КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№1 (9), 2020
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2020.9.170181
УДК 004.056.53

Гнатюк Сергій Олександрович
д.т.н., доцент, заступник декана Факультету кібербезпеки, комп'ютерної та програмної інженерії
Національний авіаційний університет, Київ, Україна
ORCID: 0000-0003-4992-0564
s.gnatyuk@nau.edu.ua,

Сидоренко Вікторія Миколаївна
к.т.н., доцент кафедри безпеки інформаційних технологій
Національний авіаційний університет, Київ, Україна
ORCID: 0000-0002-5910-0837
v.sydorenko@ukr.net

Сотніченко Юлія Олексіївна
здобувач PhD
Національний авіаційний університет, Київ, Україна
ORCID: 0000-0002-1281-9238
yu.sotnichenko@gmail.com

БАЗОВІ АСПЕКТИ ЗАХИСТУ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ НА ОБ'ЄКТАХ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ

Анотація. Стрімкий розвиток інформаційно-комунікаційних технологій спричинив збільшення уразливостей різноманітних мереж, систем та об'єктів і значно ускладнив забезпечення їх надійного захисту й безпеки. Усі ці чинники обумовили те, що провідні держави світу стали приділяти значну увагу кібербезпеці та кіберзахисту об'єктів критичної інформаційної інфраструктури держави. Проте, не дослідженим залишаються питання захисту різних видів інформації з обмеженим доступом (зокрема, конфіденційної інформації) на об'єктах критичної інфраструктури. З огляду на це, у роботі проведено аналіз існуючих підходів провідних держав світу до захисту конфіденційної інформації на об'єктах критичної інфраструктури. У результаті аналізу було встановлено, що на сьогодні немає комплексних, багатофункціональних методик захисту конфіденційної інформації на об'єктах критичної інформаційної інфраструктури. Крім того, в роботі розроблено класифікацію об'єктів критичної інформаційної інфраструктури за вимогами безпеки інформації, яка за рахунок визначення виду оброблювальної інформації, можливих режимів доступу та категорії критичності, дозволяє забезпечити єдність підходів щодо захисту цих об'єктів, що відносяться до різних типів, включаючи інформаційні системи, автоматизовані системи управління та інформаційно-телекомунікаційні мережі.

Ключові слова: кібербезпека, критична інформаційна інфраструктура, інформаційно-комунікаційні технології, конфіденційна інформація, вимоги безпеки, класифікація.

1. ВСТУП

Сучасні загрози інформаційній безпеці (кібербезпеці [1]) характеризуються асиметричністю та гнучкістю, а самі кібератаки уже давно перестали бути самоціллю – вони стали ефективним засобом для досягнення широкого спектру цілей, різноманітність яких обмежена лише уявою та фантазією порушників. Відповідно до [2], усі кібератаки можна поділити на три категорії – це кібератаки, що впливають на конфіденційність, цілісність чи доступність (КЦД) інформації, а всі інші види є похідними від них. Цей факт підтверджується і самим визначенням кібератаки у

законі [3], де *кібератака* – це спрямовані (навмисні) дії в кіберпросторі, які здійснюються за допомогою засобів електронних комунікацій та спрямовані на досягнення однієї або сукупності таких цілей: порушення КЦД електронних інформаційних ресурсів, що обробляються (передаються, зберігаються) в комунікаційних та / або технологічних системах, отримання несанкціонованого доступу до таких ресурсів; порушення безпеки, сталого, надійного та штатного режиму функціонування комунікаційних та / або технологічних систем; використання комунікаційної системи, її ресурсів та засобів електронних комунікацій для здійснення кібератак на інші об'єкти кіберзахисту. Крім того, відповідно до [3], *основними об'єктами кібербезпеки та кіберзахисту* є об'єкти критичної інфраструктури (КІ) та об'єкти критичної інформаційної інфраструктури (КІІ) держави.

Постановка проблеми. Що стосується забезпечення базових властивостей безпеки інформації на об'єктах КІ та КІІ, то згідно до постанови [4], впровадження заходів до кіберзахисту дозволить підприємствам, установам та організаціям, які відповідно до законодавства віднесені до об'єктів КІ, забезпечити захист від кібератак, запобігти порушенню КЦД своїх інформаційних ресурсів, порушенню режиму сталого функціонування об'єкта КІ. Проте не дослідженим лишаються питання визначення та захисту конфіденційної інформації на об'єктах КІ та КІІ держави – саме цим важливим аспектам і присвячена ця стаття.

