DOI: **0.33099/2311-7249/2024-50-2-29-36**

УДК: 621.39

Гульков Микола Олександрович
Ганненко Світлана Олександрівна (кандидат технічних наук)

Національний університет оборони України, Київ, Україна

УДОСКОНАЛЕНИЙ МЕТОД ВИЗНАЧЕННЯ ЗАЛИШКОВОГО РИЗИКУ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ ПІД ЧАС ОЦІНЮВАННЯ ВРАЗЛИВОСТІ ІНФОРМАЦІЇ

Залишковий ризик є важливим аспектом управління безпекою інформації, оскільки він визначає ризики, що залишаються після впровадження заходів забезпечення безпеки інформації. Визначення залишкового ризику завдяки включенню послуг спостережності за діями користувачів буде сприяти зниженню впливу на безпеку інформації в інформаційно-комунікаційних системах і підвищенню ефективності заходів захисту. Метою статті є удосконалення методу визначення залишкового ризику під час оцінювання вразливості інформації в інформаційно-комунікаційних системах шляхом підвищення точності визначення порушення (подолання, злому) комплексної системи захисту у процесі втрати оператором керованості комп'ютерною системою. Удосконалення здійснюється завдяки введенню ймовірності реалізації загрози подолання захисту неправомірними діями користувачів у інформаційно-комунікаційних системах. Під час написання статті застосовано такі методи дослідження: системний аналіз – під час проведення аналізу інформаційної безпеки; порівняльний аналіз – у процесі проведення аналізу відповідності безпеки інформації до вимог державних стандартів; факторний аналіз – для оцінювання вразливості інформації в інформаційно-комунікаційних системах завдяки підвищенню точності розрахунку ймовірності подолання засобів захисту під час втратою комп'ютерною системою керованості; емпіричного дослідження – у процесі дослідження впливу інформаційних потоків на функціонування інформаційної безпеки. Зазначений методичний підхід дав змогу впроваджувати системи аналізу керування інформаційно-комунікаційної системи та проводити контроль за внесенням будь-яких змін до комп'ютерних систем, що, в свою чергу, конкретизує вимоги до створення стандартів комплексу засобів захисту комп'ютерної системи. Запропоновано удосконалення методу визначення залишкового ризику в інформаційно-комунікаційних системах за оцінювання вразливості інформації шляхом комплексного використання кількісних характеристик у вигляді ймовірностей реалізації загрози подолання конфіденційності цілісності доступності з додаванням ймовірності реалізації загрози подолання захисту, що є наслідком неправомірних дій користувачів в інформаційно-комунікаційній системі. Наведено вираз, що враховує послуги спостережності безпеки інформації у вигляді складових ймовірності реалізації загрози подолання захисту інформаційно-комунікаційної системи неправомірними діями користувачів, а саме від: небезпечних для комп'ютерної системи дій, пов'язаних із процесом розпізнання (порушення реєстрації) користувача, втручання в процес передачі інформації, помилкових неавторизованих дій, порушення цілісності комплексу засобів захисту, внутрішнього шахрайства та неавторизованого підключення, відмови від авторства та одержання інформації. Науковою новизною викладеного у статті визначено удосконалення методів визначення залишкового ризику для забезпечення безпеки та надійності інформаційно-комунікаційних систем шляхом підвищення точності розрахунку ймовірності реалізації загрози подолання засобів захисту за втрати користувачем керованості комп'ютерною системою. Теоретичне значення полягає у подальшому розвитку методів визначення залишкового ризику для забезпечення безпеки та надійності інформаційно-комунікаційних систем за рахунок підвищення точності розрахунку ймовірності реалізації загрози подолання засобів захисту під час втрати керованості комп'ютерної системою. Практичним значенням отриманих результатів є можливість впровадження удосконаленого методу визначення залишкового ризику за оцінювання вразливості інформації в інформаційно-комунікаційних системах органів військового управління Збройних Сил України та Сил оборони держави в цілому, а також під час проведення командно-штабних навчань та тренувань. Напрямом подальших досліджень слід вважати розроблення методики оцінювання безпеки інформації в інформаційно-комунікаційній системі під час втрати оператором керованості комп'ютерною системою органу військового управління.

***Ключові слова**: інформаційно-комунікаційна система, комплексна система захисту, залишковий ризик, ймовірність реалізації загрози, подолання захисту, втрата керованості.*

Вступ

Сучасний розвиток людської цивілізації, характеризується найбільш інтенсивним використанням комп'ютерних інформаційних технологій у всіх сферах суспільного життя. Що робить цілком закономірною і дуже актуальною проблему захисту інформації в інформаційно-комунікаційних системах [1; 2].

Інформація як предмет праці, стає все більшою мірою стратегічним ресурсом суспільства, його рушійною продуктивною силою [3; 4]. Інформаційно-комунікаційні системи (далі – ІКС) займають ключову роль у сучасному цифровому світі, забезпечуючи передачу, обробку та зберігання інформації. Однак, разом із зростанням їх важливості зростає і загроза їх безпеці. Визначення та оцінювання ризиків є критично важливими завданнями для забезпечення безпеки інформації в інформаційно-комунікаційних системах.

