КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (10), 2020
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2020.10.98112
УДК 316.776:004.58

Літвінчук Ірина Сергіївна
Науковий співробітник
Військова частина А1906, Київ, Україна
ORCID: 0000-0002-0854-5393
Litvinchuk.irina94@gmail.com

Корчомний Руслан Олександрович
Науковий співробітник
Військова частина А1906, Київ, Україна
ORCID: 0000-0002-2457-6675
Rra30@ukr.net

Коршун Наталія Володимирівна
Доктор технічний наук, доцент, професор кафедри інформаційної та кібернетичної безпеки
Київський університет імені Бориса Грінченка, Київ, Україна
ORCID: 0000-0003-2908-970X
N.korshun@kubg.edu.ua

Ворохоб Максим Віталійович
Аспірант кафедри інформаційної та кібернетичної безпеки
Київський університет імені Бориса Грінченка, Київ, Україна
ORCID: 0000-0001-5160-7134
M.vorokhob@kubg.edu.ua

ПІДХІД ДО ОЦІНЮВАННЯ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЛЯ АВТОМАТИЗОВАНОЇ СИСТЕМИ КЛАСУ «1»

Анотація. Стаття присвячена оцінці ризиків інформаційної безпеки в автоматизованих системах класу «1». Запропоновано адаптований підхід до оцінки ризиків інформаційної безпеки в таких АС з використанням Методики та вимог стандартів ГСТУ СУІБ 1.0/ISO/IEC 27001:2010 та ГСТУ СУІБ 2.0/ISO/IEC 27002:2010. Працездатність та способи реалізації підходу доведено на прикладі розгляду реальних загроз та вразливостей АС класу "1". Основною вимогою при створенні системи управління інформаційною безпекою в організації є оцінювання ризиків та визначення загроз для інформаційних ресурсів, які обробляються в інформаційно-телекомунікаційних системах та АС. Розглянуто базові стандарти щодо інформаційної безпеки в Україні, які дають загальні рекомендації щодо побудови і оцінювання ризиків інформаційної безпеки в рамках СУІБ. Проаналізовано найпоширеніші методи й методології з оцінювання ризиків інформаційної безпеки міжнародного зразка, зокрема, CRAMM, OCTAVE, NIST SP800-30 визначено їх переваги і недоліки. Визначено порядок проведення робіт з оцінки ризиків інформаційної безпеки АС класу «1». Наведено вразливості, що враховуються експертом відповідно до стандарту ISO/IEC 27002:2005 та Методики а також умовну шкалу визначення впливу на реалізацію загроз цілісності, доступності, спостережності. Запропоновані заходи та засоби протидії виникненню загроз. Даний підхід можна використовувати як для безпосереднього оцінювання інформаційного ризику, так і в навчальних цілях. Він дозволяє отримати кінцевий результат незалежно від досвіду та кваліфікації фахівця, що проводить оцінку ризиків, з подальшим впровадженням та удосконаленням існуючої системи управління ризиками в організації..

Ключові слова: автоматизована система; управління ризиками; система управління інформаційною безпекою; вразливість

1. ВСТУП

Постановка проблеми. В сучасних умовах розвитку комп'ютерних та інформаційно-комунікаційних технологій, а також глобальної мережі Інтернет захист інформації в питаннях щодо державного суверенітету та цілісності посідає вагоме місце. Щоденно виникають загрози кібервтручань та дестабілізуючих впливів на певні об'єкти з використанням технологічних можливостей інформаційного та кіберпросторів [1]. Повсякчас фахівці з інформаційної безпеки мають справу зі спробами несанкціонованого доступу до інформації. Відомості щодо техніки та технологій, програмних та апаратних засобів, цивільних та військових об'єктів, персональних даних, державних інформаційних ресурсів, а також інформація з обмеженим доступом є базовою складовою кожної держави. Тому для захисту таких важливих ресурсів у кіберпросторі передбачено ряд методів та засобів, що забезпечують цілісність, конфіденційність і доступність інформації за умов впливу на неї різноманітних загроз. Передумовою забезпечення інформаційної безпеки є реалізація існуючих та/або розробка нових методологій визначення інформаційного ризику в певних інформаційно-телекомунікаційних (автоматизованих) системах.

