DOI https: //doi.org/10.36486/mst2411–3816
DOI (Issue): https: //doi.org/10.36486/mst2411–3816.2023.1(72)

МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
ДЕРЖАВНИЙ НАУКОВО-ДОСЛІДНИЙ ІНСТИТУТ

СУЧАСНА СПЕЦІАЛЬНА ТЕХНІКА

НАУКОВО-ПРАКТИЧНИЙ ЖУРНАЛ

№ 1(72), 2023

ВИДАЄТЬСЯ ЩОКВАРТАЛЬНО

ЗАСНОВНИК

Державний науково-дослідний інститут МВС України; Національний авіаційний університет; Національна академія внутрішніх справ

НАКАЗОМ

МОН України від 17.03.2020 № 409 науково-практичний журнал “Сучасна спеціальна техніка” включено до Переліку наукових фахових видань України відповідно до списку згідно з додатком 1 (категорія “Б”)

ЗАРЕЄСТРОВАНО

Міністерством юстиції України 13 лютого 2015 року

Свідоцтво – серія КВ № 21221-11021Р

Науково-практичний журнал “Сучасна спеціальна техніка” внесено до переліку міжнародної науковометричної бази

Index Copernicus International Journal Master List

Рекомендовано до друку рішенням Вченої ради ДНДІ МВС України
(протокол від 27.04.2023 № 3)

Науково-практичний журнал посів ІІІ місце в конкурсі на краще наукове періодичне видання в системі МВС України у 2017 році та І місце у 2020 році

Київ 2023

ISSN 2411-3816 (Print)

СУЧАСНА СПЕЦІАЛЬНА ТЕХНІКА
MODERN SPECIAL TECHNICS

DOI (Issue): https: //doi.org/10.36486/mst2411–3816.2023.1(72)

Issue 1(72) 2023

ЗМІСТ

СИСТЕМИ ТА МЕТОДИ ОБРОБКИ ІНФОРМАЦІЇ

Бабенко Ю.М. Метод диференційованого кодування сегментів на основі врахування структурно-статистичної насиченості 5

Бараннік В.В., **Гаврилов Д.С.**, **Колесник В.О.**, **Цімура Ю.В.**, **Сіненко Д.В.**, **Заїчко К.В.** Метод оцінювання швидкодії селективної обробки даних у просторово-часовій області 19

Бараннік В.В., **Шульгін С.С.**, **Яковенко О.В.**, **Ревва К.В.** Метод форматування системи координат спектральних компонент для підвищення ефективності технологій кодування 32

Зимовченко В.О. Аналіз дефіциту електронних компонентів: причини, наслідки та чинники 46

Розорінов Г.М., **Сірченко І.А.**, **Неня О.В.**, **Фесенко М.А.**, **Березненко Н.М.** Оцінка залишкового ризику при забезпеченні функціонування захищеної мережі розповсюдження аудіовізуального контенту 58

ІНФОРМАЦІЙНЕ ТА НОРМАТИВНЕ ЗАБЕЗПЕЧЕННЯ НАУКОВОЇ ДІЯЛЬНОСТІ

Подойніцин В.М., **Подойніцин М.В.**, **Теслицький А.А.**, **Норенко Н.А**. Актуальні аспекти програми оборонної стандартизації Міністерства оборони США 71

Смерницький Д.В., **Тригубенко М.В.** Участь громадських об'єднань у діяльності технічних комітетів 79

Шапочка Т.І., **Біляєва О.Д.** Управління ризиками в відділі випробувань ДНДІ МВС України 85

ТЕХНІКА, ЗБРОЯ, ТРАНСПОРТ ТА ОБМУНДИРУВАННЯ

Будзинський М.П., **Бакал В.П.**, **Диких О.В.**, **Кисіль М.В.**, **Приходько В.І.**, **Заровна І.О.** Спеціальні причепи для перевезення вибухонебезпечних предметів та основні технічні вимоги до них 93

Власов В.А., **Бакал М.А.**, **Подойніцин В.М.** Аналіз сучасних технологій виробництва шоломів кулезахисних 104

Вяткіна Л.П., **Іванілова Н.А.** Зброя холодна: деякі аспекти класифікації ножів 115

Сергієнко Л.Г., **Будзинський М.П.**, **Бакал В.П.** Міжопераційний контроль як засіб підвищення якості одностроюю 123

СПЕЦІАЛЬНІ РОЗРОБКИ

Мельник В.Є. Створення сучасних приладів для проведення вибухових робіт електричним способом 132

Мусієнко Д.І. Фактори, що впливають на дальність функціонування радіолінії керування вибуховими пристроями 141

Смерницький Д.В., **Демченко В.Г.**, **Рябий С.М.**, **Коник А.В.**, **Марченко О.С.**, **Жванко Ю.П.** Багатофункціональний транспортабельний теплоакумулятор ємнісного типу: актуальність та доцільність використання в підрозділах системи МВС 153

ISSN 2411-3816 (Print)
СУЧАСНА СПЕЦІАЛЬНА ТЕХНІКА
MODERN SPECIAL TECHNICS
DOI (Issue): https: //doi.org/10.36486/mst2411–3816.2023.1(72)
Issue 1(72) 2023

УДК 004.621.3

Розорінов Георгій Миколайович,
доктор технічних наук, професор, професор Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського", м. Київ, Україна,
ORCID ID 0000-0002-6095-7539
Сірченко Іван Анатолійович,
аспірант Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського", м. Київ, Україна,
ORCID ID 0000-0001-5060-234X
Неня Олена Володимирівна,
кандидат юридичних наук, старший дослідник, т.в.о завідувача науково-дослідної лабораторії Державного науково-дослідного інституту МВС України, м. Київ, Україна,
ORCID ID 0000-0001-9721-5718
Фесенко Максим Анатолійович,
кандидат технічних наук, доцент, провідний науковий співробітник Державного науково-дослідного інституту МВС України, м. Київ, Україна,
ORCID ID 0000-0001-8218-4154
Березненко Наталія Михайлівна,
кандидат технічних наук, доцент, провідний науковий співробітник Державного науково-дослідного інституту МВС України, м. Київ, Україна,
ORCID ID 0000-0003-4589-3829

