Белецкий Анатолий Яковлевич, доктор технических наук, профессор кафедры электроники Национального авиационного университета.
E-mail: abelnau@ukr.net
Білецький Анатолій Якович, доктор технічних наук, професор кафедри електроніки Національного авіаційного університету.
Beletsky Anatoly, Doctor of Science, Professor of Department Electronics of National Aviation University.

Навроцький Денис Олександрович, аспірант кафедри електроніки Національного авіаційного університету.
E-mail: sg6336@yandex.ua
Навроцкий Денис Александрович, аспирант кафедры электроники Национального авиационного университета.
Navrotskyi Denys, Postgraduate student of Department Electronics of National Aviation University.

Семенюк Олександр Іванович, студент кафедри електроніки Національного авіаційного університету.
E-mail: sovist9@mail.ru
Семенюк Александр Иванович, студент кафедры электроники Национального авиационного университета.
Semenjuk Alexander, Student of Department Electronics of National Aviation University.

УДК 004.056.5

ЗАГРОЗИ ДЕРЖАВНИМ ІНФОРМАЦІЙНИМ РЕСУРСАМ: ТЕРМІНИ ТА ВИЗНАЧЕННЯ

Олександр Юдін, Сергій Бучик

Проведено аналіз існуючого нормативно-правового та законодавчого забезпечення, вітчизняних і міжнародних стандартів галузі «Інформаційна безпека». Детально розглянуто напрями, що регламентують питання поняття загрози, загрози інформаційній безпеці, загрози інформації. Проведено нормативно-правовий аналіз, на основі якого приведено найповніше поняття загроз державним інформаційним ресурсам та атаки на державні інформаційні ресурси. Визначено недоліки та встановлено відсутність загального системного підходу (методології побудови) до формування моделі порушника і моделі загроз державним інформаційним ресурсам на базі вітчизняних і міжнародних вимог і стандартів.

Ключові слова: *державні інформаційні ресурси, загроза, загроза інформації, загроза державним інформаційним ресурсам, атака на державні інформаційні ресурси.*

Вступ. Стрімке зростання новітніх технологій, а також розвиток інфраструктури інформаційно-комунікаційних мереж державного та загального призначення, призвело до створення інтегрованого інформаційного простору держави та всього суспільства. Інформаційні технології знаходять ширше застосування у таких сферах, як: державні системи управління, фінансовий обіг і ринок цінних паперів, розвинута система електронних платежів, система послуг зв'язку та телебачення, системи управління транспортом, високотехнологічні виробництва (особливо атомних, хімічних тощо) та ін. Будь-яке несанкціоноване та противоправне втручання у інформаційний простір наведених сфер життєдіяльності держави й суспільства може призвести до тяжких та не передбачуваних наслідків.

Особливого значення вирішення проблеми інформаційної безпеки державних інформаційних ресурсів (ДІР) набуває у сучасних умовах глобалізації інформаційних процесів, а також в умовах цілеспрямованих дій ряду розвинених держав та ІТ- корпорацій досягти домінування у світовому інформаційному просторі й на ринку ІТ- послуг.

Міжнародний та вітчизняний досвід демонструє, що забезпечення безпеки інформаційних ресурсів повинно носити комплексний характер. Однак, організація процесів безпеки має бути не просто комплексною складовою, але ще й засновуватися враховуючи всебічний аналіз можливих негативних загроз ДІР та їх можливих наслідків.

Здійснюючи аналіз напрямків забезпечення інформаційної безпеки держави, які являють нормативно-правові, організаційні, інженерно-технічні категорії, орієнтовані на забезпечення комплексного захисту інформації від внутрішніх та зовнішніх загроз на державному рівні, особисте значення набуває такий напрямок, як *правовий. Правовий захист ДІР* повинен формуватися на тлі загальної та спеціальної законодавчої бази держа-

ви, інших нормативних актів, постанов, стандартів, правил, що забезпечують захист інформації та безпосередньо її властивостей: конфіденційності, доступності, цілісності [2, 6].

