УДК 351: 65.012.8:33
DOI https://doi.org/10.32840/1813-3401.2022.4.4

О. М. Возненко
аспірант кафедри теорії та практики управління
Національного технічного університету України
«Київський політехнічний інституту імені Ігоря Сікорського»

УПРАВЛІННЯ РИЗИКАМИ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ: ДЕРЖАВНО УПРАВЛІНСЬКИЙ АСПЕКТ

Стаття присвячена висвітленню питань державного управління ризиками об'єктів критичної інфраструктури (ОКІ). Визначено загальносвітову тенденцію щодо ускладнення проявів таких ризиків. Виділено механізми управління ризиками об'єктів критичної інфраструктури, які поділено на такі групи: правові; організаційні; техніко-технологічні та програмні; фінансові; наукові; військово-оборонні та розвідувально-агентурні; інформаційні; освітні; дипломатичні. Детально охарактеризовано перші три групи. Показано, що, незважаючи на прийняті стратегічні документи та профільний закон, відсутнє визначення понять «ризики критичної інфраструктури» та «ризики об'єктів критичної інфраструктури», що ускладнює їх ідентифікацію та управління такими ризиками. Обґрунтовано необхідність розширення кола юридичних і фізичних осіб, які мають бути залучені до управління ризиками ОКІ. Зокрема, має бути сформована система дорадчих органів, які визначають можливість загроз ОКІ на етапі залучення іноземних інвестицій, підготовки проєктної документації тощо.

Факти атак на ОКІ показують, що зростаюча цифровізація критичної інфраструктури зробила її вкрай вразливою. Паралельно із програмним забезпеченням захисту об'єктів критичної інфраструктури розвивається та поширюється зловмисне програмне забезпечення, яке може нанести національним об'єктам нищівного удару. Це означає, що техніко-технологічні та програмні механізми захисту ОКІ мають іти на випередження появі зловмисного програмного забезпечення, слід створювати бази даних щодо можливих розробників таких програм та відстежувати їх активність.

Показано, що форми, прояви та наслідки ризиків, які наносяться об'єктам критичної інфраструктури, значно різняться між собою, однак викликають значні порушення в роботі важливих для забезпечення життєдіяльності суспільства структур. Це передбачає застосування складних механізмів державного управління такими ризиками, які спрямовані на організацію превентивної роботи щодо захисту об'єктів критичної інфраструктури, ідентифікацію якомога більшого числа таких ризиків, визначення заходів зменшення наслідків матеріалізації ризиків, формування широкого кола інституцій для боротьби з порушеннями в функціонуванні таких об'єктів.

Ключові слова: *об'єкти критичної інфраструктури, державне управління, ризики, механізми управління ризиками об'єктів критичної інфраструктури, загрози об'єктам критичної інфраструктури, інцидент критичної інфраструктури.*

Постановка проблеми. Сьогодні, як ніколи раніше в сучасній історії нашої держави, актуалізуються проблеми захисту об'єктів критичної інфраструктури. Важливість вирішення таких складних завдань потребує від публічних органів реалізації стратегічного підходу до їх ідентифікації та вирішення; визначення ключових факторів, що впливають на появу та посилення загроз об'єктам критичної інфраструктури (ОКІ); розроблення та застосування системи механізмів публічного управління, що може запобігти загрозам та/або зменшити негативні наслідки від їх матеріалізації.

Зазначимо, що в окремі періоди розвитку країни ті чи інші об'єкти, які раніше не вважались об'єктами критичної інфраструктури, можуть бути віднесені до таких. Це зумовлює появу нових ризиків та ускладнення проявів тих, що вже ідентифіковано. Також характерним для нападів на об'єкти критичної інфраструктури є те, що частіше всього не вдається знайти винуватця, за виключенням досить примітивних атак на об'єкти водопостачання, транспортної інфраструктури тощо. Будь-яка операція із залученням високих технологій, кібератаки, може

бути здійснена настільки майстерно, що знайти замовника, а навіть і виконавця, неможливо. Ці обставини зумовлюють необхідність перманентних зусиль органів публічного управління щодо виявлення ризиків, забезпечення безпеки ОКІ, створення системи сучасних інструментів і методів локалізації та упередження виникнення таких загроз.