Останнім часом значна увага надається питанням захищеності інформації в інформаційно-комунікаційних системах Збройних Сил України, а особливо з моменту початку широкомасштабної збройної агресії російської федерації проти України. Застосування комп'ютерних інформаційних технологій у Збройних Силах містить багато проблемних питань щодо захисту інформації, а саме забезпечення безпеки інформації в автоматизованих та комп'ютерних системах.

Постановка проблеми. Важливою проблемою, під час забезпечення захисту інформації, є управління ризиками в ІКС з метою підтримки її безпеки на достатньому рівні, що є важливою функцією органу військового управління (далі – ОВУ) та реалізується завдяки комплексним системам захисту (далі – КСЗ) інформації. Для визначення потрібної та достатньої сукупності засобів захисту інформації розробляються рекомендовані переліки організаційних заходів, спрямованих на зниження ризиків інформаційній безпеці та архітектури системи інформаційної безпеки ОВУ. Однак більшість фахівців під час експлуатації автоматизованих систем користуються вже створеними шаблонами послуг безпеки від певної загрози, не враховуючи залишковий ризик після впровадження заходів забезпечення безпеки інформації в інформаційно-комунікаційній системі. Нездатність ІКС ефективно протистояти реалізації певної загрози може призвести до втрати інформації та знищення системи в цілому, тому протягом всього життєвого циклу інформаційно-комунікаційної системі потрібно постійно та якісно проводити оцінювання вразливості ІКС.

Сукупність заходів, що проводяться стосовно оцінювання ризику, вибору, реалізації і впровадження заходів забезпечення безпеки, спрямовані на досягнення прийнятного рівня залишкового ризику. Для визначення ризику в інформаційно-комунікаційних системах використовуються різні методи, а саме кількісні, якісні та комбіновані [15]. Кожен з цих методів має свої переваги та недоліки, які варто враховувати під час вибору методу оцінювання ризиків для конкретних реалізацій ІКС.

Для покращення точності та об'єктивності визначення залишкового ризику пропонується використання комбінованих методів, що поєднують переваги кількісних та якісних підходів оцінювання. Також важливим є врахування контекстуальних факторів і специфіки інформаційно-комунікаційних систем, впроваджених у діяльність органів управління Збройних Сил України та Сил оборони держави.

Аналіз останніх досліджень і публікацій. У нормативно-правових актах [1; 2] регулюються відносини у сфері захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах. У нормативно-правових документах [3; 4] визначено інструкції про порядок ведення обліку, зберігання, використання і знищення документів та інших матеріальних носіїв інформації, що містять службову інформацію та положення про технічний захист інформації в Україні.

Державними стандартами України [5–7] регулюється порядок проведення робіт із стандартизації та нормування в галузі технічного захисту інформації.

Нормативними документами [8–13] регулюються вимоги до порядку розробки комплексної системи захисту інформації в автоматизованій системі, що передбачає об'єднання в єдину систему всіх необхідних заходів і засобів захисту від різноманітних загроз безпеці інформації на всіх етапах життєвого циклу автоматизованої системи. Вищезазначені документи визначають лише створення умов безпеки інформації, але не визначають її практичної складової в контексті критеріїв захищеності інформації.

Нормативним документом [14] система розглядається як набір функціональних послуг. Кожна послуга являє собою набір функцій, що дають змогу протистояти певній множині загроз. Кожна послуга може включати декілька рівнів. Чим вище рівень послуги, тим більш повно забезпечується захист від певного виду загроз.

У наукових дослідженнях Матова О. Я., Василенко В. С., Будько М. М., Заячук Я. І., Осташа П. С. [16; 17] авторами запропоновано критерії оцінювання захищеності інформації в комп'ютерних системах від несанкціонованого доступу, аналіз та оцінювання ризиків вразливості локально-обчислювальної мережі, що є актуальним на даний час. Але в зазначених наукових дослідженнях не розглядаються критерії спостережності, які необхідно також ураховувати під час оцінювання вразливості інформації в ІКС.

Актуальність наукового завдання полягає у можливості впровадження послуг спостережності за діями користувачів у процесі визначення

залишкового ризику під час оцінювання вразливості інформації в інформаційно-комунікаційних системах органів військового управління Збройних Сил України, а також Сил оборони України в цілому.

Метою статті є удосконалення методу визначення залишкового ризику під час оцінювання вразливості інформації в інформаційно-комунікаційних системах шляхом підвищення точності визначення порушення (подолання, злому) комплексної системи захисту у процесі втрати оператором керованості комп'ютерною системою. Удосконалення здійснюється завдяки введенню ймовірності реалізації загрози подолання захисту неправомірними діями користувачів у інформаційно-комунікаційних системах.

Виклад основного матеріалу дослідження

цінність набувають люди – носії знань, найкращі передавачі технологічної інформації і передового досвіду. Для їх ефективної участі в інформаційних процесах створюється потужна інфраструктура засобів комп'ютерної та комунікаційної техніки, що змінює не лише процес і характер трудової діяльності, а й сам спосіб життя і систему цінностей людини.

Сучасні інформаційні технології набувають глобального характеру, охоплюючи всі сфери життєдіяльності людини, формуючи інформаційне єдність всієї людської цивілізації. За допомогою глобальної обчислювальної мережі Інтернет об'єднуються і переміщаються на будь-які відстані гігантські обсяги інформації, забезпечується доступ численних користувачів, розташованих на практично необмеженій території, до інформаційних ресурсів всієї світової спільноти.

