ISSN 2225-5036 (Print), ISSN 2411-071X (Online)
http://infosecurity.nau.edu.ua; http://jrnl.nau.edu.ua/index.php/Infosecurity

БАЗОВА МНОЖИНА УЗАГАЛЬНЕНИХ КРИТЕРІЇВ ВІДНЕСЕННЯ ОБ'ЄКТІВ ДО КРИТИЧНОЇ ІНФРАСТРУКТУРИ ДЕРЖАВИ

Юрій Дрейс, Леонід Деркач

Національна академія СБ України, Україна

ДРЕЙС Юрій Олександрович, к.т.н., доцент.

Рік та місце народження: 1984 рік, смт. Червоноармійськ, Житомирська область, Україна.
Освіта: Житомирський військовий інститут радіоелектроніки ім. С.П. Корольова, 2007 рік.
Посада: старший науковий співробітник Національної академії СБ України з 2019 року.
Наукові інтереси: охорона державної таємниці, захист інформації з обмеженим доступом, критична інформаційна інфраструктура, інформаційна та кібербезпека.
Публікації: понад 100 наукових публікацій, серед яких підручник, навчальні посібники, методичні рекомендації, наукові статті та авторські свідоцтва на комп'ютерні програми.
E-mail: academy@ssu.gov.ua.
ORCID: 0000-0003-2699-1597.

ДЕРКАЧ Леонід Васильович

Рік та місце народження: 1939 рік, м. Дніпро, Україна.
Освіта: Дніпровський національний університет імені Олеся Гончара, 1970 рік.
Посада: старший науковий співробітник Національної академії СБ України.
Наукові інтереси: національна та державна безпека.
Публікації: понад 10 наукових публікацій та праць.
E-mail: academy@ssu.gov.ua.
ORCID: 0000-0002-2078-0003.

Анотація. *Відсутність реєстрів об'єктів критичної інфраструктури держави та їх інформаційно-телекомунікаційних систем призводить до невизначеності у кількості необхідних ресурсів для забезпечення їх захисту від можливих кібератак. З огляду на обмеженість таких ресурсів, важливим і актуальним науково-практичним завданням є визначення повноти та меж пріоритетності кіберзахисту зазначених об'єктів. Формування таких реєстрів відбувається за методикою віднесення об'єктів до критичної інфраструктури держави, основаної у т.ч. на відповідних критеріях, які визначатимуть належність певного об'єкту до такого, що є критичним для держави. Проведений аналіз існуючих критеріїв віднесення об'єктів до критичної інфраструктури держави, показує, що в Україні існує низка інших критеріїв (і які слід також враховувати), задіяних у формуванні реєстрів важливих для держави об'єктів, наприклад «Державний реєстр потенційно небезпечних об'єктів». Отже, пропонується сформувати перелік таких узагальнених критеріїв віднесення об'єктів до критичної інфраструктури держави у вигляді базової множини, яка інтегрує десять ознак з можливістю подальшого розширення. Таку множину можна використати для визначення пріоритетності кіберзахисту інформаційно-телекомунікаційних систем (об'єктів критичної інформаційної інфраструктури) об'єктів критичної інфраструктури держави.*

Ключові слова: *об'єкти критичної інфраструктури держави, множина критеріїв критичності, критична інформаційна інфраструктура.*

Вступ

Дедалі частіше об'єктами кібератак та кіберзлочинів стають інформаційні ресурси фінансових установ, підприємств транспорту, зв'язку, енергозабезпечення, органів державної влади, які забезпечують національну безпеку та оборону, захист від надзвичайних ситуацій (НС). Новітні технології застосовуються не лише для скоєння традиційних видів злочинів, але і для принципово нових, притаманних суспільству з високим рівнем інформатизації.

Існуюче нормативно-правове забезпечення захисту об'єктів критичної інфраструктури (ОКІ) свідчить про наявність низки проблем в енергетичній, інформаційній та інших сферах [1-3], що мають малосистемний характер відповідної діяльності, спостерігається нечітка спрямованість формування переліку інформаційно-телекомунікаційних систем (ІТС) ОКІ тощо. Крім того, на концептуальному та нормативному рівнях не проведено класифікацію ОКІ держави (ОКІД) [4-7], не сформовано перелік їх ІТС як об'єктів критич-

ної інформаційної інфраструктури (ОКІІ), а також відсутні критерії щодо оцінювання негативних наслідків, до яких може призвести кібератака на ІТС ОКІД [8-11].

Актуальність та новизна

Оскільки ресурси, що направлені на забезпечення кібербезпеки є обмеженими (людські, часові, матеріальні тощо), то необхідно встановити пріоритетність (рівень критичності) тих чи інших об'єктів та їх ІТС для забезпечення їх першочергового захисту. Така оцінка приорітетності можлива за рахунок створення множини критеріїв віднесення об'єктів до ОКІД.

Отже, з метою розробки чіткого механізму визначення повноти та меж критичної інформаційної інфраструктури держави суб'єктами забезпечення її кіберзахисту, актуальним є побудова базової множини узагальнених критеріїв віднесення об'єктів до ОКІД.

Аналіз публікацій та досліджень

Відповідно до [12] критерії та порядок віднесення об'єктів до ОКІ, перелік таких об'єктів, загальні вимоги до їх кіберзахисту, у тому числі щодо застосування індикаторів кіберзагроз та вимоги до проведення незалежного аудиту інформаційної безпеки затверджуються Кабінетом Міністрів України (КМУ).

