УДК 32.019.51:323.28:323.2(477)

ФЕДИК В.Р., здобувач другого рівня вищої освіти Київського університету інтелектуальної власності та права "ОЮА".
ORCID: https://orcid.org/0009-0009-7215-6702.
ДЕНИСЕНКО Г.В., *доктор філософії (Ph.D.),* науковий співробітник НА СБ України.
ORCID: https://orcid.org/0000-0002-0820-9605.

ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ПІДХОДИ ДО УПРАВЛІННЯ РИЗИКАМИ КІБЕРБЕЗПЕКИ НА ОБ'ЄКТАХ КРИТИЧНОЇ ІНФРАСТРУКТУРИ: РЕАГУВАННЯ НА КІБЕРІНЦИДЕНТИ ТА МЕНЕДЖМЕНТ КРИЗОВИХ СИТУАЦІЙ

Анотація. *Робота присвячена аналізу та розробці теоретико-методологічних рекомендацій щодо управління ризиками кібербезпеки на об'єктах критичної інфраструктури. Визначено та описано процес управління кіберризиками, визначено кібернетичні виклики та розглянуто систему управління кіберризиками. Рекомендації стосуються розширення співпраці, вдосконалення систем моніторингу, підготовки персоналу, правового регулювання та участі в міжнародних ініціативах. Ці заходи спрямовані на підвищення ефективності управління кіберризиками для забезпечення національної безпеки.*

Ключові слова:*національна безпека, інформація з обмеженим доступом, кібербезпека, кіберризик, об'єкти критичної інфраструктури, управління ризиками.*

Summary. *The research is devoted to analyzing and developing theoretical and methodological recommendations for cybersecurity risk management at critical infrastructure facilities. The paper defines and describes the cyber risk management process, identifies cyber challenges, and considers the cyber risk management system. Recommendations include expanding cooperation, improving monitoring systems, staff training, legal regulation, and participation in international initiatives. These measures are aimed at improving the effectiveness of cyber risk management to ensure national security.*

Keywords: *national security, classified information, cybersecurity, cyber risk, critical infrastructure, risk management.*

Постановка проблеми. До питання забезпечення захисту та безпеки об'єктів національної критичної інфраструктури сьогодні як ніколи раніше звертаються органи державної влади, науковці та представники вітчизняного бізнесу. В умовах повномасштабної військової інтервенції з боку рф, зокрема активного застосування гібридних методів ведення війни у вигляді перманентних кібератак на об'єкти критичної інфраструктури, виникає нагальна необхідність переосмислення теоретичного підґрунтя про систему безпеки та методів захисту таких об'єктів з метою подальшого застосування на практиці.

Результати аналізу наукових публікацій. Станом на сьогодні законодавчий фундамент у галузі забезпечення кібербезпеки на об'єктах критичної інфраструктури складають такі нормативно-правові акти, як Закон України "Про національну безпеку України" від 21.06.18 р. № 2469-VIII, Закон України "Про основні засади забезпечення кібербезпеки України" від 05.10.17 р. № 2163-VIII, Постанова КМУ "Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури" від 19.06.19 р. № 518,

© Федик В.Р., Денисенко Г.В., 2024

Рішення РНБО “Про Стратегію кібербезпеки України” від 14.05.21 р., Рішення РНБО “Про План реалізації Стратегії кібербезпеки України” від 30.12.21 р.

Стратегією кібербезпеки України від 2021 року визначено ряд стратегічних завдань, серед яких, в тому числі, впровадження ризик-орієнтованого підходу в частині заходів забезпечення кібербезпеки об’єктів критичної інфраструктури та державних органів, зокрема, розроблення методики ідентифікації та оцінки кіберризиків на національному рівні та для секторів критичної інфраструктури держави, врегулювання на законодавчому рівні обов’язковості здійснення періодичної оцінки ризиків на підставі розроблених методик [1].

