УДК 656.025: 330.131.7
DOI: 10.34029/2311-4061-2024-152-3-24-31

***Канд. техн. наук Щека В.І.,***
***канд. техн. наук Ящук К.І.,***
***аспірант Тімар С.В.***

**ТЕХНІКИ ІТ-РИЗИК МЕНЕДЖМЕНТУ ДЛЯ ЗАЛІЗНИЧНОГО ТРАНСПОРТУ**

IT-RISK MANAGEMENT TECHNIQUES FOR RAILWAY TRANSPORT

***Ключові слова****: ІТ-ризик менеджмент, фреймворк, управління ІТ-ризиками, залізничний транспорт.*

**Вступ**

Робота залізниці є складним процесом, при виконанні якого необхідно забезпечити безпеку та надійність перевезень вантажів та пасажирів, навіть у найважчих умовах. Загроз для нормальної роботи залізниці в Україні надзвичайно багато: вандалізм, застаріле обладнання (яке інколи неможливо відремонтувати або замінити через відсутність виробництва відповідних деталей в країні), відсутність кваліфікованих кадрів, конкуренція інших логістичних засобів (авто, річковий/морський транспорт і т.д.), військовий конфлікт (що створює не тільки нові ризики, але і додаткове навантаження на залізниці через необхідність доставки нетипових вантажів). Системи автоматизованого управління залізничними перевезеннями також працюють сьогодні в надважких умовах. Тому галузевим службам управління важливо мати ефективну систему управління ризиками, яка дозволить забезпечити безпеку та неперервність роботи залізниці навіть у найскладніших умовах.

Впровадження інформаційних технологій значно полегшує управління залізничними перевезеннями, забезпечуючи швидку обробку даних, відслідковування поїздів та оптимізацію їх руху. Однак з іншого боку, такі системи створюють нові можливості для кібератак та інших форм злочинності, які можуть призвести до серйозних порушень у роботі залізничних систем або втраті критично важливої інформації чи засобів управління та контролю, тому розробка ефективних стратегій управління ІТ-ризиками стає надзвичайно важливою для забезпечення безперебійності роботи систем залізничних перевезень. Це включає в себе не лише аналіз та контроль зовнішніх загроз, але й внутрішніх вразливостей, таких як помилки в програмному забезпеченні, недбалість персоналу, порушення правил безпеки або експлуатації ІТ-систем.

Підтвердженням актуальності цієї проблеми є статистичні дослідження, що проведені компанією IBM, і згідно яких витрати на відновлення ІТ-систем після кібератак на транспортні компанії можуть сягати, в середньому, 1,2 мільйона доларів США [1]. Також важливо враховувати, що близько 60 % транспортних компаній залишаються уразливими перед кібератаками через недостатній рівень контролю вразливостей та їх мінімізації [2].

**Мета**

Ця стаття спрямована на доведення результатів дослідження ролі ІТ-ризик менеджменту у забезпеченні безперебійності роботи системи залізничних перевезень. Основними завданнями публікації є розгляд існуючих технік ІТ-ризик менеджменту, їх переваг та недоліків, а також аплікабельності до залізничних процесів.

**Роль ІТ ризик менеджменту в сучасних залізничних системах передових країн**

Управління ІТ-ризиками є критично важливим аспектом забезпечення безпеки. Наприклад, федеральна залізнична адміністрація США (FRA) розробила комплексну програму зменшення ризиків, яка спрямована на виявлення, збір та аналіз даних про аварії, задля виявлення ризиків, що передують їм, розробку добровільних пілотних програм у співпраці із зацікавленими

сторонами, спрямованих на пом'якшення виявлених і потенційних ризиків, а також поширення найкращих практик для всієї залізничної галузі. На додаток до цього, FRA також розробило методологію аналізу ризиків кібербезпеки для підключених залізничних технологій на основі зв'язку. Цю методологію можна пристосувати до конкретних випадків використання та дизайну існуючих систем. Завдяки застосуванню методологічної основи дослідження можна визначити потенційні загрози кібератак, їх уразливості та наслідки для кожного випадку і таким чином оцінити існуючий ризик та рекомендувати стратегії зменшення ризику. Вибрані сценарії використання технологій підключеної залізниці включають програму радіокодової лінії Advanced Train Control System, системи дистанційного контролю та інші системи залізничної автоматики. У кожному конкретному випадку аналіз узагальнює профілі кіберризиків і надаєв практичні рекомендації щодо покращення кібербезпеки.

