УДК 006.013

к.н.держ.упр. **Живило Є.О.** (НУОУ)
к.військ.н. **Шевченко Д.Г.** (НУОУ)

DOI: https://doi.org/10.17721/2519-481X/2022/75-07

ОЦІНКА РИЗИКІВ КІБЕРБЕЗПЕКИ ТА КОНТРОЛЮ КОНФІДЕНЦІЙНОСТІ В ІНФОРМАЦІЙНИХ СИСТЕМАХ ДЕРЖАВНОГО УПРАВЛІННЯ

***Актуальність** данної роботи обумовлена затвердженням Адміністрацією Державної служби спеціального зв'язку та захисту інформації України "Методичних рекомендацій щодо підвищення рівня кіберзахисту критичної інформаційної інфрасируктури" у жовтні 2021 року. Рекомендації було розроблено на основі найкращих світових підходів – NIST CyberSecurity Framework. Наразі розроблені Рекомендації Держспецзв'язку частково втратили свою актуальність та потребують корегування з виходом NIST Special Publication 800-53A Revision 5 "Assessing Security and Privacy Controls in Information Systems and Organizations" та NISTIR 8286C (Draft) "Staging Cybersecurity Risks for Enterprise Risk Management and Governance Oversight", дата публікації: січень 2022 року. Ці документи завершують цикл інтеграції управління ризиками кібербезпеки (CSRM) та управління ризиками підприємства (ERM).*

***Зазначені** проєкти описують методи поєднання інформації про ризики усих активів системи, мережі організації (підприємства) включаючи умовні приклади для агрегування та нормалізації результатів з реєстрів ризиків кібербезпеки (CSRR) з урахуванням параметрів ризику, критеріїв та впливу на стале функціонування комунікаційних систем. В результаті інтеграція та нормалізація інформації про ризики дають змогу приймати рішення та здійснити моніторинг ризиків на всих рівнях системи, що допомагає створити вичерпну картину загального кіберризику. У наведених документах описано створення профілю ризиків організації (ERP), який підтримує порівняння та управління кіберризиками разом з іншими типами ризиків в цілому. Доволі цікавими є погляди авторів розроблених документів, щодо контролю конфіденційності, пов'язаного із системами та їх середовищем розповсюдження, їх функціонуванням. Обгрунтовано, що якісна системна оцінка допомагає визначити наявну дійсність засобів контролю, що містяться в організації відповідно до плану безпеки та конфіденційності, які згодом використовуються в організаційно-штатних системах та середовищі експлуатації. За цих умов, контроль оцінки є вказівкою з виконання конкретних кроків у структурі управління ризиками який цілодобово сприяє ефективному підходу до процесів сталого управління ризиками шляхом виявлення слабких місць, або недоліків в системах, що дозволяє організації визначати порядок реагування на ті, чи інші кіберзагрози.*

***Отже,** для вирішення завдань, з врегулювання та імплементації норм та правил міжнародних організацій сфери кібербезпеки та кібероборони пропонується провести аналіз викладених документів та висунити відповідні пропозиції, щодо корегування та доповнення раніше затверджених Держпецзв'язку "Методичних рекомендацій…". В свою чергу це дозволить не лише забезпечити захист критичної інформаційної інфраструктури держави від кібератак, а й провести превентивні наступальні операції у кіберпросторі, що включає виведення з ладу критично важливих об'єктів інфраструктури противника шляхом руйнування комунікаційних систем, які управляють такими об'єктами.*

***Ключові слова:** кіберпростір, кібербезпека, кіберзагрози, управління ризиками кібербезпеки, оцінка ризиків кібербезпеки, реєстр ризиків кібербезпеки, комунікаційні системи, нормативно-правовий акт, об'єкт критичної інформаційної інфраструктури.*

Вступ та постановка задачі чи проблеми. Відповідно до Закону України "Про основні засади забезпечення кібербезпеки України", "Загальних вимог до кіберзахисту об'єктів критичної інфраструктури", затверджених постановою Кабінету Міністрів України від 19 червня 2019 року № 518 та безпосередньо вимог Наказу Адміністрації Держспецзв'язку від 06 жовтня 2021 року № 601 "Про затвердження Методичних рекомендацій щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури" визначено систему (таксономію) заходів кіберзахисту для досягнення конкретного цільового стану кібербезпеки

що вже впроваджені на об’єктах критичної інфраструктури організаціями в будь-яких секторах економіки [1].

Методичні рекомендації описують загальний підхід до забезпечення кібербезпеки, що дозволяє [2]:

здійснити аналіз та надати характеристику поточного стану кібербезпеки об’єкт критичної інформаційної інфраструктури (далі – ОКІІ);

описати цільовий стан кібербезпеки ОКІІ;

ідентифікувати та визначити пріоритети, рівень упровадження заходів кіберзахисту в контексті безперервного та повторюваного процесу управління ризиками у сфері кібербезпеки ОКІІ;

оцінити прогрес у досягненні цільового стану кібербезпеки ОКІІ;

забезпечити комунікацію між суб’єктами, які безпосередньо знаходяться на ОКІ, та із суб’єктами, які є партнерами організації щодо управління ризиками у сфері кібербезпеки.

З опублікуванням чергового релізу NIST Special Publication 800-53A Revision 5 та NISTIR 8286C (Draft) постає доволі суттєва проблема, щодо внесення змін та корегування існуючого нормативно-правового поля Адміністрацією Державної служби спеціального зв’язку та захисту інформації України щодо ефективності засобів контролю безпеки та конфіденційності, питань категоризації кібербезпеки, системи та оцінки ризику конфіденційності цих систем.