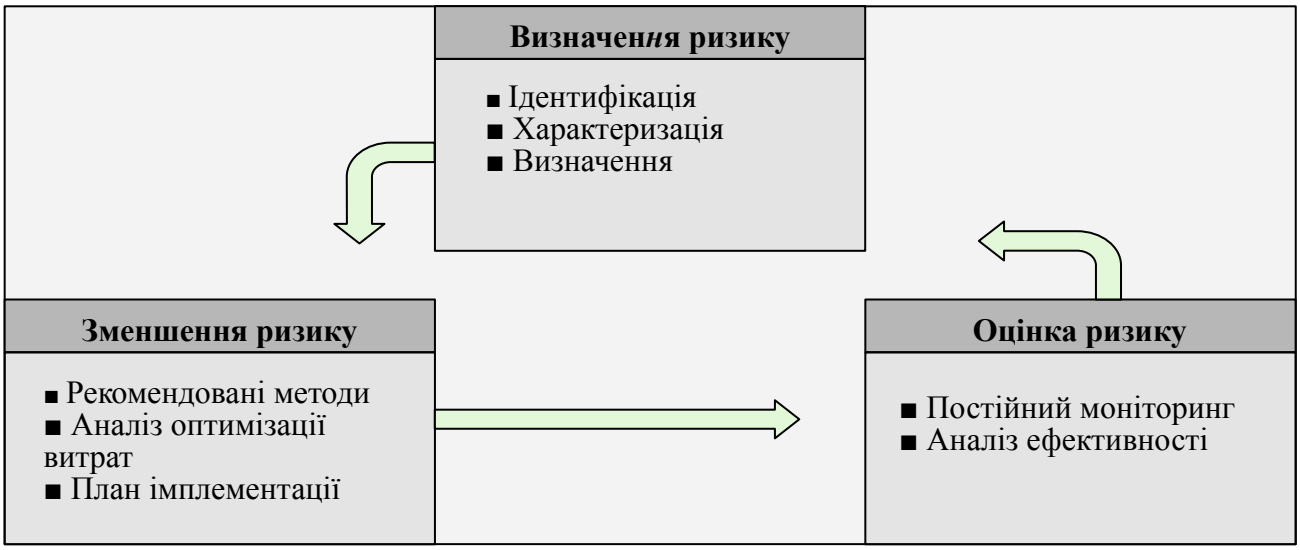
Крім того, така потреба закріплена на законодавчому рівні. Зокрема у пп. 3, ст. 5 Закону України “Про критичну інфраструктуру” визначено те, що до завдань формування і реалізації державної політики у сфері захисту критичної інфраструктури належать створення, впровадження, розвиток та забезпечення функціонування національної системи захисту критичної інфраструктури [2].

Нові умови сьогодення викликають потребу в дедалі глибшому залученні науково-експертного кола для створення рекомендацій щодо оновлення уявлення про систему безпеки, як стан захищеності критичної інфраструктури, а також підходів до захисту, як видів діяльності, що спрямовані на своєчасне виявлення, запобігання і нейтралізацію загроз безпеці об’єктів критичної інфраструктури, а також мінімізацію та ліквідацію наслідків у разі їх реалізації.

Метою статті є удосконалення управління ризиками кібербезпеки на об’єктах критичної інфраструктури.

Виклад основного матеріалу. Управління ризиками кібербезпеки (див. Рис.1) є неодмінною складовою забезпечення безперебійного функціонування інформаційних систем в організаціях будь-якої форми власності. Особливо важливою вона стає в організаціях та державних установах, які для своєї діяльності безпосередньо залежать від мереж і систем інформаційних технологій (далі – ІТ).

Рис. 1. ***Схема управління ризиками***



Так, поділяючи думку колег з КНТЕУ Волосович С., Клапків Л., поняття кіберризик в широкому значенні означає ймовірність загрози інтерактивним цифровим мережам, що використовуються для передачі, модифікації та зберігання інформації (кіберпростору) [3].

Натомість управління ризиками – це процес виявлення вразливостей і загроз інформаційних ресурсів, що використовуються організацією для досягнення цілей і прийняття рішень про те, які контрзаходи, якщо такі є, повинні вживатися задля зниження ризику до прийнятного рівня на основі цінності інформаційного ресурсу для організації [4, с. 297].

Умовно процес управління ризиками можна поділити на три етапи: a) визначення ризиків; b) зменшення ризиків; c) оцінка ризиків.

Більше того, управління ризиками кібербезпеки передбачає ідентифікацію, оцінку, зниження та контроль ризиків, пов'язаних з кіберзагрозами. Це можливо завдяки впровадженню адекватних заходів технічного, організаційного та правового характеру. Наприклад, встановлення захисту мереж, використання сучасних антивірусних програм, вчасне оновлення компонентів безпеки програмного забезпечення, регулярний аудит систем безпеки, навчання персоналу правилам кібербезпеки.