Відповідно до вимог із реалізації інформаційної безпеки в кожній автоматизованій системі (АС) оцінюється стан захищеності інформаційних ресурсів із певною періодичністю, що дає змогу визначити ризики (загрози) для АС. Отримані результати з оцінки ризиків (загроз) дозволяють фахівцям у сфері інформаційної безпеки, де вже впроваджена система управління інформаційною безпекою (СУІБ), розставити пріоритети, спрямувати управлінські рішення щодо запобігання визначеним ризикам.

Аналіз останніх досліджень і публікацій. Основною вимогою при створенні СУІБ в організації (установі) є оцінювання ризиків та визначення загроз для інформаційних ресурсів, які обробляються в інформаційно-телекомунікаційних системах (далі – ІТС) та АС.

У секторі інформаційної безпеки є безліч нормативних документів, що регламентують вимоги до інформаційної безпеки. Наводимо базові стандарти щодо інформаційної безпеки в Україні (які лише дають загальні рекомендації побудови і щодо оцінювання ризиків інформаційної безпеки в рамках СУІБ):

- ГСТУ СУІБ 1.0/ISO/IEC 27001:2010 Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Вимоги. (ISO/IEC 27001:2005, MOD)
- ГСТУ СУІБ 2.0/ISO/IEC 27002:2010 Інформаційні технології. Методи захисту. Звід правил для управління інформаційною безпекою. (ISO/IEC 27002:2005, MOD).

Теоретичні засади оцінки ризиків інформаційної безпеки та управління ними досліджували О.Г. Корченко, О.Є. Архипов, С.В. Казмірчук, О.В. Потій, Я.В. Рой та інші. В роботі [2] вказано, що існують дві основні групи методів розрахунку ризиків безпеки: перша група, що дозволяє встановити рівень ризику шляхом оцінки ступеня відповідності певним наборам вимог (нормативно-правовим документам підприємства, вимогам чинного законодавства, рекомендаціям міжнародних стандартів або компаній-виробників), та друга, що базується на визначенні ймовірності реалізації атак та рівнів збитку. Разом з тим, в багатьох них відсутні чіткі рекомендації щодо виконання певного алгоритму дій або їх складно втілити.

ISSN 2663 - 4023

Мета статті. У статті наведено практичний досвід оцінювання ризиків інформаційної безпеки в комерційних та некомерційних організаціях, застосування набутих знань щодо державних організацій, а також створення удосконаленого підходу до оцінювання ризиків (загроз). Метою статті є опис вдосконаленого та адаптованого підходу, який дозволить спростити процес оцінки ризиків по відношенню до фахівця та отримання зіставного та кінцевого результату по визначенню ризиків інформаційної безпеки з використанням базових методик та вимог міжнародних стандартів.

2. ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ

Нами проаналізовано найпоширеніші методи й методології з оцінювання ризиків інформаційної безпеки міжнародного зразка, а саме:

1. Аналіз і управління ризиками – метод розроблений Центральним комп'ютерним і телекомунікаційним агентством (Велика Британія), реалізований у вигляді програмного забезпечення CRAMM (CCTA Risk Analysis and Managment Method).

Цей метод передбачає комплексний підхід до оцінювання ризиків, поєднуючи кількісні та якісні оцінки. Є універсальним і підходить як для великих, так і для малих ІТС й АС, як для державного, так і для комерційного сектора. CRAMM орієнтований на різні типи організацій (установ), що різняться між собою базами знань. Для комерційних організацій застосовують комерційний профіль (Commercial Profile), а для державних – державний профіль (Government profile) [3].

Переваги: ідентифікація елементів ризику – матеріальних і нематеріальних активів та їх цінностей, загроз, заходів безпеки, величини потенційного збитку і ймовірності реалізації загрози.

Недоліки: відсутність звітів з оцінених ризиків; перерахунку максимально допустимих величин ризиків. Є трудомістким і тривалим процесом з оцінювання ризиків, його застосування потребує залучення фахівців високої кваліфікації, оброблення вручну сотень сторінок звітної документації, що генеруються програмним інструментарієм CRAMM. Крім того, слід зазначити високу вартість ліцензії [4].

2. Оцінка активів та вразливостей інформаційної безпеки – методологія OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation) розроблена у Сполучених Штатах Америки в Інституті програмної інженерії при Університеті Карнегі–Меллона (Software Engineering Institute і Carnegie Mellon University).

