DOI: 10.18372/2410-7840.19.11900
УДК 004.056 (045)

АНАЛІЗ БАЗОВОЇ ТЕРМІНОЛОГІЇ І НЕГАТИВНИХ НАСЛІДКІВ КІБЕРАТАК НА ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНІ СИСТЕМИ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ДЕРЖАВИ

Юрій Дрейс

У статті проводиться аналіз базової термінології і різновиди негативних наслідків до яких може привести кібератака на інформаційно-телекомунікаційні системи об'єктів критичної інфраструктури в різних країнах світу, в т.ч. і в Україні, наприклад у разі витоку інформації з обмеженим доступом або державних інформаційних ресурсів, які обробляються в цих системах. Виявлено додаткову необхідність враховувати й інші тяжкі наслідки для національних інтересів від розголошення відомостей, що становлять саме державну таємницю в результаті можливої реалізації такої кібератаки при формуванні переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави. Представлені пропозиції до формування єдиного класифікатора негативних наслідків кібератак на інформаційно-телекомунікаційні системи об'єктів критичної інфраструктури держави з урахуванням обробки в цих системах й інших видів інформації з обмеженим доступом, таких як конфіденційної (в.ч. персональні дані) і службової інформації.
Ключові слова: *кібератака, інформація з обмеженим доступом, інформаційно-телекомунікаційна система, критична інфраструктура держави, негативні наслідки, оцінювання шкоди.*

Актуальність. Різноманітні способи застосування кібератак у розвідувально-підривній діяльності іноземних спецслужб або під час ведення кібервійни країною-агресором направлені саме на зупинку у роботі, втрату контролю або виведення з ладу інформаційних систем, які забезпечують першочергові потреби людини, суспільства і держави (води, тепла, світла, транспорту, банківських операцій, систем зв'язку тощо) задля породження хаосу, посилення суспільної напруги, дестабілізації країни в цілому. Через збільшення кількості випадків успішних кібератак, у більшості провідних країнах світу з метою зведення до єдиної системи важливих об'єктів й найуразливіших інформаційно-телекомунікаційних систем та мереж, втрата або порушення сталого функціонування яких призведе до значних або навіть непоправних негативних наслідків для національної безпеки і оборони, введено термін «критична інфраструктура».

В Україні, з огляду на останні події, кількість реалізованих кібератак значно збільшується і оцінка уразливості та потенційних наслідків припинення або руйнування об'єктів інфраструктури стає однією із основних функцій держави. І тому, в інтересах забезпечення національної безпеки виникає питання необхідності підвищення ефективності використання та захисту державних інформаційних ресурсів (ДІР), особливо інформації з обмеженим доступом, яка обробляється в інформаційно-телекомунікаційних системах об'єктів критичної інфраструктури, втрата якої може завдати й інших (додаткових) тяжких наслідків. Так як в основу порядку формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави з метою їх першочергового захисту від кібератак покладено принцип «негативний наслідок – критична інфраструктура», тому питання визначення ступеня тяжкості негативних наслідків й величини завданої шкоди та інших можливих витрат на обмеження доступу та захист інформації з обмеженим доступом від її витоку, до якого може призвести кібератака, є актуальним.

Аналіз останніх досліджень і постановка завдання. Аналіз праць [1-8] вітчизняних науковців (Д. Бірюков, С. Кондратов, О. Суходоля, С. Гнатюк, О. Юдін) виявив наявність значної кількості проблем у сфері захисту критичної інфраструктури держави, починаючи з відсутності базових необхідних понять, наприклад «захист критичної інфраструктури» та «захист критичної інформаційної інфраструктури», нормативного-правового забезпечення даної сфери (закону, концепції, стратегії, доктрини тощо) і до необхідності формування державної системи забезпечення захисту критичної інфраструктури у цілому. Але всі вони зазначають про те, що існуючий складний стан кіберпростору України вимагає віднесення захисту критичної інфраструктури до пріоритетних напрямів протидії загрозам національній безпеці задля попередження можливої потенційної шкоди державі та усунення негативних наслідків від їх реалізації.

Метою статті є аналіз потенційних негативних наслідків, до яких може призвести кібератака

на інформаційно-телекомунікаційну систему об'єкта критичної інфраструктури, яка обробляє інформацію з обмеженим доступом (ІзОД) (або ДІР) з метою подальшої уніфікації їх у єдиний класифікатор негативних наслідків кібератак при проведенні процедури оцінювання шкоди національній безпеці України у разі її витоку.