Аналіз останніх досліджень и публікацій. Проблематика захисту критичної інфраструктури знайшла відображення у роботах Д.С. Бірюкова [1], Д.Г.Бобро [2], О.І.Іваненка, О.М. Суходелі [3], В.І. Франчука [10] та ін. Водночас, існує багато аспектів дослідження цієї складної проблематики, які потребують подальших розробок.

Мета статті. Метою даної публікації є визначення напрямів і механізмів управління ризиками об'єктів критичної інфраструктури в умовах сучасних викликів і загроз.

Виклад основного матеріалу. Поняття ризику трактується в цій роботі відповідно до стандартів ISO 31000:2018 як вплив невизначеності на цілі, що має прояв як відхилення від очікуваного рівня. Це відхилення може бути позитивним, негативним, може стосуватися можливостей і загроз. Ризик зазвичай виражається через джерела ризику, потенційні події, їхні наслідки та їхню ймовірність [13].

Ризик об'єктам критичної інфраструктури ми пропонуємо трактувати як відхилення в роботі таких об'єктів, що завдає загроз населенню, майну, довкіллю, засобам для існування та життєдіяльності, престижу, інформаційній безпеці, території та соціальним відносинам.

Управління ризиками об'єктів критичної інфраструктури передбачає створення низки механізмів. Їх можна умовно поділити на такі групи:

– правові – створення нормативно-правової бази для формування понятійного апарату, правового врегулювання ідентифікації загроз та вирішення питань управління забезпеченням безпеки ОКІ;

– організаційні – виокремлення інституції, яка безпосередньо має «опікуватися» проблемами забезпечення безпеки ОКІ, налагодження її роботи та взаємодії з іншими організаціями та підприємствами, юриичнимита фізичними особами;

– техніко-технологічні та програмні – формування системи технічних, технологічних і програмних чинників, умов і рішень, що унеможливлюють суттєві загрози й ризики ОКІ та/або зменшують негативний вплив від їх матеріалізації;

– фінансові – визначення обсягу та надійних джерел фінансування запобіжних заходів і формування резерву на випадок настання ризикової ситуації незалежно від ступеню навмисності дій щодо ОКІ;

– наукові – наукове обґрунтування принципів, методів, форм, інструментів і заходів превенції та захисту ОКІ;

– військово-оборонні та розвідувально-агентурні – протидія за допомогою спеціальних засобів появі та посиленню ворожих і зловмисних дій, що спрямовані на ОКІ;

– інформаційні – розроблення інформаційних повідомлень і їх розповсюдження щодо форми, проявів і наслідків посилення ризиків загроз ОКІ, дій щодо їх настання, відстеження ворожих інформаційних закликів і загроз;

– освітні – навчання, підготовка, підвищення кваліфікації спеціалістів з управління ризиками КІ;

– дипломатичні – встановлення дипломатичним шляхом границь втручання в соціально та суспільно значимі системи та активи, врегулювання конфліктів, які посилюють загрози ОКІ.

У рамках даної публікації неможливо охарактеризувати всі зазначені механізми управління ризиками ОКІ та їх складові в повному обсязі, тому ми зупинилася на деяких пріоритетних напрямах зосередження зусиль публічних органів щодо управління такими ризиками.

Розглянемо групу факторів формування правового поля для врегулювання проблем, що пов'язані з об'єктами критичної інфраструктури.

Вперше в офіційних документах України термін «критична інфраструктура» вжито у 2005 році в тексті Рекомендацій парламентських слухань з питання розвитку інформаційного суспільства. Зокрема, Кабінету міністрів доручалось підготувати пропозиції щодо визначення та захисту критичних інформаційних інфраструктур [5].

Іншим стратегічним документом, в якому згадувалося про критичну інфраструктуру, була Стратегія національної безпеки України «Україна у світі, що змінюється», затверджена Указом Президента України від 12 лютого 2007 року №105. У цьому документі захист критичної інфраструктури пов'язувався з паливно-енергетичним комплексом, а загрози їй – з еколого-техногенними впливами та зловмисними діями (п.4.3.4). Також акцентувалась увага на забезпеченні інформаційної безпеки (п. 4.3.8), причому, в аспекті систем управління об'єктами критичної інфраструктури [9].

У 2015 році було прийнято Указ Президента України «Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року «Про Стратегію національної безпеки України» (із змінами, внесеними згідно з Указом Президента № 392/2020 від 14.09.2020). Стратегія визначала ключовий слоган національного фронту дій: «Безпека людини – безпека країни» [6].