Кібернетичні виклики, з якими сьогодні стикаються державні та недержавні актори, – це складні цільові атаки з боку потужних хакерських об'єднань за якими часто приховуються державні спецслужби; розподілені відмови в наданні послуг (іншими словами DDoS-атаки), які здійснюються за допомогою так званих "ботнетів"[1], що складаються з величезного набору Інтернет-пристроїв, заражених шкідливими програмами та контрольованих злочинними угрупуваннями; застосування кіберзброї, яка здатна виводити з ладу об'єкти критичної інфраструктури. Окреслені виклики призводять до вкрай негативних наслідків для економік окремих регіонів, цілих держав та, в умовах глобалізації, навіть всього розвинутого світу [5, с. 110].

Початковим кроком на першому етапі управління ризиками є ідентифікація ризику та його складових, таких як потенційні загрози, вразливості та ймовірність в рамках чітко визначеної області. Після цього проводиться аналіз впливу цього ризику. Іншими словами, метою визначення ризику є створення повного опису цього ризику та оцінка його важливості на підставі встановлених параметрів – характеризація ризику.

Під час наступного етапу, враховуючи можливий вплив виявлених ризиків, здійснюється прийняття рішень щодо застосування конкретної політики відносно кожного з них. За своєю природою такі заходи можуть бути різноманітними: юридичними або адміністративними, організаційними або процедурними, технічними або технологічними.

Далі розпочинається фаза зменшення ризиків – етап, на якому вкрай важливо визначити пріоритети та раціонально розподілити наявні ресурси. Основною метою цієї фази є планування та реалізація заходів, спрямованих на зменшення виявлених ризиків або контроль над ними, з урахуванням економічної ефективності.

Після впровадження запланованих заходів настає фаза оцінки ризиків, яка включає постійний моніторинг визначеного ризику та аналіз ефективності вжитих заходів. Якщо ризик зменшується до прийнятного рівня, захід вважається успішним. В іншому випадку, або якщо з'являється новий ризик, ініціюється новий цикл управління, починаючи з першої фази – визначення ризиків.

В сучасних моделях державного управління досить часто зустрічається проактивний підхід до врегулювання тих чи інших внутрішніх та зовнішніх проблем.

[1] Відповідно до визначення Кембриджського словника, "ботнет" – це мережа комп'ютерів, що контролюється вірусним програмним забезпеченням без відома власників таких комп'ютерів. Метою ботнетів є секретне самовстановлення та підключення до каналу віддаленого контролю на заражених комп'ютерних пристроях для виконання різного роду злочинних команд.

Дослідники А.М. Грант та С. Дж. Ешфорд вказують на те, що проактивність відображає дії на випередження, які орієнтовані на зміну середовища [6].

В свою чергу, Х. Ву, К. Копер і К. Лам у своїй праці аналізують використання принципу проактивності в діяльності поліції, коли поліцейські не лише реагують на виклики громадян, але й обробляють великі масиви даних з метою попередження можливих правопорушень [7].

На основі аналізу наукової літератури можна сформулювати визначення принципу проактивності в управлінській діяльності. Так, проактивний підхід – це діяльність, що передбачає застосування превентивних і стратегічних заходів з метою формування образу ймовірної події та її наслідків. Загалом, проактивний підхід характеризується стратегічним передбаченням, адаптивністю та готовністю реагувати на виклики ще до того, як вони переростуть в кризове явище.

Поруч із принципом проактивності застосовується системний підхід та активна позиція в управлінській діяльності, спрямована на передбачення та попередження виникнення проблем та негативних наслідків, а також на своєчасну реакцію на зміни у соціальному, економічному, політичному та кібернетичному середовищі. Принцип базується на активному виявленні можливих ризиків, вдосконаленні регулюючих механізмів та використанні інноваційних методів для досягнення позитивних результатів у державному управлінні.

Зокрема, принцип проактивності першочергово передбачає розробку плану реагування на можливі надзвичайні ситуації, регулярну та своєчасну перевірку конфігурації системи, визначення рівня оновлення програмного забезпечення, аналіз ефективності системних та програмних обмежень для запобігання несанкціонованому доступу до кіберсистеми та її ресурсів, а також проведення аудиту системних та мережевих журнальних записів (логів).