За цих умов, суб’єкти (власники) ОКІ держави мають змогу отримати: відповідні оцінки в режимі реального часу, на основі впроваджених політик безпеки та вимог, відомості про існуючі загрози та відповідні вразливості, час на оперативне реагування, змогу реконфігурувати систему або платформу на відмовостійкість в залежності до існуючого ризику.

Також, слід зазначити, що вдосконалення існуючого нормативно-правового поля, його формування та гнучке використання буде позитивно сприяти послідовному застосуванню заходів безпеки та конфіденційності в загальнодержавній структурі управління ризиками.

В подальшому це дозволить Національному координаційному центру кібербезпеки у взаємодії з іншими суб’єктами забезпечення кібербезпеки держави, мережею ситуаційних центрів органів державної влади (резервних, на рухомій базі) означити потенційні загрози та проблеми за категоріями:

- визначення слабких місць та недоліків, пов’язаних з безпекою та конфіденційністю в системі та в середовище, в якому працює система;
- концентрація пріоритету в прийнятті рішень щодо реагування на ризики та реалізації механізмів активного впливу на загрози в кібернетичному просторі;
- системний підхід в розгляді виявлених слабких місць та виявлених недоліків в експлуатаційному середовищі;
- моніторингова діяльність на ситуації які циркулюють в комунікаційному просторі щодо кібербезпеки та конфіденційність усвідомлення ситуації яка склалась;
- сприяння всім типам рішень щодо авторизації системи на одній платформі в режимі реального часу;
- складання середньострокових бюджетних рішень та перспективних планів на капітальні інвестиції.

Отже, удосконалення існуючої нормативно-правової бази, підготовка проектів нормативно-правових актів, нормативне врегулювання питань з реалізації заходів, що забезпечують оцінку ризиків кібербезпеки та контролю конфіденційності в інформаційних системах державного управління в її кінцевому результаті дозволять надавати, майже в режимі реального часу інформацію, пов’язану з безпекою та конфіденційністю посадових осіб установи, щодо поточного стану безпеки та конфіденційності їхніх систем та мереж.

Аналіз останніх досліджень. Сучасні підходи до оцінки ризиків інформаційних технологій (на підтримку впровадження галузевих стандартів інформаційної безпеки ГСТУ СУІБ 1.0/ISO/IES 27001:2010 та ГСТУ СУІБ 2.0/ISO/IES 27002:2010) змістовно представлені

для надання змоги організаціям узгодити свою систему управління інформаційною безпекою з відповідними вимогами системи управління або інтегрувати її в них. Ними передбачено використання процесійного підходу для розроблення, впровадження, забезпечення функціонування, моніторингу, аналізу, підтримання та поліпшення системи управління інформаційною безпекою, визначено порядок впровадження загальноприйнятих заходів інформаційної безпеки. Зазнчені документи імплементовані в Україні у відповідності до міжнародних нормативно-правових документів, вони є галузевими стандартами.

Також, методологія оцінки ІТ ризиків доволі змістовно описані Національним Інститутом стандартів та технологій США (National Institute of Standards and Technology – NIST). Зазначеними вище документами NIST та NISTIR визначається природа уразливості, ефективність існуючих заходів безпеки, методологія оцінки ризиків, методологія аналізу факторів ризиків інформаційних технологій, заходи з оцінки ризиків, вхідних та вихідних даних, ідентифікація загроз, ідентифікація уразливостей, аналіз заходів захисту та імовірність реалізації загроз [8]. При цьому, пріоритетними сферами, до яких NIST вносить поправки і на яких планує концентрувати свої зусилля є криптографія, освіта, новітні технології, управління ризиками, ідентифікація та управління доступом, вимірювання, конфіденційність, надійність мережі та стале функціонування платформ.

Аналіз існуючої нормативно-правової бази України щодо кіберзахисту державних інформаційних ресурсів свідчить про те, що уніфікація чималої кількості діючих керівних нормативно-правових документів та стандартів відбувається з урахуванням норм міжнародного права, галузевих стандартів та директив ЄС та НАТО, що зафіксовано у Законах та нормативно-правовій базі України [6, 5, 9]. Проведений змістовний аналіз існуючих Законів України та інших нормативно-правових актів України, ЄС, НАТО, провідних країн світу та зокрема США наведено в [4].

Детально розглядаючи питання щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури держави слід зауважити що в цьому напрямку переважаючими темпами рухається Адміністрація Державної служби спеціального зв’язку та захисту інформації України. При цьому, все ж таки домінуюча кількість документів сфер захисту в кіберпросторі державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом [3], кіберзахисту критичної інформаційної інфраструктури трансформована у відповідності до міжнародних та галузевих стандартів провідних країн світу.

Враховуючи зазначене вище, слід зауважити, що відповідні “Методичні рекомендації…”, розроблені Держпецзв’язку також не є виключенням. Вони були розроблені з урахуванням Настанови для підвищення кібербезпеки критичної інфраструктури (Framework for Improving Critical Infrastructure Cybersecurity, реліз 1), виданої у 2014 році та оновлені у вигляді релізу 2, у 2018 році Національним інститутом стандартів та технології Сполучених Штатів Америки [7].

Сьогодні членами NIST є понад 1300 фірм, більше 400 виробничих і торгових компаній, науково-технічних та інженерних товариств, персонал інституту становить 2900 штатних працівників, та 1800 асоційованих співробітників, представників американських компаній та закордонних спеціалістів. Людський потенціал Держпецзв’язку складає лише понад 10 тис. фахівців. Порівнюючи ці дві організаційні структури слід зазначити, що оперативно реагувати в відповідній ІТ динаміці на розробку та корегування нормативно-правової бази цей орган державної влади не має змоги.