Зауважимо, що Стратегія національної безпеки України, що була затверджена Указом Президента України від 14 вересня 2020 року № 392/2020, містила і положення щодо загроз критичній інфраструктурі, і напрями дій щодо їх долання [7].

Зокрема, у розділі ІІ серед поточних і прогнозованих загроз національній безпеці та національним інтересам України названо погіршення технічного стану критичної інфраструктури, відсутність інвестицій в її оновлення та розвиток, несанкціоноване втручання в її функціонування, зокрема фізичного і кіберхарактеру, тривалими бойовими діями, а також тимчасовою окупацією частини території України (п. 27) [7].

Розділ ІІІ, в якому висвітлено основні напрями зовнішньополітичної та внутрішньополітичної діяльності держави для забезпечення її національних інтересів і безпеки, містив як одне із завдань створення ефективної системи безпеки та стійкості критичної інфраструктури, що заснована на чіткому розподілі відповідальності її суб'єктів та державно-приватному партнерстві (п. 48) [7].

У «Заключних положеннях» визначено, що Стратегія національної безпеки має бути основою для розроблення інших стратегічних документів, зокрема стратегії енергетичної безпеки, стратегії інформаційної безпеки, стратегії кібербезпеки [7].

У Стратегії забезпечення державної безпеки від 16 лютого 2022 року № 56/2022 [8] об'єкти критичної інфраструктури згадані серед об'єктів забезпечення державної безпеки нарівні з державним суверенітетом, конституційним ладом і територіальною цілісністю країни, що свідчить про високий рівень їх значимості. Констатовано, що має місце високий рівень загроз ОКІ з боку суб'єктів розвідувально-підривної діяльності, погіршення технічного стану такої інфраструктури (п.19). Отже, до основних завдань державної політики належить удосконалення контррозвідувального забезпечення об'єктів критичної інфраструктури від впливу суб'єктів розвідувально-підривної діяльності; протидія встановленню контролю ворожих сил над стратегічно важливими об'єктами критичної інфраструктури та окремими підприємствами (п. 24) [8].

У листопаді 2021 року було прийнято Закон України «Про критичну інфраструктуру» (далі – Закон) [4]. Безперечним кроком уперед було розмежування в Законі ненавмисних загроз безпеці ОКІ (інцидентів безпеки КІ), навмисних загроз ОКІ (несанкціоноване втручання) та кризових ситуацій, пов'язаних з їх функціонуванням.

Також визначено завдання та функції основних суб'єктів забезпечення безпеки критичної інфраструктури. Зокрема, в ст. 22 Закону встановлено, що «Кабінет Міністрів України встановлює вимоги щодо управління ризиками безпеки на об'єктах критичної інфраструктури І категорії критичності… та встановлює вимоги щодо управління ризиками безпеки» [4]. Національний банк України відповідає за означені питання щодо банків, інших осіб, які здійснюють діяльність на ринках фінансових послуг, платіжних організацій, учасників платіжних систем, операторів послуг платіжної інфраструктури. Кабінет Міністрів України затверджує перелік об'єктів критичної інфраструктури, включених до Реєстру, страхових ризиків настання кризової ситуації на таких об'єктах, які підлягають страхуванню, а також мінімальний ліміт відповідальності (у разі страхування відповідальності перед третіми особами). Реєстр об'єктів критичної інфраструктури у сфері фінансових послуг та інші питання погоджуються з Національним банком України. Також було встановлено, що під час дії воєнного стану, а також протягом 12 місяців після його припинення чи скасування повноваження уповноваженого органу у сфері захисту критичної інфраструктури України … здійснюються Державною службою спеціального зв'язку та захисту інформації України [4].

У Законі також обґрунтовано необхідність проведення науково-дослідних робіт щодо впливу новітніх і проривних технологій на формування нових індикаторів потенційних ризиків та загроз об'єктам критичної інфраструктури, а також підготовку на основі результатів наукових досліджень рекомендацій для операторів об'єктів критичної інфраструктури.

Висновки і пропозиції. Водночас зауважимо, що поняття «ризики критичної інфраструктури» не знайшло відображення в цьому Законі, хоча в преамбулі було дано тлумачення таким важливим поняттям, як безпека критичної інфраструктури, інцидент безпеки критичної

інфраструктури, кризова ситуація, національна система захисту критичної інфраструктури, несанкціоноване втручання, стійкість.