В зазначеному документі також надано і визначення ОКІ та ОКІІ. Так, з урахуванням [13, 26], до ОКІ можуть бути віднесені підприємства, установи, організації незалежно від форми власності, які: провадять діяльність та надають послуги в галузях енергетики, хімічної промисловості, транспорту, інформаційно-комунікаційних технологій, електронних комунікацій, у банківському та фінансовому секторах, у сферах життєзабезпечення населення, зокрема, у сферах централізованого водопостачання, водовідведення, постачання електричної енергії і газу, виробництва продуктів харчування, охорони здоров'я; є аварійними та рятувальними службами, службами екстреної допомоги населенню; включені до переліку підприємств, що мають стратегічне значення для економіки і безпеки держави; є об'єктами, що підлягають охороні та обороні в умовах надзвичайного стану і особливого періоду; є об'єктами потенційно небезпечних технологій і виробництв.

Але, як зазначено у [13], віднесення таких об'єктів до ОКІ відбувається за сукупністю критеріїв, що визначають їх важливість для реалізації життєво-важливих функцій та надання життєво-важливих послуг, свідчать про існування ризиків і загроз для них, можливість виникнення кризових ситуацій через втручання в їх функціонування, припинення функціонування, людський чинник чи природні лиха, тривалість робіт для усунення таких наслідків до повного відновлення штатного режиму, а саме: «…існування викликів, ризиків і загроз, що можуть виникати щодо ОКІ; уразливості цих об'єктів, тяжкості настання можливих негативних наслідків, внаслідок чого буде заподіяна значна шкода: здоров'ю населення (визначається кількістю постраждалих, загиблих та осіб, які отримали значні травми, а також чисельністю евакуйованого населення); соціальній сфері (руйнація систем соціального захисту населення і надання соціальних послуг, втрата спроможності держави задовольнити критичні потреби суспільства); економіці (вплив на ВВП, розмір економічних втрат, як прямих, так і опосередкованих); природним ресурсам загальнодержавного значення; обороноздатності; іміджу країни; масштабності негативних наслідків для держави, які: вплинуть на діяльність стратегічно важливих об'єктів для кількох секторів економіки чи призведуть до втрати унікальних національно значущих активів, систем і ресурсів, матимуть тривалі наслідки для держави і позначаються на діяльності низки інших секторів; тривалості ліквідації таких наслідків та дією подальшого негативного впливу на інші сектори держави; впливу на функціонування суміжних секторів критичної інфраструктури» [13].

Тобто, відповідно до запропонованого у [13] принципу «віднесення таких об'єктів до ОКІ визначається за сукупністю критеріїв», якщо в об'єкті інфраструктури не визначено хоча б одного із вищенаведених критеріїв, то такий об'єкт не може бути віднесений до ОКІ, що є досить дискусійним і суперечливим твердженням, тому й було виключене з кінцевої редакції [14].

Мета роботи

Виходячи з викладеного, *метою роботи* є формування базової множини узагальнених критеріїв віднесення об'єктів до ОКІ для подальшої оцінки пріоритетності їх кіберзахисту.

Основна частина

Провівши аналіз наукових праць і узагальнення діючих нормативно-правових документів [1-26], пропонується *перелік узагальнених критеріїв віднесення об'єктів до ОКІД* за низкою нижченаведених ознак:

1) За сферою діяльності та надання послуг у секторі критичної інфраструктури (табл. 1) [1-3, 8, 9, 12, 13, 15, 26]:

Таблиця 1

Група	*Елемент*	*Умовні позначення*
Підприємства (об'єкти), установи та організації незалежно від форми власності *{ПУО}*	*{*Комунальні, Аварійно-рятувальної служби, Служби екстреної допомоги населенню*}*; *{*У переліку, що мають стратегічне значення для економіки і безпеки держави*}*; {Потенційно небезпечних технологій і виробництв*}*; *{*Включеними до Державного реєстру потенційно небезпечних об'єктів*}*; *{*Підвищеної небезпеки (у т.ч. перелік особливо небезпечних підприємств, припинення діяльності яких потребує проведення спеціальних заходів щодо запобігання заподіянню шкоди життю та здоров'ю громадян, майну, спорудам, природному довкіллю)*}*; *{*Об'єктами державної важливості*}*; *{*Під обов'язковою охороною підрозділами ДСО за договорами*}*; *{*Під охороною і обороною в умовах надзвичайних ситуацій і в особливий період*}*; *{*Національною системою конфіденційного зв'язку*}*; *{*Платіжними системи*}*; *{*Системою екстреної допомоги населенню за єдиним номером 112*}*; *{*Нерухомими об'єктами культурної спадщини*}*	*{К, АРС, СЕД}*; *{ПСЗ}*; *{ПНВ}*; *{ОПН}*; *{ПНО}*; *{ОДВ}*; *{ОО}*; *{ООО}*; *{НСКЗ};{ПС}*; *{СЕД}*; *{НОКС}*

Сектор критичної інфраструктури держави *{СКІ}*	*{*Паливно-енергетичний*}*; *{*Інформаційний (інформаційно-комунікаційних технологій, електронних комунікацій*)}*; *{*Систем життєзабезпечення (Централізованого водопостачання, Водовідведення, Постачання електричної енергії і газу, Виробництва продуктів харчування, Сільського господарства*)}*; *{*Харчової промисловості*}*; {Агропромислового комплексу*}*; *{*Охорони здоров'я*}*; {Фінансовий*}*; {Банківський*}*; *{*Транспорту і пошти*}*; {Промисловість (хімічна, металургійна, оборонна, космічна, авіаційна, суднобудівна*)}*; *{*Цивільного захисту населення та територій*}*	*{ПЕ}*; *{І}*; *{СЖ (ЦВ, В, ЕЕГ, ВПХ, СГ)}*; *{ХП}*;*{АП}*;*{ОЗ}*; *{Ф}*; *{Б}*; *{ТП}*; *{П (Х,М,О,К,А,С)}*; *{ЦЗ}*

2)За критеріями включення до переліку окремих особливо важливих об'єктів права державної власності, охорона яких здійснюється виключно державними підприємствами та організаціями на підставі договорів про надання охоронних послуг (табл. 2) [17].

