Коваленко Юлия Борисовна, кандидат педагогических наук, доцент кафедры безопасности информационных технологий Национального авиационного университета.
E-mail: yleejulee22@gmail.com.
Коваленко Юлія Борисівна, кандидат педагогічних наук, доцент кафедри безпеки інформаційних технологій Національного авіаційного університету.
Kovalenko Yulia, PhD, Associate Professor of IT-Security Academic Department, National Aviation University.
Гололобов Андрей Юрьевич, аспирант кафедры безопасности информационных технологий Национального авиационного университета.
E-mail: burn2dust@gmail.com.
Гололобов Андрій Юрійович, аспірант кафедри безпеки інформаційних технологій Національного авіаційного університету.
Gololobov Andrew, postgraduate student of IT-Security Academic Department, National Aviation University.

УДК 004.056.5

КЛАСИФІКАЦІЯ ЗАГРОЗ ДЕРЖАВНИМ ІНФОРМАЦІЙНИМ РЕСУРСАМ НОРМАТИВНО-ПРАВОВОГО СПРЯМУВАННЯ. МЕТОДОЛОГІЯ ПОБУДОВИ КЛАСИФІКАТОРА

Олександр Юдін, Сергій Бучик

У статті проведено узагальнений авторами аналіз власних останніх досліджень та публікацій за тематикою побудови методології класифікатора загроз державним інформаційним ресурсам. Вказано, що підґрунтям для формування «Класифікатора загроз державним інформаційним ресурсам» є запропонований авторами метод «подвійної трійки захисту» інформаційних ресурсів, основою якого є дві платформи захисту. Перша платформа інформаційної безпеки – складові, що підлягають захисту (властивості інформації): конфіденційність; цілісність; доступність. Друга платформа інформаційної безпеки – складові, що реалізують систему захисту (методи та засоби): нормативно-правові; організаційні; інженерно-технічні. Показано місце загроз державним інформаційним ресурсам нормативно-правового спрямування в загальній системі класифікатора. Здійснено уточнення семантики класифікатора з урахуванням поділу загроз на стратегічні, до яких відносяться загрози, що стосуються питань національної безпеки, відсутності або невиконання цільових програм чи доктрин, послаблення галузевих взаємозв'язків органів державної й законодавчої влади, тощо та тактичні, що направлені безпосередньо на інформаційні системи обробки, зберігання і передачі державних інформаційних ресурсів. Визначені загрози нормативно-правового спрямування з урахуванням досвіду авторів, існуючої нормативно-правової бази та інших джерел інформації. Для здійснення подальшої кодифікації надалі кожну загрозу віднесено до певних параметрів: за джерелом загрози; за відношенням до інформаційного об'єкту; за характером загрози; за структурою впливу; за рівнем впливу. Намічено напрямки подальших досліджень, які мають бути направлені на визначення загроз організаційного та інженерно-технічного спрямування. Вказано на необхідність подальшого вдосконалення нормативної бази з метою захисту державних інформаційних ресурсів.

Ключові слова: *державні інформаційні ресурси, класифікатор загроз, загроза, нормативно-правове спрямування, конфіденційність, цілісність, доступність.*

Актуальність дослідження. Спираючись на дослідження, які були проведені авторами та опубліковані раніше [1, 2, 3], виникає необхідність в здійсненні (в деяких випадках уточнені та приведенні з точки зору розширеного визначення державних інформаційних ресурсів [1]) розкриття загроз державним інформаційним ресурсам (ДІР) як нормативно-правового спрямування (НПС), що є предметом розгляду даної статті, так і організаційного та інженерно-технічного спрямування. Це в свою чергу обумовлює актуальність даної тематики.

Аналіз останніх досліджень та публікацій. Як вказано вище, авторами здійснено ретельний аналіз проблеми створення методології побудови класифікатора загроз ДІР, основи якого закладені в роботах [4, 5], де викладено ряд сучасних теоретичних та практичних підходів до вирішення нормативно-правових та організаційно-технічних завдань для реалізації процесу захисту інформаційних ресурсів. Також основою для цього послужили роботи із нормативно-правового аналізу захисту ДІР [6], їх уразливості [7] та визначення переліку загроз [8]. В подальшому авторами визначено правові аспекти формування системи ДІР [1], уточнено деякі визначення, що відносяться до понять загроза ДІР та атака на ДІР [3] та, як результат, запропонована методологія

побудови класифікатора загроз ДІР [2]. Узагальнений авторами аналіз їх останніх досліджень та публікацій представлено на рис. 1.

Мета статті. Виходячи з наведеного, мета статті полягає у здійсненні визначення загроз державним інформаційним ресурсам нормативно-правового спрямування з урахуванням розробленої методології побудови їх класифікатора та подальшого удосконалення самого класифікатора [2].