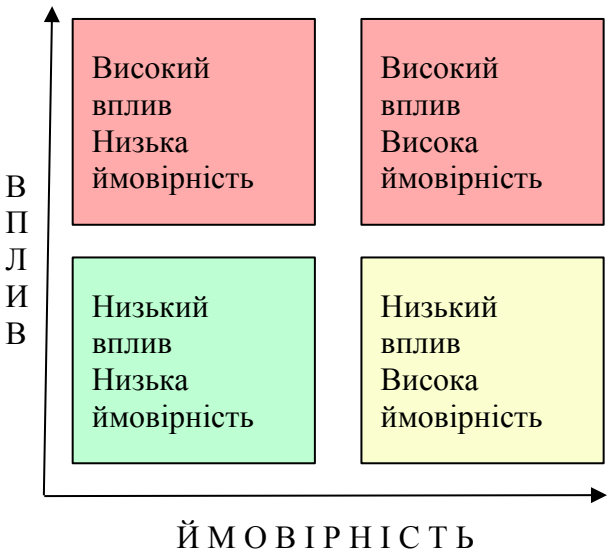
В більшості випадків такий алгоритм дії дозволяє вчасно виявити місце виникнення можливої кібератаки та визначити ресурси, які постраждали. Після цього для відновлення нормального режиму функціонування відповідної кіберсистеми вживаються заходи, передбачені завчасно розробленим планом реагування на надзвичайні ситуації.

До системи управління ризиками входить оцінка ризиків кібербезпеки. Змістовне визначення даному поняттю дає дослідниця Департаменту інформатики Лондонського Королівського коледжу Євгенія Кузьміних, яка підкреслює, що оцінка ризиків інформаційної (кібер) безпеки є важливою частиною практики управління організаціями, що допомагає виявити, кількісно оцінювати та пріоритизовувати ризики з врахуванням критеріїв прийнятності ризиків та цілей, які стосуються конкретної організації чи установи [8].

Зазвичай оцінювання ризиків проводиться методом поєднання анкетування і спільних семінарів за участю експертів з різних дисциплін або в межах окремо утвореної робочої групи всередині організації.

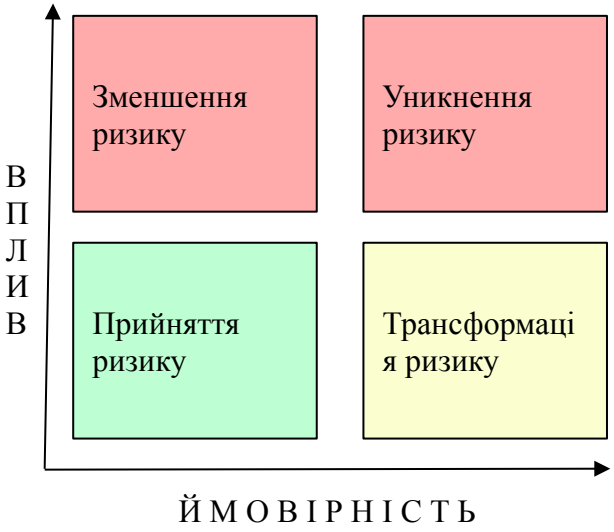
Оцінка ризику, умовно, може мати значення “високий”, “середній” та “низький” рівні, або відповідні числові значення на шкалі в залежності від потрібної точності. Це засновано на суб’єктивній думці експертів щодо ймовірності та впливу конкретного ризику.

Рис. 2. ***Матриця ризиків***



При якісному оцінюванні ризику кібербезпеки, як правило, використовується матриця ризиків, де на горизонтальній вісі відображається ймовірність виникнення конкретного ризику, а на вертикальній - його вплив. У цьому випадку події з високою ймовірністю та високим впливом займають верхній правий кут. Водночас ризики з низькою ймовірністю та низьким впливом розташовані в протилежному куті матриці. Ця концепція базується на тому, що вища експертна оцінка вказує на більш важливий параметр. Такий прямолінійний та інтуїтивно зрозумілий спосіб відображення забезпечує розуміння рівня ризику, особливо для тих, хто приймає рішення, але не є експертами у питаннях безпеки.

Рис. 3. ***Матриця стратегій управління***



У галузі управління ризиками, існують чотири широко розповсюджені стратегії: зменшення ризику; уникнення ризику; прийняття ризику; трансформація ризику.