ОЦІНКА ЗАЛИШКОВОГО РИЗИКУ ПРИ ЗАБЕЗПЕЧЕННІ ФУНКЦІОНУВАННЯ ЗАХИЩЕНОЇ МЕРЕЖІ РОЗПОВСЮДЖЕННЯ АУДІОВІЗУАЛЬНОГО КОНТЕНТУ
(Частина 1)

Запропоновані підходи до оцінки величини залишкового ризику системи захисту мережі розповсюдження аудіовізуального контенту, зокрема оцінці можливого рівня заподіяної шкоди.

Розроблено моделі процесів захисту функціональних властивостей захищеності системи, для чого проаналізовано взаємодію атак на функціональні властивості мережі з засобами протидії цим загрозам. Визначено математичні співвідношення для оцінки кількісних характеристик. Знайдено ті елементи, через які захищеність контенту є найбільш вразливою для загроз.

Ключові слова: *аудіовізуальний контент, мережа, методика оцінки, залишковий ризик, захищеність контенту, конфіденційність ресурсів, мінімізації процедур.*

DOI (Article): https: //doi.org/10.36486/mst2411–3816.2023.1(72).5
Issue 1(72)2023
http://suchasnaspectehnika.com/

DOI (Issue): https: //doi.org/10.36486/mst2411–3816.2023.1(72) Issue 1(72) 2023

Вступ

Контент – це термін, яким зазвичай називають наповнення (склад) певного інформаційного ресурсу. Цей термін використовується у сфері інтернет-ресурсів, і під його характеристику підпадають: текстові, аудіо-, відеоматеріали, записи, зображення тощо [1].

Весь контент на офлайн- та онлайн-майданчиках (просторах) можна розділити на дві великі групи, а саме: аудіо- і візуальний контенти [2].

Аудіоконтент – це інформація, що сприймається на слух. Перевагою такого контенту можна визнати доступність та можливість прослуховування фоном.

Візуальний контент – це та інформація, яку ми сприймаємо за допомогою очей. Основна його перевага полягає в тому, що він чудово привертає увагу.

Сучасні технології дозволили поєднати дві ці групи воєдино, створивши мову аудіовізуальних образів, завдяки чому глядач якнайповніше репрезентує картину дійсності. У зв'язку зі спрощенням поширення аудіовізуального контенту, створюється нова екранна реальність, у якій формуються система цінностей, світогляд, естетичні й етичні смаки та розуміння світу сучасною людиною.

Сучасний інформаційно-комунікаційний простір дає змогу людині, а також різним організаціям (підприємствам) не лише споживати аудіовізуальну продукцію, а й самостійно створювати, транслювати її онлайн у соцмережах, а також бути власником каналів, наприклад, на відеохостингу YouTube.

Аудіовізуальна продукція являє собою особливий об'єкт авторських прав.

Відповідно до ч. 3 ст. 426 ЦК України, використання об'єкта права інтелектуальної власності іншою особою повинно здійснюватися виключно з дозволу правовласника, крім випадків правомірного використання без такого дозволу [3].

Сучасна практика використання інформації (аудіовізуальної продукції, контенту) характеризується великою кількістю і постійним зростанням числа порушень як авторського права, так і інформаційної безпеки. Так, за результатами кримінологічного аналізу порушень авторського права в мережі Інтернет за період 2015–2020 років питома вага порушень авторського права в Інтернеті становить 42,8 % від усіх злочинів, передбачених ст. 176 КК України [4].

Одним із важливих чинників цього є постійно зростаюча доступність сучасних інформаційних технологій для злочинців, а також постійно зростаюча привабливість інформаційних систем як потенційних об'єктів нападу.

Також важливою обставиною є постійне ускладнення і зростання розмаїття інформаційних систем, що використовуються, і, зокрема, програмних продуктів. Наприклад, з урахуванням того, що в середньому кожна тисяча рядків програмного коду може містити, наприклад, від 5 до 15 помилок, поява дедалі більшого числа різних вразливостей, які створюють загрози для інформаційної безпеки, стає практично неминучою. Результатом цього є постійне зростання кількості різних порушень, пов'язаних з інформаційною безпекою.

Таким чином, усі зазначені обставини: зростання ріозмаїття можливих порушень, збільшення їх кількості, складності інформаційних технологій, постійно зростаюча доступність комп'ютерів і телекомунікаційних засобів для злочинців – пояснюють зростання потреби власників інформаційних ресурсів у реалізації систематичних, всеосяжних заходів щодо забезпечення інформаційної безпеки.

DOI (Article): https: //doi.org/10.36486/mst2411–3816.2023.1(72).5
Issue 1(72)2023 http://suchasnaspectehnika.com/

Важливим завданням при побудові систем захисту мереж розповсюдження аудіовізуального контенту (далі – МР АВК) є оцінка залишкового ризику. Це стосується, перш за все, складу та параметрів або необхідних кількісних характеристик окремих складових системи захисту, які забезпечують певну властивість захищеності інформаційних ресурсів, а також системи захисту в цілому. З урахуванням вимог нормативних документів одним із основних показників захищеності слід вважати залишковий ризик при забезпеченні функціональних властивостей захищеності МР АВК [5–9].

Проблемам інформаційної безпеки та захисту інформаційного простору приділяють увагу багато науковців. Серед зарубіжних вчених вагомий внесок у дослідження цього питання зробили П. Друкер, Г. Кіссінджер, К. Мак-Коннел, Ч. Флавін. Серед вітчизняних науковців зазначені питання висвітлюються в працях: О.В. Адамчука, Г.А. Атаманова, О.І. Барановського, А.Ю. Берко, О.В. Глазової, В.М. Грубова, В.В. Домарьова, В.Б. Дудикевича, В.В. Карасюка, О.О. Левіна, О.С. Олексюка, І.В. Рішняк, М.А. Судейко, І.О. Трубіна та інших [10].