Для держав сучасного світу стає очевидним, що відставання в області інформатизації може виявитися непереборною перешкодою для їх подальшого розвитку, привести до істотних, а часом драматичних наслідків у всіх сферах життєдіяльності, перетворити їх на сировинний придаток інформаційно і промислово розвинених країн.

Порушення розмежування доступу є однією з найбільш серйозних загроз заволодіння інформацією. Несанкціонований доступ до інформації може бути реалізований, за таких обставин [11]:

1. Переважна частина персональних електронних обчислювальних машин (далі – ПЕОМ) розташовується безпосередньо в робочих кімнатах фахівців, що створює сприятливі умови для доступу до них сторонніх осіб.

2. Багато ПЕОМ є колективним засобом обробки інформації, що знеособлює відповідальність, зокрема і за захист інформації.

3. Сучасні ПЕОМ оснащені незнімними накопичувачами тобто жорсткими магнітними дисками надвеликої місткості, інформація на яких зберігається навіть у знеструмленому стані.

4. Електронні машинні носії інформації виробляються в такій масовій кількості, що використовуються для поширення інформації так само, як і паперові носії;

5. Спочатку ПЕОМ створювалися саме як персональний засіб автоматизованої обробки інформації, а тому і обладнувалися комплексними засобами захисту від несанкціонованого доступу.

Ідентифікація та автентифікація за допомогою блоків-додатків полягає в тому, що технічні засоби оснащуються спеціальними пристроями, генерується індивідуальними сигналами. З метою попередження перехоплення цих сигналів і подальшого їх злочинного використання вони можуть передаватися в зашифрованому вигляді, причому періодично може змінюватися не лише ключ шифрування, але й використовуваний спосіб (алгоритм) криптографічного перетворення.

Автентифікація за процедурою «запит-відповідь» зводиться до того, що в запам'ятовуючому пристрої автоматизованої системи завчасно вноситься відповідна інформація про адресата. Для попередження перехоплення і злочинного використання надісланих ідентифікаційних даних може здійснюватися їх криптографічне закриття.

Саме розмежування доступу може здійснюватися декількома способами, а саме за:

рівнями (кілець) обмеження доступу;

спеціальними списками;

матрицями повноважень;

спеціальними мандатами.

Розглянемо коротку характеристику перерахованих способів. *Розмежування доступу за рівнями (кілець) обмеження доступу* полягає в тому, що дані розподіляються по масивах (баз) так, щоб в кожному масиві (кожної бази) містилися дані одного рівня обмеження доступу до інформації. Тоді користувачеві надається доступ до масиву (бази) свого рівня та забороняється доступ до масивів (баз) більш високих рівнів.

Розмежування доступу за спеціальними списками зводиться до того, що для кожного елемента даних, що захищаються (файлу, папки), складається список всіх тих користувачів, яким надано право доступу до відповідного елементу, або, навпаки, для кожного зареєстрованого користувача складається список тих елементів даних, що захищаються, до яких йому надано право доступу.

Розмежування доступу за матрицями повноважень передбачає формування двовимірної матриці, по рядках якої містяться ідентифікатори елементів зареєстрованих користувачів, а по стовпцях – ідентифікатори елементів, що захищаються (дані). Елементи матриці містять інформацію про рівень повноважень відповідного користувача відносно відповідного елемента.

Розмежування доступу за мандатами є спосіб разового дозволу на допуск до захищеного

елементу даних. Він полягає у тому, що кожному захищеному елементу надається персональна унікальна мітка, після чого доступ до цього елемента буде дозволений тільки тому користувачеві, який в своєму запиті пред'явить мітку елемента (мандат), яку йому може видати адміністратор захисту.

Актуальність вирішення проблеми захисту інформаційних ресурсів вимагає протидію певним загрозам. Поява ризиків, які виникають під час використання інформаційних ресурсів, призводить до знищення, спотворення, модифікації інформації. Для визначення вимог та оцінювання вразливості інформації в інформаційно-комунікаційних системах використовуються критерії оцінки захищеності [14]. Відомо також, що досягнуті результати із забезпечення ефективності захисту інформації можна оцінювати або величиною можливих збитків за кожним із класів порушень, або за допомогою залишкового ризику.

Залишковий ризик є тим ризиком, який залишається після виконання заходів із керування ризиками. Він може виникнути через недосконаліть або недостатність застосованих заходів протидії загрозам. Для вирішення проблемних питань керування ризиками та з метою забезпечення безпеки інформації під час її обробки потрібно [14]:

1. Провести аналіз ризиків за різними напрямами для:

об'єктів інформаційно-комунікаційної системи;

процесів, процедур і програм обробки інформації;

каналів зв'язку;

побічних електромагнітних випромінювань і наведень;

механізмів керування системою захисту.

2. Провести оцінювання ризиків:

можливих втрат у результаті реалізації загроз;

ймовірності виявлення вразливостей системи, що впливає на результат оцінювання можливих втрат;

витрат на впровадження заходів і засобів захисту, що скорочують ризик до прийнятного рівня (рис. 1).