Для кожного виявленого ризику важливо вибрати відповідну стратегію управління. Серед розповсюджених підходів найбільш популярною є стратегія зменшення ризику (подолання негативних наслідків). Цей підхід передбачає встановлення контролю за завданою шкодою та використання компенсаційних заходів, спрямованих на зниження ймовірності виникнення конкретного ризику або пом'якшення його негативних наслідків до прийнятного рівня. У галузі ІТ такою практикою є регулярне оновлення програмного забезпечення.

Трансформація ризику – це практика страхування (перекладання відповідальності за негативні наслідки при реалізації ризиків на іншу сторону). Прикладами використання цієї стратегії є страхування життя або майна. У сфері ІТ таку роль можуть виконувати Хмарні технології, антивірусні компанії тощо.

Прийняття ризику – це практика свідомого допущення роботи системи з відомим ризиком. Багато ризиків з невеликим впливом просто допускаються. Цей підхід також може використовуватися для ризиків, де зменшення негативних наслідків може бути невиправдано дорогим.

Натомість уникнення ризику передбачає усунення вразливого елементу системи або, у крайньому випадку, навіть відмову від самої системи.

Вибір відповідної стратегії зазвичай приймає керівник або уповноважена особа, іноді у письмовій формі.

Аналіз доповіді Національного інституту стандартів та технологій США дає можливість зробити висновок, що для задоволення організаційних потреб можна

застосовувати три підходи до управління інформаційною безпекою: (a) централізований підхід; (b) децентралізований підхід; (c) гібридний підхід. Відповідальність і повноваження щодо прийняття рішень, пов'язаних з інформаційною безпекою та управлінням ризиками, різняться в кожному підході. Структура управління організацією варіюється в залежності від багатьох факторів. Наприклад, потреб організації/держави; культури та її розмірів; географічного розподілу організаційних операцій, активів та окремих осіб; терпимість до ризиків. Структура управління інформаційною безпекою узгоджена з іншими структурами управління, наприклад управління інформаційними технологіями, з метою забезпечення сумісності з усталеними практиками управління в рамках організації та підвищення її загальної ефективності [9, F 1-2].

Централізований підхід. У централізованих структурах управління повноваження, відповідальність і прийняття рішень покладаються виключно на центральні органи. Центральні органи затверджують політику, процедури та правила для забезпечення загально організаційного залучення до розробки та реалізації стратегій управління ризиками та інформаційної безпеки, рішень щодо ризиків та інформаційної безпеки, створення міжорганізаційних та внутрішньо організаційних механізмів комунікації. Централізований підхід до управління вимагає сильного, добре інформованого центрального керівництва, що забезпечуватиме послідовність дій у всій організації. Централізовані структури управління також передбачають меншу автономію для підпорядкованих організацій, які входять до їх структурних підрозділів.

Децентралізований підхід. У децентралізованих структурах управління безпекою відповідальність та повноваження щодо прийняття рішень належать та делегуються окремим підпорядкованим органам організації, наприклад, агентства/департаменти в межах виконавчого департаменту федерального уряду або бізнес-підрозділів у межах корпорації. Підлеглі органи встановлюють власну політику, процедури та правила для забезпечення загально організаційної участі в розробці та реалізації стратегій управління ризиками та інформаційної безпеки, рішень щодо ризиків та інформаційної безпеки та створення механізмів для комунікації всередині такого органу. Децентралізований підхід до управління інформаційною безпекою вміщує підлеглі органи з різними місійними/бізнес/державними потребами та операційними середовищами за рахунок узгодженості всієї організації в цілому. Ефективність такого підходу значно збільшується за рахунок обміну інформацією, пов'язаною з ризиками, між підлеглими органами, щоб жодний підпорядкований орган не зміг передати ризик іншому без інформованої згоди останнього. Важливо також, щоб підпорядковані органи ділилися інформацією, пов'язаною з ризиками, з центральним органом (організацією), оскільки такі ризики можуть мати вплив на організацію в цілому.