Однак попри вагомий внесок перелічених науковців, враховуючи стрімкий розвиток комп'ютерних технологій і постійний вплив зовнішніх та внутрішніх чинників впливу на інформаційні системи, доцільним є детальніший розгляд питання розвитку систем інформаційної безпеки. Ретельного розроблення (удосконалення), зокрема, потребують форми та методи діяльності служб правоохоронної сфери в комплексному забезпеченні інформаційної безпеки як однією з найважливіших напрямів гарантування національної безпеки держави загалом.

Метою роботи є розроблення методики оцінки величини залишкового ризику системи захисту мережі розповсюдження аудіовізуального контенту.

Досягнення поставленої мети, на нашу думку, потребує вирішення трьох основних завдань: введення кількісних характеристик функціональних властивостей захищеності МР АВК на основі визначених класу і структури таких мереж; оцінка можливостей реалізації загроз контенту, що передбачає вивчення моделей порушника та загроз і є підставою для формування в подальшому моделей забезпечення захищеності контенту в мережі; аналіз можливих наслідків від реалізації потенційних загроз, тобто оцінку можливого рівня заподіяної ними шкоди – можливого залишкового ризику [8, 11–14].

Для цього необхідно:

– розробити моделі процесів захисту функціональних властивостей захищеності системи та проаналізувати взаємодію атак на функціональні властивості мережі з засобами протидії цим загрозам;

– визначити математичні співвідношення для оцінки кількісних характеристик;

– знайти ті елементи, через які захищеність контенту є найбільш вразливою для загроз.

Кількісні характеристики функціональних властивостей захищеності контенту

Розглянемо найбільш поширену ієрархічну МР АВК, яка складається з вузлів декількох рівнів, поєднаних між собою елементами телекомунікаційної мережі [6, 15–17]. Нехай основою вузлів є локальні обчислювальні мережі (крайній

DOI (Article): https: //doi.org/10.36486/mst2411–3816.2023.1(72).5
Issue 1(72)2023 http://suchasnaspectehnika.com/

випадок такої мережі – відокремлений комп'ютер) з відповідним базовим та прикладним програмним забезпеченням на будь-яких апаратних платформах. Тоді основними місцями, де циркулює інформація, є комп'ютери (процесори та запам'ятовуючі пристрої будь-якого типу), канали обміну, шлюзи (маршрутизатори, мережні сервери, сервери повноважень тощо) та інші елементи локальних та розподілених мереж. При цьому необхідно забезпечити захищеність інформаційних об'єктів, які зберігаються чи циркулюють:

– на "твердих" носіях – паперових носіях, магнітних, оптичних чи твердотільних (напівпровідникових) носіях в спеціальних сховищах чи приміщеннях (приклад – бібліотеки секретної літератури);

– на елементах комп'ютерів – зовнішніх запам'ятовуючих пристроях (на магнітних, оптичних, твердотільних носіях);

– на елементах комп'ютерів – в енергозалежних чи енергонезалежних запам'ятовуючих пристроях;

– в каналах обміну як локальних, так і розподілених інформаційно-обчислювальних мереж.

Візьмімо за факт те, що обладнання кожного з вузлів розташовується в межах певних будівель, приміщень з системою організаційного обмеження доступу – системою територіального захисту [18] (відомчої чи іншої охорони, перепускним режимом тощо), первинних технічних засобів захисту, у тому числі з системами охоронної та пожежної сигналізації, а одним із елементів МР АВК є підсистема захисту контенту [13, 14, 19]. До складу підсистеми захисту контенту слід включати її ядро з функціями управління усіма компонентами підсистеми та забезпечення такої функціональної властивості захищеності ресурсів МР АВК як спостережність. Крім цього, у підсистему інтегровані: засоби та механізми управління (адміністрування) доступом; засоби криптографічного захисту контенту; засоби управління фізичним доступом до приміщень та елементів

МР АВК (датчиків доступу до системних блоків, засобів блокування клавіатури та ін.); засоби захисту інформації в телекомунікаційній мережі; засоби захисту МР АВК від витоку технічними каналами та спеціального впливу на неї.

Для введення кількісних характеристик функціональних властивостей захищеності системи врахуємо, що рівень технічного захисту ресурсів МР АВК можна оцінювати за допомогою величини можливих збитків (шкоди) по кожному з класів порушень, та за допомогою залишкового ризику, застосування якого рекомендується НД ТЗІ 1.4–001–2000 [8]. Нагадаємо, що в цьому нормативному документі залишковий ризик оцінюється за якісною шкалою.

Звернемо увагу на те, що для оцінки величини можливих збитків (шкоди) необхідним є знання ймовірності виявлення і подальшої протидії загрозі i-го типу $p_{\text{ві}}$, чи зворотньої до неї величини $q_{\text{і}}$ – ймовірності невиявлення загрози цього ж типу. Тобто $q_i\left(i=1...3\right)$ є, за сутністю, величинами, які можна використати для кількісної оцінки залишкового ризику. Тому в якості оцінок залишкового ризику використаємо:

1) імовірність порушення конфіденційності $q_{\text{і}}$ – імовірність отримання інформації порушником з розкриттям її змісту, яка визначається:

DOI (Article): https: //doi.org/10.36486/mst2411–3816.2023.1(72).5
Issue 1(72)2023 http://suchasnaspectehnika.com/

– ймовірністю несанкціонованого доступу (при забезпеченні конфіденційності лише засобами обмеження доступу – порушення послуг довірчої чи адміністративної конфіденційності);

