спеціального призначення. *Системи управління, навігації та зв'язку.* 2020. Том 4. № 62. С. 109-114.

4. Федієнко О.П. Міжнародні стандарти оцінки кіберстійкості. *Інформація і право.* 2024. №3 (50). С. 124-135.

5. Панченко О.А. Актуальні питання оцінювання ризиків кіберзагроз: аналіз зарубіжного досвіду. *Інформація і право.* 2021. №4(39). С. 106-112.

6. Ткаченко І.В., Козачок В.А., Гахов С.О., Дмітрієв В.Є. Оцінка стану кібербезпеки критичної інформаційної інфраструктури в ході виявлення та відслідковування кризових індикаторів. *Сучасний захист інформації.* 2020. №1. С.54-57.

7. Положенцев А., Сидоренко В. Метод визначення рівня кібербезпеки об'єктів критичної інфраструктури держави. *Матеріали XVIII міжнар. наук.-практ. конф. молодих учених і студентів «ПОЛІТ-2018. Сучасні проблеми науки»,* м. Київ, 4-6 квітня 2018 р., С. 102-103.

8. Живило Є.О., Шевченко Д.Г. Оцінка ризиків кібербезпеки та конторолю конфіденційності в інформаційних системах державного управління. *Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка.* 2020. № 75. С. 66-77.

9. Про затвердження плану заходів на 2025 рік з реалізації Стратегії кібербезпеки України: Розпорядження Кабінету Міністрів України від 07.03.2025 року №204-р. URL: https://zakon.rada.gov.ua/laws/show/204-2025-р#Text.

10. Про рішення Ради національної безпеки і оборони України від 30 грудня 2021 року «Про План реалізації Стратегії кібербезпеки України»: Указ Президента України від 01 лютого 2022 року № 37/2022. URL: https://www.president.gov.ua/documents/372022-41289.

11. Про затвердження Методики та Критеріїв і показників оцінки стану захищеності об'єктів критичної інфраструктури: наказ Адміністрації Держспецзв'язку України від 14.01.2025 року №17. URL: https://zakon.rada.gov.ua/laws/show/z0375-25#Text.

12. Про затвердження вимог щодо управління ризиками безпеки на об'єктах критичної інфраструктури I категорії критичності: Постанова Кабінету Міністрів України від 01.04.2025 року № 367. URL: https://zakon.rada.gov.ua/laws/show/367-2025-п#Text.

13. *Zákon č. 69/2018 Z.z o kybernetickej bezpečnosti* 30.01.2018. URL: https://static.slov-lex.sk/static/SK/ZZ/2018/69/vyhlasene_znenie.html.

14. Slovakia - National Cybersecurity Strategy 2021-2025. URL: https://digital-skills-jobs.europa.eu/en/actions/national-initiatives/national-strategies/slovakia-national-cybersecurity-strategy-2021-2025.

15. Metodika analýzy rizík kybernetickej bezpečnosti 13.12.2021. URL: https://www.studocu.com/row/document/slovenska-technicka-univerzita-v-bratislave/bezpecnost/metodika-analyza-rizik-v1/66427889.

16. The Cybersecurity Strategy of Latvia 2023-2026 of 28.03.2023. URL: https://digital-skills-jobs.europa.eu/en/actions/national-initiatives/national-strategies/latvia-cybersecurity-strategy-2023-2026.

17. The announcement of the Saeima of July 2, 2020 «On the National Development Plan for Latvia 2021-2027». URL: https://www.mk.gov.lv/en/media/15165/download?attachment.

18. Par Digitālās transformācijas pamatnostādnēm 2021.-2027. 07.07.2021. № 490 URL: https://likumi.lv/ta/id/324715-par-digitalas-transformacijas-pamatnostadnem-20212027-gadam.

19. Overview of the cybersecurity status in Lithuania: Key information 2023. URL: https://kam.lt/wp-content/uploads/2024/06/KS-ataskaitos-2023-Santrauka-EN_final.pdf.

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