3) За сукупністю критеріїв, що визначають їх важливість для реалізації життєво важливих функцій та послуг, свідчать про існування ризиків і загроз для них, можливість виникнення кризових ситуацій через втручання в їх функціонування, припинення функціонування, людський чинник чи природні лиха, тривалість робіт для усунення наслідків до відновлення штатного режиму (табл. 3) [2, 13, 18].

Таблиця 2

Група	*Елемент*	*Умовні позначення*
Щодо зберігання {ЗБ}	*{*Наркотичних засобів, Психотропних речовин, Прекурсорів*}*; *{*Історичних та культурних цінностей загальнодержавного значення*}*	*{НЗ, ПР, П}*; *{ІКЦ}*
Щодо виробництва та/або зберігання {ВЗ}	*{*Озброєння, Ракет, Боєприпасів, Вибухових речовин, Вогнепальної зброї, Спортивно-мисливської зброї, Спеціальних засобів заряджених речовинами сльозоточивої та дратівної дії, Засобів активної оборони*}*; *{*Запасів пально-мастильних матеріалів, Речового майна, Продовольчого майна*}*	*{О, Р, ВР, ВЗ, СМЗ, СЗ, ЗАО}*; *{ПММ, РМ, ПМ}*
Щодо провадження діяльності {ПД}	*{*Водопостачання населених пунктів з резервуарами питної води*}*; {Захоронення радіоактивних відходів*}*; *{*Охорони державної таємниці*}*; *{*Дорогоцінними металами, Дорогоцінним камінням, Дорогоцінним камінням органогенного утворення, Напівдорогоцінним камінням*}*; *{*Оцінювання якості освіти, Проведення та перевірки результатів зовнішнього незалежного оцінювання*}*; державних *{*Спортивних заходів, Розважальних заходів*}*; *{*Надання медичної допомоги, Медичних послуг*}*	*{ВР}*; *{ЗРВ}*; *{ОДТ}*; *{ДМ, ДК, ДКОУ, НК}*; *{ОЯО, ЗНО}*; *{СЗ, РЗ}*; *{МД, МП}*
Щодо розміщення {Р}	*{*Органів державної влади*}*, {Органів місцевого самоврядування*}*	*{ОДВ}*, *{ОМС}*

Таблиця 3

Група	*Елемент*	*Умовні позначення*
Уразливості цих об'єктів, тяжкості настання можливих негативних наслідків, шкоди {УО}	*{*Від викликів, ризиків і загроз (кібератак), що можуть виникати щодо ОКІ*}*; *{*Здоров'ю населення (визначається кількістю постраждалих, загиблих та осіб, які отримали значні травми, а також чисельністю евакуйованого населення*)}*; *{*Соціальній сфері (руйнація систем соціального захисту населення і надання соціальних послуг, втрата спроможності держави задовольнити критичні потреби суспільства*)}*; *{*Економіці (вплив на ВВП, розмір економічних втрат, як прямих, так і непрямих*)}*; *{*Природним ресурсам загальнодержавного значення*}*	*{КА}*; *{УЗН}*; *{УСС}*; *{УЕ}*; *{УПР}*
Масштабності негативних наслідків для держави {МНН}	*{*Вплинуть на діяльність стратегічно важливих об'єктів для кількох секторів економіки*}*; *{*Призведуть до втрати унікальних національно значущих активів, систем і ресурсів*}*; *{*Матимуть тривалі наслідки для держави і позначаються на діяльності низки інших секторів*}*; *{*Від тривалості ліквідації таких наслідків та дією подальшого негативного впливу на інші сектори держави*}*; *{*Від впливу на функціонування суміжних секторів критичної інфраструктури*}*; *{*Від завдання значної шкоди нормальним умовам життєдіяльності населення*}*	*{ВСО}*; *{ВУА}*; *{ТНД}*; *{ТН}*; *{ВСС}*; *{ШНУ}*

4) За наслідками порушення сталого функціонування ОКІ, які можуть спричинити кібератаки [8, 10, 13, 15]: «{Виникнення надзвичайної ситуації техногенного характеру та/або негативний вплив на стан екологічної безпеки держави (регіону)}={Н1}; {Негативний вплив на стан енергетичної безпеки держави (регіону)}={Н2}; {Негативний вплив на стан економічної безпеки держави}={Н3}; {Негативний вплив на стан обороноздатності, забезпечення національної безпеки та правопорядку у державі}={Н4}; {Негативний вплив на систему управління державою}={Н5}; {Негативний вплив на суспільно-політичну ситуацію в державі}={Н6}; {Негативний вплив на імідж держави}={Н7}; {Порушення сталого функціонування фінансової системи держави}={Н8}; {Порушення сталого функціонування транспортної інфраструктури держави (регіону)}={Н9}; {Порушення сталого функціонування інформаційної та/або телекомунікаційної інфраструктури держави (регіону), в тому числі її взаємодії з відповідними інфраструктурами інших держав}={Н10}».