Аналіз останніх досліджень і публікацій. Забезпечення КЦД на об'єктах КІ держави є одними з базових вимог із забезпечення кіберзахисту об'єктів КІ. Відповідно до [4], перелік основних заходів, які повинні бути впроваджені під час створення комплексної системи захисту інформації (системи інформаційної безпеки) об'єкта КІІ, мають містити такі дії:

– на об'єкті КІ повинен бути визначений перелік інформаційних, програмних та апаратних ресурсів об'єкта КІІ, рівень їх критичності та можливий рівень наслідків у випадку порушення КЦД інформації, недоступності служб об'єкта КІІ, порушення функціонування компонентів об'єкта;

– на об'єкті КІІ передача даних бездротовими мережами повинна здійснюватися виключно захищеними з'єднаннями із забезпеченням її конфіденційності та цілісності. Забороняється використання на об'єкті КІІ об'єкта КІ технологій Wi-Fi та Bluetooth;

– для захисту даних, які передаються через незахищене середовище між віддаленими користувачами, адміністраторами та об'єктом КІІ, між компонентами об'єкта, між об'єктом КІІ та іншими (зовнішніми) ІТС, необхідно використовувати захищені з'єднання із забезпеченням конфіденційності та цілісності цих даних.

У проєкті Закону України «Про критичну інфраструктуру та її захист» [5] вперше описуються *основні принципи розбудови та функціонування державної системи захисту КІ,* до якої належать: координованість, єдність методологічних засад, державно-приватна взаємодія, забезпечення конфіденційності, міжнародне співробітництво. Також запропоновано визначення, описані права, обов'язки та завдання операторів КІ. Серед основних завдань операторів КІ слід виділити п. 14, статті 31 – захист інформації про системи управління, зв'язку, фізичну та кібернетичну безпеку, забезпечення відповідно до встановлених законодавством вимог конфіденційності інформації під час оброблення даних про об'єкти КІ.

Не дивлячись на те, що 29 серпня 2019 проєкт закону було відхилено, сам проект спричинив ажіотаж та бурхливе обговорення. Наприклад, у [6] висловлена ціла низка небезпек, а саме: СБУ зможе отримувати доступ до конфіденційної інформації операторів об'єктів КІ, серед яких можуть бути не лише державні органи, але й

приватні суб'єкти; будь-яка інформація «щодо об'єктів КІ», а також «технологічна інформація» (дані, що обробляються в системах управління технологічними процесами об'єктів КІ) буде обмеженою в доступі. Це суттєво звузить право громадян на доступ до публічної інформації, зокрема, до інформації про підприємства, що надають комунальні послуги, послуги у сфері виробництва продуктів, харчування, охорони здоров'я тощо.

Зважаючи на те, що операторами об'єктів КІ можуть бути не лише державні органи, але й приватні суб'єкти, надання автоматичного доступу до будь-якої, в першу чергу конфіденційної інформації, яка ними зберігається, може становити втручання в підприємницьку діяльність. Відповідно до статті 7 Закону України [7], конфіденційна інформація про особу може поширюватися у визначеному нею порядку за їхнім бажанням відповідно до передбачених ними умов, тобто, за згодою такої особи. Поширення конфіденційної інформації без згоди допускається лише в інтересах національної безпеки, економічного добробуту та прав людини у визначеному законом порядку. Зазначений проєкт [5] передбачає лише повноваження щодо доступу до інформації з обмеженим доступом, але не встановлює порядок такого доступу.

Крім цього, проєкт [5] передбачає введення до Закону України «Про інформацію», *нового виду інформації – «технологічної».* До неї відноситимуться дані, що обробляються (приймаються, передаються, зберігаються) в системах управління технологічними процесами об'єктів КІ. Відповідно до пропонованих змін, технологічна інформація вважатиметься конфіденційною. Водночас, до технологічної інформації заборонено відносити інформацію «про випадки виведення з ладу або порушення функціонування об'єкта КІ, які можуть справити негативний вплив на стан національної безпеки і оборони України, навколишнього природного середовища, заподіяти майнову шкоду та/або становити загрозу для життя і здоров'я людей».

Відповідні зміни до статті 21 Закону України «Про інформацію» передбачають доповнення визначення «конфіденційна інформація» – інформація про фізичну особу, технологічна інформація, а також інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень. Водночас, чинне визначення конфіденційної інформації дозволяє підприємствам, установам та організаціям, які не є суб'єктами владних повноважень, самостійно визначати, яка інформація про їх діяльність належить до конфіденційної, тому додаткове дублювання поняття «технологічна інформація» до визначення конфіденційної інформації не є необхідним. У випадку, коли йдеться про «технологічну інформацію» суб'єктів владних повноважень, доцільно відносити її до таємної або службової за умови дотримання відповідних вимог ч. 2 статті 6 Закону України «Про доступ до публічної інформації»:

1) виключно в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою запобігання заворушенням чи злочинам, для охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя;

2) розголошення інформації може завдати істотної шкоди цим інтересам;

3) шкода від оприлюднення такої інформації переважає суспільний інтерес в її отриманні [6-7].