Постановка задач досліджень. Проведений аналіз нормативно-правового забезпечення захисту державних інформаційних ресурсів (ДІР) в інформаційній сфері нашого суспільства свідчить про малосистемний характер відповідної діяльності, спостерігається нечітка спрямованість визначення класів загроз різним видам ДІР (мало деталізовані або відсутні). Крім того, на концептуальному та нормативному рівні не визначено перелік і класифікацію загроз інформаційним ресурсам держави, не розроблено нормативно-правового документу, стандарту із визначенням поняття *державних інформаційних ресурсів*, його складових та відповідної їм моделі загроз [2, 3, 6].

Звертаючись до теми загроз ДІР, їх класифікації в цілому, слід зазначити, що даному питанню приділяли увагу, як вітчизняні так і зарубіжні вчені. До них можна віднести: Новікова О.М., Богуша В.М., Мохора В.В., Горбенко І.Д., Хорошко В.О., Корнейко О.В., Грайворонського М.В., Корченка О.Г., Марущака А.І., Мельнікова В.П., Віхорева С.В., Касперского Е.В., Медведовського І.Д., Олійника О.В., Сосніна О.В. та ін. Але питанню створення класифікації та в подальшому моделі загроз ДІР (не тільки нормативно-правового спрямування) приділялось не достатньо уваги, про що свідчить існуюче нормативно-правове забезпечення захисту інформації.

Мета статті. Виходячи з наведеного, *мета статті* полягає у проведенні аналізу існуючого нормативно-правового та Законодавчого забезпечення (НПЗ), вітчизняних і міжнародних стандартів галузі «Інформаційна безпека», деталізації напрямків, що регламентують питання класифікації загроз ДІР, проведенні аналітично-правового аналізу, як підґрунтя для побудови моделі загроз ДІР, а також дослідженні загально-сформованої системи та найбільш поширених класів загроз інформаційним ресурсам підприємств, організацій і установ з різними формами власності. Як наслідок даного дослідження – надання більш розширених визначень таким поняттям як загроза ДІР та атака на ДІР.

Аналітично-правовий аналіз. Проводячи аналітично-правовий аналіз побудови класифікатора та моделі загроз ДІР, а також розглядаючи загально-сформовану систему та найбільш поширені класифікації загроз інформаційним ресурсам підприємств, організацій і установ з різними формами власності, можна зробити висновок про відсутність загально-спрямованої системи класифікації загроз ДІР.

Відповідна діяльність органів державної влади, носить розрізнений відомчий характер щодо формування реєстру ДІР, та безпосередньо системи класифікації загроз ресурсам держави. Не розроблено положення про модель загроз і порушника ДІР, за якою можна було би визначити вірогідні наміри порушника, ступінь небезпечності дій та несанкціонованих процесів; категорію осіб, серед яких може бути порушник, припущення про кваліфікацію та характер його дій, тощо. Не в повній мірі стандартизована політика безпеки державних інформаційних ресурсів, яка б представляла певний набір вимог, правил, обмежень, рекомендацій згідно класифікації ресурсів і загроз. З приведеного аналізу можна бачити, що ця проблематика існує, а деякі питання потребують негайного подальшого вдосконалення.

Матеріал представлений авторами має достатнє підґрунтя, що сформоване спираючись на попередні дослідження та встановлені підходи до аналізу системи загроз ДІР. Тому, що б не втратити логіку викладення матеріалу статті, запропонуємо основні отримані висновки і положення з зазначеного напрямку [2, 3, 4, 5, 6]. Авторами було сформовано сучасне визначення ДІР, а саме:

Державні інформаційні ресурси – це результати інтелектуальної та практичної діяльності, що сформовані в усіх сферах життєдіяльності людини, суспільства і держави, зафіксовані і систематизовані на відповідних матеріальних носіях інформації, як окремі документи і масиви документів, банки і бази даних та знань, усі види архівів і бібліотек, музейні фонди, інформаційні ресурси які обробляються й передаються у інформаційних системах державного і/або загального призначення, інші ресурси, що містять дані, відомості і знання, які *є об'єктом права власності держави* незалежно від форми власності на час їх створення і мають споживчу цінність, а також такі, що призначені для розвитку і задоволення потреб громадян, суспільства, держави та підлягають захисту згідно визначеної політики безпеки й чинного законодавства.