5) За методикою ідентифікації потенційно небезпечних об'єктів (табл. 4, 5) [18-22]:

Таблиця 4

Група	*Елемент*	*Умовні позначення*
За видом небезпеки {ВН}	*{*Бактеріологічна*}; {*Біологічна*}; {*Вибухопожежна*}; {*Гідродинамічна*}; {*Пожежна*}; {*Радіаційна*}; {*Фізична*}; {*Хімічна*}; {*Екологічна*}*	*{Б};{БЛ};{ВП}; {Г}; {П}; {Р}; {Ф}; {Х}; {Е}*
За класифікацією та кодом НС {КНС}	*{*Техногенні*}; {*Природні*}; {*Соціально-політичні*}; {*Воєнні*}*	*{Т}; {П}; {С-П}; {В}*
За рівнем можливої НС {РМНС}	*{*Державний*}; {*Регіональний*}; {*Місцевий*}; {*Об'єктовий (локальний)*}*	*{Д}; {Р};{М}; {О}*

Залежно від обсягів заподіяних наслідків, технічних і матеріальних ресурсів, необхідних для їх ліквідації, НС класифікується як: *{Д}; {Р}; {М}; {О}*. Для визначення відповідного рівня НС встановлюються критерії, що наведені у табл. 5 [19], де *РЗ* – розмір збитків, завданих уражальними чинниками джерела НС, розраховується відповідно до «Методики оцінки збитків від наслідків НС техногенного і природного характеру».

Таблиця 5

Рівень НС	*Територіальне поширення та обсяги технічних і матеріальних ресурсів, що необхідні для ліквідації наслідків НС*	*Кількість людей, які внаслідок дії уражальних чинників джерела НС загинули або постраждали, або нормальні умови життєдіяльності яких порушено (п.н.у.ж.)*	*РЗ (тис. мінімальних розмірів заробітної плати (м.р.з.п.))*
{Д}	територію інших держав; або територія двох чи більше регіонів України (Автономної Республіки Крим, областей, м. Києва та Севастополя), а для її ліквідації необхідні матеріальні і технічні ресурси в обсягах, що перевищують можливості цих регіонів, але не < 1% від обсягу видатків відповідних місцевих бюджетів (НС державного рівня за територіальним поширенням)	загинуло – [10; ∞[; постраждало – [300; ∞[; п.н.у.ж. – [50 000; ∞[(більш як на 3 доби)	[150; ∞[, який у інших випадках, передбачених актами законодавства, за своїми ознаками визначається як {Д}
		або загинуло – [5; 10[; постраждало – [100; 300[; п.н.у.ж. – [10 000; 50 000[(більш як на 3 доби)	[25; 150] (на час виникнення НС)
{Р}	територія двох чи більше районів (міст обласного значення) Автономної Республіки Крим, областей, а для її ліквідації необхідні матеріальні і технічні ресурси в обсягах, що перевищують можливості цих районів, але не < 1% обсягу видатків відповідних місцевих бюджетів (НС регіонального рівня за територіальним поширенням)	загинуло – [3; 4]; постраждало - [50; 100[; п.н.у.ж. – [1000; 10 000[;	[15; 25]
		(більш як на 3 доби)	[5; 15]
{М}	за межами території потенційно небезпечного об'єкта, загрожує довкіллю, сусіднім населеним пунктам, інженерним спорудам, а для її ліквідації необхідні матеріальні і технічні ресурси в обсягах, що перевищують власні можливості потенційно небезпечного об'єкта	загинуло - [1; 2]; постраждало – [20; 50[; п.н.у.ж. – [100; 1000[;	[2; 5]
		(більш як на 3 доби)	[0,5; 2]
{О}	визнається НС, яка не підпадає під названі вище визначення		

6) За категорією критичності [3, 13, 26]: {I категорія критичності – особливо (критично) важливі об'єкти}=*{ОВО}*; {II категорія критичності – життєво важливі об'єкти}=*{ЖВО}*; {III категорія критичності – важливі об'єкти}=*{ВО}*; {IV категорія критичності – необхідні об'єкти}=*{НО}*.

7) За класами наслідків (відповідальності) від категорії складності об'єкта (табл. 6) [23, 24]: {Незначні наслідки – I та II категорія складності}=*{СС-1}*: «Об'єкти промисловості, енергетики, транспорту і зв'язку, сільського господарства і переробки сільгосппродукції, що не віднесені до класів СС3 і СС2; громадські будівлі, об'єкти фізкультури та спорту, що не віднесені до класів СС3 і СС2, а також усі тимчасові об'єкти, мобільні будинки; об'єкти внутрішньовиробничих доріг, комунікацій і продуктопроводів; парники, теплиці; опори розподільної мережі низької напруги, освітлювальні опори» [23]; {Середні наслідки – III та IV категорія складності}=*{СС-2}*: «Об'єкти металургійної промисловості, важкого машинобудування, нафтохімії, суднобудування, оборонної промисловості (доменні і мартенівські цехи, складальні корпуси, високі димові труби тощо); копри, машинні відділення добувних машин; об'єкти гідро- і теплоенергетики потужністю <1,0 млн. кВт, розподільні системи основних електромереж високої напруги (включаючи опори ліній електропередачі і відкритих розподільних пристроїв); ємкості для нафти і нафтопродуктів; шляхові полотна магістральних автодоріг, злітно-посадкові смуги, мости і тунелі протяжністю <1000 м, канатні дороги, вокзали, аеровокзали, вертолітні станції; магістральні трубопроводи; великі готелі, гуртожитки; об'єкти водопроводу і каналізації (включаючи водонапірні башти, очисні споруди, водозабори) промислових підприємств і населених пунктів; будівлі видовищних і спортивних підприємств, підприємств торгівлі, громадського харчування, служби побуту, установи охорони здоров'я; будівлі і споруди центральних складів для забезпечення життєвих потреб населення, склади особливо цінного устаткування і матеріалів, військові склади; житлові, громадські або бага-