Мета статті. Метою даної статті є аналіз існуючих підходів провідних держав світу до захисту конфіденційної інформації на об'єктах КІІ та розробка класифікації об'єктів КІІ відповідно до вимог безпеки інформації (кібербезпеки).

ISSN 2663 - 4023

2. ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ

Якщо процедура захисту *критично важливих об'єктів інфраструктури* (КВОІ) є основою будь-якої взаємопов'язаної стратегії, обмін інформацією є її життєвою силою. Коректний обмін інформацією сприяє досягненню захисту КВОІ (ЗКВОІ) на всіх рівнях і на всіх етапах – це ключовий чинник, на якому базуються державно-приватні партнерства. Як показує міжнародний досвід [8], ефективність обміну інформацією про ЗКВОІ залежить від двох основних чинників:

– можливості провідних агентств створювати довіру серед зацікавлених сторін;

– забезпечення адекватних рівнів захисту конфіденційної інформації, обмін якою є необхідним та дозволеним відповідно до угод ЗКВОІ.

Створення захищеного середовища для обміну інформацією залежить від встановлення чітких правових і операційних меж для захисту спільно використовуваних конфіденційних даних. При розробці таких меж головною метою, є сприяння поширенню інформації для цілей ЗКВОІ, з урахуванням необхідності дотримання чинних документів, що стосуються прав на недоторканність приватного життя і захисту даних.

3. РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

3.1. Базові аспекти захисту конфіденційної інформації на об'єктах КІІ

Відповідно до статті 8 Хартії основних прав ЄС [8-9], *персональні дані* «повинні оброблятися тільки для певних цілей і на основі згоди відповідної особи або будь-якої іншої законної підстави, встановленої законом. Кожен має право на доступ до даних, які були зібрані стосовно нього, а також мати право на їх виправлення».

Визначення *«конфіденційної інформації, що відноситься до ЗКВОІ»*, наведено у Директиві Ради ЄС 2008/114/ЕС наступним чином: «Факти про критично важливу інфраструктуру, які в разі її розкриття можуть бути використані для планування і реалізації дій з метою порушення або руйнування КВОІ» [8, 10]. У статті 9, тієї ж Директиви висловлюється «особливий принцип», згідно з яким «держави-члени, Комісія і відповідні наглядові органи повинні забезпечувати, щоб конфіденційна інформація, пов'язана із захистом європейської КВОІ, яка надається державам-членам або самій Комісії, не використовувалася для будь-яких цілей, крім ЗКВОІ. Що стосується операторів КВОІ приватного сектора, то вони будуть обмінюватися даними про інциденти або чинники уразливості тільки в тому випадку, якщо отримають відповідні запевнення в тому, що розкриття конфіденційної інформації не зробить на ці об'єкти негативного впливу (наприклад, це не дасть конкурентам переваги або не буде використано проти них державними органами з метою, відмінною від ЗКВОІ).

Не вся інформація, пов'язана з КВОІ, повинна розглядатися конфіденційно. Аналогічно, як і не вся інформація, яка вважається «конфіденційною», заслуговує однакових рівнів захисту. Обмеження на поширення інформації, пов'язаної з КВОІ, можуть приймати різні форми і бути більш або менш суворими в залежності від конкретних обставин та цілей певного типу обміну інформацією. Наприклад, у Новій Зеландії установлено базовий принцип, згідно з яким інциденти повинні розглядатися на найнижчому рівні конфіденційності в якості способу раннього і ефективного поширення КВО серед всіх респондентів, які відповідають за зниження його впливу.

Захист інформації, пов'язаної з КВОІ, має починатися з прийняття законодавства, згідно з яким вихід конфіденційних даних може становити загрозу для національної безпеки або громадської безпеки. На практиці існує ряд методів і рішень для захисту розповсюдження конфіденційної інформації. Як правило, вони зосереджені навколо таких основних взаємодоповнюючих процедур:

1) Допуск і перевірка благонадійності

Уряди можуть надати допуски до секретної інформації для ключових сторін, яким необхідний доступ до конфіденційної інформації, пов'язаної з КВОІ. Згідно з Директивою [10], «будь-яка особа, яка обробляє секретну інформацію відповідно до цієї Директиви від імені держави-члена або Комісії, повинна мати відповідний рівень перевірки благонадійності. Платформи для обміну інформацією можуть також застосовувати спеціальні критерії відбору для прийому нових членів, наприклад, на основі згоди існуючих учасників або у формі фонової перевірки, співбесіди з державними органами, що відповідають за платформу тощо. У деяких випадках може виникнути небажання учасників ділитися інформацією взагалі, через залучення до платформи членів правоохоронних органів. Для стратегій по ЗКВОІ важливо враховувати ці потенційні труднощі і знаходити способи їх подолання.