Стосовно організаційного механізму, то зазначимо, що до управління ризиками та забезпечення безпеки об'єктів критичної інфраструктури України залучено органи управління, центральні та місцеві органи виконавчої влади, органи місцевого самоврядування, військово-цивільних адміністрацій, оператори критичної інфраструктури, різні дорадчі комітети та комісії. Водночас, далеко не всі зазначені органи діють в рамках превенції загроз об'єктам критичній інфраструктурі. Превентивні заходи щодо зменшення ризиків функціонування об'єктів критичної інфраструктури мають бути реалізовані ще на стадії залучення іноземних інвестицій, як це демонструє досвід Ізраелю.

В Ізраелі при Міністерстві фінансів створено консультативний комітет з метою оцінки аспектів національної безпеки іноземних інвестицій (далі – Комітет) на чолі з головним економістом Міністерства фінансів (або старшим представником за його дорученням). В складі Комітету передбачена участь високопоставлених представників Ради національної безпеки (далі – РНБ) та Міністерства оборони. Комітет також має право запрошувати представників відомств з питань оборони, зовнішніх відносин і кібербезпеки для участі в обговореннях, а також додаткових представників відповідних міністерств. Він збирається на вимогу будь-кого з його членів. Метою його створення є розгляд та оцінка іноземних інвестицій з позиції дотримання національної безпеки та національних інтересів і надання підготовлених документів регуляторам. Цей орган діє виключно як дорадчий. У положенні визначено, що регулятори можуть приймати інші рішення, ніж ті, які рекомендовані Комітетом [14]. Водночас, вплив оцінок, які зроблено Комітетом, на прийняття рішень щодо інвестицій є значним. Вважаємо, що в Україні також має бути створено низка дорадчих органів, які мають аналізувати загрози та ризики об'єктам критичної інфраструктури на стадіях залучення інвестицій, підготовки проєктної документації та освоєння капітальних інвестицій в об'єкти критичної інфраструктури.

Сучасний світ підготував багато техніко-технологічних рішень щодо ідентифікації, упередження та ліквідації загроз ОКІ. Водночас, активні процеси диджиталізації спричиняють майже стільки ж проблем, скільки вирішують.

Зазначимо, що факти атак на ОКІ показують, що зростаюча цифровізація критичної інфраструктури зробила її вразливою, як ніколи раніше. У зв'язку з наростанням числа кібератак у наукових колах вже ведуть мову про настання «кібер-зими».

Загальновідомим прикладом такого нападу є Stuxnet, кібератака на іранські ядерні об'єкти, що була виявлена трохи більше десяти років тому. Під час цієї атаки комп'ютерна система влучила в системи керування Siemens, змусив іранські центрифуги розпастися на частини. Водночас, комп'ютерні засоби злочинців майстерно «запевнили» системи моніторингу, що все гаразд [11].

У травні 2020 року Shodan, спеціалізована пошукова система, яка каталогізує пристрої, підключені до Інтернету, знайшла понад 112 000 промислових систем керування з відкритими портами – по суті, віртуальними дверима у широкий світ [11]. Їх кількість значно посилилась в умовах дистанційної роботи, що спричинена пандемією та іншими форс-мажорними обставинами.

У розвинутих країнах світу створено величезну кількість промислових систем контролю (Industrial control systems, ICS), які відслідковують стан об'єктів, починаючи від кондиціонеру і до потужних турбін [15].

Контроль здійснюється і в системі віддаленого доступу, який спрямовано на перевірку осіб, які входить в автоматизовану систему віддалено, а також створення віртуального буферу («jump box») та спрямування трафіку через сервери тощо. Розроблено, популяризуються та використовуються такі ресурси, як BACnet, DNP3 (Distributed Network Protocol), EtherNet/IP, IEC 60870-5-104, MELSEC-Q, Modbus, S7 Communication та ін.

Однак зауважимо, що чим більше відкритих «зон», доступ до яких має місце в управлінні складними системами, тим більше ризиків їх взламу та здійснення відповідних кібернетичних атак. А це напряму загрожує національно значущим ресурсам, активам і об'єктам. Про це переконливо свідчать дані табл. 1.