– криптографічною стійкістю зашифрованої інформації (при забезпеченні конфіденційності лише засобами криптографічного перетворення інформації);

– ймовірністю несанкціонованого доступу та криптографічною стійкістю зашифрованої інформації (при забезпеченні конфіденційності як засобами обмеження доступу, так і засобами криптографічного перетворення інформації);

2) імовірність порушення цілісності q_2, яка залежить від:

– ймовірності порушення цілісності шляхом несанкціонованого доступу (при забезпеченні цілісності лише засобами обмеження доступу – порушення послуг довірчої чи адміністративної цілісності);

– ймовірності виводу з ладу носіїв чи накопичувачів інформації (при навмисних чи випадкових впливах користувачів на фізичні ресурси);

– ймовірності виходу з ладу носіїв чи накопичувачів інформації (при впливах природних факторів на фізичні ресурси);

– ймовірності викривлення інформації (за випадкових впливів користувачів, а також за впливів природних факторів на інформаційні ресурси).

3. Ймовірність порушення доступності $q_{зі}$. яка залежить від:

– ймовірностей (аналогічно до ймовірностей щодо цілісності) виводу або виходу з ладу носіїв чи накопичувачів інформації, або спотворення інформації, залежно від того, здійснюється вплив на фізичні чи на інформаційні ресурси;

– ймовірності того, що середнє значення (математичне сподівання) часу затримки в доступі до ресурсу перевищує допустиме (наперед визначене) значення.

Визначення величин означених кількісних характеристик дозволяє оцінити рівень захищеності інформації засобами захисту, які застосовуються. При цьому враховуються можливості порушників щодо загроз з їх боку ресурсам МР АВК з метою завдання їм шкоди (моделі порушників), а також наявність можливих каналів впливу та види цих загроз.

Аналіз ризиків безпеки МР АВК

У загальному випадку, побудова систем моніторингу, що виявляють атаки зловмисників, можуть здійснюватися з використанням однієї з двох технологій [20]:

– виявлення зловживань (Misuse Detection – MD);

– виявлення аномалій (Anomaly Detection – AD).

Першу технологію моніторингу MD порівняємо з антивірусними системами, підключеними до комп'ютерної мережі. MD містить набір сигнатур, що описують типи з'єднань і трафіків, які вказують на те, що здійснюється конкретна атака на комп'ютерну систему.

Друга технологія моніторингу AD використовує набори моделей "нормального" мережевого трафіка, які оновлюються з часом. Відхилення від "еталонних моделей" відзначаються як аномальні і досліджуються засобами служби адміністратора системи безпеки.

Використання другої технології AD набуває дедалі більш широкого поширення, зокрема розроблено більше 50 таких підсистем. Велика кількість підсистем моніторингу орієнтовані на одну операційну систему, як правило, UNIX (наприклад

DOI (Article): https: //doi.org/10.36486/mst2411–3816.2023.1(72).5
Issue 1(72)2023 http://suchasnaspectehnika.com/

Cerberus), інші налаштовуються на конкретну архітектуру мережі й операційну систему (Satan) або призначені для виявлення конкретного типу аномалій (атак) (Crack).

За винятком перерахованих вище, натепер до практичних розробок доведена ще ціла низка механізмів й засобів моніторингу безпеки в комп'ютерних системах. Велика кількість поширених операційних системи декларують наявність досить розвинених засобів захисту інформаційних ресурсів. Навіть якщо реалізація цих засобів достатня з погляду прийнятої політики безпеки, необхідно враховувати ще дві множини ризиків: ризики, пов'язані з неправильною конфігурацією системи і ризики, що виникають внаслідок помилок у програмному забезпеченні [15].

Рекомендації за другою групою ризиків значною мірою залежать від політики, операційної системи, що проводиться виробником: якою мірою система є відкритою, наскільки для виробника допустиме визначення наявності помилок в своєму програмному забезпеченні, яка його оперативність при їх виправленні.

Для перевірки коректності системних установок (або їх незмінності з моменту останньої перевірки) існують програмні продукти класу "сканер безпеки системи". Ці продукти на сьогоднішній день існують для більшості операційних систем і їх кількість перевищує 10. До них належать такі продукти, як ASET (для операційної системи Solaris), KSA (для NetWare і NT) та SSS (System Security Scanner для Unix).

З огляду на те, що саме мережеві сервіси в багатьох випадках слугують об'єктом атак на розподілені інформаційні системи, існує завдання автоматизованої перевірки мережевих систем на уразливість з боку відомих атак. Уразливості, закладені в реалізації мережевих сервісів протоколу TCP/IP, достатньо добре проаналізовані. Першим продуктом, що виконував функцію оцінки уразливості мережевих сервісів, був пакет програм Satan. До складу пакету включені близько 20 перевірок уразливості мережевих сервісів. Якщо вимоги до системи включають періодичні перевірки за якнайповнішим списком уразливості (це, наприклад, необхідно для міжмережевих екранів, де такі перевірки повинні проводитися періодично), то необхідно використовувати більш сучасні засоби сканування уразливості, такі як, наприклад, Internet Scanner SAEsuite.

Задача автоматичного виявлення несанкціонованих дій і реакції на них логічно пов'язана із завданням автоматичного діагностування системи. Одним із засобів, що реалізовує такі дії на рівні мережевих сервісів, є RealSecure.

Інструментальний засіб RealSecure призначений для адміністративного управління великими об'ємами мережевої інформації. Він може бути використаний як для реєстрації подій, що відбуваються, наприклад, атак хакерів, так і для організації комплексу активних захисних заходів, які доповнюють функцію міжмережевого екрана. Особливість RealSecure полягає в тому. що він створений спеціально для роботи в мережі великих організацій і здатен одночасно відслідковувати події, що порушують безпеку, у безперервному режимі роботи. RealSecure включає в себе дві програмні підсистеми: підсистему фільтрації, що здійснює спостереження і активне управління мережевими подіями, і графічну підсистему, призначену для користувача інтерфейсу, за допомогою якої користувач отримує інформацію

DOI (Article): https: //doi.org/10.36486/mst2411–3816.2023.1(72).5
Issue 1(72)2023 http://suchasnaspectehnika.com/

про поточні події, може керувати ними в реальному масштабі часу, а також встановлювати і змінювати робочу конфігурацію пакету.