2) Системи колірного кодування

Ці системи засновані на принципі, згідно з яким той, хто надає інформацію, визначає ступінь її розповсюдження. Протокол світлофора (TLP) застосовує цю концепцію позначаючи інформацію одним з чотирьох кольорів:

– *червоний:* тільки для іменованих одержувачів;

– *бурштиновий:* обмежений тираж, очікується, що відправник визначить межі і умови обміну інформацією;

– *зелений:* інформація може поширюватися всередині певної спільноти, але не може бути загальнодоступною (наприклад, в Інтернеті) або поширюватися за межами певної спільноти;

– *білий:* необмежена циркуляція інформації.

Перевага TLP полягає в його зручності для користувача та у встановленні чітких меж між обов'язками відправника і одержувача.

3) Електронні інструменти

Щоб забезпечити обмін інформацією, деякі платформи використовують електронні інструменти, такі як *екстранет* – це телекомунікаційна мережа, що використовує Інтернет-технології, метою якої є сприяння обміну даними між основним суб'єктом і двома або більше партнерами, що знаходяться географічно віддалено. Партнери повинні пройти аутентифікацію, щоб мати можливість переглядати мережеву інформацію.

3.2. Національні підходи провідних держав світу, щодо захисту конфіденційної інформації, що відноситься до КВОІ

Австралія. створена Урядом Австралії в 2003 році, довірена мережа обміну інформацією (TISN) є основним механізмом взаємодії інформації між бізнесом і урядом. Відповідно до [11], TISN забезпечує безпечне середовище, в якому власники та оператори КВОІ існуючих галузевих груп, регулярно зустрічаються для обміну інформацією, співпраці, вирішенню проблем безпеки та безперервності бізнесу. Галузеві групи TISN включають: банківську справу і фінанси, зв'язок, енергетику, продукти харчування і продовольство, охорону здоров'я, транспорт і водопостачання. Крім того, існують спеціалізовані форуми (міжсекторні групи за інтересами), які допомагають у тимчасовому вивченні комплексних питань, а також експертно-

консультативна група, що відповідає за організацію стабільності. Координаційне і стратегічне керівництво для TISN відбувається у Консультативній раді з критично важливої інфраструктури (CIAC), яка складається з голів кожної з груп TISN, головних представників уряду Австралії та відповідних установ.

Франція. Директиви і плани, прийняті в рамках національної системи забезпечення безпеки життєдіяльності (SAIV), згідно [12] класифікуються за рівнями конфіденційного захисту. Будучи відправником або одержувачем, оператор КВОІ забезпечує знищення секретних документів, які йому більше не потрібні, особливо коли: засекречений документ переглянутий або скасований; «життєво важлива точка» скасовується; «життєво важлива зона» скасовується; оператор втрачає свій статус «життєво важливого оператора».

Канада. Однією з цілей національної стратегії та плану дій по ЗКВОІ є своєчасний обміну інформацією та захисту між партнерами КВОІ. Для досягнення цієї мети уряд закликає створювати Інформаційний портал КВОІ (CI Gateway) [13], який буде розміщуватися в домені громадської безпеки Канади. Уряд Канади прагне успішного запуску CI Gateway, гарантуючи, що членство у ньому охопить десять ключових секторів КВОІ та інші зацікавлені сторони, заохочуючи до участі у членстві і сприяючи його використанню галузевими мережами для обміну інформацією і передовим досвідом, а також для спільної роботи над специфічними проектами. Що стосується надання доступу до конфіденційної інформації зацікавленим сторонам з приватного сектора, то переважна частина інформації, зібраної канадським співтовариством з безпеки та розвідки, є конфіденційною і може передаватися тільки особам з відповідним допуском [8]. Державна безпека Канади прагне співпрацювати з провідними федеральними департаментами та агентствами, щоб збільшити кількість зацікавлених сторін в приватному секторі.