Основна частина дослідження. Основне базове поняття *інформаційно-телекомунікаційної системи* (ІТС) як сукупності інформаційних та телекомунікаційних систем, які у процесі обробки інформації діють як єдине ціле, наведено у Законі України «Про захист інформації в інформаційно-телекомунікаційних системах» [9], який регулює відносини у сфері захисту інформації в інформаційних, телекомунікаційних та ІТС. Цим законом [9] наведені й інші поняття, необхідні для проведення досліджень у даній сфері такі як:

– *телекомунікаційна система* (ТС) – сукупність технічних і програмних засобів, призначених для обміну інформацією шляхом передавання, випромінювання або приймання її у вигляді сигналів, знаків, звуків, рухомих або нерухомих зображень чи в інший спосіб;

– *інформаційна (автоматизована) система* (ІС(АС)) – організаційно-технічна система, в якій реалізується технологія обробки інформації з використанням технічних і програмних засобів;

– *захист інформації в системі* – діяльність, спрямована на запобігання несанкціонованим діям щодо інформації в системі;

– *несанкціоновані дії щодо інформації в системі* – дії, що провадяться з порушенням порядку доступу до цієї інформації, установленого відповідно до законодавства;

– *обробка інформації в системі* – виконання однієї або кількох операцій, зокрема: збирання, введення, записування, перетворення, зчитування, зберігання, знищення, реєстрації, приймання, отримання, передавання, які здійснюються в системі за допомогою технічних і програмних засобів;

– *знищення інформації в системі* – дії, внаслідок яких інформація в системі зникає;

– *витік інформації* – результат дій, внаслідок яких інформація в системі стає відомою чи доступною фізичним та/або юридичним особам, що не мають права доступу до неї;

– *користувач інформації в системі* (користувач) – фізична або юридична особа, яка в установленому законодавством порядку отримала право доступу до інформації в системі;

– *доступ до інформації в системі* – отримання користувачем можливості обробляти інформацію в системі;

– *порядок доступу до інформації в системі* – умови отримання користувачем можливості обробляти інформацію в системі та правила обробки цієї інформації;

– *комплексна система захисту інформації* (КСЗІ) – взаємопов'язана сукупність організаційних та інженерно-технічних заходів, засобів і методів захисту інформації;

– *криптографічний захист інформації* (КЗІ) – вид захисту інформації, що реалізується шляхом перетворення інформації з використанням спеціальних (ключових) даних з метою приховування/відновлення змісту інформації, підтвердження її справжності, цілісності, авторства тощо;

– *технічний захист інформації* (ТЗІ) – вид захисту інформації, спрямований на забезпечення за допомогою інженерно-технічних заходів та/або програмних і технічних засобів унеможливлення витоку, знищення та блокування інформації, порушення цілісності та режиму доступу до інформації;

– *блокування інформації в системі* – дії, внаслідок яких унеможливлюється доступ до інформації в системі;

– *порушення цілісності інформації в системі* – несанкціоновані дії щодо інформації в системі, внаслідок яких змінюється її вміст;

– *власник системи* – фізична або юридична особа, якій належить право власності на систему;

– *володілець інформації* – фізична або юридична особа, якій належать права на інформацію.

Також законодавчо визначено [9], що об'єктом захисту в ІТС є інформація, яка обробляється в ній, та програмне забезпечення, яке призначено для обробки цієї інформації.

Наразі загальними вимогами та організаційними засадами забезпечення захисту інформації в інформаційних, телекомунікаційних та ІТС є «Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» [10], які містять поняття автентифікації та ідентифікації, і конкретизують інформацію, яка підлягає захисту в ІТС, а саме [10]: відкрита інформація, яка належить до ДІР, а також відкрита інформація про діяльність суб'єктів владних повноважень, військових формувань, яка оприлюднюється в Інтернеті, інших глобальних інформаційних мережах і системах або передається телекомунікаційними мере-

жами (відкрита інформація); конфіденційна інформація (у т.ч. персональні дані); службова інформація; інформація, яка становить державну або іншу передбачену законом таємницю (таємна інформація); інформація, вимога щодо захисту якої встановлена законом.

На виконання плану заходів щодо захисту ДІР затвердженого Розпорядженням КМУ №1135 від 05.11.2014 року та з метою підвищення рівня захисту інформаційних ресурсів, що обробляється в ІТС об'єктів критичної інфраструктури держави, визначено механізм, за яким відбуватиметься формування їх переліку. Зокрема, розроблено «Порядок формування переліку ІТС об'єктів критичної інфраструктури держави» [11] (далі – Порядок), який затверджено Постановою КМУ№ 563 від 23.08.2016 року за якою державні органи, органи центральної виконавчої влади, інші заінтересовані державні органи повинні сформувати та подати Державній службі спеціального зв'язку та захисту інформації (Держспецзв'язку) пропозиції для формування переліку ІТС об'єктів критичної інфраструктури держави [11]. У відповідності до цих пропозицій заінтересовані органи мають визначити негативні наслідки та вказати їх умовне позначення, до яких може призвести кібератака на ІТС із приведеного у порядку переліку із зазначенням виду інформації, яка обробляється. І якщо вказати, що в ІТС обробляється ІзОД, тоді виникає питання щодо необхідності врахування й інших тяжких наслідків, які визначаються при обмеженні доступу до такої інформації як державна таємниця [12], та зазначення їх у пропозиціях, до яких може призвести кібератака на ІТС у разі її витоку. У Порядку [11] містяться такі поняття та визначення як:

– *заінтересовані органи* – державні органи, органи місцевого самоврядування, органи управління Збройних Сил, інших військових формувань, утворених відповідно до законів, правоохоронні органи, у власності чи розпорядженні яких є об'єкт критичної інфраструктури держави та/або до сфери управління яких належать (перебувають в управлінні) підприємства, установи та організації, що є власниками (розпорядниками) такого об'єкта);

– *кібератака* – несанкціоновані дії, що здійснюються з використанням інформаційно-комунікаційних технологій та спрямовані на порушення конфіденційності, цілісності і доступності інформації, яка обробляється в інформаційно-телекомунікаційній системі, або порушення сталого функціонування такої системи);

– *критична інфраструктура* – сукупність об'єктів інфраструктури держави, які є найбільш важливими для економіки та промисловості, функціонування суспільства та безпеки населення і виведення з ладу або руйнування яких може мати вплив на національну безпеку і оборону, природне середовище, призвести до значних фінансових збитків та людських жертв);

– *об'єкти критичної інфраструктури* – підприємства та установи (незалежно від форми власності) таких галузей як енергетика, хімічна промисловість, транспорт, банки та фінанси, інформаційні технології та телекомунікації (електронні комунікації), продовольство, охорона здоров'я, комунальне господарство, що є стратегічно важливими для функціонування економіки і безпеки держави, суспільства та населення).

Також, судячи зі змісту положень пп. 4, 5 Порядку [11], під *критичною інформаційною інфраструктурою держави* (КІІД) слід розуміти включені до переліку ІТС об'єктів критичної інфраструктури, що захищаються від кібератак у першу чергу (пріоритетно) власником (розпорядником) таких систем відповідно до законодавства у сфері захисту інформації та кібербезпеки.

У додатку цього Порядку [11] приведені пропозиції до формування переліку ІТС об'єктів критичної інфраструктури держави (табл. 1), які після погодження з СБУ надаються заінтересованими органами до Адміністрації Держспецзв'язку. Окремо слід зазначити про наявність «Методичних рекомендацій державним експертам з питань таємниць щодо визначення підстав для віднесення відомостей до державної таємниці та ступеня її секретності» (далі – Методичні рекомендації) [12], які також містять поняття *інших тяжких наслідків* (ІТН) (негативні зміни у зазначених сферах (головним чином у сферах зовнішніх відносин, державної безпеки і охорони правопорядку), які відбулися чи можуть відбутися внаслідок розголошення конкретних відомостей, що становлять державну таємницю і які не піддаються економічному обрахунку у кількісному (вартісному) виразі) та вказують на необхідність їх визначення при встановленні ступеня секретності за приведеним у п. 3.2 переліком відповідно до певної категорії (табл. 2). На основі проведеного аналізу [1-13] експертних думок, наукових праць та відповідних нормативно-правових документів побудовано порівняльний аналіз негативних наслідків кібератак на КІІД у різних країнах світу (табл. 3).

Таблиця 1

Пропозиції до формування переліку ІТС об'єктів критичної інфраструктури держави

Порядковий номер	*Назва інформаційно-телекомунікаційної системи, форма власності*	*Найменування власника (розпорядника) інформаційно-телекомунікаційної системи*	*Вид інформації, що обробляється в інформаційно-телекомунікаційній системі (відкрита, конфіденційна, службова або таємна інформація згідно із Законом України "Про інформацію")*	*Негативні наслідки, до яких може призвести кібератака на інформаційно-телекомунікаційну систему**	*Дані про осіб (адміністраторів безпеки), відповідальних за функціонування інформаційно-телекомунікаційної системи (прізвище, ім'я, по батькові, номер телефону, адреса електронної пошти, тощо)*	*Примітка*
1	*2*	*3*	*4*	*5*	*6*	*7*

**Зазначаються умовні позначення негативних наслідків згідно з п.8 Порядку формування переліку ІТС об'єктів критичної інфраструктури держави.*

Таблиця 2

Перелік важливих ІТН для інтересів держави від розголошення державної таємниці, упорядкованих за ступенем їх тяжкості в балах [12]