Однак, після формування матеріалу, 09 квітня 2014 року ВР України прийнято в цілому проект Закону про внесення змін до Закону України «Про Державну службу спеціального зв'язку та захисту інформації України» (№1194-18). У згаданому Законі наведений оновлений термін для ДІР: *державні інформаційні ресурси* – систематизована інформація, що є доступною за допомогою інформаційних технологій, право на володіння, використання або розпорядження якою належить органам державної влади, іншим державним ор-

ганам, військовим формуванням, а також інформація, створення якої передбачено законодавством, та яка обробляється фізичними або юридичними особами відповідно до наданих їм повноважень суб'єктами владних повноважень.

Загрози державним інформаційним ресурсам. Визначення. Інтереси держави в інформаційній сфері полягають у створенні умов для гармонійного розвитку інформаційної інфраструктури держави, реалізації конституційних прав і свобод людини і громадянина в інтересах зміцнення конституційного ладу, суверенітету і територіальної цілісності країни, встановлення політичної і соціальної стабільності, економічного процвітання, безумовного виконання законів і підтримки міжнародного співробітництва на основі партнерства.

Проведений аналіз висвітлює існуючу проблематику та подальші напрями досліджень – відсутність детального визначення й стандартизації класифікації ДІР, ускладнює або унеможливлює побудову *моделі загроз* ресурсам держави.

Загрози інформаційній безпеці [information security threat] – сукупність умов і факторів, що створюють небезпеку життєво важливим інтересам особистості, суспільства і держави в інформаційній сфері [1].

На даний час, існує достатньо великий перелік визначень поняття загроз інформації. Це різноманіття характеризується напрямами і видами інформаційних систем, а також структурою й призначенням комплексних систем захисту інформаційних ресурсів, деталізацією структури згідно впроваджених послуг і сервісів, тощо. Наведемо основні діючі нормативні визначення.

Загроза для інформації – витік, можливість блокування чи порушення цілісності інформації; таке визначення дає *ДСТУ 3396.2–97* «Захист інформації. Технічний захист інформації. Терміни та визначення».

Загроза інформації – будь-які обставини чи події, що можуть спричинити порушення політики безпеки інформації та (або) нанесення збитку інформаційно-комунікаційній системі (ІКС) [5].

Загроза інформації (дія) – це можлива небезпека (потенційна або така, що існує реально) вчинення будь-якого діяння (дії або бездіяльності), спрямованого проти об'єкта захисту (інформаційних ресурсів), яке завдає збитку власнику або користувачу, що проявляється як небезпека спотворення або втрати інформації [5].

Загроза (threat) – будь-які обставини або події, що можуть бути причиною порушення політики безпеки інформації і/або нанесення збитків АС [НД ТЗІ 1.1-003–99 «Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу»].

До захищених інформаційних систем належать інформаційні системи, які у певних умовах експлуатації забезпечують політику безпеки інформаційних ресурсів (конфіденційність, цілісність, доступність), що належать системі, та підтримують свою працездатність в умовах впливу на них заданої множини загроз.

Політика безпеки інформації (information security policy), визначена в державі нормативним документом НД ТЗІ 1.1-003–99 «Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу», як: сукупність законів, правил, обмежень, рекомендацій, інструкцій тощо, які регламентують порядок оброблення інформації.

Під загрозою безпеки інформаційним ресурсам будемо розуміти дії, які можуть призвести до спотворення, несанкціонованого використання або, навіть, до руйнування інформаційних ресурсів керованої системи, а також програмних і апаратних засобів [5]. Таким чином, *загроза* в загальному вигляді буде представляти собою будь-який потенційно можливий несприятливий вплив (дію або бездіяльність), який (яка) завдає збиток суб'єкту інформаційної діяльності і\або власнику ресурсів.

В цілому, будь яка інформаційна система піддана впливу наступним основним групам загроз щодо порушення властивостей інформаційних ресурсів [2]: конфіденційності, цілісності, доступності.

Сучасні інтереси інформаційного суспільства та держави, що вступила у стадію постіндустріального розвитку, полягають у захисті життєво важливих інтересів у цій сфері, забезпечення реалізації конституційних прав і свобод громадянина в інтересах зміцнення демократії, досягнення і підтримування суспільної злагоди, підвищення творчої активності населення.

Одним із базових джерел загроз інтересам суспільства в інформаційній сфері є безперервне ускладнення інформаційних систем і мереж передачі ДІР, критично важливих інфраструктур забезпечення життя суспільства.