Методологія OCTAVE дає змогу розробити практичні методи й рекомендації для оцінювання ризиків. Визначає стратегію оцінювання й планування дій щодо забезпечення безпеки інформації на основі оцінювання ризиків [3].

Переваги: передбачає оцінювання різних ризиків, які, за винятком технічних ризиків і ризиків порушення законодавства, безпосередньо не включені в методологію (з'ясовується в ході проведення опитування).

Недоліки: не дає чітких інструкцій з організації моніторингу стану ризиків; не дає кількісної оцінки ризиків [4].

3. Управління ризиками в системі інформаційних технологій – методологія оцінки ризиків SP800-30 (Special Publications) Національного Інституту Стандартів і Технологій (National Institute of Standards and Technology – NIST) - NIST SP800-30.

Методологія NIST SP800-30 детально описує всі можливі ризики для інформаційних активів і може використовуватися для підприємств різної величини.

Недоліком цієї методології є довготривалий процес аналізу і відсутність автоматизації деяких функцій [3].

Аналіз більшості методик показав, що вони є мало продуктивними та інформативними для застосування на практиці. В них відсутні чіткі рекомендації й настанови щодо виконання певного алгоритму дій, вони базуються на стандартах тієї держави, в якій розроблені, у відповідності до цього визначають не рівень безпеки, а відповідність стандарту. Більшість методик міжнародного зразка залишаються недосяжними для українського ринку хоча б із урахування фінансової можливості. Також слід зазначити, що використання чи втручання «людиною» в процес оцінки ризиків інформаційної безпеки «машиною» залишається.

У 2011 році було розроблено Методичні рекомендації щодо впровадження системи управління інформаційною безпекою та методики оцінки ризиків відповідно до стандартів Національного банку України (далі – Методика). Основні засади для оцінки ризиків зазначеної Методики буде використано у даній статті із вдосконаленим та адаптованим підходом до визначення ступеня ризиків. Такий підхід дозволить отримати кінцевий результат незалежно від досвіду та кваліфікації фахівця, що проводить оцінку ризиків, з подальшим впровадженням та/або удосконаленням існуючої системи управління ризиками в організації.

3. РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Основною складовою кожного нормативного документу є складання плану дій або певного алгоритму до подальшої роботи. Беручі за основу Методику, визначається наступний порядок проведення робіт з оцінки ризиків інформаційної безпеки:

1. Створюються загальні переліки загроз та можливих вразливостей;
2. Створюються актуальні пари загроза/вразливість (з врахуванням особливостей бізнес-процесу та ієрархії вимог);
3. Оцінюється (за визначеною шкалою оцінки) умовна ймовірність реалізації загрози з використанням вказаної вразливості;
4. Оцінюється (за визначеною шкалою оцінки) вплив реалізації загрози на цілісність, конфіденційність, доступність та спостереженість до інформаційних ресурсів;
5. Розраховуються ризики за відповідним процесом (відповідно до п. 6.2 Методики) [5].

Для вищезазначеного підходу визначення ризиків інформаційної безпеки даний порядок дій є досить ефективним та продуктивним. Але його необхідно адаптувати до АС класу “1”, що в подальшому буде основою й для створення удосконаленого підходу, тому представляється декілька кроків адаптування.

Крок 1. Визначити основу складову захисту в АС класу “1”, так званий “актив” для подальшого захисту його від можливих загроз та вразливостей. “Активом” може бути не лише фізичний об'єкт (сервери, жорсткі диски, друковані документи, тощо), але й інформація, яка зберігається та оброблюється в АС класу “1” (рис. 1).

ISSN 2663 - 4023

Рис.1. Інформація, яка обробляється в АС класу "1"

Крок 2. Створити перелік можливих загроз та вразливостей з урахуванням особливостей оброблюваної інформації в АС (табл. 1). Для цього необхідно визначити вразливості (організаційні та технічні), притаманні АС класу "1".