Послідовність визначення залишкового ризику наведена на рис. 1

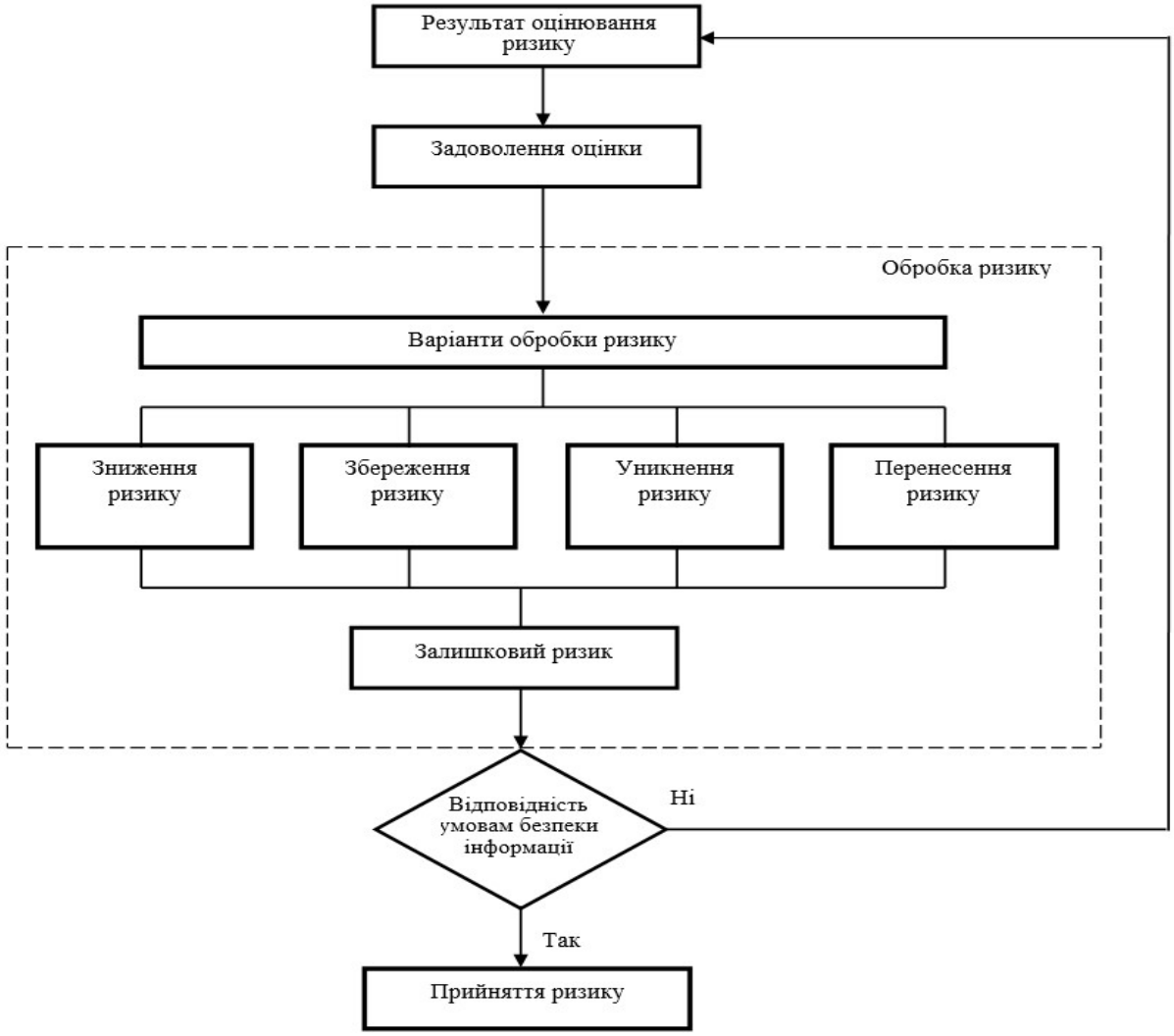

Рисунок 1 – Схема визначення залишкового ризику

Обробка ризиків здійснюється у такій послідовності [14]:

вибір варіанту обробки ризику;

реалізація обраного варіанту та отримання залишкового ризику;

оцінювання залишкового ризику та його прийняття.

Існує чотири варіанти обробки ризиків [14]:

зниження ризику;

збереження ризику;

уникнення ризику;

перенесення ризику.

Зниження ризику. Якщо рівень ризику є неприйнятним, приймається рішення про зниження ризику, що реалізується шляхом впровадження необхідних заходів і засобів захисту. Їх ефективність при обробці ризику має бути такою, щоб залишковий ризик став прийнятним.

Засоби технічного захисту інформації (далі – ТЗІ) можуть забезпечувати один або декілька варіантів захисту від негативних дій: їх виключення, попередження, зменшення їх впливу, стримування, виправлення. Під час вибирання засобів важливо «зважувати» вартість їх придбання, реалізації, функціонування, адміністрування та технічної підтримки по відношенню до цінності активів.

Існують обмеження, які можуть впливати на вибирання засобів ТЗІ. Наприклад, вони можуть понизити продуктивність роботи системи. Тому необхідно приймати таке рішення, яке задовольняє вимогам продуктивності і в той же час гарантує достатній рівень захисту. Результатом цього кроку є складання переліку можливих засобів ТЗІ з порівняльним аналізом їх вартості, недоліків, переваг та пріоритетів реалізації.