Зважаючи на пророблену роботу Адміністрацією Держпецзв’язку, та враховуючи часткову втрату своєї актуальності і потребу в корегуванні документів інформаційного та рекомендаційного характеру з виходом NIST Special Publication 800-53A Revision 5 і NISTIR 8286C (Draft) вважається за необхідне в цій роботі зосередити увагу на вдосконаленні існуючого нормативно-правового поля по застосуванню заходів безпеки та конфіденційності в загальнодержавній структурі управління ризиками.

Виклад основного матеріалу. З початку повномасштабної агресії з боку Російської Федерації було оперативно виявлено та нейтралізовано понад 120 потужних кібератак на ресурси органів державної влади та військового управління України (за даними Microsoft, за останні місяці було проведено 237 кібератак з території Росії). Продовжується поширення дезінформації про війну в Україні. Активну роботу пов'язану з цим виявили у восьми соціальних мережах, зокрема у Telegram, Twitter, Facebook і TikTok та інших.

У відповідь Україна з 24 лютого змінила свою стратегію і стала не лише захищатись від російських кібератак, а й здійснювати кібератаки на ресурси Російської Федерації. За повідомленням віце-прем'єр-міністра - міністра цифрової трансформації України Михайла Федорова, Міністерство цифрової трансформації концентрувалося на постійному захисті від російських кібератак та на створенні продуктів та сервісів [10]. За його словами, вже зламано десятки баз даних Росії і персональні дані громадян викладено у відкритий доступ, також пошкоджено телекомунікаційну інфраструктуру та інфраструктуру багатьох державних реєстрів.

Слід зазначити, що напередодні повномаштабної агресії у ніч із 13-го на 14 лютого хакери зламали понад 70 урядових сайтів. Деструктивному кібервпливу протягом кількох годин підлягали вебресурси Міноборони, МЗС, ДСНС, «Дія». Завдяки оперативним діям наших фахівців вдалось зберегти контент сайтів та захистити дані відповідних користувачів. В цілому за останні місяці українські держоргани та банки вже пережили дві помітні кібератаки. Так, на початку травня противником було відновлено DDoS-атаки на урядові електроні ресурси та телекомунікаційне обладнання інших силових відомств. На складнощі з доступом до програм кілька годин скаржилися користувачі ПриватБанку, Ощадбанку, Monobank, А-Банку та Альфа-Банку. Атака тривала близько доби, її вартість коштувала Росії – мільйони доларів.

У цих умовах Національним центром оперативно-технічного управління мережами телекомунікацій здійснюється контроль над телеком-мережами держави. На базі Держспецзв'язку України спільно з Національним центром було проведено спеціальні навчання, під час яких основну увагу було зосереджено на відпрацюванні: процедур взаємодії операторів та держорганів; питань гнучкої та оперативної зміни архітектури маршрутизації мережі; порядку відновлення зв'язку у разі пошкодження регіональних (територіальних) вузлів зв'язку; порядку використання резервного обладнання та каналів передачі даних.

Тож зараз відкривається доволі серйозний напрямок супротиву між Києвом та Москвою на теренах співвдіношення обізнаних фахівців в "одиничках-нуликах". На кіберфронті зараз весь світ воює проти Росії, співвідношення 99 до 1, РФ взагалі немає союзників. Тобто на технічно-технологічному полі агресора за напрямком комунікаційні сервіси, технології та мережі відбувається "Death match", зазначене надає можливість будь-якій організації, установі, об'єднанню осіб відкритий коридор, щодо відточення своїх практичних навиків, іншими словами "зламати" можна все.

У Росії хакери відносяться в основному до силовиків, тобто ними керують ГРУ, ФСБ, Управління "К" МВС РФ, група ІВ,… і це далеко не добровольці, тобто це люди, які в погонах системно служать у російській армії. А весь світ активістів, ті самі Anonymous, "Мамкины хакеры", "No name", зараз "ламають" Російську Федерацію…

Отже, оцінка ризиків кібербезпеки та контролю конфіденційності в інформаційних системах державного управління на протязі всього життєвого циклу є дійсно роботою на упередження деструктивному впливу з боку противника. В цих умовах процедури, з охорони і оцінки конфіденційності повинні регулярно проводиться під час розробки/придбання на всьому етапі реалізації життєвого циклу системи. Проведення оцінок під час фази розробки/придбання та впровадження допомагає забезпечити наявність необхідних засобів контролю системи. Вкрай важливо проводити етап модернізації відповідно до цілей управління ризиками, організаційного забезпечення, інформаційної безпеки, кібербезпеки та архітектури конфіденційності [3].

Так, слабкі сторони та недоліки, пов'язані з безпекою та конфіденційністю, виявлені на початку етапу розробки системи життєвого циклу можуть бути вирішеними швидше і рентабельніше, ніж недоліки виявлені на наступних фазах життєвого циклу. Завчасне виявлення слабких місць і недоліків, пов'язаних із безпекою та конфіденційністю, у вибраних засобах контролю безпеки та конфіденційності полегшує визначення та впровадження відповідних заходів реагування на ризики та забезпечує ефективність реалізації контрольних заходів, які підлягають перевірці під час проектування та тестування системи.