Для виявлення вразливостей, в залежності від особливостей оброблюваної інформації, а також від інформаційно-телекомунікаційних технологій, можуть використовуватися різні прогресивні методи тестування. Вони включають:

1. Визначення зловмисників серед користувачів системи;
2. Спеціальний автоматичний інструментарій для сканування вразливостей;
3. Тестування та оцінку безпеки;
4. Тести на проникнення;
5. Перегляд коду програмно-технічних комплексів;
6. Аналіз відомих порушень безпеки;
7. Аналіз відомих вразливостей (наприклад, операційних систем, баз даних, телекомунікаційних технологій, протоколів тощо) [6].

Крок 3. Створити актуальні пари загроза-вразливість (табл. 1) [7].

Організаційні та технічні вразливості встановлюються експертом (це може бути адміністратор безпеки – особа, яка встановлює та керує комплексом засобів захисту інформації, та/або системний адміністратор – особа, яка встановлює та керує програмним та апаратним забезпеченням АС), який аналізує застосування організаційних заходів захисту інформації. У таблиці 1 описано вразливості, враховані експертом та взяті до використання передбачених стандартом ISO/IEC 27002:2005, а також відповідно до Методики.

Крок 4. Оцінити за умовною шкалою ймовірність реалізації загрози з урахуванням вказаної вразливості (табл. 1).

Ймовірність реалізації загрози визначається за такою шкалою:

1 – виникнення інциденту практично неможливе;

2 – виникнення інциденту малоймовірне (не більше 1разу на рік);

3 – виникнення інциденту ймовірне до 1 разу на 3 місяці;

4 – виникнення інциденту ймовірне до 1 разу на тиждень;

5 – виникнення інциденту ймовірне до 1 разу на добу [4].

Крок 5. Оцінити за умовною шкалою вплив реалізації загрози на цілісність, конфіденційність, доступність та спостереженість оброблюваної інформації (табл. 1).

Умовна шкала впливу реалізації загрози на цілісність, конфіденційність, доступність та спостережність оброблюваної інформації приведена в таблиці 2.

Величина ризику обчислюється за формулою:

$$В_Р = (К + Ц + Д + С) \cdot Р_З, \quad (1)$$

Де $В_Р$ – величина ризику, К – конфіденційність, Ц – цілісність, Д – доступність, С – спостереженість, $Р_З$ – ймовірність реалізації загрози.

Якщо величина ризику буде складати:

100-80 балів – високий ризик. Це означає, що необхідно застосувати контроль ризиків, які допоможуть знизити ймовірність його реалізації або вкажуть на необхідність повністю переглянути способи та засоби захисту. У загальному випадку високий ризик означає критичний стан щодо захисту та той факт, що реалізація загроз й відчутних наслідків має високу ймовірність.

Таблиця 1

Оцінка ризиків інформаційної безпеки

№ п/п	Вразливість	Загрози	Конфіденційність	Цілісність	Доступність	Спостережність	Ймовірність реалізації загрози	Величина ризику	Заходи та засоби протидії	
									Індивідуальні	Загальні (спільні)
1.	Розміщення обладнання в зоні, якій загрожує затоплення, відсутність фізичного захисту будівлі, дверей та вікон та ін.	Порушення фізичної цілісності об'єкта (окремих компонентів, пристроїв, обладнання, носіїв інформації).	3	3	3	2	2	22	Призначення відповідального за експлуатацію.	Забезпечення пропускного режиму на контрольовану територію, обмеження доступу в приміщення, де розміщена АС та допоміжне обладнання. Визначення персональної відповідальності співробітників за збереження обладнання та носіїв інформації.
2.	Нестабільне електроживлення, стрибки напруги, відсутність схеми періодичної заміни обладнання, неякісна проводка та ін.	Порушення режимів функціонування (виведення з ладу) систем життєзабезпечення об'єкта.	1	5	5	2	3	39	Призначення відповідальних за експлуатацію основних, допоміжних технічних засобів приймання, обробки, зберігання і передачі інформації та систем життєзабезпечення.	
3.	Неадекватний контроль змін конфігурацій і налаштувань політик, несвоєчасне оновленя програмного забезпечення та ін.	Порушення режимів функціонування АС (обладнання і програмного забезпечення).	5	5	5	2	3	51	Призначення відповідальних за експлуатацію основних, допоміжних технічних засобів приймання, обробки, зберігання і передачі інформації. Визначення режимів функціонування та порядку настройки програмного забезпечення.	