Важливо зазначити, що програма зниження ризиків FRA та методологія аналізу ризиків кібербезпеки є лише двома прикладами того, як управління ІТ-ризиками реалізовано в залізничній системі США. Інші організації можуть мати різні підходи до управління ІТ-ризиками залежно від своїх конкретних потреб, обставин та прогнозованих портретів атакуючих обставин.

Агентство Європейського Союзу з кібербезпеки (ENISA) опублікувало звіт «Кібербезпека залізниці – передові практики в управлінні кіберризиками» [3]. Цей звіт має на меті стати орієнтиром для поточних передових практик щодо підходів до управління кіберризиками, які можуть бути застосованими до залізниці, як сектора. Він пропонує інструкцію для залізничних підприємств та менеджерів інфраструктури щодо вибору, комбінування або коригування методів управління кіберризиками відповідно до потреб їх організації. У звіті містяться дієві вказівки, перераховуються загальні проблеми, пов'язані з виконанням відповідних заходів, і окреслюються передові практики, які можуть бути легко прийняті та адаптовані окремими організаціями. Крім того, доступний перелік корисних довідкових матеріалів разом із практичними прикладами та відповідними стандартами.

Звіт ґрунтується на звіті ENISA про кібербезпеку в залізничному секторі за 2020 рік [3], у якому оцінено рівень впровадження заходів кібербезпеки в залізничному секторі. Належні практики, представлені у звіті, ґрунтуються на відгуках зацікавлених сторін. Вони включають такі інструменти, як перелік активів і послуг, сценарії кіберзагроз і відповідні заходи кібербезпеки, засновані на стандартах і належній практиці, що використовуються в секторі. Ці ресурси можуть бути використані як основа для управління кіберризиками для залізничних компаній. Згаданий звіт ENISA є лише одним із прикладів опису того, як управління ІТ-ризиками впроваджується в європейській залізничній системі. Інші організації можуть мати різні підходи до управління ІТ-ризиками залежно від своїх конкретних потреб і обставин.

Залізнична галузь Канади, наприклад, запровадила різні заходи для забезпечення безпечної та надійної роботи, включаючи управління ризиками. Канадський метод оцінки ризиків для залізничних систем (The Canadian Method for Risk Evaluation and Assessment – CM-REA) [4] – це система управління ризиками, яка містить вказівки щодо дотримання еквіваленту правових європейських регламентів та загальні методи оцінки безпеки та ризиків. CM-REA базується на інтегрованому підході, який зосереджується на ключових сферах ризику, таких як сигнали, станції та мости. Залізничні компанії в Канаді зобов'язані дотримуватися норм і правил, встановлених Транспортною службою Канади, яка контролює технічні нормативні стандарти залізничної галузі. Ця служба встановила різні правила та вказівки для забезпечення безпеки залізничного транспорту, включаючи ІТ-системи.

**Процес управління ІТ-ризиками**

В основу будь якої техніки управління ІТ-ризиком покладено базовий процес управління, який може бути представлений у вигляді циклічного процесу, що включає кілька етапів. Основні етапи можливого процесу управління ІТ-ризиками представлені на рисунку 1, які містять наступні дії:

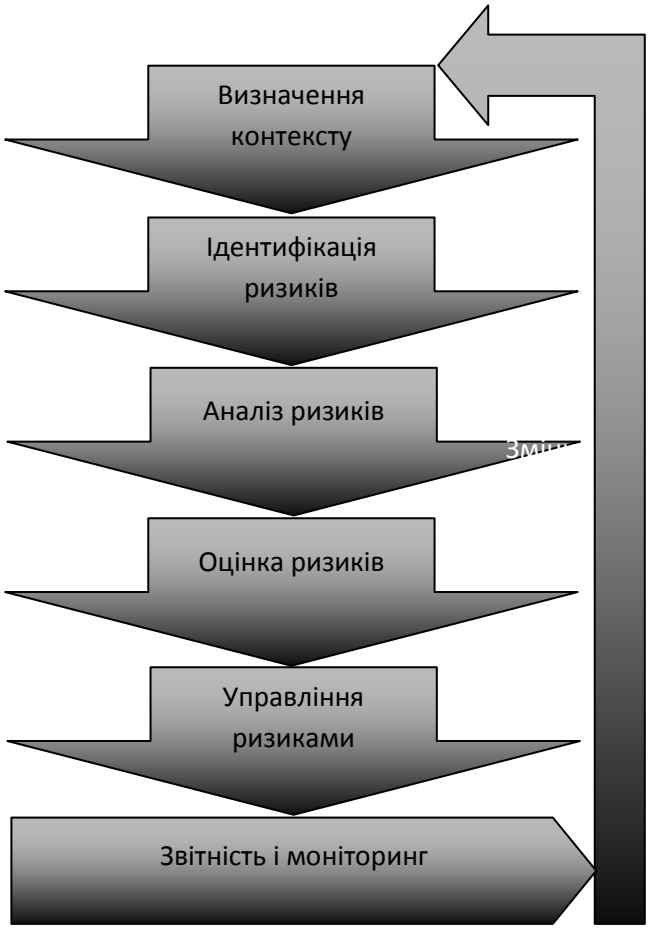


*Рис. 1 – Основні етапи процесу управління ІТ-ризиками*

- «Визначення контексту» – встановлення контексту для управління ризиками, включаючи визначення мети та обсягу управління ризиком;
- «Ідентифікація ризиків» – визначення потенційних загроз і небезпек, які можуть вплинути на цілі організації;
- «Аналіз ризиків» – оцінка і аналіз ризиків з урахуванням ймовірності їх виникнення та величини можливих збитків;
- «Оцінка ризиків» – визначення рівня ризику для кожного ідентифікованого ризику на основі їх аналізу;
- «Управління ризиками» – розроблення та впровадження стратегій управління ризиками, включаючи прийняття заходів щодо зменшення, уникнення, передачі або прийняття ризику;
- «Звітність і моніторинг» – постійний моніторинг ризиків, ефективності впроваджених заходів управління ризиками, а також звітність про результати управління ризиками.

Цей процес є ітеративним та циклічним, оскільки ризики можуть змінюватися в результаті впливу внутрішніх та зовнішніх факторів. Процес управління ризиком вимагає постійного оновлення і адаптації. Моніторинг та аналіз ризиків може знаходити новий контекст або ідентифікувати нові ризики. Контекст, оцінка ризиків та методи управління ними у АТ «Укрзалізниця» можуть змінюватися з часом внаслідок дії багатьох факторів, від зміни голови правління чи наглядової ради товариства до розробки нових методів управління рухомим складом галузі.

Згідно з дослідженням компанії Deloitte, ітеративний процес управління ІТ-ризиками дозволяє організаціям бути більш гнучкими та відповідати зовнішньому середовищу, яке швидко змінюється. Стверджується, що «постійне оновлення та адаптація стратегій управління

ризиками дозволяє організаціям забезпечувати ефективну захищеність від ризиків та збільшувати свою конкурентоспроможність» [5].

**Техніки управління ІТ-ризиками**

На сьогоднішній день існують багато технік з ІТ-ризик менеджменту. Вони називаються фреймворками або стандартами, основна задача яких – створення структурованого підходу до ідентифікації, оцінки та пом'якшення ризиків для інформаційних активів. Фреймворки бувають як військові (наприклад Department of Defense Risk Management Framework (DoD RMF), США [6], так і цивільні (National Institute of Standards and Technology (NIST) Cybersecurity Framework 2.0 (NIST CSF) [7], різні стандарти International Organization for Standardization (ISO) та багато інших). Крім того фреймворки бувають з гнучкою (Operational Risk Management (COSO), США [8] чи Factor Analysis of Information Risk (FAIR), США [9], та ін.) або не гнучкою (Payment Card Industry Data Security Standard (PCI DSS), США [10], Health Insurance Portability and Accountability Act (HIPAA), США [11], Control Objectives for Information and Related Technologies (COBIT), США [12] та ін.) формою імплементації, з вимогами виконувати кожний пункт фреймворку.