Збереження ризику. Ризик може бути збережений, якщо його рівень відповідає критеріям прийняття ризику. У такому разі немає потреби реалізовувати додаткові засоби захисту.

Уникнення ризику. Якщо витрати на обробку ризику перевищують бюджет, може бути прийняте рішення про уникнення цього ризику, що може бути реалізоване як відмова від діяльності, пов'язаної з цим ризиком, або зміна її умов. Наприклад, відносно ризиків, що викликаються стихійними лихами, найбільш вигідною альтернативою може бути фізичне переміщення засобів обробки інформації туди, де ймовірність таких ризиків дуже мала.

Перенесення ризику. Якщо витрати на обробку ризику перевищують бюджет, може бути прийняте рішення про перенесення ризику, що може бути реалізоване за допомогою систем аутсорсингу та/або страхування. Вибір цих систем залежить від вартості їх використання.

Прийняття ризиків є підсумковим кроком визначення залишкових ризиків. Рішення щодо прийняття ризику можуть внести поправки до вибору заходів і засобів захисту. Коли властивості запропонованих заходів і засобів захисту відомі, можна повторно провести перевірку залишкового ризику та визначити, чи досягнуто рівень прийнятності ризику або необхідно змінити рішення щодо його прийнятності, щоб відобразити інформацію про властивості запропонованих заходів і засобів захисту.

Після того, як всі заходи і засоби захисту реалізовані, перевірені та визначені ефективними, результати перевірки прийнятності ризику мають бути повторно вивчені. Ризик, пов'язаний зі співвідношенням загроза/вразливість, тепер має бути скорочений до прийнятного рівня або усунуто. Якщо ці умови не дотримані, то рішення, прийняті на попередніх кроках, мають бути переглянуті для визначення належних заходів захисту.

Так, результати аналізу досліджень [16; 17] свідчать, що визначення показників захищеності інформації не враховують послуги спостережності за діями користувачів. Ці показники є якісними, а не кількісними, що на етапах проєктування та вибору системи технічного захисту інформації потрібної якості зменшує можливості оцінювання рівня та ефективності захищеності ресурсів, насамперед, захищеності інформації. Наприклад, з погляду оптимального співвідношення витрат на засоби захисту та досягнутих при цьому результатів (можливості з оптимізації параметрів систем захисту).

Методи, наведені в [16; 17] дають змогу отримати величину загального залишкового ризику у вигляді ймовірності реалізації загрози $q_{пз}$ порушення (подолання, злому) комплексної системи захисту (далі – КСЗ) за виразом:

$$q_{ПЗ} = 1-(1-q_{ПК})(1-q_{ПЦ})(1-q_{ПД}), \qquad (1)$$

де $q_{пк}$ – ймовірність реалізації загрози подолання конфіденційності;

$q_{пц}$ – ймовірність реалізації загрози подолання цілісності;

$q_{пд}$ – ймовірність реалізації загрози подолання доступності.

Аналіз виразу (1) свідчить, що визначення ймовірності порушення КСЗ здійснюється через ймовірності реалізації загрози подолання конфіденційності, цілісності та доступності в інформаційно-комунікаційних системах. Водночас, у зазначених в [16; 17] методах, ймовірність реалізації загрози впливу загроз на інформацію здійснюється не безпосередньо, а опосередковано. Наприклад, втрата оператором керованості інформаційно-комунікаційної системи може призвести до нездатності протистояти певним загрозам і, як наслідок, до втрати певних властивостей оброблюваної інформації. Під час урахування ймовірності впливу загроз на інформацію стає завдання визначення і оцінювання можливих потенційних втрат від недостатньої захищеності інформаційних ресурсів та інформаційно-комунікаційних систем.

Згідно з вимогами керівних документів [1–4] під час обробки інформації в інформаційно-

комунікаційних системах має забезпечуватися спостережність за діями користувачів, а саме ідентифікація, контроль і керованість ІКС.

Спостережність забезпечується в інформаційно-комунікаційній системі такими послугами [14]:

реєстрація (аудит);

ідентифікація й автентифікація;

створення достовірного каналу;

розподіл обов'язків;

перевірка цілісності комплексу засобів захисту;

проведення самотестування.

Тому для визначення ймовірності порушення (подолання, злому) $q_{ПЗ}$ комплексної системи захисту пропонується введення ймовірності реалізації загрози подолання захисту, що є наслідком неправомірних дій користувачів в ІКС $q_{ПЗНДК}$, що враховує послуги спостережності. Тоді вираз (1) буде мати такий вигляд:

$$q_{ПЗ} = 1-(1-q_{ПК})(1-q_{ПЦ})(1-q_{ПД})(1-q_{ПЗНДК}), \quad (2)$$

У виразі (2) ймовірність реалізації загрози подолання захисту ІКС неправомірними діями користувачів доцільно визначити за виразом [14]:

$$q_{ПЗНДК} = 1-(1-q_{ПР})(1-q_{ПДК})(1-q_{ПРО})\times \times(1-q_{ПЦКЗЗ})(1-q_{ВШНП})(1-q_{ВАОІ}), \quad (3)$$