4.	Відсутність оновлень програмного забезпечення, яке використовують для захисту від шкідливих кодів (вірусів) та ін.	Застосування комп'ютерних вірусів.	5	5	5	3	4	72	Призначення відповідального за оновлення антивірусного забезпечення, визначення порядку його застосування.	Обмеження (заборона) використання програмного забезпечення, отриманого з ненадійних джерел. Визначення переліку програмного забезпечення, дозволеного для використання в АС. Забезпечення цілісності ресурсів засобами комплексу засобів захисту. Застосування антивірусного програмного забезпечення.
5.	Відсутня процедура та документи щодо встановлення програмного забезпечення, відсутні засоби захисту та ін.	Впровадження програмних закладок та апаратних закладних пристроїв.	5	5	1	2	2	26	Проведення спеціальних перевірок обладнання. Застосування програмного забезпечення виявлення програм-шпигунів, визначення порядку його застосування.	
6.	Невмотивовані та незадоволені співробітники, неправильний підбір співробітників та ін.	Використання (шантаж, підкуп тощо) з корисливою метою працівників.	5	4	2	2	2	26		Проведення профілактичних заходів службою власної безпеки. Забезпечення
7.	Відсутня процедура навчання працівників, неякісний підбір персоналу	Невиконання організаційних вимог, встановлених розпорядчими документами, чинними в організації	5	5	2	4	3	48		

	та ін.	для АС.								пропускного режиму на контрольовану територію, обмеження доступу в приміщення, де розміщена АС.
8.	Неефективна система охорони контрольованої зони, недостатній контроль за переміщенням майна, відсутня нормативна база щодо утилізації та знищення документів та ін.	Крадіжки носіїв інформації, виробничих відходів (роздруківок, записів тощо).	5	3	3	2	2	36	Встановлення порядку друкування та знищення документів, що містять інформацію з обмеженим доступом. Визначення персональної відповідальності працівників за порушення порядку поводження з матеріальними носіями секретної інформації, організація та забезпечення контролю. Запровадження контролю засобами комплексу засобів захисту подій, пов'язаних з друкуванням інформації в АС.	
9.	Відсутній порядок поводження з зовнішніми носіями та ін.	Навмисне пошкодження носіїв інформації.	2	5	5	2	3	42	Встановлення порядку поводження з носіями інформації. Визначення персональної відповідальності користувачів за порушення встановленого порядку.	
10.	Відсутній комплекс засобів захисту та ін.	Використання засобів перехвату побічних електромагнітних випромінювань і наводок, акустоелектричних перетворень інформаційних сигналів.	5	2	2	2	1	11	Проведення спеціальних досліджень та розміщення технічних засобів приймання, обробки, зберігання і передачі інформації відповідно до вимог приписів на експлуатацію та нормативних документів з заходами з протидії технічним засобам розвідки.	
11.	Відсутня процедура моніторингу дій співробітників, відсутні засоби захисту щодо моніторингу копіювання інформації та ін.	Несанкціоноване копіювання інформації.	5	2	2	2	3	33	Встановлення порядку копіювання інформації з використанням зовнішніх носіїв. Визначення персональної відповідальності працівників за порушення порядку копіювання інформації з обмеженим доступом. Забезпечення перепускного режиму на контрольовану територію, обмеження доступу в приміщення, де розміщена АС. Запровадження контролю засобами комплексу засобів захисту подій, пов'язаних з копіюванням	