Категорія	**Наслідки**
Перша (більше 200 балів)	– повний розрив дипломатичних відносин, що може призвести до озброєного нападу на Україну чи її союзників або воєнних дій; – повний контроль державного шифрованого листування з боку іншої держави;
Друга (100-200 балів)	– розрив дипломатичних відносин з однією або з кількома розвиненими державами; – повне або часткове (30% і більше) розкриття розвідувальних можливостей держави за кордоном; – загроза життю чи свободі особам, які виконують розвідувальні чи контррозвідувальні завдання;
Третя (70-100 балів)	– розрив дипломатичних відносин з іншими державами (державою); закриття посольства (представництва) України у будь-якій країні; – зниження рівня представництва України у будь-якій країні; – повне або часткове (30% і більше) зниження ефективності оперативно-стратегічних планів; – повна або часткова (30% і більше) втрата бойового управління військами, необхідність розробки нових алгоритмів систем управління військами, створення нових пунктів управління; – часткове (до 30%) розкриття розвідувальних можливостей держави за кордоном;
Четверта (50-70 балів)	– зрив укладення Україною міжнародного договору; – зрив чи неможливість виконання розвідувальної, контррозвідувальної чи іншої спеціальної операції; – часткове (до 30%) зниження ефективності оперативно-стратегічних планів; – часткова (до 30%) втрата бойового управління військами, необхідність розробки нових алгоритмів системи бойового управління військами; – розкриття даних про особу, яка виконує на негласній основі розвідувальне, контррозвідувальне чи інше оперативне завдання; – розкриття сил чи засобів негласного оперативного контролю, що застосовуються державними органами для виконання оперативно-розшукової діяльності;
П'ята (10-50 балів)	– зрив переговорів з питань озброєння-роззброєння; – економічні санкції проти України; – розрив торговельно-економічних зв`язків з іншими державами; – несанкціонований доступ (проникнення) на об`єкти, де впроваджено режим спеціального допуску і охорони.

Таблиця 3

Порівняльний аналіз негативних наслідків кібератак на КІД

Держава	**Нормативний документ, що визначає негативні наслідки кібератак**
Україна	*Порядок формування переліку ІТС об'єктів критичної інфраструктури держави*
	Негативними наслідками є: – виникнення надзвичайної ситуації техногенного характеру та/або негативний вплив на стан екологічної безпеки держави (регіону) (Н.1); – негативний вплив на стан енергетичної безпеки держави (регіону) (Н.2); – негативний вплив на стан економічної безпеки держави (Н.3); – негативний вплив на стан обороноздатності, забезпечення національної безпеки та правопорядку у державі (Н.4); – негативний вплив на систему управління державою (Н.5); – негативний вплив на суспільно-політичну ситуацію в державі (Н.6); – негативний вплив на імідж держави (Н.7); – порушення сталого функціонування фінансової системи держави (Н.8); – порушення сталого функціонування транспортної інфраструктури держави (регіону) (Н.9); – порушення сталого функціонування інформаційної та/або телекомунікаційної інфраструктури держави (регіону), в тому числі її взаємодії з відповідними інфраструктурами інших держав (Н.10).
Росія	*Методика віднесення об'єктів державної та недержавної власності до критично важливих об'єктів для національної безпеки Російської Федерації*
	Значимість об'єкта для економіки держави: – вартість річного випуску товарної продукції, млн. руб. (П.1); – загальна чисельність виробничого персоналу, тис. осіб (П.2); – балансова вартість основних виробничих фондів, млн. руб. (П.3); – складова основної продукції об'єкта в продукції того ж виду, що випускається в державі % (П.4). *Нанесення шкоди престижу держави:* – порушення керованості держави або регіону (П.5); – -нанесення шкоди авторитету держави, у тому числі на міжнародній арені (П.6); – розкриття державних секретів, конфіденційної науково-технічної та комерційної інформації (П.7); – порушення боєготовності та боєздатності Збройних Сил (П.8); – порушення стабільності фінансової і банківської систем (П.9). *Можливі загрози населенню і територіям:* – широкомасштабне знищення національних ресурсів (природних, сільськогосподарських, продовольчих, виробничих, інформаційних) (П.10); – територія зараження (забруднення) у разі аварії на об'єкті (П.11); – чисельність населення, яке може постраждати у разі надзвичайної ситуації на об'єкті (П.12); – порушення систем забезпечення життєдіяльності міст та населених пунктів (П.13); – масові порушення правопорядку (П.14); – зупинка безперервних виробництв (П.15); – аварії та катастрофи регіонального масштабу (П.16).
Австралія	*Стратегічний план Австрійської програми захисту життєво важливої інфраструктури*
	– кількість залучених громадян (здоров'я та соціальні наслідки); – економічний ефект; – вплив на навколишнє середовище; – психологічний ефект; – політичні наслідки; – масштабність за територією; – тривалість; – відсутність варіантів заміщення; – взаємозалежність секторів критичної інфраструктури (наслідком руйнації одного є руйнація інших).