Гібридний підхід. У гібридних структурах управління безпекою повноваження, відповідальність та прийняття рішень розподіляються між центральним органом(організацією) та окремими підпорядкованими органами. Центральний орган встановлює політику, процедури та правила для забезпечення широкої участі організації в частині стратегій управління ризиками та інформаційної безпеки та рішень, що впливають на всю організацію (наприклад, рішення, пов'язані з спільною інфраструктурою або загальними службами безпеки). Підлеглі органи подібним чином встановлюють відповідні політики, процедури та правила для забезпечення їх участі в частині стратегій управління ризиками та інформаційної безпеки та рішень, які є специфічними для їхніх потреб та середовища діяльності. Гібридний підхід до управління вимагає сильного, добре інформованого керівництва не лише в

центральному органі, але й в підпорядкованих йому органах, з метою забезпечення послідовності щодо управління ризиками та безпекою у всій організації.

Висновки.

У зв'язку зі зростаючими загрозами, які виникають у сучасному світі, особливо в контексті кібербезпеки об'єктів критичної інфраструктури, дослідження та розробка ефективних теоретико-методологічних підходів до управління кіберризиками стає проблемою національної безпеки. Актуальність цього питання визначається не лише сучасними тенденціями у кіберпросторі, але й геополітичними реаліями, зокрема військовою інтервенцією рф на території України та застосуванням гібридних методів ведення війни, включаючи кібератаки на об'єкти критичної інфраструктури.

У ході дослідження було визначено, що управління ризиками кібербезпеки на об'єктах критичної інфраструктури вимагає комплексного підходу. На першому етапі, важливо визначити та оцінити ризики, пов'язані з можливими кібератаками. Далі, необхідно розробити та впровадити систему управління кіберризиками, яка охоплює процеси моніторингу, аналізу, виявлення та відповіді на потенційні загрози.

Основні рекомендації передбачають:

– *розширення співпраці та обміну інформацією.* Важливо розвивати співпрацю між державними органами, приватними компаніями та академічними установами для обміну інформацією щодо кіберзагроз та визначення ефективних стратегій управління ризиками.

– *створення ефективних систем моніторингу.* Необхідно вдосконалювати та розширювати системи моніторингу для невідкладного виявлення та реагування на кібератаки, враховуючи нові технології та методи злому.

– *постійна підготовка та тренування персоналу.* Потрібно забезпечення постійної підготовки персоналу, яка охоплює не лише технічні аспекти, але й аспекти управління та взаємодії під час кризових ситуацій.

– *вдосконалення правового регулювання.* Необхідна розробка та впровадження ефективного правового регулювання щодо кібербезпеки, включаючи визначення відповідальності та покарання за кіберзлочини.

– *активна участь в міжнародних ініціативах.* Україна повинна активно брати участь у міжнародних ініціативах з кібербезпеки та спільно з іншими країнами розвивати стандарти та підходи до управління ризиками в цій сфері.

Використана література

1. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про стратегію кібербезпеки України": Указ Президента України від 26.08.21 р. № 447/2021. URL: https://www.president.gov.ua/documents/4472021-40013

2. Про критичну інфраструктуру: Закон України від 16.11.21 р. № 1882-IX. URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text (дата звернення: 31.10.2023).

3. Волосович С., Клапків Л. Детермінанти виникнення та реалізації кіберризиків. *Зовнішня торгівля: економіка, фінанси, право*. 2018. № 3. С. 101-115.

4. Даник Ю.Г., Воробієнко П.П., Чернега В.М. Основи кібербезпеки та кібероборони: підручник. Вид. 2-е, перероб. та доп. Одеса: ОНАЗ, 2019. 320 с.

5. Алексєєв М.М. Аналіз методологічних підходів щодо застосування технологій управління ризиками у сфері кібербезпеки. *Modern Information Technologiesinthe Sphere of Security and Defence*. 2019. № 1(34). С. 109-114.

6. Grant, A.M., Grant, S.J The dynamics of proactivity at work Ashford. *Research in Organizational Behavior*. 2008. № 28. P. 3-34.

7. Wu, X. Koper, C., Lum, C. Measuring the Impacts of Everyday Police Proactive Activities: Tackling the EndogeneityProblem. *Journal of Quantitative Criminology*. 2021. № 4. P. 58-61.

8. Information Security Risk Assessment / I. Kuzminykh, B. Ghita, V. Sokolov, T. Bakhshi. *MDPI Encyclopedia*. 2021. № 1. P. 602-617.

9. National Institute of Standards and Technology U.S. Report. Managing Information Security Risk: Organization Mission and Information System View.

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