Загалом для реалізації моніторингу безпеки в наявних інформаційних системах є потреба активізувати засоби верифікації захисту в тих частках інформаційної системи, з якими пов'язані найбільші ризики для інформаційних ресурсів.

При розробленні засобів захисту і моніторингу безпеки виділяють три основні види загроз: загрози порушення конфіденційності оброблюваної інформації, загрози порушення цілісності оброблюваної інформації й загрози порушення працездатності системи.

Оптимальним є вибір таких методів і засобів захисту комп'ютерних систем і мереж, які забезпечили б найменший ризик реалізації загрози у кожному конкретному випадку. При розробленні засобів моніторингу безпеки одним з ключових питань є методика оцінки надійності і захищеності контрольованої системи. Загальним недоліком наявних натепер методик оцінки надійності і захищеності систем є суб'єктивність оцінки ризиків виникнення різних загроз [21, 22].

У загальному випадку об'єктом захисту є інформація. У свою чергу, її цінність – реальна вартість або величина збитків у випадку її знищення або втрати конфіденційності, змінюється з часом залежно від виду інформації.

Відповідно до цього можна таким чином класифікувати інформацію залежно від динаміки зміни її цінності в часі:

1) цінність інформації стаціонарна в часі (бази даних, інформація у яких актуальна впродовж тривалих періодів часу);

2) цінність інформації постійно зростає (бази даних на час накопичення інформації);

3) цінність інформації постійно зменшується (бази даних, актуальність інформації в яких знижується);

4) цінність інформації має верхній екстремум (інформація, яка в певний момент часу змінює свій статус, наприклад, при розробленні, яку патентують);

5) цінність інформації має нижній екстремум (теоретично можливий випадок).

На рис. 1 наведені усереднені оцінки залежності кількості звернень до інформації від часу відповідно до її цінності (номери кривих відповідають класифікації).

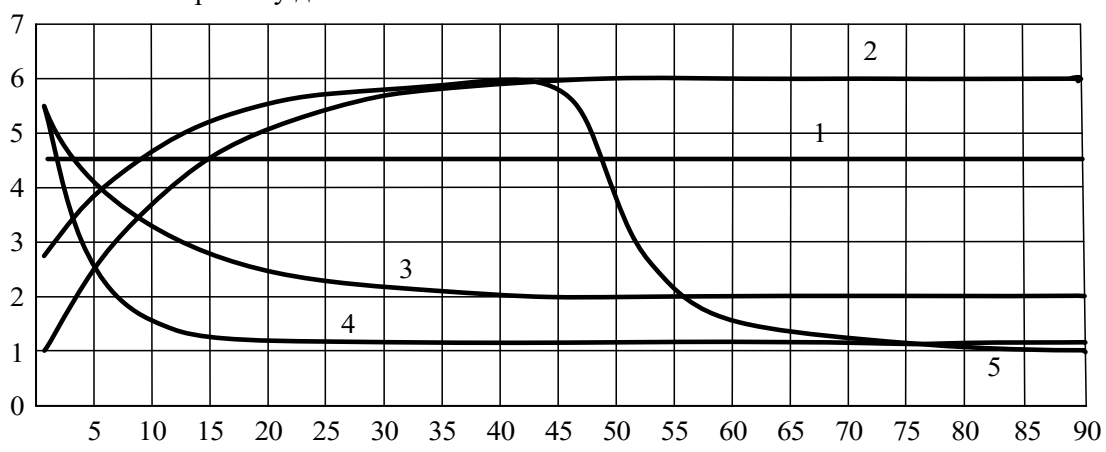

Рис. 1. Залежність кількості звернень до інформації у відповідності до її цінності

При оцінці надійності й захищеності МР АВК послідовно вирішуються чотири субзадачі:

– виділення факторів ризику й їх оцінка вагомості при порушенні системи захисту з врахуванням динаміки зміни цінності інформації;

– побудова загальної моделі функціонування мережі в умовах дії факторів ризику;

– ранжування за рівнем небезпеки слабких ланок мережі;

– визначення рівня захищеності мережі.

У загальному випадку можна вважати, що МР АВК складається з вузлів, які поєднані певним середовищем передачі даних, причому як для вузлів, так і для середовища передачі існують канали для здійснення несанкціонованого доступу [17, 21, 22]. Під здійсненням несанкціонованого доступу розуміємо подію, яка призводить до одного з таких результатів: порушення конфіденційності, порушення цілісності, відмова в обслуговуванні. Імовірність здійснення несанкціонованого доступу певним каналом і є ризик, а канал, яким несанкціонований доступ може бути здійснений, є фактором ризику.

Нехай i – фактор ризику з безлічі N ризиків. Нехай A_i, $i=1,N$ – подія, що призводить до здійснення несанкціонованого доступу, і P_i – імовірність події A_i, обумовленої фактором ризику. У загальному випадку вважатимемо, що події із безлічі A_i незалежні. Імовірність можна поділити на три види залежно від методики її визначення:

– стаціонарна (є однозначна закономірність її розрахунку);

– нестаціонарна (закономірність неоднозначна, використовуються експертні оцінки, статистичні методи);

– така, яку важко визначити (імовірність того, що подія, яка спричиняє загрозу, обумовлену неврахованим фактором ризику).