де $q_{ПР}$ – ймовірність реалізації загрози від небезпечних для комп'ютерної системи дій, пов'язаних із процесом розпізнання (порушення реєстрації) користувача;

$q_{ПДК}$ – ймовірність реалізації загрози від втручання в процес передачі інформації (підслуховування або модифікації інформації) тобто порушення достовірного каналу;

$q_{ПРО}$ – ймовірність реалізації загрози від помилкових неавторизованих дій користувачів або адміністратора (порушення розподілу обов'язків);

$q_{ПЦКЗЗ}$ – ймовірність реалізації загрози від порушення цілісності комплексу засобів захисту;

$q_{ВШНП}$ – ймовірність реалізації загрози від внутрішнього шахрайства та неавторизованого підключення;

$q_{ВАОІ}$ – ймовірність реалізації загрози від відмови від авторства та одержання інформації.

Отже, вираз (2) дає змогу визначити величину загального залишкового ризику як ймовірності реалізації загрози порушення (подолання, злому) комплексної системи захисту з урахуванням ймовірності подолання захисту ІКС неправомірними діями користувачів, що визначається виразом (3).

Висновки й перспективи подальших досліджень

Удосконалення методу визначення залишкового ризику є важливим кроком за напрямом підвищення рівня безпеки інформації в інформаційно-комунікаційних системах. Врахування специфіки роботи органів військового управління і контекстуальних умов виконання ними завдань дає змогу забезпечити ефективне управління ризиками та зниження його негативного впливу на функціонування інформаційно-комунікаційної системи.

Урахування ймовірності прояву загрози інформації в інформаційно-комунікаційних системах під час втрати оператором керованості комп'ютерної системою дає змогу точніше визначити ймовірність реалізації загрози порушення (подолання, злому) комплексної системи захисту.

Отриманий вираз визначення ймовірності реалізації загрози подолання захисту інформаційно-комунікаційної системи неправомірними діями користувачів потенційно дає змогу уникнути диспропорційних витрат під час створення комплексної системи захисту інформації в інформаційно-комунікаційній системі, в якій циркулюватиме інформація з обмеженим доступом. Такий підхід оцінювання ризиків може покращити стан захищеності інформаційно-комунікаційних систем в органах військового управління Збройних Сил України та для Сил оборони України в цілому.

Напрямом подальших досліджень слід вважати розроблення методики оцінювання безпеки інформації в інформаційно-комунікаційній системі під час втрати оператором керованості комп'ютерною системою.

Список бібліографічних посилань

1. Про захист інформації в інформаційно-комунікаційних системах: Закон України від 05.07.1994 № 80/94-ВР в редакції Закону України № 1089-XI від 16.12.2020. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text (дата звернення: 05.04.2024). **2. Про затвердження Правил** забезпечення захисту інформації в інформаційних, комунікаційних та інформаційно-комунікаційних системах: постанова Кабінету Міністрів України від 29.03.2006 № 373 зі змінами 2021 році. URL: https://zakon.rada.gov.ua/laws/show/373-2006-%D0%BF#Text (дата звернення: 05.04.2024). **3. Про затвердження Типової інструкції** про порядок ведення обліку, зберігання, використання і знищення документів та інших матеріальних носіїв інформації, які містять службову інформацію: постанова Кабінету Міністрів України від 19.10.2016 № 736. URL: https://zakon.rada.gov.ua/laws/show/736-2016-%D0%BF#Text (дата звернення: 05.04.2024). **4. Про затвердження Положення** про технічний захист інформації в Україні: указ Президента України від 27.09.1999 № 1229, зі змінами 2008 році. URL: https://zakon.rada.gov.ua/laws/show/1229/99#Text (дата звернення: 05.04.2024). **5. ДСТУ 3396.0-96.** Захист інформації. Технічний захист інформації. Основні положення. [Чинний від 01.01.1997 р.]. URL: https://tzi.com.ua/downloads/DSTU%203396.0-96.pdf (дата звернення: 05.04.2024). **6. ДСТУ 3396.1-96.** Захист інформації. Технічний захист інформації. Порядок проведення робіт. [Чинний від 01.01.1997 р.]. URL: https://tzi.com.ua/downloads/DSTU%203396.1-96.pdf (дата звернення: 05.04.2024). **7. ДСТУ 3396.2-97.** Захист