Виклад основного матеріалу. Перед тим, як навести опис загроз ДІР НПС, нагадаємо про складові, що відносяться до методології побудови класифікатора загроз та внесемо певні зміни до нього. Як визначено в [2], підґрунтям для формування «Класифікатора загроз ДІР» є запропонований авторами метод «подвійної трійки захисту» інформаційних ресурсів, основою якого є дві платформи захисту. Перша платформа інформаційної безпеки (ІБ) – складові, що підлягають захисту (властивості інформації): конфіденційність; цілісність; доступність. Друга платформа ІБ – складові, що реалізують систему захисту (методи та засоби): нормативно-правові; організаційні; інженерно-технічні.

Відповідно до цього отримана наступна початкова класифікація для ДІР (рис. 2):

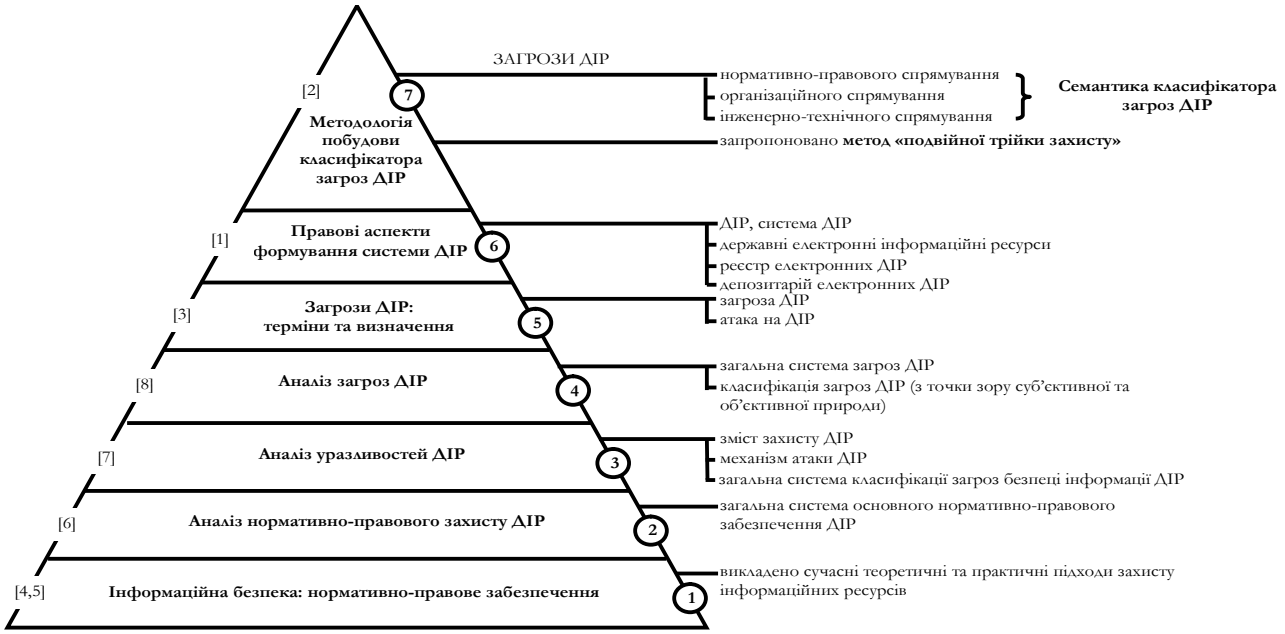

Рис. 1. Узагальнений авторами аналіз їх останніх досліджень та публікацій

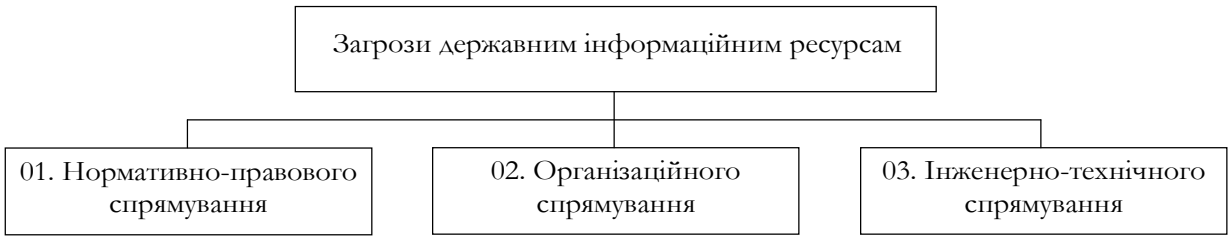

Рис. 2. Класифікація загроз ДІР за характером спрямування

де загрози *нормативно-правового спрямування (01)* – представляють собою загрози, які виникають в разі навмисного або ненавмисного порушення (впливу або/та дії на процес створення та застосування) спеціальних законів, інших нормативно-правових актів, правил, процедур та заходів, що забезпечують захист інформації на правовій основі (в даній статті розглядаємо загрози тільки НПС, визначення загроз інших спрямувань приведено в [2]).

Пропонується ввести додаткові принципи класифікації (представлені в середній частині рис.3), по-перше: загрози ДІР стратегічного характеру (01_1). До них требо віднести загрози, що стосуються питань національної безпеки, відсутності або не виконання цільових програм чи доктрин, послабленням галузевих взаємозв'язків органів державної й законодавчої влади, тощо. Практично всі ці загрози загального типу та мають вплив на всі три властивості ресурсу одночасно: конфіденційність, цілісність, доступність (01_1.1_2_3.1, К,Ц,Д 01,02,03). Більшість зазначеного типу загроз представлено в законодавчих та нормативних актах, таких як: Концепції, Доктрини, Державні Програми тощо.