У таблиці 1 наведено загрози таким відкритим системам[1]. Зокрема, EternalBlue Vulnerable – кодове ім'я експлойта, який експлуатує комп'ютерну уразливість у Windows-реалізації протоколу SMB, до розробки якого, як вважається, причетно Агентство національної без-

[1] Для опису таких загроз використовувались відкриті джерела інформації.

Таблиця 1

Огляд впливу небезпек на Інтернет деяких країн

	Країна				
	Україна:	**Німеччина**	**Франція**	**В'єтнам**	**Білорусь**
Відкриті порти	1,781,591	35,245,284	11,618,222	4,757,848	219,379
Промислові системи контролю (Industrial Control Systems)	368	5,031	5,584	636	484
Зламані (скомпрометовані) бази даних	836	1,212	737	195	6
BlueKeep Unpatched	861	1664	837	621	300
Вразливі до Heartbleed	3,067	8,513	7,204	3,042	88
Уразливі до EternalBlue	103	238	279	125	2
Аутентифікація SMB[1]	6618 (89,5%)	63615 (92,2%)	42,104 (24,8%)	20720 (87,4%)	378 (92,6%)

Примітка: Вибірка зроблена за [12]

пеки (США). Вперше використання EternalBlue було зареєстровано в квітні 2017 року, коли програма-бекдор DoublePulsar вразило більш ніж 200 тисяч комп'ютерів протягом кількох днів.

BlueKeep, що уражає Microsoft Windows, потенційно може спустошити мережі як хробак, який без сторонньої допомоги поширюється від комп'ютера до комп'ютера. Спалах BlueKeep може стати цільовою загрозою майнінгу криптовалюти.

Heartbleed (CVE-2014-0160) – це помилка у криптографічному програмному забезпеченні OpenSSL, що дозволяє несанкціоновано зчитувати інформацію в пам'яті на сервері, зокрема для вилучення його закритого ключа. Інформація про вразливість була опублікована у квітні 2014 року, і на той момент кількість вразливих веб-сайтів оцінювалася в півмільйона, а це становило близько 17% захищених веб-сайтів Інтернету.

Фактично, паралельно із програмним забезпеченням захисту об'єктів критичної інфраструктури розвивається software різних кримінальних структур, які можуть нанести національним об'єктам нищівного удару. Це означає, що техніко-технологічні та програмні механізми захисту ОКІ мають іти на випередження появі зловмисного програмного забезпечення. Доцільно створювати бази даних щодо можливих розробників таких програм та здійснювати моніторинг їх активності.

Об'єктами ударів, і не лише ракетних, а й терористів й інших осіб, можуть стати об'єкти управління та надання публічних послуг, водопостачання та водовідведення, енергозабезпечення, організації забезпечення продовольством, об'єкти хімічної та фармацевтичної промисловості (зокрема, виготовлення вакцин), біологічні лабораторії, структури, що надають інформаційні та фінансові послуги, електронні комунікації, підприємства та організації транспортного забезпечення, оборони, державної безпеки, правопорядку, судові органи, цивільного захисту населення та територій, служби порятунку та науково-дослідні інституції.

Отже, прояви ризиків, які наносяться об'єктам критичної інфраструктури, є різними, значимими, вони викликають значні порушення в роботі важливих для забезпечення життєдіяльності суспільства структур. Це ускладнює державне управління такими ризиками, що передбачає розроблення системи механізмів, які б всебічно розгортали превентивно-запобіжну роботу щодо захисту об'єктів критичної інфраструктури, зменшували наслідки матеріалізації ризиків, формували широкий фронт боротьби з порушеннями в функціонуванні таких об'єктів.

Список використаної літератури:

1. Бірюков Д. С. Про доцільність та особливості визначення критичної інфраструктури в Україні: *Аналітична записка*. URL: http://www.niss.gov.ua/articles/1026/
2. Бобро Д. Г. Методологія оцінки рівня критичності об'єктів інфраструктури. *Strategic Priorities. 2016. № 3(40). С. 77-85.*
3. Зелена книга з питань захисту критичної інфраструктури в Україні : зб. матеріалів між-

[1] Server Message Block (SMB) забезпечує аутентифікований механізм процесу внутрішнього зв'язку для спільного використання файлів або ресурсів (файлів, папок, принтерів) на сервері. SMB надає клієнтам можливість редагувати файли, видаляти їх, ділитися файлами, переглядати мережі, друкувати служби тощо через мережу.