Ці загрози можуть проявлятися у вигляді як навмисних, так і ненавмисних помилок, збоїв і відмов інтегрованих інформаційно-комунікаційних систем і програмного забезпечення, шкідливого впливу зі сторони злочинних структур і кримінальних елементів. Об'єктами реалізації таких структур можуть виступати системи військової, енергетичної, транспортної, комунікаційної і деяких інших інфраструктур.

Під *загрозою державним інформаційним ресурсам* (ЗДІР) можна розуміти протиправні дії, які можуть призвести до спотворення, несанкціонованого використання або руйнування державних інформаційних ресурсів (їх безпосередніх властивостей: конфіденційності, цілісності, доступності), які є власністю держави та необхідність захисту яких визначено законодавством [5].

Підсумовуючи все вищевикладене, можна дати визначення *загрози державним інформаційним ресурсам*.

Загроза державним інформаційним ресурсам – це потенційний або реальний стан небезпеки державним інформаційним ресурсам та безпосередньо їх властивостям (конфіденційності, цілісності, доступності), який може бути сформовано на основі реалізації будь-якого процесу та/або вчиненні діяння (та/або бездіяльності), спрямовано на порушення політики безпеки об'єкта інформаційної діяльності (державних інформаційних ресурсів) та такий, що завдає збитку державі.

Носіями загроз безпеці інформації є джерела загроз. Джерелами загроз можуть бути як суб'єктивні, так і об'єктивні прояви. Загрози, як можливі небезпечності здійснення будь-якої дії, спрямованої проти об'єкта захисту, проявляються не самі по собі, а через уразливості (фактори), що призводять до порушення безпеки інформації на конкретному об'єкті інформаційної діяльності.

Уразливості це властиві об'єкту інформатизації, невіддільні від нього, що обумовлюються недоліками процесу функціонування, властивостями архітектури автоматизованих систем, протоколами обміну та інтерфейсами, програмним забезпеченням і апаратною платформою, умовами експлуатації та розташування.

Джерела загроз можуть використовувати уразливості для порушення безпеки інформації, одержання незаконної вигоди (нанесення збитків власникові, користувачеві інформації). Крім того, можливі не зловмисні дії джерел загроз з активізації інших уразливостей, що приносять шкоду.

Кожній загрозі можуть бути зіставлені різноманітні уразливості. Усунення або суттєве послаблення уразливостей впливає на можливість реалізації загроз безпеці інформації.

Існують декілька напрямів при формуванні переліку актуальних загроз на об'єкті інформаційної діяльності експертно-аналітичним методом. Як правило, спочатку визначається перелік інформаційних ресурсів, що підлягають захисту та піддаються впливу тієї чи іншої загрози, встановлюються характерні джерела цих загроз і уразливості, що сприяють реалізації загроз. На основі аналізу експертів складається таблиця взаємозв'язку джерел загроз і уразливостей на основі яких визначаються можливі наслідки реалізації загроз (атаки) та встановлюється (обчислюється) коефіцієнт небезпеки цих атак. Коефіцієнт небезпеки атак є добуток коефіцієнтів небезпеки відповідних загроз (ймовірність реалізації загрози) та джерел загроз, визначених попереднім аналізом. При цьому передбачається, що атаки, які мають ймовірність небезпеки менше 0,1 або іншого встановленого рівня (припущення експертів або статистика), в подальшому можуть не розглядатися із-за малої ймовірності їх реалізації на об'єкті захисту. Після виявлення найбільш актуальних загроз, приймаються заходи з вибору методів і засобів для їх відбивання та мінімізації збитків на об'єкті інформаційної діяльності.

Таким чином, завжди існує сталий взаємозв'язок, між загрозою та ймовірністю її реалізації. При формуванні визначення – загроза, край необхідно мати висвітлення взаємно залежному з ним поняттю: *атака*. Атака, це наслідки загрози, що реалізована з встановленою (або не встановленою) ймовірністю. Ґрунтуючись на зазначеному та враховуючи попередні дослідження, надамо визначення поняттю атаки на ДІР [1, 2, 4]:

Атака на державні інформаційні ресурси – це можливі наслідки реалізації загрози державним інформаційним ресурсам, що сформовані на основі взаємодії джерела загрози через наявні фактори уразливості об'єкту інформаційної діяльності та такі, що приводять до різних видів збитків державі.