Під час експлуатації та технічному обслуговуванні також повинні проводитись оцінки безпеки та конфіденційності на всіх етапах життєвого циклу, щоб гарантувати, що засоби контролю продовжують бути ефективними в операційній діяльності мережі/системи та здійснюється захист від ризиків та загроз що постійно розвиваються. Після первинної авторизації організація оцінює систему контролю безпеки та конфіденційності відповідно до його політики безпеки.

Процедура оцінювання повинна складатися з набору цілей оцінювання, кожна з яких має відповідний набір потенційних методів оцінки та об'єктів оцінки. Ціль оцінки включає одну або більше детермінаційних заяв. Методи оцінки це конкретні засоби захисту та контрзаходи, що містять апаратне, програмне або мікропрограмне забезпечення використовуються в системі або в системі загального контролю. Об'єкти оцінки визначають конкретні предмети, обладнання які оцінюються як частина даного контролю та включають специфікації, механізми, види діяльності та окремих осіб.

Таблиця 1 ілюструє приклад процедури оцінки контролю, яка розробляється для оцінки ефективності комунікаційної системи, виходячи з технічних вимог, розроблених спеціалістами організації на конкретну систему відповідно.

Таблиця 1. Приклад процедури оцінювання контролю

Віддалений доступ/Віддалене адміністрування	
МЕТА ОЦІНЮВАННЯ	Оберіть визначений варіант, якщо:
	політики безпеки щодо обмеження використання встановлені та задокументовані для кожного елемента системи, віддалений доступ дозволений
	вимоги до конфігурації/підключення встановлені та задокументовані, віддалений доступ дозволений для кожного типу обладнання системи
	для кожного типу встановлені та задокументовані рекомендації щодо налагодження та впровадження політик безпеки, віддалений доступ дозволений
	кожен тип віддаленого доступу до системи підтверджується процесом авторизації користувача
МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ ПОТЕНЦІАЛУ	Виберіть з:
	політика контролю доступу; впровадження та використання (включаючи обмеження) процедур, що стосуються віддаленого доступу; план управління конфігурацією; налаштування конфігурації системи та пов'язана документація; дистанційний доступ до алгоритму авторизації; автоматична система запису процесів аудиту; план безпеки системи; інші відповідні документи або записи
	організаційний персонал з відповідальністю ставиться до підключення за допомогою віддаленого доступу; наявні в управлінні організації/підприємстві адміністратори системи/мережі; організаційною структурою передбачено персонал, який відповідає за кібербезпеку
	можливість керування віддаленим доступом системи/мережою

Методи оцінювання визначають характер дій оцінювача і включають обстеження, співбесіду, і тест.

• Метод огляду – це процес перегляду, інспектування, спостереження, вивчення чи аналіз одного або кількох об'єктів оцінки (специфікації, механізми, устрій або їх спільні дії) щоб полегшити розуміння оцінювачам, отримати роз'яснення або отримати докази.

• Метод інтерв'ю – це процес проведення дискусій з окремими особами або групою осіб в організації, щоб полегшити оцінювачу розуміння, досягнення роз'яснення або отримання доказів.

• Метод тестування – це процес виконання на одному або кількох об'єктах оцінювання (діяльність або механізми) за певних умов для порівняння фактичного стану об'єкту до бажаного стану, або очікуваної поведінки об'єкта. У всіх трьох методах оцінки результати використовуються для прийняття конкретних необхідних визначень у детермінаційних заявах і таким чином досягаються цілі оцінки процедури.

За цих обставин процес оцінки контролю повинен включать:

• діяльність, яку здійснюють організації та оцінювачі для підготовки до безпеки та оцінки контролю конфіденційності;

• розробку планів оцінки безпеки та конфіденційності;

• проведення контролю оцінки та аналіз, документування та звітність результатів оцінки;

• аналіз звіту після оцінки та подальші заходи.

На цих умовах, порядок проведення тестування на проникнення проводиться як контрольована спроба порушити безпеку та конфіденційність засобів контролю, що застосовані в системі, використовуючи методи зловмисника та відповідне телекомунікаційне обладнання і спеціальне програмне забезпечення. Тестування на проникнення являє собою результати конкретного оцінювача або групи оцінювачів у певний момент часу з використанням узгоджених правил роботи. Враховуючи складність інформаційних технологій, які сьогодні зазвичай використовують організації, тестування на проникнення можна розглядати не як засіб для перевірки функцій безпеки та конфіденційності системи, а як засіб для покращення розуміння архітектурної побудови системи, виявлення слабких місць, або недоліків в системі з розрахунком відповідних сил та засобів, необхідних для недопущення порушення сталого функціонування системи, а у разі загострення ситуації – варіантів з відновлення її роботи.

Вправи з тестування на проникнення можуть бути запланованими та/або випадковими відповідно до визначених політик безпеки. Можна розглянути виконання тестів на проникнення на будь-якій нещодавно розробленій або застарілій системі, яка проходить оновлення. Організації активно контролюють системне середовище та середовище загроз – Sandboxie (наприклад, нові вразливості, методи атаки, розгортання нових технологій, безпека користувачів, обізнаність та навчання щодо конфіденційності) [11], щоб визначити зміни, які потребують виходу з циклу тестування на проникнення.

Тест на проникнення повинен розроблятись завчасно з огляду на визначені критерії, як правило їх елементами є:

1. Сканування вразливостей за межами топології мережі, при цьому враховуючи всі існуючі ризики, у тому числі застосовуючи індикатори кіберзагроз, що попереджає заподіянню шкоди сталому, надійному та штатному режиму функціонування комунікаційних та/або технологічних систем.

2. Критична оцінка ситуації, щодо невірної конфігурації системи, настройки обладнання, використання сервісів та технологій, здійснення обміну даними і т.і..