По-друге, необхідно професійно деталізувати питання захисту інформаційних ресурсів безпосередньо для самої інформаційної системи обробки, а також процесів зберігання і передачі ДІР (ІС ДІР, РеєстрЕлДІР, ДепозитарійЕлДІР) – загрози ДІР тактичного характеру (01_2). Однак, формалізуємо цей розподіл тільки підкреслюючи додаткові принципи класифікації за стратегічним або тактичним характером, а кодифікацію зробимо наскрізну за наявністю повного переліку загроз.

Рис. 3. Поділ загроз нормативно-правового спрямування у відповідності до основаних властивостей інформації

Уточнена семантика класифікатора загроз з урахуванням поділу на стратегічні та тактичні загрози ДІР представлена на рис. 4. Опис класифікатора складається з п'яти числових частин. Класифікатор включає: позначення спрямування загрози (01 – нормативно-правове, 02 – організаційне, 03 – інженерно-технічне); позначення, що характеризує рівень загроз (0х_1 – стратегічний, 0х_2 – тактичний); позначення, що характеризує тип загроз (0х_х.1 – конфіденційність, 0х_х.2 – цілісність , 0х_х.3 – доступність); позначення виду загрози в залежності від типу (0х_х.1.х, 0х_х.2.х, 0х_х.3.х); додаткова інформація про направленість загрози. Всі частини класифікатора відділяються один від одного крапкою, лише рівень загроз нижнім підкреслюванням (рис. 4).

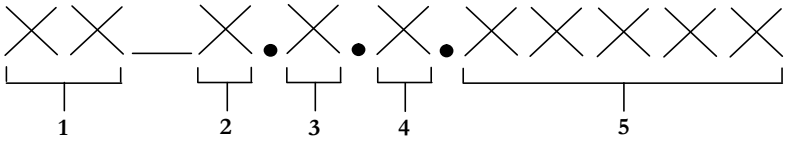

Рис. 4. Класифікатор загроз державним інформаційним ресурсам (1 – спрямування, 2 – рівень, 3 – тип, 4 – вид, 5 – додаткова інформація)

Також в [2] приведені в якості прикладу основні загрози ДІР нормативно-правового спрямування, але з урахуванням поділу за рівнем загроз (стратегічний, тактичний) здійснимо їх уточнення. Зрозуміло, що даний перелік не є повним та догматичним. Більш широкий опис буде представлено в монографії "Класифікатор загроз державним інформаційним ресурсам". Також даний класифікатор повинен постійно оновлюватись в залежності від розвитку інформаційного суспільства.

Таким чином до ***основних стратегічних загроз ДІР нормативно-правового спрямування (01_1.1_2_3)*** можна віднести наступні:

Стратегічні 01_1.1_2_3.

01_1.1_2_3.1 загрози державній політики України в сфері інформатизації та її безпеки ^{к,ц,д,01,02};

01_1.1_2_3.2 діяльність іноземних політичних, економічних і військових розвідувальних та інформаційних структур, спрямована проти інтересів України в інформаційній сфері ^{к,ц,д,01,02,03};

01_1.1_2_3.3 розробка деякими державами концепцій *інформаційних воєн*, що передбачають створення засобів небезпечного впливу на інформаційні сфери інших країн, порушення нормального функціонування інформаційних і телекомунікаційних систем зберігання інформаційних ресурсів, одержання несанкціонованого доступу до них (в т.ч. ДІР) ^{к,ц,д,01,02,03};

01_1.1_2_3.4 недостатня координація діяльності органів державної влади з формування і реалізації єдиної державної політики в галузі забезпечення інформаційної безпеки України та захисту ДІР, а також низький організаційно-технічний рівень інформатизації органів державної влади ^{к,ц,д,01,02};

01_1.1_2_3.5 недосконаліть нормативної правової бази, що регулює відносини в інформа-

ційній сфері, а також недостатня практика застосування норм права к,ц,д,01,02;

01_1.1_2_3.6 нерозвиненість інститутів громадянського суспільства і недостатній державний контроль за розвитком ДІР та інформаційного ринку України к,ц,д,01,02;

01_1.1_2_3.7 відсутність Державних економічних програм та недостатнє фінансування заходів із забезпечення інформаційної безпеки держави, а також недосконаліть системи страхування інформаційних ризиків фізичних і юридичних осіб к,ц,д,01,02;

01_1.1_2_3.8 зниження ефективності системи освіти і виховання, недостатня кількість кваліфікованих кадрів в галузі забезпечення інформаційної безпеки, а також зниження наукового потенціалу в галузі інформатизації та безпеки інформаційних технологій к,ц,д,01,02;

01_1.1_2_3.9 недостатня активність органів державної влади щодо інформування суспільства про свою діяльність, роз'яснення прийнятих рішень, формування системи відкритих державних ресурсів і розвитку системи доступу до них громадян к,ц,д,01,02,03;