Висновки. Проведено аналіз існуючого нормативно-правового та Законодавчого забезпечення, вітчизняних і міжнародних стандартів галузі «Інформаційна безпека». Деталізовано напрями, що регламентують питання класифікації загроз державним інформаційним ресурсам, проведено аналітично-правовий аналіз визначень загроз ДІР, а також досліджено загальносформовану систему та найбільш поширені підходи до формування загроз інформаційним ресурсам підприємств, організацій і установ з різними формами власності. Надано розширені визначення понять *загроза державним інформаційним ресурсам* та *атака на державні інформаційні ресурси.*

ЛІТЕРАТУРА

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

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

[3]. Юдін О.К., Бучик С.С. Державні інформаційні ресурси. Нормативно-правовий аналіз, зміст та визначення / Безпека інформації. – 2014. – Вип. 1 (20). – С. 72-75.

[4]. Юдін О.К., Бучик С.С. Концептуальний аналіз уразливості державних інформаційних ресурсів / Наукоємні технології.–2013.–№3(19) / Технічні науки. – С. 299–304.
[5]. Юдін О.К., Бучик С.С. Аналіз загроз державним інформаційним ресурсам / Проблеми інформатизації та управління. – 2013. – №4(44) / Технічні науки. – С. 93–99.
[6]. Yudin O., Buchyk S. The analysis of normatively–legal providing of defence of state informative resources in information–telecommunication systems / Science-based technologies . – 2013. – №2 (18) / Engineering Sciences. – P. 202-206.

REFERENCES

[1]. Bogush V., Yudin A. (2005) "Information security of the state", K.: MK-Press, 432 p.
[2]. Yudin O.K.. (2011) "Informative security. Normatively legal providing", K.: NAU, 640 p.
[3]. Yudin O., Buchyk S. (2014) "State information resources. Analysis of the normative legal documents and definition of Abstract", Ukrainian Scientific Journal of Information Security, №1, pp. 72-75.
[4]. Yudin O., Buchyk S. (2013) "The conceptual analysis of vulnerability of state informative resources is conducted", Science-based technologies, №3(19), Engineering sciences, P. 299-304.
[5]. 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.
[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), Engineering Sciences, P. 202-206.

УГРОЗЫ ГОСУДАРСТВЕННЫМ ИНФОРМАЦИОННЫМ РЕСУРСАМ: ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Проведен анализ существующего нормативно правового и Законодательного обеспечения, отечественных и международных стандартов отрасли «Информационная безопасность». Детально рассмотрены направления, которые регламентируют вопрос понятия угроза, угрозы информационной безопасности, угрозы информации. Проведен аналитически-правовой анализ, на основе которого приведено более полное понятие угроз государственным информационным ресурсам и атака на государственные информационные ресурсы. Определены недостатки и установлено отсутствие в общих чертах системного подхода (методологии построения) по формированию модели нарушителя и модели угроз государственным информационным ресурсам на базе отечественных и международных требований и стандартов.

Ключевые слова: государственные информационные ресурсы, угроза, угроза информации, угроза государственным информационным ресурсам, атака на государственные информационные ресурсы.

GOVERNMENT INFORMATION RESOURCES THREAT: TERMS AND DETERMINATIONS

The analysis of the existent normatively-legal and Legislative providing, domestic and international standards of industry is conducted "Information security". Directions which regulate the question of concept threat are considered in detail, threat to informative safety, threat of information. An analytically-legal analysis on the basis of which more complete concept over of threats is brought to the state informative resources and attack on state informative resources is conducted. Defects are certain and absence is set in general lines approach (methodologies of construction) of the systems to forming of model of violator and model of threats to the state informative resources on the base of domestic and international requirements and standards.

Keywords: state informative resources, threat, threat of information, threat to the state informative resources, attack, are on state informative resources.

Юдін Олександр Костянтинович, доктор технічних наук, професор. 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. 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 Eng., professor. Laureate of the State Prize of Ukraine in Science and Technology. Director of computer information technologies institute, Head of computerized security systems academic department, 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.