УДК 004.621.3
DOI https://doi.org/10.32838/2663-5941/2022.2/06

Розорінов Г.М.
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»

Сірченко І.А.
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»

МОДЕЛЮВАННЯ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ ДЛЯ МЕРЕЖ РОЗПОВСЮДЖЕННЯ АУДІОВІЗУАЛЬНОГО КОНТЕНТУ

Акцентується увага на тому, що при моделюванні безпечного віддаленого доступу або безпечного з'єднання із віддаленим об'єктом в мережах розповсюдження аудіовізуального контенту головним є зіставлення наявних захисних засобів і ступеня жорсткості політики безпеки організації відносно контролю такого доступу та дотримання конфіденційності інформації при її передачі по незахищених мережах. При цьому потрібно враховувати статистику випадків несанкціонованого доступу в мережі, що мали місце раніше.

Розглянуті моделі безпечного модемного з'єднання, безпечного з'єднання через роутер, захисту інформації в мережах розповсюдження аудіовізуального контенту та безпечного Інтернет з'єднання.

Із розгляду представлених моделей взаємодії засобів реалізації атак з засобами забезпечення кожної з функціональних властивостей захищеності мереж розповсюдження аудіовізуального контенту робиться висновок про те, що для унеможливлення подолання неавторизованим користувачем системи захисту мережі необхідно застосовувати: організаційні заходи – зовнішня охорона, перепускний режим; первинні технічні заходи – блокування витоків інформації чи блокування спеціального впливу на неї технічними каналами, унеможливлення фізичного доступу до ресурсів мережі та до матеріальних носіїв даних; основні технічні заходи – засоби адміністрування чи управління доступом, засоби контролю чи контролю та поновлення цілісності та засоби криптографічного захисту інформації у відокремлених терміналах та їх мережах.

На основі розглянутих моделей побудовано загальну модель взаємодії атак та засобів захисту ресурсів мережі. Вона дає можливість отримати, окрім імовірнісних та часових характеристик конфіденційності, цілісності, доступності інформації, узагальнені кількісні характеристики системи захисту та оцінки тих характеристик чи параметрів відповідних засобів, які впливають на можливість забезпечення функціональних властивостей інформації. Загальна модель дозволяє визначити ті елементи, через які захищеність інформації у мережах розповсюдження аудіовізуального контенту є найбільш вразливою для загроз.

Ключові слова: *віддалений доступ, захищеність, контент, модель, показник.*

Постановка проблеми

При моделюванні безпечного віддаленого доступу або безпечного з'єднання із віддаленим об'єктом в мережах розповсюдження аудіовізуального контенту (МР АВК) головним є зіставлення наявних захисних засобів (активізованих і регулярно використовуваних) і ступеня жорсткості політики безпеки організації відносно контролю такого доступу та дотримання конфіденційності інформації при її передачі по незахищених мережах [1–4]. При цьому потрібно враховувати статистику випадків несанкціонованого доступу (НСД) в мережі, що мали місце раніше. В роботах [5, 6] приведений варіант таблиці показників, якими оперують при моделюванні віддаленого доступу (табл. 1).

Метою роботи є визначити можливий склад заходів та засобів для забезпечення кожної з властивостей захищеності МР АВК та розробити загальну модель взаємодії атак та засобів захисту ресурсів МР АВК.

Виклад основного матеріалу

1. Модель безпечного модемного з'єднання

Імовірність несанкціонованого доступу в локальну мережу через модемне з'єднання можна розрахувати таким чином:

$$P_M^P = M_{ДЗ} \cdot M_{МЛ} \cdot D \cdot P \cdot (1 - M_{ІА} \wedge M_{ВР}) \cdot (1 - M_Ф), \quad (1)$$

де P – імовірність здійснення спроби несанкціонованого доступу в локальну мережу через комутоване з'єднання. Визначається методом