тофункціональні будівлі заввишки до 100 м.» [23]; {Значні наслідки – V категорія складності}={*СС-3*}: «Об'єкти нафто- і газодобувної, газопереробної, металургійної, хімічної та інших галузей промисловості, обладнані пожежо- і вибухонебезпечними ємкостями і сховищами рідкого палива, газу і газопродуктів, особливо при їх зберіганні під тиском (технологічні трубопроводи, апарати, котли, газгольдери, ізотермічні резервуари ємністю >10 тис. кубометрів, резервуари для зберігання нафти та нафтопродуктів ємністю >30 тис. кубометрів, посудини високого тиску тощо); об'єкти хімічної, нафтохімічної, біотехнологічної, оборонної та інших галузей, що пов'язані з використанням, переробкою, виготовленням і зберіганням хімічно токсичних, вибухо- і пожежонебезпечних речовин і промислових вибухових матеріалів, біологічно небезпечних речовин тощо; об'єкти вугільної і гірничорудної промисловості, небезпечні щодо пожежі, вибуху і газу відповідно до класифікації Держнаглядохоронпраці; будівлі головних вентиляційних систем на копальнях і рудниках; об'єкти атомної енергетики (АЕС, АЕТС, АСТ), включаючи сховища і заводи з переробки ядерного палива і радіоактивних відходів, а також інші радіаційне небезпечні об'єкти за класифікацією Держатомнагляду; об'єкти гідро- і теплоенергетики (ГЕС, ГРЕС, ТЕС, ТЕЦ, ГАЕС) потужністю >1,0 млн. кВт; мости і тунелі на дорогах вищої категорії, або протяжністю >1000 м чи прогоном >300 м; стаціонарні споруди знаків навігаційної обстановки; шлюзи і основні портові споруди на водних шляхах 1-го і 2-го класів ДСТУ Б В.2.3-1; будівлі і споруди крупних залізничних вокзалів і аеровокзалів; магістральні трубопроводи діаметром >1000 мм, або з робочим тиском >2,5 МПа, а також ділянки магістральних трубопроводів меншого діаметра і з меншим робочим тиском у місцях переходів через водні перешкоди, залізничні та автомобільні дороги; гідротехнічні споруди меліоративних систем із площею зрошення і осушення >300 тис. га і водоймищ об'ємом >1 кубічний кілометр; крупні елеватори і зерносховища, млинарські комбінати; житлові, громадські або багатофункціональні будівлі заввишки >100 м; будівлі основних музеїв, державних архівів, сховищ національних історичних і культурних цінностей; видовищні об'єкти з масовим перебуванням людей (стадіони, театри, кінозали, цирки, виставкові приміщення тощо); будівлі університетів, інститутів, шкіл, дошкільних закладів тощо; великі лікарні та інші заклади охорони здоров'я; універсами та інші великі торговельні підприємства; об'єкти життєзабезпечення великих районів міської забудови і промислових територій; великі об'єкти захисно-запобіжного характеру (протиселеві, протизсувні, протилавинні споруди, захисні дамби тощо)» [23].

Таблиця 6

Характеристики можливих наслідків від відмови будівлі або споруди за класами наслідків (відповідальності) [24]

Клас наслідків (відповідальності) будівлі або споруди	*Характеристики можливих наслідків від відмови будівлі або споруди*					
	Можлива небезпека для здоров'я і життя людей (кількість осіб)			*Обсяг можливого економічного збитку (м.р.з.п.)*	*Втрата об'єктів культурної спадщини (за рівнем НС)*	*Припинення функціонування комунікацій транспорту, зв'язку, енергетики, інших інженерних мереж (рівень НС)*
	які постійно перебувають на об'єкті	*які періодично перебувають на об'єкті*	*які перебувають поза об'єктом*			
{СС-3}	[400; ∞[	[1000; ∞[	[50 000; ∞[	[50 000; ∞[	*{Н}*	*{Д}*
{СС-2}	[50, 400[	[100; 1000[	[100, 50 000[	[2500; 50 000[	*{М}; {О}*	*{Р}; {М}*
{СС-1}	[0; 50[	[0; 100[	[0; 100[	[0; 2500[	–	–

8) За наявністю ОКІІ [12, 14, 24]: {Комунікаційна система}={КС}; {Технологічна система}=*{ТС}*; {Інформаційні системи}=*{ІС}*; {Інформаційно-телекомунікаційні системи та мережі}=*{ІТС}*; {Автоматизовані системи управління технологічним процесом}=*{АСУ}*.

9) За ознаками ідентифікації об'єктів підвищеної небезпеки (табл. 7) [20-22].

10) За видом інформації, що обробляється (табл. 8) [12, 14, 15].

Таблиця 7

Група	*Елемент*	*Умовні позначення*
За категорією наявних небезпечних речовин {КНР}	*{*Горючі (займисті) гази*}*; *{*Горючі рідини*}*; *{*Горючі рідини, перегріті під тиском*}*; *{*Вибухові речовини*}*; *{*Речовини-окисники*}*; *{*Високотоксичні та токсичні речовини*}*; *{*Речовини, які становлять небезпеку для довкілля (високотоксичні для водних організмів)*}*	*{ГГ}*; *{ГР}*; *{ГПТ}*; *{ВР}*;*{Р-О}*; *{ВТР}*; *{РНД}*
За видами та впливом уражальних факторів аварій, що можуть статися виходячи з властивостей небезпечних речовин {УФА}	*{*Група 1 (вибух)*}*; *{*Група 2 (пожежа)*}*; *{*Група 3 (шкідливі для людей і довкілля)*}*	*{Г1}*; *{Г2}*; *{Г3}*