									інформації в АС.	
12.	Невизначеність процедури та контролю за завершеністю сеансу працівника, відсутність політик повторного використання об’єктів та ін.	Читання залишкової інформації з оперативної пам'яті.	5	1	1	1	2	16	Визначення порядку завершення сеансів роботи працівниками в АС та стирання інформації. Впровадження програмного забезпечення для стирання інформації на машинних носіях. Запровадження засобами комплексу засобів захисту політики повторного використання об’єктів.	
13.	Відсутність або неефективність ідентифікації та аутентифікації співробітника, неефективне або відсутнє розмежування прав доступу до програмного забезпечення/даних та ін.	Одержання атрибутів доступу з подальшим їх використанням для маскування під зареєстрованого користувача (“маскарад”).	5	2	2	2	3	33	Встановлення порядку зберігання, заборона розголошення атрибутів доступу (електронних ключів, паролів). Визначення порядку дій на випадок компрометації атрибутів доступу. Встановлення вимог щодо складності, повторюваності, термінів дії паролів. Забезпечення засобами комплексу засобів захисту розмежування доступу до паролів, що зберігаються в системі.	
14.	Відсутність або неефективність процедури контролю вводу програмного забезпечення, неефективне розмежування прав доступу щодо встановлення /налаштування програмного забезпечення та ін.	Впровадження і використання забороненого політикою безпеки програмного забезпечення або несанкціоноване використання програмного забезпечення.	5	5	1	4	3	45	Визначення порядку інсталяції програмного забезпечення, заборона використання програмного забезпечення, отриманого з ненадійних джерел. Визначення переліку програмного забезпечення, дозволеного для використання в АС. Покладання прав та обов’язків щодо інсталяції програмного забезпечення на адміністратора безпеки. Забезпечення цілісності ресурсів засобами комплексу засобів захисту.	
15.	Необізнаність працівників,	Ненавмисне пошкодження носіїв	2	5	5	2	3	42	Встановлення порядку поводження з носіями	

	незахищене зберігання даних та ін.	інформації. Помилки при введенні даних в АС.							інформації, визначення персональної відповідальності працівників за порушення встановленого порядку.	
16.	Відсутня процедура навчання працівників, відсутній контроль та процедура за діями працівників щодо зберігання ключів та паролів доступу та ін.	Ненавмисні дії, що можуть призвести до розголошення конфіденційних відомостей, атрибутів доступу, втрати атрибутів тощо.	5	2	2	2	3	33	Встановлення порядку поводження з інформацією з обмеженим доступом та її матеріальними носіями. Заборона розголошення атрибутів доступу (електронних ключів, паролів). Визначення порядку дій на випадок компрометації атрибутів доступу. Забезпечення засобами комплексу засобів захисту розмежування доступу до паролів, що зберігаються в системі.	
17.	Відсутність навчання співробітників, відсутні відповідальні за дотримання порядку використання засобів захисту та ін.	Некомпетентне застосування засобів захисту.	5	5	5	5	2	40	Визначення порядку застосування засобів захисту, режимів роботи АС, комплексу засобів захисту, допоміжного обладнання. Призначення адміністратора безпеки, організація та проведення занять з працівниками та адміністраторами щодо порядку застосування засобів захисту.	
18.	Несвоєчасне та/або неякісне обслуговування комунікаційних мереж та систем та ін.	Зміна умов фізичного середовища (вологість, запиленість, коливання температури).	5	5	2	1	2	26	Визначення та додержання умов фізичного середовища, передбаченого для роботи обладнання. Визначення порядку прибирання приміщень, проведення профілактичних робіт систем життєзабезпечення.	
19.	Відсутнє резервне обладнання та процедура швидкого відновлення роботи технічних засобів та ін.	Збої і відмови у роботі обладнання та технічних засобів.	2	5	5	5	2	34	Визначення порядку технічного обслуговування, ремонту технічних засобів. Забезпечення необхідним комплектом запасного обладнання.	

ISSN 2663 - 4023

Таблиця 2

Шкала визначення впливу на реалізацію загроз цілісності, доступності, спостережності

Оцінка	Цілісність	Конфіденційність	Доступність	Спостережність
1	Практично не призводить до наслідків з втратами інформації	Практично не призводить до розкриття інформації	Практично не впливає на доступність до інформації	Практично не впливає
2	Призводить до незначних втрат інформації, має незначний вплив на роботу структури	Призводить до розкриття окремих документів, які не відносяться до інформації з обмеженим доступом	Вплив на доступність незначний (не більше 1/10 від максимально допустимого часу простою роботи структури)	Вплив незначний
3	Призводить до значних втрат інформації, має значний вплив на роботу структури	Призводить до розкриття окремих документів, які відносяться до інформації з обмеженим доступом і має незначний вплив на роботу структури	Вплив на доступність середній (не більше 1/2 від максимально допустимого часу простою роботи структури)	Призводить до неможливості відстежити частину дій працівників
4	Призводить до великих втрат інформації, має значний вплив на роботу структури, може призвести до зупинки її роботи	Призводить до розкриття документів, які відносяться до інформації з обмеженим доступом і до зупинки роботи структури	Вплив на доступність значний (до максимально допустимого часу простою для роботи структури)	Призводить до неможливості відстежити будь-які дії працівників
5	Призводить до зупинки роботи структури, порушує законодавство України	Призводить до зупинки роботи структури, порушує законодавство України	Призводить до зупинки роботи структури натривалий час, який перевищує максимально допустимий час простою	Призводить до неможливості відстежити будь-які дії працівників, порушує законодавство України