01_1.1_2_3.10 відставання України від провідних країн світу за рівнем інформатизації органів державної влади і місцевого самоврядування, промисловості, сфери послуг і побуту громадян, тощо к,ц,д,01,02,03;

01_1.1_2_3.11 відсутність (або\чи часткова) діяльності державних органів виконавчої влади із застосування правових норм, включаючи попередження і припинення правопорушень в інформаційній сфері, а також виявлення, викриття і притягнення до відповідальності осіб, що скоїли злочини та інші правопорушення в цій сфері к,ц,д,01,02;

01_1.1_2_3.12 відсутність системи удосконалення процесів сертифікації інформаційно-телекомунікаційного обладнання, систем захисту інформації, а також програмного забезпечення автоматизованих систем обробки інформації на відповідність вимогам к,ц,д,01,02.

Тактичні 01_2

До основних *тактичних* ***загроз конфіденційності ДІР нормативно-правового спрямування (01_2.1)*** можна віднести наступні:

01_2.1.1 відсутність (не виконання) сформованої політики безпеки при зберіганні, обробці, передачі та відображенні ДІР в автоматизованих (інформаційній) системах різних класів к,ц,д,01,02,03;

01_2.1.2 не виконання вимог до впровадження (відсутність впровадження, повна\часткова) та реалізації організаційних заходів захисту ДІР згідно Законодавчої бази, Державних стандартів, нормативних документів і інструкцій, інших виробничих документів (в т.ч. загрози безпеці інформації обмеженого доступу (ІзОД), зокрема державної таємниці) к,ц,д,01,02;

01_2.1.3 порушення встановленого законодавством режиму проектування, технічного обладнання та впровадження приміщень призначених для обробки, зберігання, передавання і відображення ДІР к,ц,д,01,02;

01_2.1.4 відсутність (повна\часткова) правил та вимог (в т.ч. відповідальність) до розподілу обов'язків осіб, що відповідають за процеси розробки, впровадження і супроводу інформаційних систем, а також комплексів засобів захисту ДІР к,ц,д,01,02;

01_2.1.5 порушення режиму охорони об'єкту (об'єкту інформаційної діяльності), а також несанкціоноване проникнення на територію та приміщення де оброблюються й зберігаються ДІР к,ц,д,01,02;

01_2.1.6 порушення пропускного режиму безпосередньо до інформаційної системи (ІС) й технічних засобів обробки, зберігання, передавання і відображення ДІР к,ц,д,01,02;

01_2.1.7 відсутність системи підготовки кадрів (в т.ч. підвищення кваліфікації), а також порушення процедур при підборі фахівців для роботи з ДІР к,ц,д,01,02;

01_2.1.8 невиконання договірних зобов'язань, щодо захисту ДІР та правил доступу до даних і послуг третьою стороною к,ц,д,01,02;

01_2.1.9 оброблення, зберігання, передача і відображення інформації в АС ДІР без застосування комплексної системи захисту інформації (КСЗІ) з підтвердженою відповідністю ресурсу до ІзОД к,ц,д,01,02,03;

01_2.1.10 відсутність (повна\часткова) політики управління доступом до ДІР в розподіленому та об'єднаному інформаційному середовищі (або\чи узгодженості між політиками різних систем, що співпрацюють), а також відсутність класифікації інформації з обмеженим доступом (в наразі, якщо ДІР до неї відноситься) та правил доступу до ІзОД к,ц,д,01,02;

01_2.1.11 використання не ліцензійного програмного забезпечення (ПЗ), а також не атестованих (або\чи не сертифікованих) програмно-апаратних комплексів зберігання, обробки, передачі та захисту ДІР в автоматизованих (інформаційних) системах різних класів к,ц,д,01,02;

01_2.1.12 порушення або не виконання єдиної системи Державних стандартів та правових

норм криптографічного та технічного захисту інформації (безпосередньо захист ДІР) у відповідності до чинного законодавства к,ц,д,01,02;

01_2.1.13 невиконання організаційно-технічних вимог та розпорядчих документів, що стосуються розробки, впровадження і реалізації політики безпеки інформаційних систем ДІР, РеєструЕлДІР та ДепозитаріюЕлДІР к,ц,д,01,02;

01_2.1.14 відсутність або порушення загальної встановленої системи розподілу доступу (моделі доступу, матриці доступу, атрибутів доступу, системи ідентифікації і автентифікації, тощо), не виконання правил і вимог зміни паролів або ідентифікаторів до інформаційних ресурсів або\чи інформаційної системи ДІР к,ц,д,01,02,03;

01_2.1.15 несанкціоноване перехоплення, одержання та використання атрибутів доступу з наступним їхнім використанням для процедур маскування під авторизованого Адміністратора (власника інформаційної системи, адміністратора безпеки, користувача, тощо) інформаційної системи ДІР, РеєструЕлДІР або ДепозитаріюЕлДІР к,ц,д,01,02,03;