Якщо розглядати атаку на МР АВК як дію, що повторюється (пуасонів потік), то в загальному випадку:

$$P_i = e^{-\frac{\lambda_i}{\mu_i}} \frac{\left(\frac{\lambda_i}{\mu_i}\right)^{x_i}}{x_i}, \qquad (1)$$

де P_i – імовірність того, що атака на МР АВК по i-му каналу призведе до несанкціонованого доступу x_i разів; λ_i– інтенсивність дій i-м каналом;

μ_i – інтенсивність обслуговування дій в мережі.

Розглянемо окремий випадок, коли $x_i=1$, оскільки момент першої вдало реалізованої спроби несанкціонованого доступу найбільш важливий. Крім того, після успішної спроби несанкціонованого доступу слід очікувати збільшення значення μ_i як реакції з боку комп'ютерної системи, і збільшення λ_i, як реакції атакуючої сторони на успішну спробу, що дозволяє рахувати вхідний потік дій пуасоновим лише з певним ступенем наближення. Тоді при $x_i=1$:

DOI (Article): https: //doi.org/10.36486/mst2411–3816.2023.1(72).5
Issue 1(72)2023 http://suchasnaspectehnika.com/

$$P_i = e^{-\frac{\lambda_i}{\mu_i}} \frac{\lambda_i}{\mu_i}. \quad (2)$$

Розподіл щільності ймовірності несанкціонованого доступу по i-му каналу:

$$P(t_i) = e^{-\frac{t_i\lambda_i}{\mu_i}} \frac{\lambda_i}{\mu_i}. \quad (3)$$

У цьому випадку величина λ_i перебуває в функціональній залежності від цінності інформації, а μ_i є мірою захищеності мережі i-м каналом, і при $\mu_i \to \infty$ можна вважати, що канал повністю закритий від спроб несанкціонованого доступу.

Функціональні залежності $P(t_i)$ для різних випадків залежності цінності інформації від часу наведені на рис. 2.

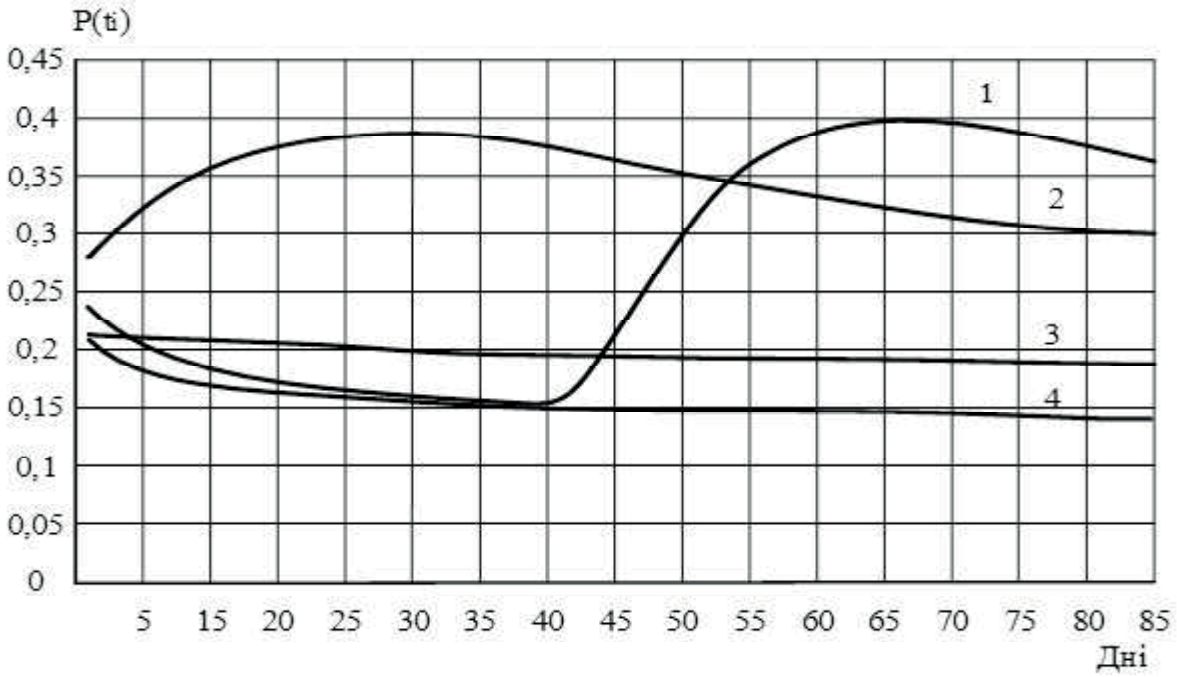

Рис. 2. Розподіл щільності ймовірності несанкціонованого доступу i-му каналом залежно від цінності інформації

На рис. 2 позначено: 1 – цінність інформації зростає; 2 – цінність інформації від часу має верхній екстремум; 3 – цінність інформації зменшується; 4 – цінність інформації практично постійна.

Після проведення оцінки P_i для ряду найбільш характерних факторів ризику виконується спільна оцінка безпеки мережі.

DOI (Article): https: //doi.org/10.36486/mst2411–3816.2023.1(72).5
Issue 1(72)2023 http://suchasnaspectehnika.com/

У першій частині статті запропоновано підходи до оцінки величини залишкового ризику системи захисту мережі розповсюдження аудіовізуального контенту. На відміну від наявних підходів, у тих, що пропонуються, враховуються зміни цінності інформації з часом, і, відповідно, ймовірність здійснення несанкціонованого доступу. При цьому атаки представляються як дії, які повторюються, що дає змогу використовувати математичний апарат теорії ймовірностей. Крім того, комплексне визначення ступеня захисту МР АВК забезпечує оптимальний рівень їх безпеки з огляду на різні критерії.