Російська Федерація: Незалежно від типу системи, до якої належить об'єкт критично важливої інформації (КВІ), основним ресурсом, схильним до зміни у кіберпросторі, є інформація. Основними завданнями системи безпеки об'єктів КВІ згідно [14], є запобігання неправомірному доступу, знищення, перекручення, блокування, копіювання та поширення інформації, що захищається, інші неправомірні дії по відношенню до такої інформації, недопущення впливу на технічні засоби обробки інформації, в результаті якого може бути порушено і (або) припинено функціонування об'єкта КВІ. Від систем безпеки також потрібно відновлення функціонування об'єктів КВІ. Виходячи з цього значимі об'єкти КВІ є об'єктами захисту інформації, до яких повинні бути пред'явлені вимоги з безпеки інформації та реалізовані заходи щодо захисту інформації. Кожному визначеному об'єкту КВІ повинно бути присвоєно клас безпеки. У роботі [14] відображені пропозиції до класифікації об’єктів КІІ за основними вимогами безпеки інформації, а саме рівня конфіденційності інформації Російської Федерації, категорію значимості об'єкта КВІ та режим доступу до інформації. У якій представлені об'єкти КВІ, що включають 15 класів в складі 5 груп. За можливим рівнем конфіденційності виділяють: відкриту інформацію, конфіденційну інформацію, інформацію з грифом «таємно», інформацію з грифом «цілком таємно», інформацію з грифом «особливої важливості». За можливим режимом доступу виділяють: об’єкти з однаковими правами доступу до інформації та об’єкти, які потребують розмежування прав доступу. За категорією значимості об’єкта КВІ поділяють на три рівні критичності. Для визначення комплексного показника важливості того чи іншого об'єкта КІ розроблена «Методика віднесення об'єктів державної і недержавної власності до критично важливих об'єктів (КВО) для

національної безпеки Російської Федерації». Відповідно до [15], в Методиці використовується три групи показників: значимість об'єкта для економіки країни; нанесення шкоди престижу держави та можливі загрози населенню і територіям. За захист конфіденційної інформації відповідає друга категорія показників П6-П9, а саме П7 – розкриття державних таємниць, конфіденційної науково-технічної та комерційної інформації. У роботі [16], запропоновано класифікацію КВОІ за вимогами фізичного захисту з використанням методів кластерного аналізу. Забезпечення надійного функціонування ОІ КВО досягається реалізацією на об'єкті комплексу засобів і систем інформаційної безпеки (для забезпечення КЦД) і його фізичного захисту від несанкціонованого доступу. Не існує реально двох ОІ, які б володіли однаковими властивостями інформаційної безпеки та фізичного захисту. Різниця визначається ступенем цінності оброблюваної інформації, її конфіденційністю, штатною кількістю користувачів, застосуванням засобів фізичного захисту і т.д. Важливу роль при цьому відіграють призначення і характеристики КВО. Однак деякі ОІ КВО мають близькі за деякими критеріями властивостями або подібні ознаки. Це дозволяє провести розбиття всієї множини ОІ на непересічні групи і розробити для кожної групи типові вимоги безпеки. Типові вимоги будуть виступати в якості основи для формування вимог інформаційної безпеки та фізичного захисту до конкретної реалізації ОІ.

3.3. Захист конфіденційної інформації авіаційної безпеки

ICAO розробила загальні керівні принципи захисту інформації про безпеку польотів, пов'язаної з авіацією. Ці принципи описані у [17], повинні обмежувати тих осіб, які потребують використання конфіденційної інформації при виконанні своїх обов'язків а, отже, мають право доступу до неї. До конфіденційної інформації про авіаційну безпеку повинні застосовуватися захисні заходи, а ступінь захисту повинна бути вказана або державою, або відповідними суб'єктами, враховуючи національні вимоги щодо захисту конфіденційної інформації, встановлені відповідними органами. Захисні заходи можуть також знадобитися при ідентифікації, класифікації, отриманні, збереженні, розкритті, поширення або утилізації конфіденційної інформації з авіаційної безпеки.

Конфіденційна інформація з авіаційної безпеки повинна зберігатися належним чином, коли вона не використовується, задля запобігання несанкціонованого доступу. Наприклад, використання шаф безпеки, кімнат, що замикаються або сейфів можна також вважати способом забезпечення захисту. Електронні копії конфіденційних документів з авіаційної безпеки повинні бути еквівалентно захищені. Державам і відповідним суб'єктам слід вжити заходів для забезпечення того, щоб уповноважені особи, які мають доступ до конфіденційної інформації з авіаційної безпеки, не розкривали таку інформацію стороннім особам. Наприклад, слід розглянути питання про те, щоб уповноважені особи підписали «угоду про нерозголошення», перш ніж їм буде дозволений доступ до такої інформації.

Кожен раз, коли необхідно обмінюватися інформацією між державами, країни повинні чітко виділяли конфіденційну інформацію з авіаційної безпеки та повідомляти про будь-які конкретні вимоги до захисних заходів, які повинні застосовуватися до передачі такої інформації іншим державам. Держави, які отримують конфіденційну інформацію про авіаційну безпеку, повинні застосовувати необхідні захисні заходи для запобігання несанкціонованого використання або розголошення.