3. Чітко визначений обсяг архітектурної побудови системи:

- визначення середовища, що підлягає тестуванню (наприклад засоби, абоненти/користувачі, організаційні групи);

- визначення поверхні атаки, що підлягає перевірці (наприклад сервери, настільні системи, бездротові мережі, веб-додатки, виявлення та запобігання вторгненням системи,

брандмауери, облікові записи електронної пошти, безпека та конфіденційність користувачів і алгоритм реагування на інцидент, включаючи порушення персональних даних/інформації);

- визначення джерел загроз для моделювання (перелік зловмисників, їх профілі, які будуть використовуватися, наприклад внутрішній зловмисник, випадковий зловмисник, поодинокий або група зовнішніх цільових зловмисників);

- визначення цілей для імітованого зловмисника (наприклад отримання домену доступу адміністратора до LDAP організації - Lightweight Directory Access Protocol-структуру, з доступом до утентифікації (bind), пошуку (search) та порівняння (compare), а також операції додавання, зміни або видалення записів) [12];

- визначення рівня затрат (наприклад, часу та ресурсів).

4. Ретельна інтерпретація файлів даних системного журналу, включаючи всі виявлені вразливості та кіберінциденти.

5. Проникнення в систему як індикатор стійкості системи.

6. Перевірка існуючих засобів контролю безпеки та конфіденційності (включаючи механізми зменшення ризику, такі як брандмауери та системи виявлення та запобігання вторгненням).

7. Перевірка і відтворення, у разі потреби, журналу усих дій виконаних під час тесту.

8. Підготовка та надання звіту про результати тесту з інформацією про можливі заходи з відновлення після успішно проведених атак.

Основна мета звітів про оцінку безпеки та конфіденційність – це передача результатів оцінки контролю безпеки та конфіденційності відповідним посадовим особам організації. Звіт про оцінку безпеки та звіт про оцінку конфіденційності включені в авторизацію системи одним цілим разом із планом безпеки системи та планом конфіденційності (або аналог з метою здійснення загального контролю), план дій і етапи, а також узагальнені дані які мають інформацію, необхідну для прийняття рішень посадовою особою на основі ризиків щодо того, чи починати функціонування системи (продовжити її роботу).

Оцінка та авторизація набуває більш динамічного характеру, більшою мірою покладаючись на безперервний моніторинг аспектів процесу протягом всього життєвого циклу системи з можливістю оновлення звітів про оцінку безпеки та конфіденційність, що в свою чергу стає критичним аспектом програм інформаційної безпеки та конфіденційності.

Звіти про оцінку безпеки та конфіденційності забезпечують дисциплінований та структурований підхід до документування висновків оцінювача та рекомендацій щодо їх виправлення слабких сторін або недоліків в контролі безпеки та конфіденційності.

Ключові елементи звітності про оцінку безпеки та конфіденційність:

• Ім’я системи;
• Категоризація безпеки;
• Оцінка сайту(ів) та дата(и) оцінки;
• Ім’я/ідентифікація оцінювача;
• Попередні результати оцінки (у разі повторного використання);
• Позначник контролю безпеки/конфіденційності або покращення контролю;
• Вибрані методи та об’єкти оцінки;
• Значення атрибутів глибини та покриття;
• Підсумок результатів оцінки;
• Коментарі оцінювача (відзначені слабкі сторони або недоліки);
• Рекомендації оцінювача (пріоритети, виправлення, коригувальні дії або покращення).

Під час фактичної оцінки безпеки та контролю конфіденційності результати оцінки, коментарі та рекомендації документуються за допомогою відповідних форм звітності, визначених організацією або платформою. В наведеній таблиці 2 нижче представлений приклад результату оцінки безпеки та конфіденційності.

Таблиця 2

ПОШУК ІМОВІРНОСТЕЙ		
МЕТА ОЦІНЮВАННЯ Визначте, якщо:	ОЦІНКА ПОШУКУ	КОМЕНТАРІ ТА РЕКОМЕНДАЦІЇ ОЦІНЮВАЧА
проміжок часу, протягом якого необхідно провести пошукові заходи на випадок надзвичайних ситуацій. визначено роль або відповідальність на випадок непередбачених обставин	задоволений	політика планування на випадок надзвичайних ситуацій системи визначає (визначений організацією) час. термін 4 тижні.
періодичність, з якою необхідно провести пошукові заходи в системі. визначено роль/відповідальність	задоволений	політика планування на випадок надзвичайних ситуацій в системі. визначає періодичність, як щорічну
періодичність перегляду та оновлення політик безпеки. зміст визначено	задоволений	політика планування на випадок надзвичайних ситуацій в системі. визначає періодичність, як щорічну
події, реагування на які потребує перегляду та оновлення політики безпеки. визначений	більше ніж задоволений	жодний пошук подій/вразливостей не індифікується системою, потреба в перегляді та оновлені політик безпеки тренування в надзвичайних ситуаціях
робота у випадку надзвичайних ситуацій надається користувачам системи відповідно до розмежування прав доступу, визначених часових показників. виправданий ризик та відповідальність у випадку надзвичайних ситуацій	задоволений	
надання прав користувачам до системи під час виявлення вразливостей і реагування на комп'ютерні надзвичайні події відповідно до доступу абонентів та їх відповідальність за дії в системі під час внесення змін в її роботу/налагодження	більше ніж задоволений	при позначені як "не задоволений", оцінювачам не вдалося знайти доказів підготовка користувачів системи на випадок надзвичайних ситуацій була проведена відповідно до їх категорії та обов'язків, персонал не залучався до заходів підготовки коли відбулися/були заплановані значні зміни в налагоджені системи
підготовка з користувачами у випадку надзвичайних ситуацій в системі проводиться відповідно до розподілу за категоріями, правами, політикою безпеки, періодичність визначається організацією	задоволений	
зміст навчального плану відповідає загальному плану організації відповідно до дій у надзвичайних ситуаціях періодичність перегляду та оновлення його змісту визначається організацією	задоволений	