Продовження таблиці 3

Держава	**Нормативний документ, що визначає негативні наслідки кібератак**
Іспанія	*Закон Королівства Іспанія про встановлення заходів щодо захисту критичної інфраструктури*
	– кількість залучених громадян (загиблі, поранені з тяжкими травмами та іншими серйозними наслідками для здоров'я); – економічний ефект (економічні втрати та погіршення якості продукції та послуг); – вплив на навколишнє середовище; – політичні наслідки (довіра до органів державного управління) та соціальні наслідки (фізичні страждання, порушення повсякденного життя).
Швеція	*План дій по захисту життєво важливих суспільних функцій та критичної інфраструктури Королівства Швеція*
	– кількість залучених громадян (біля 30 осіб загиблі або отримали поранення з тяжкими травмами); – настання економічного ефекту або впливу на навколишнє середовище (прямі затрати складають майже 10 млн. євро); – політичні наслідки або соціальний вплив (були вбиті громадяни, неможливість вплинути на інцидент, знизилась довіра до органів державного управління, розпочалось громадянське безладдя, пряма загроза для органів державної влади).
Нідерланди	*Директива міністерства безпеки та юстиції Нідерландів щодо підвищення стійкості*
	Категорія А – порушення інфраструктури будуть мати такі наслідки: – фінансові втрати держави більше 50 млрд. євро або падіння доходів в реальному виразі близько 5 %; – загинуть, отримають каліцтва або хронічні захворювання більше 10 тис. осіб; – більше 1 млн. осіб стануть на межу виживання або отримають серйозні моральні травми; – щонайменше два інших сектори критичної інфраструктури почнуть руйнуватись. *Категорія В – порушення інфраструктури будуть мати такі наслідки:* – фінансові втрати держави більше 5 млрд. євро або падіння доходів в реальному виразі близько 1 %; – загинуть, отримають каліцтва або хронічні захворювання більше 1 тис. осіб; – більше 100 тис. осіб стануть на межу виживання або отримають серйозні моральні травми.
Словенія	*Концепція критичної інфраструктури у Словацькій Республіці, її захисту та оборони*
	Основні критерії для визначення критичності інфраструктури є порушення системи, що призведе: – до загибелі більш ніж 50 осіб; – до впливу на здоров'я наслідком якого стане госпіталізація більш ніж 100 осіб терміном на тиждень; – до ускладнення здійснення внутрішньої безпеки держави; – втрат більш ніж 10 млн. євро на день; – неможливості постачання питної води або їжі протягом тижня для 100 тис. осіб; – неможливості постачання електроенергії протягом 3 діб або природного газу протягом тижня для населення більш ніж 100 тис. осіб; – неможливості постачання нафтопродуктів протягом тижня для населення більш ніж 100 тис. осіб; – зараження поверхні більш ніж 100 га; – втрати систем зв'язку протягом доби, що може спричинити збої в підтримці роботи інших критичних систем.
Ізраїль	*Експертне джерело*
	– звичайна (типова) надзвичайна ситуація, коли в разі виникнення якоїсь надзвичайної ситуації страждають в першу чергу географічно близькі об'єкти (малоймовірна для кібератаки); – багаторівневі каскадні збої та надзвичайні ситуації (руйнування системи управління в одній інфраструктурі (наприклад, водовідвідної інфраструктурі) призводить до збою у вторинній інфраструктурі (наприклад, в транспорті), а потім і в третинній (наприклад, ланцюжки поставок продуктів харчування та інших товарів) та ін., навіть якщо прямий вплив на зазначені інфраструктури і не відбувся (найімовірніший наслідок для успішної кібератаки); – наростаючі (збільшують) відмови (порушення роботи однієї інфраструктура (наприклад, мережі зв'язок) завдає шкоди здатності по відновленню і ліквідація наслідків інших аварій на інших інфраструктурах (відмова ліній зв'язку в ході усунення інший аварії, наприклад, на водоканал).

Продовження таблиці 3

Держава	Нормативний документ, що визначає негативні наслідки кібератак
ЄС	*Директива Європейської Комісії*
	Масштаб (географічне охоплення території, для якої втрата елементу критичної інфраструктури завдає значної шкоди): міжнародний, національний, регіональний або територіальний; Важкість можливих наслідків за такими показниками: – вплив на населення (число постраждалих, загиблих, осіб, які отримали значні травми, а також чисельність евакуйованого населення); – економічна шкода (вплив на ВВП, розмір економічних втрат, як прямих, так і непрямих); – екологічна шкода (вплив на населення та навколишнє природне середовище); – взаємозв'язок з іншими елементами критичної інфраструктури; – політичний ефект (втрата впевненості в дієздатності влади); – - тривалість впливу (як саме і коли проявлятимуться наслідки, пов'язані зі втратою чи відмовою об'єктів критичної інфраструктури).