80-60 балів – середній ризик. Означає наявні загрози, які можуть спричинити критичний стан незахищеності з малою ймовірністю їх реалізації, відчутні наслідки з середньою ймовірністю або невеликі наслідки з високою ймовірністю. Рішення щодо застосування засобів захисту до таких ризиків потрібно приймати, беручи до уваги те, що загальна вартість встановлення засобів захисту не повинна перевищувати прогнозовані втрати від реалізації загроз.

60-40 балів – низький ризик означає, що актуальні для системи загрози можуть спричинити невеликі наслідки з малою ймовірністю. Такими ризиками не варто нехтувати, а тому потрібно звернути увагу на організаційні аспекти в питаннях захисту.

40-20 балів – незначний ризик, однак, варто тримати під контролем та провести додатковий аудит загроз.

20 і нижче – малоймовірний ризик.

Крок 6. Аналізувати вплив та запропонувати заходи та засоби протидії виникнення загрозам (табл. 1).

4. ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

У статті запропоновано адаптований підхід до оцінки ризиків інформаційної безпеки в АС класу “1” з використанням Методики та вимог стандартів ГСТУ СУІБ 1.0/ISO/IEC 27001:2010 та ГСТУ СУІБ 2.0/ISO/IEC 27002:2010. Працездатність та способи реалізації підходу доведено на прикладі розгляду реальних загроз та вразливостей АС класу “1”, за аналізом експертної думки фахівців в галузі інформаційної безпеки. Підхід можна використовувати як для безпосереднього оцінювання інформаційного ризику, так і в навчальних цілях. Загрози та вразливості (перелік яких не є вичерпним, та може доповнюватись за мірою зростання та/або виникнення інцидентів), а також результати вказані в таблиці 1 можуть змінюватись і не є еталонними. У подальшому на основі досліджень можна створити підхід до оцінки ризиків інформаційної безпеки для АС інших класів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] Бурячок В.Л. Основи формування державної системи кібернетичної безпеки: Монографія. – К.: НАУ, 2013. – 432 с.

[2] Я.В. Рой, Н.П. Мазур, П.М. Складанний, «Аудит інформаційної безпеки – основа ефективного захисту підприємства», *Кібербезпека: освіта, наука, техніка*. № 1 (1). С. 86-93, 2018.

[3] Лагун А. Ризики інформаційної безпеки ІТ-підприємства [Електронний ресурс] / А. Лагун, Н. Кухарська // Захист інформації і безпека інформаційних систем: VII Міжнародна науково-технічна конференція, м. Львів, 30–31 травня 2015 року. – Режим доступу : https://webcache.googleusercontent.com/search?Q=cache:_mlalmxnnaej:https://sci.ldubgd.edu.ua/bitstream/handle/123456789/750/11.doc%3Fsequence%3D1%26isallowed%3Dy+&cd=2&hl=ru&ct=clnk&gl=ua&client=firefox-b-d.

[4] Пастоев А., «Методологии управления ИТ-рисками», *Открытые системы. СУБД.* №8. 2006. [Електронний ресурс] Режим доступу : https://www.osp.ru/os/2006/08/3584582.

[5] В.В. Єрмошин, Я.В. Невойт, «Аналіз і оцінка ризиків інформаційної безпеки для банківських та комерційних систем», *Сучасний захист інформації*. № 3. С. 26–29. 2014.

[6] Методичні рекомендації щодо впровадження системи управління інформаційною безпекою та методики оцінки ризиків відповідно до стандартів Національного банку України: Лист Національного Банку України від 03.03.2011 № 24-112/365 [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/v0365500-11#Text.