ПОШУК ІМОВІРНОСТЕЙ		
МЕТА ОЦІНЮВАННЯ Визначте, якщо:	ОЦІНКА ПОШУКУ	КОМЕНТАРІ ТА РЕКОМЕНДАЦІЇ ОЦІНЮВАЧА
тематика змісту навчального плану щодо практичних дій у надзвичайних ситуаціях переглядається та оновлюється, періодичність визначається організацією	більше ніж задоволений	

Постійна оцінка безпеки та конфіденційності – це постійна оцінка ефективності впровадження контролю безпеки та конфіденційності. Автоматизація оцінок є основним елементом допомоги організаціям в управлінні інформацією щодо ризиків безпеки конфіденційності. Загрози та зміни в обробці ідентифікаційних даних створюють проблеми для організації, які розробляють, впроваджують та експлуатують складні системи, які складаються з апаратних, мікропрограмних та програмних компонентів.

Кожна детермінаційна заява, виконана оцінювачем, призводить до одного з наступних висновків: задоволений, більше ніж задоволений.

Можливість оцінити всю реалізовану безпеку і контроль конфіденційності так часто, як це необхідно, з використанням ручних або процедурних методів став неприємлемим для більшості організацій через розмір, складність та обсяг інформації про технологічну інфраструктуру.

Для того, щоб ефективно автоматизувати оцінки контролю безпеки та конфіденційності з використанням потрібного стану стратегії специфікації, важливо відповідати наступним передумовам:

• Визначаються автоматизовані специфікації фактичного стану та поведінки;

• Визначаються специфікації бажаного стану на основі даних (порівнянні з фактичним станом);

• Метод для обчислення або виявлення дефектів (тобто відмінностей між бажаним і фактичним).

Коли передумови виконані, система оцінювання може автоматично обчислити, де виникають відмінності між бажаним і фактичним станом (дефектами). Ця інформація використовуэться для формування звітів про оцінку безпеки та конфіденційності. Зазначені звіти надаються визначеному персоналу через консоль керування безпекою та конфіденційністю (панель інструментів). Коли для проведення оцінювання використовуються автоматизовані засоби, використовується метод тестового оцінювання.

Під час фактичної оцінки безпеки та контролю конфіденційності результати оцінки, коментарі, а також рекомендації документуються за допомогою відповідних форм звітності, визначених організацією або платформою. Організаціям необхідно розробляти стандартні шаблони для звітності, які містять ключові елементи звітності про оцінку, описані вище. Коли можливо, автоматизація використовується, щоб зробити збір даних оцінки та звітність економічно ефективним та своєчасним інструментом, що є вкрай важливо.

Отже, в роботі здійснено огляд проблемного поля дослідження та корегування теоретичних підходів до реалізації нормативно-правової бази (нормативно-правових актів) які регулюється законодавством, що визначає повноваження спільних дій основних суб'єктів забезпечення кібербезпеки, суб'єктів кіберзахисту та власників (розпорядників) об'єктів критичної інформаційної інфраструктури під час попередження, виявлення, припинення кібератак та кіберінцидентів, а також при усуненні їх наслідків.

Дістали подальшого розвитку: практичний підхід до можливості здійснення кіберзахисту (у т.ч. активного кіберзахисту) власної інформаційної інфраструктури (засобів рухомого зв'язку, як апаратної, так і контентної складових, додатків та сервісів зв'язку, інших інформаційно-телекомунікаційних систем та об'єктів інформаційної діяльності суб'єктів

оборони держави) від кібератак та кібервпливу противника, що забезпечує необхідний рівень інформаційного забезпечення управління військами та зброєю.

Висновки. Виходячи з викладеного, можливо зробити наступні висновки, що інформаційні посилання, наведені в рекомендаціях Держпецзв'язку, є довідковими та не є вичерпними. В цілому рекомендації базуються на національних стандартах, нормативних документах, прийнятих в Україні, а також деякі довідкові посилання базуються на міжнародних і регіональних стандартах, нормативних документах інших країн.

Також, під час їх розроблення було враховано Настанови для підвищення кібербезпеки критичної інфраструктури (Framework for Improving Critical Infrastructure Cybersecurity, реліз 1), виданої у 2014 році та оновлені у вигляді релізу 2, у 2018 році Національним інститутом стандартів та технології Сполучених Штатів Америки.

З виходом NIST Special Publication 800-53A Revision 5 і NISTIR 8286C (Draft) зявилась потреба у вдосконаленні існуючого нормативно-правового поля по застосуванню заходів безпеки та конфіденційності в загальнодержавній структурі управління ризиками.

Тому авторським колективом було запропоновано розглянути відповідні зміни в методології оцінки ризиків кібербезпеки та контролю конфіденційності в інформаційних системах державного управління.

В подальшому використання зазначених пропозицій на об'єктах критичної інформаційної інфраструктури, гнучке їх використання буде позитивно сприяти послідовному застосуванню заходів безпеки та конфіденційності в загальнодержавній структурі управління ризиками.