На виконання вимог чинного Порядку [11], Методичних рекомендацій [12] і для удосконалення й адаптації процедури оцінювання шкоди національній безпеці у разі витоку, на прикладі державної таємниці [13], яка обробляється в ІТС об'єкта критичної інфраструктури держави від можливої реалізації кібератаки, пропонується:

1. Ввести умовне позначення ІТН приведених у Методичних рекомендаціях у форматі як «ІТН *x.y*» (де *x* – номер категорії, а *y* – номер ІТН у *x* категорії), зокрема так, як це наведено вище у переліку важливих ІТН для інтересів держави від розголошення відомостей, що становлять державну таємницю;

2. Розробити перелік важливих або інших наслідків для інтересів власника (розпорядника) ІТС, яка обробляє інші види інформації з обмеженим доступом (конфіденційну або службову інформацію), до яких може призвести кібератака;

3. Удосконалити пропозиції до формування переліку ІТС об'єктів критичної інфраструктури держави, передбачивши зазначення умовних позначень окрім негативних наслідків згідно з п. 8 Порядку [11], ще й важливих ІТН за п. 3.2 Методичних рекомендацій [12] від реалізації кібератаки на ІТС об'єкта критичної інфраструктури держави, яка обробляє державну таємницю.

Висновок. Проведено аналіз базової термінології та часткову уніфікацію можливих негативних наслідків, до яких може призвести кібератака на ІТС об'єкта критичної інфраструктури у різних державах, яка обробляє ІзОД (або ДІР). Наведено пропозиції для формування єдиного класифікатора наслідків з метою подальшого його використання при оцінюванні шкоди національній безпеці у разі її витоку.

ЛІТЕРАТУРА

[1]. Д. Бірюков, С. Кондратов, *Захист критичної інфраструктури: проблеми та перспективи впровадження в Україні: аналітична доповідь*, К: НІСД, 2012, 96 с. [Електронний ресурс]: Режим доступу: http://www.niss.gov.ua/content/articles/files/Sots_zahust-86178.pdf. [Дата доступу: серпень 2017].

[2]. Д. Бірюков, С. Кондратов, "Концепція захисту критичної інфраструктури: стан, проблеми та перспективи її впровадження в Україні", *Зб. матеріалів міжнар. наук.-практ. конф.* К: НІСД, 2014, 148 с. [Електронний ресурс]: Режим доступу: http://www.niss.gov.ua/content/articles/files/Virukov_bezprka-d05fd.pdf. [Дата доступу: серпень 2017].

[3]. О. Суходоля, "Система захисту критичної енергетичної інфраструктури України: стан та проблеми формування". *Науково-інформаційний вісник Академії національної безпеки*, Випуск 1-2 (5-6), С. 134-146, 2015.

[4]. В. Лядовська, М. Рябий, С. Гнатюк, "Визначення критичної інформаційної інфраструктури та її захист: аналіз підходів", *Зв'язок*, №4, С. 3-7, 2014.

[5]. С. Гнатюк, В. Сидоренко, О. Дуксенко, "Сучасні підходи до виявлення та ідентифікації найбільш важливих об'єктів критичної інфраструктури", *Безпека інформації*, Т. 21, № 3, С. 269-275, 2015.

[6]. О. Юдін, "Аналіз підходів до визначення критеріїв віднесення об'єктів до критичної інфраструктури на прикладі європейського союзу", *Актуальні питання забезпечення кібербезпеки та захисту інформації: ІІІ Міжнар. наук.-практ. конф.*, К.: Європейський університет, С. 187, 2017.

[7]. Ю. Дрейс, М. Мовчан "Аналіз негативних наслідків кібератак на інформаційні ресурси об'єктів критичної інфраструктури держави", *Актуальні питання забезпечення кібербезпеки та захисту інформації: третя міжнар. наук.-практ. конф.*, К.: Європейський університет, С. 71-74, 2017.

[8]. Ю. Дрейс, "Порівняльний аналіз негативних наслідків кібератак на критичну інформаційну інфраструктуру різних держав", *Інформаційна безпека та*

комп'ютерні технології: *зб. тез доповідей II Міжнар. наук.-практ. конф.*, Кропивницький: ЦНТУ, С. 40-43, 2017.