інформації. Технічний захист інформації. Терміни та визначення. [Чинний від 01.01.1998 р.]. URL: https://tzi.com.ua/478.html (дата звернення: 05.04.2024). **8. НД ТЗІ 1.1 002 99**. Загальні положення щодо захисту інформації в комп'ютерної системі від несанкціонованого доступу. Київ : ДСТСЗІ СБ України, 1999. 15 с. URL: https://tzi.com.ua/downloads/1.1-002-99.pdf (дата звернення: 05.04.2024). **9. НД ТЗІ 1.1-003-99.** Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу. URL:https://tzi.ua/assets/files/1.1_003_99.pdf (дата звернення: 05.04.2024). **10. НД ТЗІ 1.4-001-2000.** Типове положення про службу захисту інформації. Київ: ДСТСЗІ СБ України, 2000. 37 с. URL: https://tzi.com.ua/downloads/1.4-001-2000.pdf (дата звернення: 05.04.2024). **11. НД ТЗІ 2.5-004-99**. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. Київ : ДСТСЗІ СБ України, 2000. 26 с. URL: https://tzi.com.ua/downloads/2.5-004-99.pdf (дата звернення: 05.04.2024). **12. НД ТЗІ 2.5 005 99**. Класифікація АС і стандартні функціональні профілі захищеності оброблюваної інформації від НСД. Київ : ДСТСЗІ СБ України, 1999. 25 с. URL: https://tzi.com.ua/downloads/2.5-005%20-99.pdf (дата звернення: 05.04.2024). **13. НД ТЗІ 2.6-001-11**. Порядок проведення робіт з державної експертизи засобів технічного захисту інформації від несанкціонованого доступу та комплексних систем захисту інформації в інформаційно-телекомунікаційних системах. Київ : ДСТСЗІ України, 2011. 130 с. URL: https://tzi.com.ua/downloads/2.6-001-11.pdf (дата звернення: 05.04.2024). **14. Критерії оцінки** захищеності інформації в комп'ютерних системах від несанкціонованого доступу. Офіц. вид. Київ : ДСТСЗІ СБ України, 1999. 59 с. (Нормативний документ системи технічного захисту інформації). URL: https://tzi.com.ua/nd-tz-2.5-004-99.html (дата звернення: 05.04.2024). **15. Потій О. В., Горбенко Ю. І., Замула О. А., Ісірова К. В.** Аналіз методів оцінки і управління ризиками кібер- і інформаційної безпеки Радіотехніка. 2021. Вип. 206 С. 5–23. DOI: https://doi.org/10.30837/rt.2021.3.206.01. **16. Матов О. Я., Василенко В. С., Будько М. М.** Визначення залишкового ризику при оцінці захищеності інформації в інформаційно-телекомунікаційних системах. *Реєстрація, зберігання і обробки даних*. 2004. Т. 6. № 2. С. 62–74. URL: http://dspace.nbuv.gov.ua/bitstream/handle/123456789/50657/07-Matov.pdf?sequence=1 (дата звернення: 15.05.2024). **17. Заячук Я. І., Осташа П. С.** Аналіз та оцінка ризиків інформаційної безпеки локально-обчислювальної мережі. *Восточно-Европейский журнал передовых технологий.* 2012. № 58. С. 40–43. DOI: 10.15587/1729-4061.2012.5742.

AN IMPROVED METHOD FOR DETERMINING THE RESIDUAL RISK IN INFORMATION AND COMMUNICATION SYSTEMS WHEN ASSESSING INFORMATION VULNERABILITY

Hulkov Mykola
Hannenko Svitlana ***(candidate of technical sciences)***

National University of Defence of Ukraine, Kyiv, Ukraine

Formulation of the problem in general. *Residual risk is an important aspect of information security management, as it determines the risks that remain after the implementation of information security measures. Determining the residual risk by including services for monitoring user actions will help reduce the impact on information security in information and communication systems and increase the effectiveness of protection measures. The purpose of the article is to improve the method of determining the residual risk when assessing the vulnerability of information in information and communication systems by improving the accuracy of determining the breach (overcoming, hacking) of an integrated security system in the process of loss of control over a computer system by an operator. The improvement is carried out by introducing the probability of realization of the threat of overcoming protection by illegal actions of users in information and communication systems.*

Research methods. *In writing the article, the following research methods were used: system analysis in conducting information security analysis; comparative analysis - in analyzing the compliance of information security with the requirements of State standards; factor analysis - in assessing the vulnerability of information in information and communication systems by increasing the accuracy of calculating the probability of overcoming security measures when a computer system loses controllability; empirical research - in studying the impact of information flows on the functioning of information systems. This methodological approach makes it possible to implement systems for analyzing the control of an information and communication system and to control the introduction of any changes to computer systems, which in turn specifies the requirements for creating standards for a set of computer system security features.*

Analysis of recent researches and publications. *The author proposes criteria for assessing the security of information in computer systems against unauthorized access, analyzing and assessing the risks of local area network vulnerability, which is relevant at present. However, the author does not consider the observability criteria that should be taken into account when assessing the vulnerability of information in information and communication systems.*

Presenting the main material. *An improvement of the method for determining the residual risk in information and communication systems in assessing information vulnerability is proposed by means of the integrated use of quantitative characteristics in the form of probabilities of realization of the threat of overcoming the confidentiality of integrity of availability with the addition of the probability of realization of the threat of overcoming the protection resulting from illegal actions of users in the information and communication system. An expression is presented that takes into account information security surveillance services in the form*

of components of the probability of realization of the threat of overcoming the ICS protection by illegal actions of users, namely: from actions dangerous for a computer system related to the process of recognition (violation of registration) of a user, from interference with the process of information transmission, from erroneous unauthorized actions, from violation of the integrity of the complex of protection means, from internal fraud and unauthorized connection from refusal of authorship and receipt of information.