Таблиця 8

Група	*Елемент*	*Умовні позначення*
Національні електронні інформаційні ресурси {НЕІР}	*{*Публічна інформацію*}*; *{*Державні інформаційні ресурси*}*; *{*Інша інформація, призначена для задоволення життєво важливих суспільних потреб громадянина, особи, суспільства і держави*}*	*{ПІ}*; *{ДІР}*; *{ІІ}*
Інформація з обмеженим доступом {ІзОД}	*{*Конфіденційна інформація (у т.ч. персональні дані)*}*; *{*Службова інформація*}*; *{*Таємна інформація*}*	*{КІ}*; *{СІ}*; *{ТІ}*

Далі, на основі проведеного аналізу та запропонованого переліку узагальнених критеріїв віднесення об'єктів до ОКІД сформуємо відповідну базову множину:

$$\mathbf{МК} = \{\bigcup_{i=1}^{n} \mathbf{МК}_i\} = \{\mathbf{МК}_1, \mathbf{МК}_2, ..., \mathbf{МК}_n\}, \quad (1)$$

де $\mathbf{МК}_i \subseteq \mathbf{МК}$ $(i = \overline{1,n})$ – множина, що відображає *i*-й критерій, *n* – кількість цих критеріїв.

Наприклад, з урахуванням низки вищенаведених ознак, при $n = 10$, $(i = \overline{1,10})$ відповідно до [1-26], формула (1) набуде вигляду:

$$\mathbf{МК} = \{\bigcup_{i=1}^{n} \mathbf{МК}_i\} = \{\mathbf{МК}_1, \mathbf{МК}_2, ..., \mathbf{МК}_{10}\} =$$

$$= \{\boldsymbol{СД}, \boldsymbol{ОВО}, \boldsymbol{ВФП}, \boldsymbol{НК}, \boldsymbol{ПНО}, \boldsymbol{КК}, \boldsymbol{КН}, \boldsymbol{ОКІІ}, \boldsymbol{ОПН}, \boldsymbol{ВІ}\},$$

де $\mathbf{МК}_1$ = ***СД*** = «За сферою діяльності та надання послуг у секторі критичної інфраструктури», $\mathbf{МК}_2$ = ***ОВО*** = «За критеріями включення до переліку окремих особливо важливих об'єктів права державної власності, охорона яких здійснюється виключно державними підприємствами та організаціями на підставі договорів про надання охоронних послуг», $\mathbf{МК}_3$ = ***ВФП*** = «За сукупністю критеріїв, що визначають їх важливість для реалізації життєво важливих функцій та послуг, свідчать про існування ризиків і загроз для них, можливість виникнення кризових ситуацій через втручання в їх функціонування, припинення функціонування, людський чинник чи природні лиха, тривалість робіт для усунення таких наслідків до повного відновлення штатного режиму», $\mathbf{МК}_4$ = ***НК*** = «За наслідками порушення сталого функціонування ОКІ, які можуть спричинити кібератаки», $\mathbf{МК}_5$ = ***ПНО*** = «За методикою ідентифікації потенційно небезпечних об'єктів», $\mathbf{МК}_6$ = ***КК***= «За категорією критичності», $\mathbf{МК}_7$ = ***КН*** = «За класами наслідків (відповідальності) від категорії складності об'єкта», $\mathbf{МК}_8$ = ***ОКІІ*** = «За наявністю ОКІІ»; $\mathbf{МК}_9$ = ***ОПН*** = «За ознаками ідентифікації об'єктів підвищеної небезпеки», $\mathbf{МК}_{10}$ = ***ВІ*** = «За видом інформації, що обробляється».

Висновок

Сформовано перелік узагальнених критеріїв віднесення об'єктів до критичної інфраструктури держави у вигляді базової множини, яка інтегрує одинадцять ознак з можливістю подальшого розширення. Даний перелік містить критерії, які визначають належність певного об'єкту не тільки до об'єктів критичної інфраструктури держави за методикою їх віднесення, але й до інших важливих для країни об'єктів, визначених відповідними державними реєстрами.

Цю базову множину можна використати для визначення пріоритетності кіберзахисту об'єктів критичної інформаційної інфраструктури, наприклад, інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави.

Література

[1]. A. Korchenko, Y. Dreis, O. Romanenko, "Analysis problems in the field of state's critical infrastructure", *Projekt interdyscyplinarny projektem XXI wieku: Monografia. Tom 1.* – Akademia Techniczno-Humanistyczna w Bielsku-Bialej, 2017. – pp. 397 - 402.

[2]. "*Зелена книга з питань захисту критичної інфраструктури в Україні*", Д. Бірюков, С. Кондратов, О. Суходоля. – К: НІСД, С. 176, 2016. URL: http://www.niss.gov.ua/public/File/2016_book/Syxodolya_ost.pdf

[3]. *Організаційні та правові аспекти забезпечення безпеки і стійкості критичної інфраструктури України : аналіт. доп.* / [Бобро Д. Г., Іванюта С. П., Кондратов С. І., Суходоля О. М.] / за заг. ред. О. М. Суходолі. – К. : НІСД, 2019. – 224 с.

[4]. О. Корченко, Ю. Дрейс, О. Романенко, В. Бичков, "Модель класифікатора об'єктів критичної інформаційної інфраструктури держави", *Захист інформації*. – 2018. – Т. 20, № 1. – С. 5-11.

[5]. О. Корченко, Ю. Дрейс, О. Романенко, "Класифікація об'єктів критичної інформаційної інфраструктури держави", *зб. тез наук. доп. наук.-практ. конф.* (Київ, 30 березня 2018 р.). – Київ: Нац.акад.СБУ, 2018. – 408 с. – С. 95-98.