[9]. "Про захист інформації в інформаційно-телекомунікаційних системах". Верховна Рада України; Закон від 05.07.1994 № 80/94-ВР. [Електронний ресурс]. Режим доступу: http://zakon2.rada.gov.ua/laws/show/80/94-вр. [Дата доступу: серпень 2017].

[10]. "Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та [...]", Кабінет Міністрів України; Постанова, Правила від 29.03.2006 № 373. [Електронний ресурс]. Режим доступу: http://zakon5.rada.gov.ua/laws/show/373-2006-п. [Дата доступу: серпень 2017].

[11]. "Про затвердження Порядку формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави", Кабінет Міністрів України; Постанова, Порядок від 23.08.2016 № 563. [Електронний ресурс]. Режим доступу: http://zakon5.rada.gov.ua/laws/show/563-2016-п. [Дата доступу: серпень 2017].

[12]. "Методичні рекомендації державним експертам з питань таємниць щодо визначення підстав для віднесення відомостей до державної таємниці та ступеня її секретності", Державний комітет України з питань державних секретів та технічного захисту інформації. Наказ №22 від 09.11.1998 р., К.: Збірка №8, С. 4–14, 1998.

[13]. О. Корченко, О. Архипов, Ю. Дрейс, *Оцінювання шкоди національній безпеці України у разі витоку державної таємниці: монографія*, К.: Наук.-вид. центр НА СБ України, 332 с., 2014, ISBN 978-617-7092-26-0.

REFERENCES

[1]. D. Biryukov, S. Kondratov, "Protection of critical infrastructure: problems and prospects of implementation in Ukraine: analytical report". K: NISS, pp. 96, 2012. [Electronic resource]. Access mode: http://www.niss.gov.ua/content/articles/files/Sots_zahust-86178.pdf. [Date of access: august 2017].

[2]. D. Biryukov, S. Kondratov, "The Concept of protection of critical infrastructure: status, problems and perspectives of its implementation in Ukraine": *International. sci. pract. conf.*, K.: NISS, pp. 148, 2012. [Electronic resource]. Access mode: http://www.niss.gov. ua/content/articles/files/Virukov_bezprka-d05fd.pdf. [Date of access: august 2017].

[3]. O. Sukhodolya, "The Ukraine's system of protection critical energy infrastructure: status and problems to formation", *Scientific and information bulletin of the Academy of National Security,* no. 1-2 (5-6), pp. 134-146, 2015.

[4]. V. Lyadovskaya, M. Ryabiy, S. Gnatyuk "Definition of critical information infrastructure and its protection: analysis of approaches", *Communication*, no. 4, pp. 3-7, 2014.

[5]. S. Gnatyuk, V. Sydorenko, O. Duksenko "Modern approaches to critical infrastructure objects detection and identification", *Bezpeka informatsii*, vol. 21, no. 3, pp. 269-275, 2015.

[6]. O. Yudin "Analysis of approaches to determining criteria for removing objects to critical infrastructure on the example of the European Union", *Topical Issues of Cybersecurity and Information Security: Third International. sci. pract. conf.*, K.: European University, pp. 187, 2017.

[7]. Y. Dreis, M. Movchan "Analysis of the negative effects from cyberattacks on information resources of the state critical infrastructure objects", *Topical Issues of Cybersecurity and Information Security: Third International. sci. pract. conf.*, K.: European University, pp. 71-74, 2017.

[8]. Y. Dreis, "Comparative analysis of the negative effects of cyberattacks on the critical information infrastructure of different countries", *Information Security and Computer Technologies: International. sci. pract. conf.*, CNTY, pp. 40-43, 2017.

[9]. "On Information Protection in Information and Telecommunication Systems". Verkhovna Rada of Ukraine; *Law № 80/94-BP*, 1994. [Electronic resource]. Access mode: http://zakon2.rada.gov.ua/laws/show/80/94-вр. [Date of access: august 2017].

[10]. "On Approval Rules for information Protection in information, telecommunication and [...] ", Cabinet Ministers of Ukraine, *Regulation, Rules № 373*, 2006. [Electronic resource]. Access mode: http://zakon5. rada.gov.ua/laws/show/373-2006-п. [Date of access: august 2017].

[11]. "On Approval Procedure for the creation of a list of information and telecommunication systems of objects state's critical infrastructure", Cabinet Ministers of Ukraine, *Regulation, Procedure,* № 563, 2016. [Electronic resource]. Access mode: http://zakon5.rada. gov.ua/laws/show/563-2016-п. [Date of access: august 2017].

[12]. "Methodological recommendations to state experts on questions of secrecy in determining the grounds for attributing information to state secrets and the degree of its secrecy," State Committee of Ukraine on State Secrets and technical protection of information. *Order number 22 dated 09.11.1998*, K .: Collection no. 8, pp. 4-14, 1998.