Треба зауважити, що військовий фреймворк не завжди відповідає потребам цивільних компаній навіть в умовах війни, адже він створювався з урахуванням саме військових потреб, а не ризиків пов'язаних з війною. А от різниця між гнучкими і не гнучкими фреймворками є критичною для розуміння і обрання саме того підходу та фреймворку або його елементів, що максимально покриє специфіку роботи залізниці та пов'язаних ризиків. Наприклад, стандарт (Payment Card Industry Data Security Standard (PCI DSS) [10], що описує вимоги до безпеки платіжних систем та фокусується на захисті персональних та фінансових даних клієнта, є малоприйнятним для забезпечення безперервного функціонування інформаційних потоків на залізниці. Тому окремо розглянемо різницю між гнучкими і не гнучкими фреймворками.

***Особливості негнучкого фреймворку***

Негнучкий фреймворк це високоструктурований стандарт, який визначає певний набір процесів, елементів керування та вимог до документації. Він орієнтований на забезпечення відповідності і часто використовується для виконання нормативних вимог (наприклад, PCI DSS, HIPAA). Має детальні вказівки, а саме: надає чіткі вказівки щодо впровадження засобів контролю.

Переваги негнучких фреймворків:

- послідовна реалізація;
- полегшений моніторинг;
- доведена ефективність для конкретних потреб.

Недоліки:

- менша гнучкість;
- реалізація може потребувати багато часу та витрат;
- можуть потребувати специфічних знань персоналу;
- не є універсальними та можуть не підходити для окремих залізничних підрозділів.

Приклади негнучких фреймворків:

1. Стандарт безпеки даних платіжних карток (PCI DSS) [10] використовується для забезпечення безпеки обробки, зберігання та передачі кредитної карткової інформації та фокусується на захисті даних власників карток. Цей стандарт встановлює вимоги до організацій, які приймають, обробляють або зберігають платіжні карти. Він розроблений спільними зусиллями великих компаній платіжної галузі, таких як Visa, MasterCard, American Express, Discover і JCB та має на меті зменшити ризики використання платіжних карт для злочинних цілей. Відповідність вимогам PCI DSS є обов'язковою для банківських установ, які працюють з кредитними картами, і вимагає проведення регулярних аудитів безпеки та впровадження заходів для захисту конфіденційності, цілісності і доступності карткової інформації.

2. Нормативний акт (Закон) про перенесення та підзвітність медичного страхування (HIPAA) [9] використовується в США з 1996 року і спеціалізується на захисті конфіденційних даних пацієнтів в організаціях охорони здоров'я. У цілому, HIPAA спрямований на захист приватності та безпеки медичної інформації, а також на покращення якості та доступності медичної допомоги.

3. Фреймворк з контролю цілей інформаційних та суміжних технологій (COBIT) [12]. Він фокусується на структурі управління IT-процесами, із сильним акцентом на контролі. Фактично, COBIT – це набір нормативних документів та практичних інструментів, які можуть допомогти залізничній компанії ефективно управляти своїми інформаційними технологіями. COBIT розроблений ISACA (Association of Information Systems Auditors) і надає рамки та керівні принципи для управління IT-процесами, їх контролем і безпекою. Основні цілі використання COBIT включають:

- забезпечення відповідності з вимогами законодавства та стандартів безпеки даних;
- оптимізація використання інформаційних ресурсів та зменшення ризиків;
- забезпечення високої якості сервісу та відповідності до бізнес-потреб;
- забезпечення ефективного контролю та управління IT-процесами.

COBIT може допомогти залізничним підрозділам АТ «Укрзалізниця» створити цілісну систему управління IT-процесами, що відповідає стратегічним цілям товариства і України, забезпечує ефективне використання ресурсів та дозволяє вчасно реагувати на зміни в бізнес-середовищі.