[6]. О. Корченко, Ю. Дрейс, О. Романенко, "Формування множини ідентифікаторів для класифікації об'єктів критичної інформаційної інфраструктури", *«Актуальні проблеми забезпечення кібербезпеки та захисту інформації»*, тези доповідей учасників IV Міжнародної науково-практичної конференції, Закарпатська обл., с. Верхнє Студене, 21-24 лютого 2018 р. – К: Ви-во Європейського університету, 2018. – С. 81-86.

[7]. С. Гнатюк, В. Сидоренко, Н. Сєйлова, "Універсальна модель даних для формування переліку об'єктів критичної інформаційної інфраструктури держави", *Безпека інформації*, Том 23, № 2(2017 р). – С. 87–91.

[8]. О. Корченко, Ю. Дрейс, О. Романенко, "Критична інформаційна інфраструктура України: терміни, сектори і наслідки", *Захист інформації*. – 2017. – Т. 19, № 4. – С. 303-309.

[9]. Y. Dreis, M. Roshchuk, O. Romanenko, "Sectors of Critical Informational Infrastructure", *тези доповідей учасників IV Міжнародної науково-практичної конференції*, Закарпатська обл., Міжгірський р-н, с. Верхнє Студене, 21-24 лютого 2018 р. – К: Ви-во Європейського університету, 2018. – С.141-143.

[10]. Ю. Дрейс, "Аналіз базової термінології і негативних наслідків кібератак на інформаційно-телекомунікаційні системи об'єктів критичної інфраструктури держави", *Захист інформації*. – 2017. – Т. 19, № 3. – С. 214-222.

[11]. Ю. Дрейс, О. Романенко, "Розширення базової термінології у сфері захисту критичної інформаційної інфраструктури держави", *Автоматика та комп'ютерно-інтегровані технології у промисловості, телекомунікаціях, енергетиці та транспорті: матеріали всеукраїнської науково-практичної інтернет-конференції*, 16–17 листопада 2017, Кропивницький: ЦНТУ, 2017. – С. 185–187.

[12]. "*Про основні засади забезпечення кібербезпеки України*", Верховна Рада України, Закон України від

05.10.2017р. URL: http://zakon2.rada.gov.ua /laws/show /2163-19.

[13]. "*Про затвердження Загальних вимог з кіберзахисту об'єктів критичної інфраструктури, критеріїв та порядку віднесення об'єктів до об'єктів критичної інфраструктури*", проект Постанови Кабінету Міністрів України (18.05.2018), Державна служба спеціального зв'язку та захисту інформації України. [Електронний ресурс]. Режим доступу: http://195.78.68. 84/dsszzi/control/uk/publish/article?art_id=290126&cat_id =38837.

[14]. "*Про затвердження Загальних вимог з кіберзахисту об'єктів критичної інфраструктури*", Постанова №518 від 19.06.2019, Кабінет Міністрів України. URL: https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#n8.

[15]. "*Про затвердження Порядку формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави*", Кабінет Міністрів України; Постанова, Порядок від 23.08.2016 № 563. URL: http://zakon5.rada.gov.ua/laws/show/563-2016-п.

[16]. "*Про проблеми вдосконалення системи захисту критичної інфраструктури в Україні. Аналітична записка*", Національний інститут стратегічних досліджень, відділ екологічної та техногенної безпеки (Д.С. Бірюков). URL: http://old2.niss.gov.ua/ articles/1477/.

[17]. "*Про затвердження Критеріїв, відповідно до яких об'єкти включаються до переліку окремих особливо важливих об'єктів права державної власності, охорона яких здійснюється виключно державними підприємствами та організаціями на підставі договорів про надання охоронних послуг*", Міністерство внутрішніх справ, Наказ від 01.09. 2015 № 1053. URL: https://zakon.rada.gov.ua/laws/show/z1124-15.

[18]. "*Про критичну інфраструктуру та її захист*", Міністерство економічного розвитку і торгівлі України, Проект Закону України. URL: http://www. me.gov.ua/Documents/Download?id=634a8762-3d1a-45ac-b0df-be56a4f7d9d1.

[19]. "*Про затвердження Порядку класифікації надзвичайних ситуацій за їх рівнями*", Кабінет Міністрів України; Постанова, Порядок від 24.03.2004 № 368 (редакція від 11.06.2013). URL: https://zakon.rada.gov.ua/laws/show/368-2004-%D0% BF.

[20]. "*Про затвердження Методики ідентифікації потенційно небезпечних об'єктів*", Міністерство України з питань надзвичайних ситуацій та у справах захисту населення від наслідків Чорнобильської катастрофи, Наказ від 23.02.2006 № 98. URL: https://zakon.rada.gov.ua/laws/show/z0286-06.

[21]. "Про об'єкти підвищеної небезпеки ", Верховна Рада України, Закон України від 18.01.2001р. №2245-III. URL: https://zakon.rada.gov.ua/laws/show/2245-14.

[22]. "*Про ідентифікацію та декларування безпеки об'єктів підвищеної небезпеки*", Кабінет Міністрів України; Постанова від 11.07.2002 № 956. URL: https://zakon2.rada.gov.ua/laws/show/956-2002-%D0% BF.

[23]. "*Про регулювання містобудівної діяльності*", Верховна Рада України, Закон України від 17.02.2011 р. URL: https://zakon.rada.gov.ua/laws/show /3038-17.