ЛІТЕРАТУРА:

1. Постанова кабінету міністрів України від 19 червня 2019 р. № 518 Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури, [Електронний ресурс] – Режим доступу https://zakon.rada.gov.ua/go/518-2019-п.

2. Наказ Адміністрації Держспецзв'язку від 06 жовтня 2021 року № 601 Про затвердження Методичних рекомендацій щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури, [Електронний ресурс] – Режим доступу https://cip.gov.ua/ua/news/nakaz-administraciyi-derzhspeczv-yazku-vid-06-zhovtnya-2021-roku-601-pro-zatverdzhennya-metodichnikh-rekomendacii-shodo-pidvishennya-rivnya-kiberzakhistu-kritichnoyi-informaciinoyi-infrastrukturi.

3. Живило Є.О., Черноног О.О. Стратегія кібероборони України // *Збірник наукових праць Військового інституту телекомунікацій та інформатизації імені Героїв Крут.* Київ. 2017. Вип. 4 – [Електронний ресурс] – Режим доступу: //http://www.viti.edu.ua/files/zbk/2017/4/4_4_2017.pdf.

4. Живило Є.О., Черноног О.О., Вдовенко С.Г., Докіль В.М. Аналіз нормативно-правової бази функціонування системи кібероборони та системи кіберзахисту в інформаційно –телекомунікаційних системах військового призначення. *Збірник наукових праць Військового інституту Київського Національного університету імені Тараса Шевченка.* Київ. 2022. Вип. 74. С. 52-66.

5. Закон України "Про основні засади забезпечення кібербезпеки України" від 05.10.2017 р. № 2163-VIII // Законодавство України [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/2163-19#Text.

6. Стратегія кібербезпеки України, введена в дію Указом Президента України від 26 серпня 2021 року № 447/2021, [Електронний ресурс]
Режим доступу: https://www.president.gov.ua/documents/4472021-40013.

7. Методичні рекомендації щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури, [Електронний ресурс] – Режим доступу: https://dut.edu.ua/ua/news-1-569-9870-metodichni--rekomendacii--schodo--pidvischennya--rivnya-kiberzahistu-kritichnoi-informaciynoi-infrastrukturi_kafedra-cistem-tehnichnogo-zahistu-informacii.

8. Сучасні підходи до оцінки ризиків інформаційних технологій, [Електронний ресурс] – Режим доступу: https://present5.com/suchasni-pidxodi-do-ocinki-rizikiv-informacijnix-texnologij-na/.

9. Закон України "Про ратифікацію Конвенції про кіберзлочинність" від 10.03.2006 р. № 2163-VIII // Законодавство України [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/2824-15#Text.

10. Україна почала здійснювати кібератаки на ресурси рф з 24 лютого – Федоров, – 2022 [Електронний ресурс] – Режим доступу: https://www.ukrinform.ua/rubric-technology/3456506-ukraina-pocala-zdijsnuvati-kiberataki-na-resursi-rf-z-24-lutogo-fedorov.html.

11. Живило Є.О., Докіль В. М. Кібервійська України: своєчасна відповідь на виклики сьогодення. *Науковий вісник Національної академії внутрішніх справ.* Київ. 2021. Вип. 2 (47). С. 18–34. Таємно – Інв. 588 від 14.12.2021 у НАВС.

12. Синхронизация LDAP с Azure Active Directory– 2022 [Електронний ресурс] – Режим доступу: https://docs.microsoft.com/ru-ru/azure/active-directory/fundamentals/sync-ldap.

REFERENCES:

1. Postanova kabinetu ministriv Ukrayiny` vid 19 chervnya 2019 r. # 518 Pro zatverdzhennya Zagal`ny`x vy`mog do kiberzaxy`stu ob'yektiv kry`ty`chnoyi infrastruktury`, [Elektronny`j resurs] – Rezhy`m dostupu: https://zakon.rada.gov.ua/go/518-2019- p.

2. Nakaz Administraciyi Derzhspeczzv'yazku vid 06 zhovtnya 2021 roku # 601 Pro zatverdzhennya Metody`chny`x rekomendacij shhodo pidvy`shhennya rivnya kiberzaxy`stu kry`ty`chnoyi informacijnoyi infrastruktury`, [Elektronny`j resurs] – Rezhy`m dostupu: https://cip.gov.ua/ua/news/nakaz-administraciyi-derzhspeczv-yazku-vid-06-zhovtnya-2021-roku-601-pro-zatverdzhennya-metodichnikh-rekomendacii-shodo-pidvishennya-rivnya-kiberzakhistu-kritichnoyi-informaciinoyi-infrastrukturi.

3. Zhy`vy`lo Ye.O., Chernonog O.O. Strategiya kiberoborony` Ukrayiny` // Zbirny`k naukovy`x pracz` Vijs`kovogo insty`tutu telekomunikacij ta informaty`zaciyi imeni Geroyiv Krut. Ky`yiv. 2017. Vy`p. 4 – [Elektronny`j resurs] – Rezhy`m dostupu: //http://www.viti.edu.ua/files/zbk/2017/4/4_4_2017.pdf.

4. Zhy`vy`lo Ye.O., Chernonog O.O., Vdovenko S.G., Dokil` V.M. Analiz normaty`vno-pravovoyi bazy` funkcionuvannya sy`stemy` kiberoborony` ta sy`stemy` kiberzaxy`stu v informacijno – telekomunikacijny`x sy`stemax vijs`kovogo pry`znachennya. Zbirny`k naukovy`x pracz` Vijs`kovogo insty`tutu Ky`yivs`kogo Nacional`nogo universy`tetu imeni Tarasa Shevchenka. Ky`yiv. 2022. Vy`p. 74. S. 52-66.