[13]. A. Korchenko G., A. Arkhipov, Y. Dreis, *Assessment harm to the Ukraine national security in case of leakage state secrets. Monography,* K.: Scientific Publishing Center of NA SSS Ukraine, p. 332, 2014. ISBN 978-617-7092-26-0.

АНАЛИЗ БАЗОВОЙ ТЕРМИНОЛОГИИ И НЕГАТИВНЫХ ПОСЛЕДСТВИЙ КИБЕРАТАК НА ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫЕ СИСТЕМЫ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ ГОСУДАРСТВА

В статье проводится анализ базовой терминологии и разновидности негативных последствий, к которым может привести кибератака на информационно-телекоммуникационные системы объектов критической

инфраструктуры в различных странах мира, в т.ч. и в Украине, например, в случае утечки информации с ограниченным доступом или государственных информационных ресурсов, которые обрабатываются в этих системах. Выявлено дополнительную необходимость учитывать и другие тяжелые последствия для национальных интересов от разглашения сведений, составляющих именно государственную тайну в результате возможной реализации кибератаки при формировании перечня информационно-телекоммуникационных систем объектов критической инфраструктуры государства. Представлены предложения к формированию единого классификатора негативных последствий кибератак на информационно-телекоммуникационные системы объектов критической инфраструктуры государства с учетом обработки в этих системах и других видов информации с ограниченным доступом как конфиденциальная (в.ч. персональные данные) и служебная информация.

Ключевые слова: кибератака, информация с ограниченным доступом, информационно-телекоммуникационная система, критическая инфраструктура государства, негативные последствия, оценивание ущерба.

ANALYSIS OF BASIC TERMINOLOGY AND NEGATIVE CONSEQUENCES FROM CYBER ATTAKS ON INFORMATION-TELECOMMUNICATION SYSTEMS OF OBJECTS STATE'S CRITICAL INFRASTRUCTURE

The article analyzes the basic terminology and variety of negative consequences to which cyber attack can lead to information and telecommunication systems of critical infrastructure objects in various countries of the world, including. and in Ukraine, for example, in case of leakage of information with limited access or state information resources that are processed in these systems. It has been shown that it is necessary to take into account other severe consequences for national interests from disclosure of information that constitutes state secrets as a result of the possible implementation of cyber attacks in the formation of a list of information and telecommunications systems for critical infrastructure of the state. Proposals to the formation of a single classifier of the negative consequences of cyber attacks on information and telecommunications systems of critical infrastructure facilities of the state, taking into account the processing in these systems and other types of information with limited access as confidential (including personal data) and service information.

Keywords: cyberattack, restricted information, information and telecommunication system, critical infrastructure of the state, negative effects, damage assessment.

Дрейс Юрій Олександрович, кандидат технічних наук, доцент, завідувач кафедри інноваційних технологій професійної освіти Національного авіаційного університету.
E-mail: y.dreis@nau.edu.ua.
Дрейс Юрий Александрович, кандидат технических наук, доцент, заведующий кафедрой инновационных технологий профессионального образования Национального авиационного университета.
Dreis Yurii, PhD in Eng., Associate Professor, Head of the Department of Innovative Technologies Professional Education, National Aviation University (Kyiv, Ukraine).

DOI: 10.18372/2410-7840.19.11901
УДК 351.746:007–047.44

АНАЛІЗ МЕТОДІВ ЗАХИСТУ ВІД КІБЕРЗАГРОЗ В БЕЗДРОТОВИХ МЕРЕЖАХ СТАНДАРТУ IEEE 802.11

Володимир Базилевич

Функціонування будь-якого сучасного підприємства базується на використанні інформаційних технологій, зокрема комп'ютерних мереж. Сучасні реалії зобов'язують при проектуванні мереж робити акцент на мобільність та масштабованість. Для ефективного вирішення цих задач доцільно використовувати бездротові комп'ютерні мережі стандарту IEEE 802.11. В той же час використання бездротових мереж створює нові виклики, пов'язані з розробкою системи захисту від кіберзагроз. В даній статі аналізуються та порівнюються методи, які використовуються для створення відповідних систем, визначаються переваги та недоліки кожного з них, акцентуючи увагу на програмний аспект захисту, як такий, що найчастіше стає об'єктом кібератак. Проведений аналіз дозволяє визначити доцільність використання того чи іншого методу захисту або їх комбінації в залежності від вихідних умов, ресурсів та цілей, що ставляться при побудові системи захисту.

Ключові слова: *комп'ютерні мережі, стандарт IEEE 802.11, методи захисту, Wi-Fi, кібербезпека.*