01_2.1.16 відсутність вимог та технічних характеристик моніторингу і контролю (корекції процесів) за робочими процесами ІС, а також не визначення оцінки ефективності щодо захисту ДІР к,ц,д,01,02,03;

01_2.1.17 неналежне виконання Адміністратором (власником інформаційної системи, адміністратором безпеки, користувачами, тощо) інформаційної системи ДІР, РеєструЕлДІР або ДепозитаріюЕлДІР своїх обов'язків (забезпечення функціонування ІС відповідно до вимог політики безпеки, здійснення контролю доступу, створення і супровід КСЗІ, визначення оцінки ефективності КСЗІ і корекція процесів, своєчасне оновлення інформаційного ресурсу та належного ПЗ, інші роботи пов'язані з РеєстромЕлДІР або ДепозитаріємЕлДІР) к,ц,д,01,02,03;

01_2.1.18 відсутність (повна або часткова) процедур реалізації методів і засобів технічного та криптографічного захисту ДІР, а також контролю за цими процесами згідно чинного законодавства к,ц,д,01,02,03;

01_2.1.19 відсутність або порушення загальної встановленої системи розподілу доступу, зміни, збереження й управління криптографічними ключами при їх використанні згідно чинного законодавства к,ц,д,01,02,03;

01_2.1.20 відсутність (повна\часткова) внутрішніх стандартів, розпорядчих документів, щодо впровадження, використання та регулярного оновлення антивірусних баз і ПЗ к,ц,д,01,02;

01_2.1.21 відсутність організаційних заходів та їх впровадження, щодо виявлення технічних пристроїв і програм, які загрожують штатному функціонуванню інформаційних систем, запобігання перехопленню й витоку інформації технічними каналами (в т.ч. неправомірне підключення – «врізання» до комутативних або без комутативних каналів зв'язку, тощо), а також відсутність контролю за виконанням спеціальних вимог із захисту ДІР к,ц,д,01,02,03;

01_2.1.22 відсутність або\чи неналежне ведення журналів реєстрації або аудиту та інцидентів (в т.ч. розслідування інцидентів) робочих процесів к,ц,д,01,02;

01_2.1.23 втрата, викрадення або не санкціоноване знищення журналів реєстрації або аудиту та інцидентів (в т.ч. розслідування інцидентів) робочих процесів к,ц,д,01,02;

01_2.1.24 відсутність програми і порядку фінансування, що стосуються розробки, впровадження та супроводу засобів (комплексів) захисту ДІР к,ц,д,01,02;

01_2.1.25 відсутність (не виконання) *затвердженої інформаційної політики безпеки організації*, як сукупності вимог і керівних принципів в області інформаційної безпеки, якими керується у своїй діяльності організація к,ц,д,01,02;

01_2.1.26 відсутність (не виконання) *положення про відділ захисту інформації Управління безпеки організації*, яке визначає порядок діяльності відділу захисту інформації Управління безпеки, його структуру, основні завдання, функції, права, обов'язки та порядок взаємодії з іншими підрозділами організації к,ц,д,01,02;

01_2.1.27 відсутність (не виконання) *положення про відділ режиму та захисту об'єктів Управління безпеки організації*, яке визначає порядок діяльності відділу режиму та захисту об'єктів Управління безпеки, його структуру, основні завдання, функції, права, обов'язки та порядок взаємодії з іншими підрозділами організації к,ц,д,01,02;

01_2.1.28 відсутність (не виконання) *положення про забезпечення захисту інформації в інформаційно-телекомунікаційних системах*, яке визначає загальні вимоги, організаційні засади забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах організації та виконавців цих робіт к,ц,д,01,02;

01_2.1.29 відсутність (не виконання) *положення про службу безпеки організації в цілому та її підрозділів*, яке визначає порядок підпорядкованості та діяльності служби безпеки організації (підрозділів), її структуру, основні завдання, функції, права,

обов'язки та порядок взаємодії з іншими підрозділами [к,ц,д,01,02];

01_2.1.30 відсутність (не виконання) *положення про інформаційно-аналітичний відділ Управління безпеки організації*, яке визначає порядок діяльності інформаційно-аналітичного відділу Управління безпеки організації, його структуру, основні завдання, функції, права, обов'язки та порядок взаємодії з іншими підрозділами організації [к,ц,д,01,02];

01_2.1.31 відсутність (не виконання) *регламентованого порядку доступу до інформаційних ресурсів організації*, яке визначає регламент замовлення працівниками організації та погодження й затвердження прав доступу на використання інформаційних ресурсів, що використовуються у організації [к,ц,д,01,02];

01_2.1.32 відсутність (не виконання) *інструкції з пропускного і внутрішньооб'єктового режиму*, яка визначає порядок пропускного та внутрішньооб'єктового режиму, регламентує дії працівників організації у штатних і позаштатних ситуаціях [к,ц,д,01,02];

01_2.1.33 відсутність (не виконання) *положення про інформаційну політику організації*, визначає основні принципи інформаційної політики організації, перелік інформації та документів, які можуть бути розголошені перед громадськістю (Зацікавленими особами), а також встановлює порядок надання такої інформації та документів і порядок взаємодії організації та Зацікавлених осіб [к,ц,01,02];

01_2.1.34 відсутність (не виконання) *положення про організацію доступу до мережі Інтернет*, яке призначено для вдосконалення захисту інформації організації під час роботи в мережі Інтернет та підвищення ефективності використання Інтернет [к,д,01,02];

01_2.1.35 відсутність (не виконання) *положення про антивірусний захист інформації*, яке визначає перелік робіт і розподіл обов'язків працівників організації в процесі організації антивірусного захисту інформації на серверах та робочих станціях організації [к,д,01,02].