ISSN 2663 - 4023

3.4. Класифікація об'єктів КІІ за вимогами безпеки інформації

На основі пропозицій [14] та напрацювань авторів у цьому напрямку, було запропоновано класифікацію об'єктів КІІ України за основними вимогами безпеки. Розглянемо зазначену класифікацію більш детально.

За можливими видами інформації в Україні виділяють: відкриту інформацію (ВІ) та інформацію з обмеженим доступом (ІзОД), яка у свою чергу поділяється на: таємну інформацію (ТІ), Службову інформацію (СІ) та конфіденційну інформацію (КІ).

За можливим режимом доступу виділяють: об'єкти з однаковими правами доступу до інформації (О) та об'єкти, які потребують розмежування прав доступу (Р).

За категорією критичності об'єктів КІІ, відповідно до [5], виділяють:

І категорія критичності – «критично важливі об'єкти» (1КВО) це об'єкти, які мають загальнодержавне значення, розгалужені зв'язки та значний вплив на іншу інфраструктуру. Зазначені об'єкти включаються до Національного переліку об'єктів критичної інфраструктури, формуються вимоги щодо забезпечення їх захисту;

ІІ категорія критичності – «життєво важливі об'єкти» (2ЖВО), порушення функціонування яких призведе до виникнення кризової ситуації регіонального значення. Зазначені об'єкти включаються до Національного переліку об'єктів критичної інфраструктури, формуються вимоги щодо розмежування завдань й повноважень органів державної влади та операторів критичної інфраструктури, спрямованих на забезпечення їх захисту та відновлення функціонування;

ІІІ категорія критичності – «важливі об'єкти» (3ВО), пріоритетом захисту яких є забезпечення швидкого відновлення функцій за рахунок диверсифікації та резервів. Відповідальність за стійкість функціонування об'єктів несуть оператори при встановлених законодавством вимогах щодо взаємодії із органами державної влади;

ІV категорія критичності – звичайні об'єкти (4ЗО), безпосередній захист яких є відповідальністю оператора, який повинен мати план реагування на кризову ситуацію.

Запропонована класифікація об'єктів КІІ за вимогами безпеки інформації представлена в табл. 1.

Таблиця 1

Класифікація об'єктів КІІ за вимогами безпеки інформації

	Види інформації						
	ТІ		**СІ**		**КІ**		**ВІ**
Вимоги безпеки інформації	1-О-1КВО	1-Р-1КВО	2-О-1КВО 2-О-2ЖВО 2-О-3ВО 2-О-4ЗО	2-Р-1КВО 2-Р-2ЖВО 2-Р-3ВО 2-Р-4ЗО	3-О-1КВО 3-О-2ЖВО 3-О-3ВО 3-О-4ЗО	3-Р-1КВО 3-Р-2ЖВО 3-Р-3ВО 3-Р-4ЗО	4-О-1КВО 4-О-2ЖВО 4-О-3ВО 4-О-4ЗО

Остаточна класифікація об'єктів КІІ за вимогами безпеки інформації включає 22 класи у складі 4 груп.

Перша група складається з двох класів для об'єктів КІІ з інформацією рівня «таємна інформація» з однаковими (клас 1-О-1КВО) або різними (клас 1-Р-1КВО) правами доступу користувачів. Ці об'єкти КІІ повинні відповідати першій категорії значущості незалежно від фактичної категорії.

Друга група складається з восьми класів для об'єктів КІІ з інформацією рівня не вище рівня «секретної інформації» з однаковими (класи 2-О-1КВО, 2-О-2ЖВО, 2-О-3ВО, 2-О-4ЗО) або різними (класи 2-Р-1КВО, 2-Р-2ЖВО, 2-Р-3ВО, 2-Р-4ЗО) правами доступу користувачів відповідно до І-ІV категорії критичності.

Третя група складається з восьми класів для об'єктів КІІ з інформацією рівня не вище рівня «конфіденційної інформації» з однаковими (класи 3-О-1КВО, 3-О-2ЖВО, 3-О-

3ВО, 3-О-4ЗО) або різними (класи 3-Р-1КВО, 3-Р-2ЖВО, 3-Р-3ВО, 3-Р-4ЗО) правами доступу користувачів відповідно до I-IV категорії критичності.

Четверта група містить чотири класи (4-О-1КВО, 4-О-2ЖВО, 4-О-3ВО, 4-О-4ЗО) об'єктів КІІ з відкритою загальнодоступною інформацією для всіх зареєстрованих користувачів відповідно до I-IV категорії критичності.

4. ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Таким чином, у цій роботі було проаналізовано відомі підходи провідних держав світу до захисту конфіденційної інформації на об’єктах КІІ. У результаті аналізу було встановлено, що на сьогодні немає комплексних, багатофункціональних та універсальних методик захисту конфіденційної інформації на об’єктах КІІ.