експертних оцінок, шляхом урахування статистики прояву зовнішніх загроз в локальній мережі; D – кількість днів в році, в перебігу яких мережа повністю функціонує і пов'язана з видаленими мережами комутованим доступом; $M_{ДЗ}$ – середнє число вхідних дзвінків на одну лінію; $M_{МЛ}$ – кількість модемних ліній; $M_{ІА}$ – чисельний еквівалент відповідного синтаксичного показника ступеня використання алгоритмів ідентифікації і аутентифікації, що набуває значень: мінімальне – 0,1; низьке – 0,3; середнє – 0,5; високе – 0,8; максимальне – 0,95; $M_{ВР}$ – чисельний еквівалент відповідного синтаксичного показника важливості ресурсів, до яких є віддалений доступ, що набуває значень: мінімальне – 0,3; низьке – 0,5; середнє – 0,8; високе – 0,9; максимальне – 0,97; $M_{Ф}$ – чисельний еквівалент відповідного синтаксичного показника використання засобів фільтрації дзвінків, що набуває значень: мінімальне – 0,1; низьке – 0,3; середнє – 0,5; високе – 0,8; максимальне – 0,95.

Експериментальна імовірність НСД в локальну мережу через модемне з'єднання за період функціонування мережі, визначається як:

$$P_M^E = M_{ІА} \wedge M_Ч \cdot D \cdot (100 - M_П), \qquad (2)$$

де $M_Ч$ – частота випадків НСД в мережу через модем; $M_П$ – період функціонування локальної мережі.

Загальна імовірність НСД в локальну мережу через модемне з'єднання визначається як:

$$P_M^З = P_M^P \cdot (1 - K_Ф) + P_M^E \cdot K_Ф, \quad (3)$$

де $K_Ф$ – чисельний коефіцієнт, що враховує час функціонування локальної мережі, впродовж якого велася статистична обробка випадків НСД. $K_Ф$ набуває значень, відповідно: 0 – менше року; 0,2 – від року до двох років; 0,5 – від двох до чотирьох років; 0,8 – від чотирьох до семи років; 0,9 – більше семи років.

Як видно із формул (2), (3), експериментальна імовірність (яка визначається шляхом урахування статистичної обробки випадків НСД за період функціонування локальної мережі) має тим більший внесок у визначення загальної імовірності, чим за триваліший термін зібрані дані про спроби злому і, відповідно, навпаки, за відсутності тривалих спостережень загальна імовірність повністю визначається розрахунковою ймовірністю P_M^P.

Розраховану таким чином імовірність НСД в МР АВК $P_M^З$ треба зіставити з синтаксичним показником $M_{ВР,ЖБ}$ показників $M_{ВР}$ і $M_{ЖБ}$ – ступеня жорсткості політики безпеки модемного з'єднання (табл. 1). Імовірності НСД для модемного з'єднання при різних показниках $M_{ВР,ЖБ}$ зведено в табл. 2.

Розраховані ймовірності НСД для надійно захищеної мережі завжди менше приведених в табл. 2 для відповідних значень показника $M_{ВР,ЖБ}$. На основі різниці розрахованого значення $P_M^З$ і приведеного в табл. 2 визначається необхідний набір захисних засобів. При повторному порівнянні імовірності НСД з урахуванням нових значень показників прагнуть значення $P_M^З$ довести до якомога близького співпадіння відповідно до табл. 2.

Слід відзначити, що імовірність вдалої спроби НСД приведена за період часу, який дорівнює одному року.