***Особливості гнучкого фреймворку***

Гнучкий та здатний до адаптування фреймворк пропонує загальну структуру впливу на IT-процеси, яку можна налаштувати відповідно до конкретних потреб. Має підхід, що ґрунтується на оцінці ризику і зосереджується на виявленні та усуненні найбільш критичних ризиків. Високорівневе керування IT-процесами надає принципи управління ризиками, але залишає деталі реалізації на розсуд залізничної компанії.

Переваги гнучкого фреймворку:

- більш адаптований до різноманіття інформаційних процесів що існують на залізниці;
- швидше та легше реалізувати;
- більш заохочує культуру управління ризиками.

Недоліки:

- для ефективної реалізації потрібні додаткові знання персоналу;
- послідовність реалізації може бути проблемою;
- може не підходити для жорстко регульованих галузей (наприклад системи продажу квитків booking.uz.gov.ua).

Приклади гнучких фреймворків:

1. ISO 27001 [13] є міжнародним стандартом, що встановлює вимоги до систем управління інформаційною безпекою в організаціях. Цей стандарт може допомогти підприємствам АТ «Укрзалізниця» будувати, впроваджувати, вдосконалювати та підтримувати системи управління інформаційною безпекою галузі у відповідності до міжнародних стандартів. Основні цілі використання ISO 27001 включають:

- забезпечення конфіденційності, цілісності та доступності інформації;
- захист інформації від несанкціонованого доступу, використання, розкриття, зміни, руйнування або втрати;
- встановлення механізмів для виявлення та реагування на інциденти інформаційної безпеки;
- забезпечення відповідності зв'язаних з інформаційною безпекою вимог законодавства, регуляторних вимог та інших вимог, що стосуються інформаційної безпеки;
- підвищення довіри вигодонабувачів до управління інформаційною безпекою.

Міжнародний стандарт ISO 27001 допомагає впроваджувати кращі практики з управління інформаційною безпекою, зменшувати ризики втрати або пошкодження інформації, підвищувати довіру клієнтів та захищати репутацію підприємств галузі.

2. Фреймворк з кібербезпеки NIST (NIST Cybersecurity Framework (CSF)) [7] може бути використаний для покращення стану кібербезпеки на залізниці. Він був розроблений Національним інститутом стандартів і технологій (NIST) США як набір керівництв для вдосконалення кібербезпеки, які можуть бути застосовувані у різних галузях та організаціях будь-якого розміру. Основні цілі використання стандарту CSF включають:

- зміцнення кібербезпеки, що допомагає удосконалити підходи до захисту від кіберзагроз, визначити та управляти кібербезпековими ризиками;

- стандартизацію IT-процесів, що надає стандарти та рекомендації з кібербезпеки, які можна використовувати для створення або вдосконалення кібербезпекових процесів та практик;
- управління ризиками, яке допомагає виявляти, оцінювати та керувати кібербезпековими ризиками у відповідності до потреб та можливостей;
- покращення відповідності, яке може бути використаним для дотримання вимог законодавства та стандартів у галузі кібербезпеки;
- забезпечення співпраці, що сприяє покращенню взаємодії між відділами та структурами підприємства для більш ефективного управління кібербезпекою.

Загалом, фреймворк CSF допомагає підвищити рівень кібербезпеки підприємства та галузі і ефективно відповідати на кіберзагрози.

3. OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) [14], трактується як методологія для оцінки критичних загроз, активів і вразливостей і використовується для управління інформаційною безпекою та ризиками. Основна мета OCTAVE – ідентифікація та управління критичними активами, загрозами та вразливостями, які можуть призвести до втрати конфіденційності, цілісності та доступності інформації. Методологія OCTAVE дозволяє:

- визначити критичні активи, які потребують особливої уваги з точки зору захисту;
- виявити потенційні загрози та вразливості, що можуть бути використані для атак на ці активи;
- розробити стратегії та заходи для захисту активів та зменшення ризиків;
- провести оцінку ефективності управління ризиками та заходів забезпечення інформаційної безпеки.