[7] С.С. Бучик, С.В. Мельник, «Методика оцінювання інформаційних ризиків в автоматизованій системі», *Проблеми створення, випробування, застосування та експлуатації складних інформаційних систем: збірник наукових праць*. №11. С. 33–42. 2015.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (10), 2020
ISSN 2663 - 4023

Iryna S. Litvinchuk
Researcher
Military base A1906, Kyiv, Ukraine
ORCID: 0000-0002-0854-5393
Litvinchuk.irina94@gmail.com

Ruslan O. Korchomnyi
Researcher
Military base A1906, Kyiv, Ukraine
ORCID: 0000-0002-2457-6675
Rra30@ukr.net

Nataliia V. Korshun
Doctor of Technical Sciences, associate professor, Professor of the Department of Information and Cyber Security
Borys Grinchenko Kyiv University, Kyiv, Ukraine
ORCID: 0000-0002-4055-1494
N.korshun@kubg.edu.ua

Maksym V. Vorokhob
Phd student
Borys Grinchenko Kyiv University, Kyiv, Ukraine
ORCID: 0000-0001-5160-7134
M.vorokhob@kubg.edu.ua

APPROACH TO INFORMATION SECURITY RISK ASSESSMENT FOR A CLASS «1» AUTOMATED SYSTEM

Abstract. The article is devoted to the assessment of information security risks in automated systems of class "1". An adapted approach to the assessment of information security risks in such automated systems using the Methodology and requirements of the standards of GSTU SUIB 1.0 / ISO / IEC 27001: 2010 and GSTU SUIB 2.0 / ISO / IEC 27002: 2010 is proposed. The efficiency and methods of implementation of the approach are proved on the example of consideration of real threats and vulnerabilities of class 1 automated systems. The main requirement for the creation of information security management system in the organization is risk assessment and identification of threats to information resources that are processed in information and telecommunications systems and speakers. The basic standards on information security in Ukraine are considered, which give general recommendations for the construction and assessment of information security risks within the ISMS. The most common methods and methodologies for assessing information security risks of international standard are analyzed, their advantages and disadvantages are identified. The order of carrying out of works on an estimation of risks of information security of the AS of a class "1" is defined. The vulnerabilities considered by the expert according to the standard ISO/IEC 27002:2005 and the Methodology are given. A conditional scale for determining the impact on the implementation of threats to integrity, accessibility, observation is given. Measures and means of counteracting the emergence of threats are proposed. This approach can be used both for direct information risk assessment and for educational purposes. It allows to get the final result regardless of the experience and qualifications of the specialist who conducts risk assessment, with the subsequent implementation and improvement of the existing risk management system in the organization.

Keywords: automated system; risk management; information security management system; vulnerability.

REFERENCES

[1] V. Buryachok. Fundamentals of the formation of the state system of cyber security: Monograph. - K .: NAU, 2013. - 432 p.

[2] Ya.V. Roy and N.P. Mazur and P.M. Skladannyi, "Information security audit - the basis of effective enterprise protection", *Cybersecurity: education, science, technology*. № 1 (1). Pp. 86-93, 2018.

[3] A. Lagun. Risks of information security of IT-enterprises [Electronic resource] / A. Lagun, N. Kukharska // Information protection and security of information systems: VII International scientific and technical conference, Lviv, May 30-31, 2015. - Available: https://webcache.googleusercontent.com/search?Q=cache:_mlalmxnnaej:https://sci.ldubgd.edu.ua/bitstream/handle/123456789/750/11.doc%3Fsequence%3D1% 26isallowed% 3Dy + & cd = 2 & hl = ru & ct = clnk & gl = ua & client = firefox-bd [10.09.2020].

[4] Pastoev A., "Methodologies of IT risk management", Open systems. DBMS. №8. 2006. [Electronic resource] Available: https://www.osp.ru/os/2006/08/3584582 [10.09.2020].

[5] B.B. Yermoshin, Ya.V. Nevoit, "Analysis and assessment of information security risks for banking and commercial systems", *Modern information security*. № 3. Pp. 26–29. 2014

[6] Methodical recommendations for the implementation of the information security management system and risk assessment methods in accordance with the standards of the National Bank of Ukraine: Letter of the National Bank of Ukraine dated 03.03.2011 № 24-112 / 365 [Electronic resource]. Available: https://zakon.rada.gov.ua/laws/show/v0365500-11#Text [10.09.2020].

[7] S.S. Buchik, S.V. Melnyk, "Methods of assessing information risks in an automated system", *Problems of creating, testing, application and operation of complex information systems: a collection of scientific papers*. №11. Pp. 33–42, 2015.