2. Модель безпечного з'єднання через роутер

Розрахункову імовірність НСД в локальну мережу через роутер по аналогії з модемним з'єднанням можна визначити таким чином:

$$P_P^P = D \cdot P \cdot R_{АД} \cdot (1 - R_{СД})(1 - R_{КА}), \qquad (4)$$

де P – імовірність здійснення спроби НСД в локальну мережу через фізичне з'єднання. Визначається методом експертних оцінок, шляхом урахування статистики прояву зовнішніх загроз в локальних мережах; $R_{АД}$ – чисельний еквівалент відповідного синтаксичного показника ступеня активності доступу до мережі через WAN, що набуває значень: мінімальне – 0,1; низьке – 0,25; середнє – 0,5; високе – 0,85; максимальне –1; $R_{СД}$ – чисельний еквівалент відповідного синтаксичного показника ступеня довіри до організацій, які мають доступ до мережі, що набуває значень: мінімальне – 0; низьке – 0,2; середнє – 0,4; високе – 0,6; максимальне – 0,75; $R_{КА}$ – чисельний еквівалент відповідного синтаксичного показника ступеня кваліфікації адміністратора мережі, що набуває значень: мінімальне – 0; низьке – 0,2; середнє – 0,5; високе – 0,8; максимальне – 0,95.

Експериментальна імовірність НСД в локальну мережу через роутер, яка визначається за період функціонування локальної мережі, дорівнює:

$$P_P^E = R_{ІА} \wedge R_Ч \cdot D \cdot (100 - R_П). \qquad (5)$$

Загальна імовірність НСД в локальну мережу через роутер визначається як:

$$P_P^З = P_P^P \cdot (1 - K_Ф) + P_P^E \cdot K_Ф. \qquad (6)$$

Розраховану імовірність НСД в МР АВК $P_P^З$ порівнюють з відповідним синтаксичним показником $R_{ВР,ЖБ}$, який визначається співвідношенням показників $R_{ВР}$ і $R_{ЖБ}$ – ступеня жорсткості політики безпеки з'єднання через роутер (табл. 1). Імовірності НСД для з'єднання через роутер при різних показниках $R_{ВР,ЖБ}$ зведено в табл. 3.

Таблиця 1

Показники безпечного віддаленого доступу

Тип	Показник
Модемне з'єднання	
Чисельний	Кількість модемних ліній
Логічний	Наявність вбудованих в модем алгоритмів ідентифікації і аутентифікації
Синтаксичний	Ступінь використання алгоритмів ідентифікації і аутентифікації
Чисельний	Середнє число вхідних дзвінків на одну лінію
Синтаксичний	Важливість ресурсів, до яких є віддалений доступ
Логічний	Випадкі НСД в мережу через модем
Чисельний	Частота випадків НСД
Чисельний	Припинення НСД в мережу через модем
Логічний	Використання засобів фільтрації дзвінків
Синтаксичний	Ступінь жорсткості політики безпеки модемного з'єднання
З'єднання через роутер	
Синтаксичний	Ступінь активності доступу до мережі через WAN
Синтаксичний	Ступінь довіри до організацій, що мають доступ до мережі
Синтаксичний	Ступінь кваліфікації адміністратора мережі
Логічний	Випадки НСД в мережі через роутер
Чисельний	Частота випадків НСД
Чисельний	Припинення НСД в мережу через роутер
Синтаксичний	Ступінь жорсткості політики безпеки з'єднання через роутер
Захист інформації в МР АВК	
Логічний	Чи передається важлива інформація по незахищених МР АВК?
Синтаксичний	Об'єми, що передаються по МР АВК
Синтаксичний	Важливість АВК, що передається по МР
Синтаксичний	Ступінь використання криптографічних засобів
Синтаксичний	Ступінь жорсткості політики дотримання конфіденційності даних
Вихід в Інтернет	
Логічний	Чи використовується система Firewall?
Синтаксичний	Ступінь використання захисних засобів
Логічний	Наявність особи, відповідальній за безпеку
Синтаксичний	Ступінь використання антивірусних засобів
Логічний	Чи захищений прогін Java-аплетів (будь-яких інтерактивнх програм)?
Логічний	Чи завантажуються страниці тільки з сертифікованих Web-сайтов?
Синтаксичний	Ступінь контролю за імпортом програм
Синтаксичний	Ступінь навчання користувачів безпеки