У частині ІІ статті розглядатимуться питання оцінки залишкового ризику при забезпеченні конфіденційності, цілісності та доступності до інформації.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Контент. URL: https://termin.in.ua/kontent/ (дата звернення: 02.01.2023).
2. Контент. URL: https://content/glossary/%D0%BA/content/ (дата звернення: 02.01.2023).
3. Глава 35. Цивільний кодекс України.
URL: https://patrul.in.ua/doc/kod/cku/g-35-tsku/ (дата звернення: 10.01.2023).
4. *Лісовий А.К.* Запобігання порушенням авторського права в мережі інтернет: дис. ... докт. філософії: 081 – "Право". URL: http://elar.naiau.kiev.ua/bitstream/123456789 ./19543/4/%D0%94%D0%B8%D1%81%20%D0%9B%D1%96%D1%81%D0%BE%D0%B2%D0%B8%D0%B9_%D0%BD%D0%B0%20%D1%81%D0%B0%D0%B9%D1%82.pdf (дата звернення: 11.01.2023).
5. НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу.
6. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу.
7. НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу.
8. НД ТЗІ 1.4-001-2000. Типове положення про службу захисту інформації в автоматизованих системах.
9. *Сірченко І.А., Розорінов Г.М.* Розробка моделі порушника мережі розповсюдження аудіовізуального контенту. Молодий вчений. № 3(103). 2022. С. 13–17.
10. Інформаційна безпека держави. URL: http://www.investplan.com.ua/pdf/5_2021/17.pdf (дата звернення: 02.01.2023).
11. *Дмитренко А.П., Сирченко Г.А., Хорошко В.А.* Модели безопасного соединения с удаленными объектами. *Захист інформації*. 2010. № 1. С. 53–57.
12. *Василенко В.С., Короленко М.П.* Цілісність інформації в автоматизованих системах. *Корпоративні системи*. 1999. № 3. С. 52–58.
13. *Сірченко Г.А.* Задачі забезпечення цілісності та доступності інформаційних об'єктів в комунікаційних мережах. *Захист інформації*. 2010. № 2. С. 49–54.
14. *Дмитренко А.П., Сирченко Г.А., Хорошко В.А.* Статистичне моделювання для оцінки захищеності локальної мережі. *Вісник ДУІКТ*. Т. 8. 2010. № 1. С. 62–67.
15. *Левин В.К.* Защита информации в информационно-вычислительных системах и сетях. *Программирование*. 1994. № 5. С. 5–16.
16. *Широчин В.П., Мухин В.Е., Крамар Д.И.* Анализ рисков в задачах мониторинга безопасности компьютерных систем и сетей. *Захист інформації*. 2003. № 1. С. 28–34.
17. *Домарев В.В.* Безопасность информационных технологий. Системный подход. Київ: ТНД "ДС", 2004. 992 с.
18. *Рижов О.А., Андросов А.І., Іванькова Н.А.* Сучасні мережеві технології: навчально-методичний посібник для студентів-провізорів очної, заочної та дистанційної форм навчання. Запоріжжя: ЗДМУ, 2018. 68 с.
19. *Голубенко О.Л., Головань С.М., Петров О.С., Хорошко В.О., Яремчук Ю.Є.* Політика інформаційної безпеки. Луганськ: вид. СНУ ім. В. Даля, 2009. 300 с.
20. *Лукацкий А.В.* Адаптивное управление защитой. *Сети. Глобальные сети и телекоммуникации*. 1999. № 10. С. 27–35.

DOI (Article): https: //doi.org/10.36486/mst2411–3816.2023.1(72).5
Issue 1(72)2023 http://suchasnaspectehnika.com/

21. Інформаційні технології та захист інформації: *збірник наукових праць*. Запорізький юридичний інститут. Вип. 1. 1998. 100 с.

REFERENCES

1. Contents. URL: https://termin.in.ua/kontent/ (Date of Application: 02.01.2023) [in Ukrainian].

2. Contents. URL: https://rtb.sape.ru/content/glossary/%D0%BA/content/ (Date of Application: 02.01.2023) [in Ukrainian].

3. Part 35. Civil Code of Ukraine. URL: https://patrul.in.ua/doc/kod/cku/g-35-tsku/ (Date of Application: 10.01.2023) [in Ukrainian].

4. *Lisovyy Artem Kostyantynovych*. Zapobihannya porushennyam avtors'koho prava v merezhi internet. "Prevention of Copyright Infringement on the Internet": thesis ... Doctor of Philosophy degree 081 "Law" "Prevention of copyright infringement on the Internet" (Date of Application: 11.01.2023) [in Ukrainian].

5. ND TZI 1.1-002-99. General provisions on the protection of information in computer systems against unauthorized access [in Ukrainian].

6. ND TZI 2.5-004-99. Criteria for evaluating the security of information in computer systems against unauthorized access [in Ukrainian].

7. ND TZI 2.5-005-99. Classification of automated systems and standard functional profiles of protection of processed information from unauthorized access [in Ukrainian].

8. ND TZI 1.4-001-2000. Standard provision on information protection service in automated systems [in Ukrainian].

9. *Sirchenko, I.A., Rozorinov, H.M.* (2022) Rozrobka modeli porushnyka merezhi rozpovsyudzhennya audiovizual'noho kontentu. "Development of a Model of a Violator of the Audiovisual Content Distribution Network". Young Scientist 3(103), March. P. 13–7 [in Ukrainian].

10. Informatsiyna bezpeka derzhavy. State information security. URL: http://www.investplan.com.ua/pdf/5_2021/17.pdf (Date of Application: 02.01.2023) [in Ukrainian].

11. *Dmitrenko, A.P., Sirchenko, G.A., Khoroshko, V.A.* (2010) Modeli bezopasnogo soyedineniya s udalennymi ob'yektami. "Models of Secure Connection with Remote Objectst. Information, Security 1, 53–57 [in Ukrainian].

12. *Vasilenko, V.S., Korolenko, M.P.* (1999) Tselostnost' informatsii v avtomatizirovannykh sistemakh. Information Integrity in Automated Systems. Corporate Systems 3, 52–58 [in Ukrainian].