Розроблено класифікацію об’єктів КІІ за вимогами безпеки інформації, яка за рахунок визначення виду оброблювальної інформації, можливих режимів доступу та категорії критичності, дозволяє забезпечити єдність підходів щодо захисту об'єктів КІІ, що відносяться до різних типів, включаючи інформаційні системи, автоматизовані системи управління та інформаційно-телекомунікаційні мережі.

Запропонована класифікація об'єктів КІІ за вимогами безпеки інформації містить 22 класи в складі 4 груп. Кожна група може містити два, чотири або вісім класів об’єктів КІІ з однаковими або різними правами доступу користувачів відповідно до однієї із чотирьох категорій критичності.

ПОДЯКА

Дослідження було проведено в рамках наукового проєкту молодих учених МОН України (номер державної реєстрації 0120U101400), що виконується на базі Науково-дослідної лабораторії протидії кіберзагрозам в авіаційній галузі Національного авіаційного університету.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] ISO/IEC 27032, Information technology – Security techniques – Guidelines for cybersecurity, 2012, 50 p.
[2] Гнатюк С. «Кібертероризм: історія розвитку, сучасні тенденції та контрзаходи», Безпека інформації, 2013, т. 19, № 2, с. 118-129.
[3] Закон України «Про основні засади забезпечення кібербезпеки України», 05.10.2017 р., № 2163-VIII, Режим доступу: http://zakon0.rada.gov.ua/laws/show/2163-19
[4] Постанова Кабінету Міністрів України «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури», 19.06.2019 р., № 518, Інд. 49.
[5] Проект Закону України «Про критичну інфраструктуру та її захист», Режим доступу: http://search.ligazakon.ua/l_doc2.nsf/link1/JH7YW00A.html (17.07.2020).
[6] Обговорення проекту Закону України «Про критичну інфраструктуру та її захист» в Міністерстві економічного розвитку і торгівлі України. Режим доступу: https://www.ppl.org.ua/nadpovnovazhennya-dlya-sbu-i-obmezhennya-dostupu-do-informaci %D1%97-zakonoproekt-pro-kritichnu-infrastrukturu-vid-minekonomrozvitku.html (17.07.2020).
[7] Закон України «Про доступ до публічної інформації», 13.01.2011 р. № 2939-VI.
[8] Защита критически важных объектов инфраструктур от террористических атак: сборник передового опыта, Составлен ИДКТК и КТУ ООН, 2018, 152 с. Режим доступа: https://www.un.org/sc/ctc/wp-content/uploads/2019/07/RUS-compendium-final.pdf

[9] Хартія основних прав Європейського Союзу: [пер. А. Пендак], Ніццький договір та розширення Європейського Союзу, К., 2001, 124 с.
[10] Council Directive on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (CD 2008/ 114/EC) [Електронний ресурс], Режим доступу: https://eur-lex.europa.eu/legalcontent/EN/TXT/? uri=uriserv%3AOJ.L .2008.345.01.0075.01.ENG (17.07.2020).
[11] Довірена мережа обміну інформацією. Режим доступу: https://tisn.gov.au/
[12] Франция 2014, Генеральная межведомственная инструкция по безопасности жизнедеятельности, Генеральный секретариат по обороне и национальной безопасности (№6600 / SGDSN / PSE / PSN). [Електронний ресурс], Режим доступа: http://circulaire.legifrance.gouv.fr/pdf/2014/01/cir_37828.pdf (17.07.2020).
[13] Інформаційний шлюз критично важливої інфраструктури. Режим доступу:: https://cigatewav.ps.gc.ca/lavouts/pscbranding / trms- eng.pdf (17.07.2020).
[14] Михалевич И.Ф. Вопросы классификации объектов критической информационной инфраструктуры по требованиям безопасности информации, XIII Всероссийское совещание по проблемам управления ВСПУ-2019, с. 2587-2590.
[15] Методика віднесення об'єктів державної і недержавної власності до критично важливих об'єктів для національної безпеки Російської Федерації (скасована на підставі листа МНС Росії від 30.12.2019 N 43-7134-11).
[16] Мелех О.В., Максимович Е.П., Фісенко В.К. Класифікація критично важливих об'єктів інформатизації за вимогами фізичного захисту з використанням методів кластерного аналізу, Искусственный интеллект, 2010, № 4, с. 666-677.
[17] ICAO Aviation Security Manual, Doc 8973, Restricted, 2019.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (9), 2020
ISSN 2663 - 4023

Sergiy O. Gnatyuk
DSc, Associate Professor, Vice-Dean of the Faculty of Cybersecurity, Computer and Software Engineering
National Aviation University, Kyiv, Ukraine
ORCID: 0000-0003-4992-0564
s.gnatyuk@nau.edu.ua,