Основна перевага методології OCTAVE полягає в тому, що вона орієнтована на конкретні потреби та характеристики кожної конкретної організації, у тому числі сервісу залізничних перевезень, що дозволяє створити індивідуальний план управління ризиками, а також враховувати специфічні особливості її діяльності та інфраструктури галузі.

Вибір найпридатнішого фреймворку для залізничної галузі залежить від впливу кількох факторів, зокрема:

- галузевих правил та нормативів;
- розміру і складності IT-середовища підприємства;
- толерантності до ризиків що виникають;
- наявних ресурсів (бюджет, експертизи тощо).

Ефективним може бути у IT-ризик менеджменті і гібридний підхід, що поєднує елементи кількох фреймворків, у тому числі гнучких і негнучких.

**Аплікабельні для залізничного транспорту техніки управління IT-ризиками**

Залізничні системи, а особливо системи автоматизації на залізниці, суттєво відрізняються в залежності від країни, тому неможливо використовувати, наприклад CM-REA як єдину систему ризик менеджменту для використання всіма підрозділами АТ «Укрзалізниця». Для розробки методології IT-ризик менеджменту для АТ «Укрзалізниця» треба використовувати елементи різних існуючих методологій для різних елементів залізничних інформаційних систем.

Для систем, що взаємодіють з фінансовими системами та банківськими установами бажано (а у багатьох кейсах необхідно) відповідати вимогам PCI DSS, тому є сенс впроваджувати методологію ризик управління відповідно до цього фреймворку.

Для систем які зберігають та обробляють персональні данні є сенс використовувати General Data Protection Regulation (GDPR) Compliance Guidelines [15], особливо з урахуванням майбутньої інтеграції вітчизняних залізниць у залізничні системи Євросоюзу та гармонізації законодавства України з законодавством ЄС.

Для систем автоматизації управління, найбільш актуальним є OCTAVE, адже цей ризик-менеджмент фреймворк базується на розподілі активів за критичністю. Системи автоматизації при однакових функціях і елементах мають зовсім різну критичність в залежності від свого розташування. Наприклад, відмова стрілочного переводу на бічних малозадіяних коліях набагато менш критична ніж відмова стрілочного переводу у горловині станції.

Більш конкретні пропозиції щодо підходів до IT ризик-управління на залізничному транспорті будуть надані у наступних статтях.

**Висновки**

Всім підрозділам АТ «Укрзалізниця», незалежно від їхнього розміру та сфери діяльності, бажано ініціювати процес впровадження IT-ризик менеджменту, який має бути постійним і комплексним та охоплювати всі аспекти IT-інфраструктури та інформаційних систем товариства.

Непродумана імплементація готового фреймворку, навіть розробленого під потреби залізничних систем, але для умов іншої країни, може мати негативні наслідки для вітчизняних залізниць через неаплікабельні методи контролю, різницю в технологіях, законодавстві, кваліфікації робочій сили. Важливо підібрати найкращі методи IT-ризик-управління для кожної інформаційної системи та регулярно вдосконалювати ці методи у відповідності до змін у інформаційних системах, законодавстві країни, загрозах що виникають, щоб ці методи відповідали потребам та ризикам сьогодення, адже щодня виникають нові вектори атак на залізничні IT-системи.

Впровадження IT-ризик менеджменту на залізничному транспорті є економічно вигідною інвестицією, яка спрямована на уникнення значних втрат у майбутньому.