***Elements of scientific novelty** are to further develop methods for determining the residual risk to ensure the security and reliability of information and communication systems by increasing the accuracy of calculating the probability of realization of the threat of overcoming the means of protection when the computer system loses controllability.*

***Theoretical and practical significance of the article** is the possibility of implementing an improved method for determining residual risk when assessing the vulnerability of information in the information and communication systems of the military command and control bodies of the Armed Forces of Ukraine and the State Defense Forces as a whole, as well as during command and staff exercises and training.*

***Conclusion and the perspectives of future researches** Taking into account the likelihood of a threat to information in information and communication systems when an operator loses control of a computer system makes it possible to more accurately determine the likelihood of a threat to violate (overcome, hack) the integrated protection system. The direction of further research should be the development of a methodology for assessing the security of information in an information and communication system when the operator loses control of the computer system of a military command and control body.*

***Keywords**: information and communication system, integrated security system, residual risk, probability of threat realization, overcoming protection, loss of control.*

References

1. ***On the protection*** *of information in information and communication systems* [online], (1994), Zakon Ukrainy № 80/94-BP, 5 May. Available at: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text [Accessed: 05 April 2024]. **2.** ***On the approval*** *of the Rules for ensuring the protection of information in information, communication and information and communication systems* [online], (2006), Postanova Cabinetu Ministriv Ukrainy № 373, 29 March. Available at: https://zakon.rada.gov.ua/laws/show/373-2006-%D0%BF#Text [Accessed: 05 April 2024]. **3.** ***On the approval*** *of the Standard Instruction on the procedure for record-keeping, storage, use and destruction of documents and other material carriers of information containing official information*, [online], (2016), Postanova Cabinetu Ministriv Ukrainy № 736, 19 October. Available at: https://zakon.rada.gov.ua/laws/show/736-2016-%D0%BF#Text [Accessed: 05 April 2024]. **4.** ***On approval*** *of the Regulation on technical information protection in Ukraine*, [online], (1999), Ukaz Prezidenta Ukrainy № 1229, 27 September. Available at: https://zakon.rada.gov.ua/laws/show/1229/99#Text [Accessed: 05 April 2024]. **5. Derzhspozhyvstandart Ukrainy,** (1997). *Protection of information. Technical protection of information. Substantive provisions*. DSTU 3396.0-96. **6. Derzhspozhyvstandart Ukrainy,** (1997). *Protection of information. Technical protection of information. The order of work.* DSTU 3396.1-96. **7. Derzhspozhyvstandart Ukrainy,** (1998).*Protection of information. Technical protection of information. Terms and definitions*. DSTU 3396.2-97. ***8. ND TZI 1.1 002 99.*** *General provisions on protection of information in the computer system against unauthorized access* [online], (1999), Nakaz SB Ukrainy № 22, 28 April. Available at: https://tzi.com.ua/downloads/1.1-002-99.pdf [Accessed: 05 April 2024]. **9.** ***ND TZI 1.1-003-99.*** *Terminology in the field of information protection in computer systems against unauthorized access* [online], (1999), Nakaz SB Ukrainy № 22, 28 April. Available at: https://tzi.ua/assets/files/1.1_003_99.pdf [Accessed: 05 April 2024]. **10.** ***ND TZI 1.4 001 2000.*** *Standard provision on the information protection service* [online], (2000), Nakaz SB Ukrainy № 53, 04 December. Available at: https://tzi.com.ua/downloads/1.4-001-2000.pdf [Accessed: 05 April 2024]. **11.** ***ND TZI 2.5-004-99.*** *Criteria for evaluating the security of information in computer systems against unauthorized access* [online], (1999), Nakaz SB Ukrainy № 22, 28 April. Available at: https://tzi.com.ua/downloads/2.5-004-99.pdf [Accessed: 05 April 2024]. **12.** ***ND TZI 2.5 005 99.*** *Classification of AS and standard functional profiles of protection of processed information from NSD* [online], (1999), Nakaz SB Ukrainy № 22, 28 April. Available at: https://tzi.com.ua/downloads/2.5-005%20-99.pdf [Accessed: 05 April 2024]. **13.** ***ND TZI 2.6-001-11.*** *The procedure for carrying out work on state examination of means of technical protection of information against unauthorized access and complex information protection systems in information and telecommunication systems* [online], (2011), Nakaz DSSZZI Ukrainy № 65, 25 March. Available at: https://tzi.com.ua/downloads/2.6-001-11.pdf [Accessed: 05 April 2024]. **14.** ***Criteria*** *for evaluating the security of information in computer systems against unauthorized access. officer kind* [online], (1999), Nakaz SB Ukrainy № 22, 28 April. Available at: https://tzi.com.ua/nd-tz-2.5-004-99.html [Accessed: 05 April 2024]. **15 Potii, O. V., Horbenko, Yu. O., Zamula, O. A., Isirova, K. V.,** (2021). Analysis of cyber and information security risks assessment and management methods. *Radio engineering*, 206, 5–23. DOI: https://doi.org/10.30837/rt.2021.3.206.01. **16. Matov, O. Ya., Vasylenko, B. C., Budko, M. M.**, (2004). Determination of the residual risk in the assessment of information security in information and telecommunication systems. Registration, storage and processing. Danih. 6, 2, 63-74. Available at: http://dspace.nbuv.gov.ua/bitstream/handle/123456789/50657/07-Matov.pdf?sequence=1 [Accessed: 05 April 2024]. **17. Zayachuk, Y. I., Ostasha, P. S.,** (2012). Analysis and assessment of information security risks of the local computing network. *Eastern European Journal of Advanced Technologies*, 58, 40-43. DOI: 10.15587/1729-4061.2012.5742.