нар. експерт. нарад / упоряд. Д.С. Бірюков, С. І. Кондратов ; за заг. ред. О.М. Суходолі. К. : НІСД, 2016. 176 с.
4. Про критичну інфраструктуру. Закон України від 16.11.2021 №1882-IX. URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text
5. Про Рекомендації парламентських слухань з питань розвитку інформаційного суспільства в Україні. Постанова Верховної Ради України від01.12.2005№3175-IV.URL:https://zakon.rada.gov.ua/laws/show/3175-15#Text
6. Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року. Указ Президента України «Про Стратегію національної безпеки України». URL:https://zakon.rada.gov.ua/laws/show/287/2015#Text
7. Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року «Про Стратегію національної безпеки України» Указ Президента України від 14.09.2020 р. №392/202. URL: https://zakon.rada.gov.ua/laws/show/392/2020#Text
8. Про рішення Ради національної безпеки і оборони України від 30 грудня 2021 року "Про Стратегію забезпечення державної безпеки". Указ Президента України від 16.02.2022 № 56/2022. URL: https://zakon.rada.gov.ua/laws/show/56/2022#Text
9. Стратегія національної безпеки України «Україна у світі, що змінюється», затверджена Указом Президента від 12 лютого 2007 року №105 (втратила чинність). URL:https://zakon.rada.gov.ua/laws/show/105/2007#Text
10. Франчук В. І., Пригунов П. Я., Мельник С. І. Безпека об'єктів критичної інфраструктури в Україні: організаційно-нормативні проблеми та підходи. Соціально-правові студії. 2021. Випуск 3(13). С. 142–148.
11. A cyber-attack on an American water plant rattles nerves. The breach shows the dangers of connecting critical infrastructure to the internet. The Economist. Feb 9th 2021. URL: https://www.economist.com/united-states/2021/02/09/a-cyber-attack-on-an-american-water-plant-rattles-nerves.
12. Internet Exposure Observatory. URL:https://exposure.shodan.io/#/]
13. ISO 31000:2018(en). Risk management – Guidelines. URL:https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en
14. Resolution B.372 by the Ministerial Committee on National Security Affairs (State Security Cabinet), dated October 30, 2019: Establishment of a Process and Mechanism for Evaluating National Security Aspects of Foreign Investments. URL:https://www.gov.il/en/departments/policies/foreign-investment-board (an unofficial and unbinding translation to English)
15. Shodan. Сайт. URL:https://www.shodan.io/explore/category/industrial-control-systems

Voznenko O.M. Risk management of critical infrastructure objects: public administration aspect

The article is devoted to the coverage of public risk management of critical infrastructure objects (CIO). The global trend towards complicating the manifestations of such risks has been determined. The mechanisms of risk management of critical infrastructure objects are divided into the following groups: legal; organizational; technical, technological and IT; financial; scientific; military and intelligence agents; informational; educational; diplomatic. The first three groups are described in detail. It is shown that, despite the adopted strategic documents and the relevant law, there is no definition of the "risks of critical infrastructure" concept and "risks of critical infrastructure objects ", which complicates their identification and management of such risks. The need to expand the range of legal entities and individuals who should be involved in CIO risk management is substantiated. A system of advisory bodies should be formed, which determine the possibility of threats to the CIO at the stage of attracting foreign investment, preparing project documentation, etc.

The facts of the attacks on the CIO show that the growing digitalization of critical infrastructure has made it extremely vulnerable. Along with the progress in critical infrastructure protection software development, malware is evolving and spreading that can deal a crushing blow to national facilities. This means that the technical, technological and software mechanisms for protecting CIO should go ahead of the emergence of malware, you should create databases on possible developers of such programs and track their activity.

It is shown that the forms, manifestations, and consequences of risks that are inflicted on critical infrastructure objects differ significantly among themselves, but cause significant disruptions in the work of structures important for ensuring the vital activities of society. This involves the application of complex mechanisms of state management of such risks, which are aimed at organizing preventive work on the protection of critical infrastructure objects, identifying the largest possible number of such risks, determining measures to reduce the consequences of the materialization of risks, forming a wide range of institutions to combat violations in the functioning of such objects.

Key words: *critical infrastructure facilities, public administration, risks, risk management mechanisms for critical infrastructure, threats to critical infrastructure, critical infrastructure incident.*