13. *Sirchenko, H.A.* (2010) Zadachi zabezpechennya tsilisnosti ta dostupnosti informatsiynykh ob'yektiv v komunikatsiynykh merezhakh. "The Tasks of Ensuring the Integrity and Availability of Information Objects in Communication Networks". Information Protection 2, 49 54 [in Ukrainian].

14. *Dmitrenko, A.P., Sirchenko, G.A., Khoroshko, V.A.* (2010) Statisticheskoye modelirovaniye dlya otsenki zashchishchennosti local'noy seti. "Statistical Modeling for Assessing the Security of a Local Network". Bulletin of DUIKT. Vol. 8, No 1. P. 62 67 [in Ukrainian].

15. *Levin, V.K.* (1994) Zashchita informatsii v informatsionno-vychislitel'nykh sistemakh i setyakh. "Protection of Information in Informational Computing Systems and Networks". Programming 5, 5–6 [in Ukrainian].

16. *Shirochin, V.P., Mukhin, V.Ye., Kramar, D.I.* (2003) Analiz riskov v zadachakh monitoringa bezopasnosti komp'yuternykh sistem i setey. "Risk Analysis in the Tasks of Monitoring the Security of Computer Systems and Networks". Information Protection 1, 28 34 [in Ukrainian].

17. *Domarev, V.V.* (2004) Bezopasnost' informatsionnykh tekhnologiy. Sistemnyy podkhod. "Information Technology Security. Systems Approach". Kiev: TND "DS". 992 p.

18. *Ryzhov, O.A., Androsov, A.I., Ivan'kova, N.A.* (2018) Suchasni merezhevi tekhnolohiyi. "Modern Network Technologies": educational and methodological manual for pharmacist students of full-time, correspondence and distance education. Zaporizhzhia. 68 p. [in Ukrainian].

19. *Holubenko, O.L., Holovan', S.M., Petrov, O.S., Khoroshko, V.O., Yaremchuk, Yu.Ye.* (2009) Polityka informatsiynoyi bezpeky. "Information Security Policy". Luhansk: Ed. SNU named after. V. Dal. 300 p. [in Ukrainian].

20. *Lukatskiy, A.V.* (1999) Adaptivnoye upravleniye zashchitoy. "Adaptive Protection Control". Networks. Global networks and telecommunications 10, 27–35 [in Ukrainian].

21. Informatsiyni tekhnolohiyi ta zakhyst informatsiyi. Information technologies and information protection. Collection of scientific works. Zaporizhzhia: Law Institute. Issue 1, 1998. 100 p. [in Ukrainian].

UDC 004.621.3

Rozorinov Heorhii,
Doct. Sci. (Engineering), Full Professor, Professor at the National Technical University of Ukraine "Ihor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine,
ORCID ID 0000-0002-6095-7539
Sirchenko Ivan,
Postgraduate Student of the National Technical University of Ukraine "Ihor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine,
ORCID ID 0000-0001-5060-234X
Nenia Olena,
Cand. Sci. (Law), Senior Researcher, Acting Chief of the Research Lab of the State Research Institute MIA Ukraine, Kyiv, Ukraine,
ORCID ID 0000-0001-9721-5718
Fesenko Maksym,
Cand. Sci. (Engineering), Associate Professor,
Leading Researcher of the State Research Institute MIA Ukraine, Kyiv, Ukraine,
ORCID ID 0000-0001-8218-4154
Bereznenko Nataliia,
Cand. Sci. (Engineering), Associate Professor, Leading Researcher of the State Research Institute MIA Ukraine, Kyiv, Ukraine,
ORCID ID 0000-0003-4589-3829

AN ESTIMATION OF RESIDUAL RISK IN PROVIDING FUNCTIONING OF THE PROTECTED NETWORK OF AUDIOVISUAL CONTENT DISTRIBUTION

The modern practice of using information (audiovisual products, content) is characterized by a significant increase in the number of violations of both copyright and information security.

One of the important factors of this is the ever-increasing availability of modern information technologies for criminals and the attractiveness of information systems as potential targets of attack. Also an important circumstance is the ever-increasing complexity and diversity of the information systems used, and, in particular, software products.

Taking into account the increase and strengthening of the mentioned threats, there is a need for owners of information resources to implement systematic, comprehensive measures to ensure information security.

DOI (Article): https: //doi.org/10.36486/mst2411–3816.2023.1(72).5
Issue 1(72)2023 http://suchasnaspectehnika.com/

The article proposes approaches to assessing the value of the residual risk of the audiovisual content distribution network protection system (hereinafter – referred to as AVK MR). These approaches are based on solving the following tasks: the introduction of quantitative characteristics of the functional properties of the security of MR AVK based on the defined class and structure of such networks; assessment of the possibilities of implementing threats to the content, which involves the study of models of the violator and threats, and is the basis for the formation of models for ensuring the security of content in the network; analysis of possible consequences from the realization of potential threats, i.e. assessment of the possible level of damage caused by them – possible residual risk.

Models of the processes of protection of the functional properties of system security have been developed and the interaction of attacks on the functional properties of the network with means of countering these threats has been analyzed. Mathematical ratios for estimating quantitative characteristics have been determined. The elements that make content security most vulnerable to threats are found.

A comprehensive determination of the degree of protection of MR AVK ensures the optimal level of their security, based on various criteria. On the basis of the proposed approach, mechanisms are implemented as a separate subsystem in the complex of monitoring the security of computer systems and networks.

The obtained results will be useful during the creation of a system for the prevention of copyright infringements on the Internet, including in the field of law enforcement, both to ensure a sufficient level of protection of departmental information networks (resources), and to effectively solve the tasks assigned to them within the framework of the National Development Strategy areas of intellectual property.

Keywords: audiovisual content, network, evaluation method, residual risk, content security, resource confidentiality, minimization procedures.

Отримано 16.02.2023