Viktoriia M. Sydorenko
PhD, Associate Professor of IT-Security Academic Department
National Aviation University, Kyiv, Ukraine
ORCID: 0000-0002-5910-0837
v.sydorenko@ukr.net

Yuliia O. Sotnichenko
PhD Student
National Aviation University, Kyiv, Ukraine
ORCID: 0000-0002-1281-9238
yu.sotnichenko@gmail.com

BASIC ASPECTS OF CONFIDENTIAL INFORMATION SECURITY IN CRITICAL INFORMATION INFRASTRUCTURE OBJECTS

Abstract. The rapid development of information and communication technologies has increased the vulnerabilities of various networks, systems and objects as well as made it much more difficult to ensure their reliable protection and security. All these factors have led to the fact that the world's leading countries have begun to pay considerable attention to cybersecurity and critical information infrastructure protection. However, the protection of various types of information with restricted access (in particular, confidential information) at critical infrastructure objects remains unexplored. With this in mind, the paper analyzes the existing approaches of the world's leading countries to the confidential information protection at critical infrastructure. The analysis revealed that today there are no comprehensive, multifunctional methods of protecting confidential information at critical information infrastructure. In addition, the classification of critical information infrastructure objects according to information security requirements is developed. This classification by determining the type of processing information, possible access modes and criticality category, allows to ensure unity of approaches to protection of these objects belonging to different types, including information systems, automated control systems and information-telecommunication networks.

Keywords: cybersecurity; critical information infrastructure; information-communication technology; confidential information; security requirements; classification.

REFERENCES (TRANSLATED AND TRANSLITERATED)

[1] ISO/IEC 27032, Information technology – Security techniques – Guidelines for cybersecurity, 2012, 50 p.
[2] Gnatyuk S. «Cyberterrorism: history of development, modern trends and countermeasures», Bezpeka informatsii, 2013, vol. 19, № 2, pp. 118-129 (in Ukrainian).
[3] Law of Ukraine «About basic issues of cybersecurity ensuring in Ukraine», 05.10.2017 p., № 2163-VIII, Access mode: http://zakon0.rada.gov.ua/laws/show/2163-19
[4] Decision of Cabinet of Ministries of Ukraine «About General requirements for cybersecurity of critical infrastructures objects», 19.06.2019, № 518, Ind. 49.
[5] Project of Law of Ukraine «About critical infrastructure and its security», Access mode: http://search.ligazakon.ua/l_doc2.nsf/link1/JH7YW00A.html (17.07.2020).
[6] Discussion on Project of Law of Ukraine «About critical infrastructure and its security» Access mode: https://www.ppl.org.ua/nadpovnovazhennya-dlya-sbu-i-obmezhennya -dostupu-do-informaci%D1%97-zakonoproekt-pro-kritichnu-infrastrukturu-vid-minekonomrozvitku.html (17.07.2020).
[7] Law of Ukraine «About access to public information», 13.01.2011, № 2939-VI.

[8] Critical infrastructures objects security against terroristic attacks, UN, 2018, 152 p. Access mode: https://www.un.org/sc/ctc/wp-content/uploads/2019/07/RUS-compendium-final.pdf
[9] Charter on main rules of EU, Nice agreement and extension of EU, 2001, 124 p.
[10] Council Directive on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (CD 2008/ 114/EC), Access mode: https://eur-lex.europa.eu/legalcontent/EN/TXT/? uri=uriserv%3AOJ.L_ .2008.345.01.0075.01.ENG (17.07.2020).
[11] Trusted network for information exchange. Access mode: https://tisn.gov.au/
[12] France 2014, General instruction on life safety, General Secretary on defense and national security (№6600 / SGDSN / PSE / PSN). Access mode: http://circulaire.legifrance. gouv.fr/ pdf/2014/01/cir 37828.pdf (17.07.2020).
[13] Information gateway of critical infrastructure. Access mode: https://cigatewav.ps.gc.ca/lavouts/pscbranding / trms- eng.pdf (17.07.2020).
[14] Mikhalevych I.F. Issues of critical information infrastructure objects classification by information security, XIII All Russian meeting on management problems VSPU-2019, pp. 2587-2590 (in Russian).
[15] Technique for categorization the state and private objects to critical objects for national security of Russian Federation (annualized 30.12.2019 N 43-7134-11).
[16] Melekh O.V., Maksymovych E.P., Fisenko V.K. Classification of critical objects of informatisation by requirements of physical protection by claster analysis, Artificial Intelligence, 2010, № 4, pp. 666-677 (in Russian).
[17] ICAO Aviation Security Manual, Doc 8973, Restricted, 2019.