До основних *тактичних* ***загроз цілісності ДІР нормативно-правового спрямування (01_2.2)*** можна віднести наступні:

01_2.2.1–01_2.2.32 (*див. загрози 01_2.1.1–01_2.1.32*);

01_2.2.33 (*див. загрози 01_2.1.33*);

01_2.2.34 несанкціонована модифікація процедур штатного функціонування або не авторизоване внесення змін в стандартне ПЗ сервісів і додатків АС ДІР різних класів (несанкціонована фальсифікація та модифікація текстів та функцій ПЗ, нехтування правилами і проектами змін, відсутність документального оформлення порушень або змін, тощо) [ц,д,01,02,03];

01_2.2.35 несанкціонована модифікація процедур штатного функціонування або не авторизоване внесення змін в ПЗ операційної системи (ОС) АС ДІР різних класів (несанкціонована фальсифікація та модифікація текстів та функцій ОС, нехтування проектами і проектами змін, відсутність документального оформлення порушень або змін ОС, тощо) [ц,д,01,02,03];

01_2.2.36 несанкціонована модифікація процедур штатного функціонування або не авторизоване внесення змін в ПЗ, що забезпечує стандартні режими встановлених послуг АС ДІР різних класів (несанкціонована фальсифікація та модифікація текстів та функцій ПЗ, нехтування правилами і проектами змін, відсутність документального оформлення порушень або змін ПЗ, тощо) [ц,д,01,02,03];

01_2.2.37 несанкціонована модифікація процедур штатного функціонування або не авторизоване внесення змін в ПЗ системи електронного документообігу (в т.ч. електронної комерції) ІС ДІР, РеєстрЕлДІР або ДепозитарійЕлДІР (несанкціонована фальсифікація та модифікація текстів та функцій ПЗ, нехтування проектами змін, відсутність документального оформлення порушень або змін, тощо) [ц,д,01,02,03];

01_2.2.38 подання власником або\чи Адміністратором інформаційного ресурсу (власником інформаційної системи, адміністратором безпеки, авторизованими користувачами, тощо) недостовірних відомостей (даних) до інформаційної системи ДІР, РеєструЕлДІР або ДепозитаріюЕлДІР та їх навмисна (не навмисна) фальсифікація й модифікація[01,02,03].

До основних *тактичних* ***загроз доступності ДІР нормативно-правового спрямування (01_2.3)*** можна віднести наступні:

01_2.3.1–01_2.3.32 (*див. загрози 01_2.1.1–01_2.1.32, 01_2.2.1–01_2.2.32*);

01_2.3.33–01_2.3.36 (*див. загрози 01_2.2.34–01_2.2.37*);

01_2.3.37–01_2.3.38 (*див. загрози 01_2.1.34–01_2.1.35*).

Позначками у верхньому індексі проставлено вплив на властивості інформації (к – конфіденційність, ц – цілісність, д – доступність) та на відповідні спрямування (01 – нормативно-правове, 02 – організаційне, 03 – інженерно-технічне).

Надалі кожну загрозу відносимо: за джерелом загрози (антропогенні, техногенні, стихійні); за відношенням до інформаційного об'єкту (внут-

рішні, зовнішні); за характером загрози (навмисні, ненавмисні); за структурою впливу (системні, структурні, елементні); за рівнем впливу (фізичні засоби, мережне обладнання, мережні додатки та сервіси, операційна система, системи управління базами даних).

На основі вищенаведеного та з урахуванням запропонованому авторами підходу щодо класифікатора загроз ДІР [2], можна скласти наступну (як приклад) класифікацію ДІР нормативно-правового спрямування (табл. 1).