[24]. "*О безопасности критической информационной инфраструктуры Российской Федерации*", Федеральный закон от 26 июля 2017 г. N 187-ФЗ. URL: http://ivo.garant.ru/#/document/71730198/paragraph/1:0.

[25]. A. Korchenko, V. Hrebenuik, Y. Dreis, A. Hrebenuik, O. Gavrylenko, Criteria for assigning objects to critical infrastructure of Ukraine, *«Przetwarzanie, transmisja i bezpieczenstwo informacij»: Monografia, Tom 2*, Akademia Techniczno-Humanistyczna w Bielsku-Bialej, 2019. – (418 c.). – C.189-196.

[26]. "*Деякі питання об'єктів критичної інфраструктури*", Кабінет Міністрів України; Постанова від 09.10.2020 № 1109. URL: https://zakon.rada.gov.ua/laws/show/1109-2020-%D0%BF#n91.

УДК 004.056:007.2

Дрейс Ю.А., Деркач Л.В. Базовое множество обобщенных критериев отнесения объектов к критической инфраструктуры государства.

Аннотация. *Отсутствие реестров объектов критической инфраструктуры государства и их информационно-телекоммуникационных систем приводит к неопределенности в количестве необходимых ресурсов для обеспечения их защиты от возможных кибератак. Учитывая ограниченность таких ресурсов, важным и актуальным научно-практической задачей является определение полноты и границ приоритетности киберзащиты указанных объектов. Формирование таких реестров происходит по методике отнесения объектов к критической инфраструктуры государства, основанной в т.ч. на благоприятных условиях, которые будут определять принадлежность определенного объекта к такому, что является критическим для государства. Проведенный анализ существующих критериев отнесения объектов к критической инфраструктуры государства, показывает, что в Украине существует ряд других критериев (и которые следует также учитывать), задействованных в формировании реестров важных для государства объектов, например, «Государственный реестр потенциально опасных объектов». Итак, предлагается сформировать перечень таких обобщенных критериев отнесения объектов к критической инфраструктуры государства в виде базовой множества, которая интегрирует десять признаков с возможностью дальнейшего расширения. Такое множество можно использовать для определения приоритетности киберзащиты информационно-телекоммуникационных систем (объектов критической информационной инфраструктуры) объектов критической инфраструктуры государства.*

Ключевые слова: *объекты критической инфраструктуры государства, множество критериев критичности, критическая информационная инфраструктура.*

Y. Dreis, L. Derkach, Basic set of generalized criteria for assigning objects to the critical infrastructure of state.

Abstract. *The lack of registers of critical infrastructure of the state and their information and telecommunication systems leads to uncertainty in the amount of resources needed to protect them from possible cyberattacks. Given the limitations of*

such resources, an important and relevant scientific and practical task is to determine the completeness and priority of cyber protection of these objects. The formation of such registers is based on the method of assigning objects to the critical infrastructure of the state, including on the relevant criteria that will determine the affiliation of a particular object to one that is critical to the state. The analysis of the existing criteria for classifying objects as critical infrastructure of the state shows that in Ukraine there are a number of other criteria (and which should also be taken into account) involved in the formation of registers of important objects for the state, such as "State Register of Potentially Dangerous Objects". Therefore, it is proposed to form a list of such generalized criteria for classifying objects as critical infrastructure of the state in the form of a basic set, which integrates ten features with the possibility of further expansion. This set can be used to determine the priority of cyber protection of information and telecommunications systems (critical information infrastructure facilities) of critical infrastructure facilities of the state.
Key words: *objects of critical infrastructure of the state, set of criteria of criticality, critical information infrastructure.*

Дрейс Юрій Олександрович, кандидат технічних наук, доцент, старший науковий співробітник Національної академії СБ України.
Дрейс Юрий Александрович, кандидат технических наук, доцент, старший научный сотрудник Национальной академии СБ Украины.
Yurii Dreis, PhD in Eng. (Information security), Associate Professor, Senior Research Fellow of the National Academy of Security Service of Ukraine (Kyiv, Ukraine).

Деркач Леонід Васильович, старший науковий співробітник Національної академії СБ України.
Деркач Леонид Васильевич, старший научный сотрудник Национальной академии СБ Украины.
Leonid Derkach, General of the Army of Ukraine, Senior Research Fellow of the National Academy of Security Service of Ukraine (Kyiv, Ukraine).

Отримано *15 березня 2021 року*, затверджено редколегією *19 квітня 2021 року*

ПРИВАТНІСТЬ ТА ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ / PRIVACY&PROTECTION FROM IDENTITY THEFT

DOI: 10.18372/2225-5036.26.14974

РОЗСЛІДУВАННЯ КІБЕРЗЛОЧИНІВ ЗА ДОПОМОГОЮ ПРИМАНОК У ХМАРНОМУ СЕРЕДОВИЩІ

Опірський Іван, Сусукайло Віталій, Василишин Святослав

Національний університет «Львівська політехніка»

ОПІРСЬКИЙ Іван Романович, д.т.н., проф.
Рік та місце народження: 1987 рік, м. Сімферополь, АР Крим, Україна.
Освіта: Національний університет «Львівська Політехніка», 2008 рік.
Посада: професор кафедри захисту інформації з 2019 року.
Наукові інтереси: методи і засоби технічного захисту інформації, охорона державної таємниці, проектування комплексних систем захисту інформації, лазерні системи акустичної розвідки, математичні методи та моделі захисту інформації, технічні канали витоку інформації, спецвимірювання.
Публікації: більше 120 наукових публікацій, серед яких наукові статті, монографії, навчальні посібники, тези та матеріали доповідей на конференціях.
E-mail: iopirsky@gmail.com.
Orcid ID:0000-0002-8461-8996.