5. Zakon Ukrayiny` “Pro osnovni zasady` zabezpechennya kiberbezpeky` Ukrayiny`” vid 05.10.2017 r. # 2163-VIII // Zakonodavstvo Ukrayiny` [Elektronny`j resurs] – Rezhy`m dostupu: https://zakon.rada.gov.ua/laws/show/2163-19#Text.

6. Strategiya kiberbezpeky` Ukrayiny`, vvedena v diyu Ukazom Prezy`denta Ukrayiny` vid 26 serpnya 2021 roku # 447/2021, [Elektronny`j resurs] – Rezhy`m dostupu: https://www.president.gov.ua/documents/4472021-40013.

7. Metody`chni rekomendaciyi shhodo pidvy`shhennya rivnya kiberzaxy`stu kry`ty`chnoyi informacijnoyi infrastruktury`, [Elektronny`j resurs] – Rezhy`m dostupu: https://dut.edu.ua/ua/news-1-569-9870-metodichni--rekomendacii--schodo--pidvischennya--rivnya-kiberzahistu-kritichnoi-informaciynoi-infrastrukturi_kafedra-cistem-tehnichnogo-zahistu-informacii.

8. Suchasni pidxody` do ocinky` ry`zy`kiv informacijny`x texnologij, [Elektronny`j resurs] – Rezhy`m dostupu: https://present5.com/suchasni-pidxodi-do-ocinki-rizikiv-informacijnix-texnologij-na/.

9. Zakon Ukrayiny` “Pro raty`fikaciyu Konvenciyi pro kiberzlochy`nnist`” vid 10.03.2006 r. # 2163-VIII // Zakonodavstvo Ukrayiny` [Elektronny`j resurs] – Rezhy`m dostupu: https://zakon.rada.gov.ua/laws/show/2824-15#Text.

10. Ukrayina pochala zdijsnyuvaty` kiberataky` na resursy` rf z 24 lyutogo – Fedorov, – 2022 [Elektronny`j resurs] – Rezhy`m dostupu: https://www.ukrinform.ua/rubric-technology/3456506-ukraina-pocala-zdijsnuvati-kiberataki-na-resursi-rf-z-24-lutogo-fedorov.html.

11. Zhy`vy`lo Ye.O., Dokil` V. M. Kibervijs`ka Ukrayiny`: svoyechasna vidpovid` na vy`kly`ky` s`ogodennya. Naukovy`j visny`k Nacional`noyi akademiyi vnutrishnix sprav. Ky`yiv. 2021. Vy`p. 2 (47). S. 18–34. Tayemno – Inv. 588 vid 14.12.2021 u NAVS.

12. Sy`nxrony`zacy`ya LDAP s Azure Active Directory– 2022 [Elektronny`j resurs] – Rezhy`m dostupu: https://docs.microsoft.com/ru-ru/azure/active-directory/fundamentals/sync-ldap.

PhD Zhyvylo E.O., PhD Shevchenko D.G.

RISK ASSESSMENT OF CYBER SECURITY AND CONTROL OF PRIVACY IN PUBLIC ADMINISTRATION INFORMATION SYSTEMS

The relevance of this work is due to the approval by the Administration of the State Service for Special Communications and Information Protection of Ukraine "Methodological recommendations for increasing the level of cyber protection of critical information infrastructure" in October 2021. The recommendations were developed based on the world's best approaches - the NIST CyberSecurity Framework. At the moment, the developed Recommendations of the State Special Communications Service have partially lost their relevance and require adjustment with the release of NIST Special Publication 800-53A Revision 5 "Assessing Security and Privacy Controls in Information Systems and Organizations" Governance Oversight", publication date: January 2022. These documents complete the cycle of integrating cybersecurity risk management (CSRM) and enterprise risk management (ERM).

These projects describe methods for combining risk information of all system assets, an organization (enterprise) network, including conditional examples for aggregating and normalizing results from cybersecurity risk registers (CSRR) taking into account risk parameters, criteria and impact on the continuous functioning of communication systems. As a result, the integration and normalization of risk information enables decision-making and monitoring of risks at all levels of the system, which allows you to create a comprehensive picture of the overall cyber risk. These documents describe the creation of an Organizational Risk Profile (ERP) that supports the comparison and management of cyber risks along with other risk types in general.Quite interesting are the views of the authors of the developed documents regarding the control of confidentiality associated with systems and their distribution environment, their functioning. It is substantiated that a qualitative system assessment helps to determine the existing controls contained in the organization in accordance with the security and confidentiality plan, which are subsequently used in organizational systems and the operating environment. In this environment, the assessment control is an indication of the implementation of specific steps in the risk management structure, which contributes around the clock to an effective approach to sustainable risk management processes by identifying weaknesses or deficiencies in systems, which allows the organization to determine how to respond to certain cyber threats.

Therefore, in order to solve the problems of settling and implementing the norms and rules of international organizations in the field of cybersecurity and cyberdefence, it is proposed to analyze the above documents and put forward appropriate proposals for correcting and supplementing the previously approved State Communications "Methodological recommendations ...". In turn, this will allow not only to ensure the protection of the state's critical information infrastructure from cyber attacks, but also to conduct preventive offensive operations in cyberspace, which includes disabling critical enemy infrastructure facilities by destroying communication systems that control such facilities.

Keywords: cyberspace, cybersecurity, cyberthreats, cybersecurity risk management, cybersecurity risk assessment, cybersecurity risk register, communication systems, legal act, critical information infrastructure object.