Таблиця 1

Приклад класифікації загроз ДІР нормативно-правового спрямування

Спрямування загроз	**Рівень загроз**	**Вид загроз**	**Функціональний профіль загроз**	**Джерело загроз**			**За відношенню до інформаційного об'єкту**		**Характер загрози**		**Загрози за структурою впливу**			**Рівні впливу загрози**				
				Антропогенні	*Техногенні*	*Стихійні*	*Внутрішні*	*Зовнішні*	*Навмисні*	*Ненавмисні*	*Системні*	*Структурні*	*Елементні*	*Фізичні засоби (лінії зв'язку, апаратні засоби)*	*Мережне обладнання*	*Мережні додатки та сервіси*	*Операційна система*	*Системи управління базами даних*
01 Нормативно-правового спрямування	**01_1**	01_1.1_2_3 Конфіденційність Цілісність Доступність	01_1.1_2_3.1 загрози державній політики України в сфері інформатизації та її безпеки к,ц,д,01,02	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
			……	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…
	01_2	01_2.1 Конфеденційність	01_2.1.3 порушення встановленого законодавством режиму проектування, технічного обладнання та впровадження приміщень призначених для обробки, зберігання, передавання і відображення ДІР к,ц,д,01,02	1	0	0	1	0	1	0	1	1	1	1	1	0	0	0
		……	……	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…
		01_2.3 Достуність	01_2.3.24 відсутність програми і порядку фінансування, що стосуються розробки, впровадження та супроводу засобів (комплексів) захисту ДІР к,ц,д,01,02	1	0	0	1	1	1	0	1	1	1	1	1	1	1	1

Основні результати. Виходячи з вищевказаного, основним результатом дослідження автори вважають подальше удосконалення та розширення методології побудови класифікатора загроз ДІР за рахунок уточнення семантики класифікатора (введення поділу на стратегічні та тактичні загрози) та визначення основних загроз нормативно-правового спрямування з урахуванням уточненого класифікатора.

Висновок. Таким чином, в статті авторами показано взаємозв'язок останніх публікацій з тематикою дослідження, місце тематики статті в загальній системі побудови класифікатора загроз ДІР, проведено подальше уточнення семантики класифікатора, визначені загрози ДІР нормативно-правового спрямування. Намічено напрямки подальших досліджень, а саме: проведення ви-

значення загроз організаційного та інженерно-технічного спрямування.

ЛІТЕРАТУРА

[1]. Юдін О.К. Правові аспекти формування системи державних інформаційних ресурсів / О.К. Юдін, С.С. Бучик // Безпека інформації. – 2014. – Том 20 (1). – С. 76-82.

[2]. Юдін О.К. Методологія побудови класифікатора загроз державним інформаційним ресурсам / С. Бучик, А. Чунарьова, О. Варченко // Наукоємні технології. – 2014. – №2 (22). – С. 200-210.

[3]. Юдін О.К. Загрози державним інформаційним ресурсам: терміни та визначення / С.С. Бучик, О.К. Юдін // Захист інформації. – 2014. – Том 16 (2). – С. 121-125.

[4]. Богуш В.М. Інформаційна безпека держави / О.К. Юдін. – К.: "МК-Прес", 2005. – 432 с.

[5]. Юдін О.К. Інформаційна безпека. Нормативно-правове забезпечення: підруч. / О.К. Юдін. – К.: НАУ, 2011. – 640 с.

[6]. The analysis of normatively-legal providing of defence of state informative resources in information–telecommunication systems / O. Yudin, S. Buchyk // Science-based technologies. – 2013. – №2 (18). – P. 202-206.

[7]. Юдін О.К. Концептуальний аналіз уразливості державних інформаційних ресурсів / О.К. Юдін, С.С. Бучик // Наукоємні технології. – 2013. – №3 (19). – С. 299–304.

[8]. Юдін О.К. Аналіз загроз державним інформаційним ресурсам / О.К. Юдін, С.С. Бучик // Проблеми інформатизації та управління. – 2013. – №4 (44). – С. 93-99.

REFERENCES

[1]. Yudin O., Buchyk S. (2014) "Legal aspects of the state information resources system formation", Bezpeka ìnformacìì, №20 (1), P. 76-82.

[2]. Yudin O., Buchyk S., A. Chunareva, O. Frolov (2014) "Methodology of construction of classifier of threats to the state informative resources", Science-based technologies, №2 (22), P. 200-210.

[3]. Yudin O., Buchyk S. (2014) "Threat state informative resources. Terms and determinations", Zahist ìnformacìì, №16 (2), P. 121-125.

[4]. Bogush V., Yudin A. (2005) "Information security of the state", K.: MK-Press, 432 p.

[5]. Yudin O.K.. (2011) "Informative security. Normatively legal providing", K.: NAU, 640 p.

[6]. Yudin O., Buchyk S. (2013) "The analysis of normatively–legal providing of defence of state informative resources in information–telecommunication systems", Science-based technologies, №2 (18), P. 202-206.

[7]. Yudin O., Buchyk S. (2013) "The conceptual analysis of vulnerability of state informative resources is conducted", Science-based technologies, №3 (19), P. 299-304.

[8]. Yudin O., Buchyk S. (2013) "Analysis of threats to the state informative resources", Problems of informatization and management, №4 (44), Engineering sciences, P. 93-99.