***Література***


1. Cost of a Data Breach Report. – Armonk, NY : Copyright IBM Corporation, 2020. – 82 p. – Mode of access: https://www.ibm.com/security/digital-assets/cost-data-breach-report/1Cost%20of%20a%20Data%20Breach%20Report%202020.pdf
2. Cyber risk in advanced manufacturing, Deloitte and MAPI / T.Huelsman, E. Powers, S. Peasley, R. Robinson. – Deloitte Development LLC, MAPI, 2019. – 52 p. – Mode of access: https://www2.deloitte.com/content/dam/Deloitte/us/Documents/manufacturing/us-manu-cyber-risk-in-advanced-manufacturing.pdf
3. Railway Cybersecurity – Good Practices in Cyber Risk Management / M.Theocharidou, Z.Stanic, L.De Mauroy, L.Lebain, J.Haddad. – ENISA, 2021. – 57 p. – DOI 10.2824/92259. – Mode of access: https://www.enisa.europa.eu/publications/railway-cybersecurity-good-practices-in-cyber-risk-management
4. CSA R114:22. Canadian method for risk evaluation and assessment for railway systems. – Official edition. – SCA Group, 2022. – Mode of access: https://www.csagroup.org/store/product/CSA%20R114:22/
5. Managing IT Risk in Today's Digital World. – Deloitte Touche Tohmatsu India LLP, 2019. – 58 p.
6. Risk Management Framework (RMF) for DoD Information Technology: Instruction 8510.01. – Department of Defense Risk Management Framework (DoD RMF); effective from 2022-07-19. – Official edition. – 36 p.
7. The NIST Cybersecurity Framework (CSF) 2.0. – Gaithersburg, MD : National Institute of Standards and Technology, 2024. – https://doi.org/10.6028/nist.cswp.29
8. Moeller R. R. COSO Enterprise Risk Management / R. R. Moeller. – Hoboken, NJ, USA : John Wiley & Sons, Inc., 2011. – https://doi.org/10.1002/9781118269145
9. Freund J., Jones J. Chapter 4 – FAIR Terminology / J.Freund, J.Jones // Measuring and Managing Information Risk. – 2015. – P. 43–73. – https://doi.org/10.1016/b978-0-12-420231-3.00004-x
10. 4.0. PCI DSS. – Effective from 2022-03-01. – Official edition. – PCI Security Standards Council, 2022. – Mode of access: https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v4_0.pdf
11. Health Insurance Portability and Accountability Act : Congressional Report of 31.07.1996 No. H. Rept. 104-736. https://www.congress.gov/congressional-report/104th-congress/house-report/736/1
12. COBIT 5. – Effective from 2012-04-01. – Official edition. – ISACA, 2012.
13. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection. – Effective from 2022-10-01. – Official edition. – ISO, 2022. – Mode of access: https://www.iso.org/standard/27001
14. Octave v2.0 (and Octave-S v1.0 for Small and Medium Businesses). – Effective from 2005-01-01. – Official edition. – ENISA, 2005. – Mode of access: https://www.enisa.europa.eu/topics/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_octave.html.

15. Horák M. GDPR Compliance in Cybersecurity Software / M. Horák, V. Stupka, M. Husák // ARES '19: 14th International Conference on Availability, Reliability and Security, Canterbury CA United Kingdom. – New York, NY, USA, 2019. – Mode of access: https://doi.org/10.1145/3339252.3340516 (date of access: 16.02.2024).

**ВІДОМОСТІ ПРО АВТОРІВ**

**Щека Вадим Ігоревич,**
к.т.н., доцент, доцент кафедри «Автоматика та телекомунікації» ННІ «Дніпровський інститут інфраструктури і транспорту» (ДІІТ) Українського державного університету науки і технологій (УДУНТ).
Вул. Лазаряна, 2 (к. 129),
м. Дніпро, 49010, Україна.
E-mail: v.i.shcheka@ust.edu.ua.
ORCID ID: 0000-0002-2184-2827.

**Ящук Катерина Іванівна,**
к.т.н., доцент, доцент кафедри «Автоматика та телекомунікації» ННІ «ДІІТ» УДУНТ.
Вул. Лазаряна, 2 (к. 129),
м. Дніпро, 49010, Україна.
E-mail: k.i.yashchuk@ust.edu.ua.
ORCID ID: 0000-0002-8606-5790.

**Тімар Станіслав Вікторович,**
аспірант кафедри «Автоматика та телекомунікації» ННІ «ДІІТ» УДУНТ.
Вул. Лазаряна, 2 (к. 129),
м. Дніпро, 49010, Україна.
E-mail: 23056@stud.ust.edu.ua.
ORCID ID: 0009-0008-4044-9079.