КЛАССИФИКАЦИЯ УГРОЗ ГОСУДАРСТВЕННЫМ ИНФОРМАЦИОННЫМ РЕСУРСАМ НОРМАТИВНО-ПРАВОВОГО НАПРАВЛЕНИЯ. МЕТОДОЛОГИЯ ПОСТРОЕНИЯ КЛАССИФИКАТОРА

В статье проведен обобщенный авторами анализ их последних исследований и публикаций по тематике построения методологии классификатора угроз государственным информационным ресурсам. Указано, что базой для формирования «Классификатора угроз государственным информационным ресурсам» является предложенный авторами метод «двойной тройки защиты» информационных ресурсов, в основе которого лежат две платформы защиты. Первая платформа информационной безопасности - составляющие, которые подлежат защите (свойства информации): конфиденциальность; целостность; доступность. Вторая платформа информационной безопасности - составляющие, которые реализуют систему защиты (методы и средства): нормативно-правовые; организационные; инженерно-технические. Определено место угроз государственным информационным ресурсам нормативно-правового направления в общей системе классификатора. Осуществлено уточнение семантики классификатора с учетом разделения угроз на стратегические и тактические. Стратегические угрозы касаются вопросов национальной безопасности, отсутствия или невыполнения целевых программ или доктрин, ослабления отраслевых взаимосвязей органов государственной и законодательной власти и тому подобное. Тактические угрозы направлены непосредственно на информационные системы обработки, хранения и передачи государственных информационных ресурсов. Определены угрозы нормативно-правового направления с учетом опыта авторов, существующей нормативно-правовой базы и других источников информации. Для осуществления дальнейшей кодификации каждая угроза отнесена к определенным параметрам: по источнику угрозы; по отношению к информационному объекту; по характеру угрозы; по структуре влияния; по уровню влияния. Намечены пути дальнейших исследований, которые должны быть направлены на определение угроз организационного и инженерно-технического характера. Указано на необходимость дальнейшего совершенствования нормативной базы с целью защиты государственных информационных ресурсов.

Ключевые слова: государственные информационные ресурсы, классификатор угроз, угроза, нормативно-правовое направление, конфиденциальность, целостность, доступность.

CLASSIFICATION OF THREATS TO STATE INFORMATIVE RESOURCES OF NORMATIVELY-LEGAL ASPIRATION. METHODOLOGY OF CONSTRUCTION OF CLASSIFIER

In the article the analysis of their last researches and publications on the subjects of construction of methodology of classifier of threats of state informative resources generalized by the authors is conducted. It is indicated that the method of «double three of security» offered by authors is the fundamental for forming of «Classifier of threats of state informative resources» which is formed on the basis of the two platforms of security. The first platform of informative safety consists of elements which are subject to security (properties of information): confidentiality; integrity; availability. The second platform of informative safety consists of components which realize the system of security (methods and facilities): normatively-legal; organizational; technical. The place of threats of state informative resources of normatively-legal aspiration in the general system of classifier is shown. Clarification of semantics of classifier taking into account division of threats into strategic and tactical is carried out. Strategic threats concern the questions of national security, absence or non-fulfillment of the special purpose programs or doctrines, weakening of branch intercommunications of organs of state and legislative power and others like that. Tactical threats directed to the informative systems of treatment, storage and transmission of state informative resources. Certain threats of normatively-legal aspiration with taken into account experience of the authors, existent normatively-legal base and other information sources are defined. For the realization of further codification every threat is attributed to the certain parameters: according the source of threat; in relation to information holding object; by the nature of threats; by the structure of influence; by the level of influence. The ways of further researches which must be aimed at determination of threats of organizational and technical character are set. Directions of further researches are set, the necessity of further perfection of normative base with the purpose of security of state informative resources is indicated on.

Index terms: state informative resources, classifier of threats, threat, normatively-legal aspiration, confidentiality, integrity, availability.

Юдін Олександр Костянтинович, доктор технічних наук, професор. Член експертної та науково-методичної ради Міністерства освіти та науки України в галузі «Інформаційна безпека». Член-кореспондент Академії Зв'язку України. Лауреат Державної премії України у галузі науки і техніки. Директор інституту комп'ютерних інформаційних технологій, завідувач кафедри комп'ютеризованих систем захисту інформації Національного авіаційного університету.
E-mail: kszi@ukr.net.

Юдин Александр Константинович, доктор технических наук, профессор. Член экспертного и научно-методического совета Министерства образования и науки Украины в области «Информационная безопасность». Член-корреспондент Академии Связи Украины. Лауреат Государственной премии Украины в области науки и техники. Директор института компьютерных информационных технологий, заведующий кафедрой компьютеризованных систем защиты информации Национального авиационного университета.

Yudin Alexander, Dr. of Engineering, professor. Member of expert and scientifically-methodical advice of Department of education and science of Ukraine in an area «Information security». Corresponding member of Academy of Connection of Ukraine. Laureate of the State bonus of Ukraine in area of SciTech. Director of institute of computer information technologies, manager by the department of the computerized systems for information the National Aviation University.

Бучик Сергій Степанович, кандидат технічних наук, доцент, начальник кафедри автоматизованих систем управління Житомирського військового інституту імені С. П. Корольова Державного університету телекомунікацій.
E-mail: s_stbu@ukr.net.

Бучик Сергей Степанович, кандидат технических наук, доцент, начальник кафедры автоматизированных систем управления Житомирского военного института имени С.П. Королева Государственного университета телекоммуникаций.

Buchyk Sergii, PhD in Eng., chief of department of automated control the system the Zhitomir Military Institute of the name of S.P. Korolyova of the State University of Telecommunications.