Таблиця 2

Значення імовірностей НСД для модемного з'єднання при різних синтаксичних показниках $M_{ВР,ЖБ}$

Значення $M_{ВР,ЖБ}$	Імовірність P_M^3
мінімальне	>0,15
низьке	0,1 – 0,15
середнє	0,03 – 0,1
високе	– 0,03
максимальне	<0,01

Таблиця 3

Значення імовірностей НСД для з'єднання через роутер при різних синтаксичних показниках $R_{ВР,ЖБ}$

Значення $R_{ВР,ЖБ}$	Імовірність P_P^3
мінімальне	>0,15
низьке	0,1 – 0,15
середнє	0,03 – 0,1
високе	0,01 – 0,03
максимальне	<0,01

3. Модель захисту інформації в МР АВК

Модель припускає обчислення імовірності порушення конфіденційності при передаванні інформації по незахищених МР АВК:

$$P_K = C_{МП} \wedge P \cdot C_O (1 - C_{КЗ}), \qquad (7)$$

де P – імовірність перехоплення інформації в МР АВК. Вона визначається методом експертних оцінок, шляхом урахування статистики про-

яву зовнішніх загроз в розподілених мережах; C_O – чисельний еквівалент відповідного синтаксичного показника об'ємів, що передаються по МР АВК, який приймає значення: мінімальне – 0,1; низьке – 0,2; середнє – 0,5; високе – 0,8; максимальне – 1; $C_{КЗ}$ – чисельний еквівалент відповідного синтаксичного показника ступеня використання криптографічних засобів, що набуває значень: мінімальне – 0,5; низьке – 0,7; середнє – 0,8; високе – 0,95; максимальне – 0,999.

У цій моделі не представляється можливим врахувати статистику перехоплення конфіденційних повідомлень при передаванні через МР АВК, оскільки факт перехоплення або несанкціонованого ознайомлення із інформацією в розподілених мережах встановити практично неможливо. Тому в моделі застосовані криптографічні засоби, що дозволяють звести імовірність НСД до нуля [7–9].

Розраховану імовірність порушення конфіденційності при передачі інформації по незахищених каналах зв'язку P_K порівнюють з відповідним синтаксичним показником $C_{ВР,ЖБ}$, який визначається співвідношенням показників $C_{ВР}$ і $C_{ЖБ}$ – ступеня жорсткості політики дотримання конфіденційності даних (табл. 1) подібно до попередніх моделей [10]. Значення імовірностей порушення конфіденційності при різних синтаксичних показниках $C_{ВР,ЖБ}$ зведені в табл. 4.

Таблиця 4

Значення імовірностей порушення конфіденційності при різних синтаксичних показниках $C_{ВР,ЖБ}$

Значення $C_{ВР,ЖБ}$	**Імовірність P_K**
мінімальне	>0,001
низьке	0,001 – 0,0001
середнє	0,0001 – 0,000001
високе	0,000001 – 0,000001
максимальне	0,0000001

4. Модель безпечного Інтернет з'єднання

Модель безпечного Інтернет з'єднання відповідно до ступеня ризику МР АВК передбачає наявність набору захисних засобів, сумарний ваговий коефіцієнт яких відповідно до табл. 5 знаходиться у межах: низький ризик – 0…3, середній ризик – 4…10, високий ризик – більше 10. Таблиця 5 містить такі позначення: $K_{СН}$ – ступінь навчання користувачів безпеки, $K_{ПА}$ – чи захищений прогін Java-аплетів (будь-яких інтерактивнх програм)?, $K_{СС}$ – чи завантажуються страниці тільки з сертифікованих Web-сайтов?, $K_{ІП}$ – ступінь контролю за імпортом програм, $K_{АЗ}$ – ступінь використання антивірусних засобів, $K_{ВБ}$ – наявність особи, відповідальній за безпеку, K_{FW} – чи використовується система Firewall?

5. Загальна модель системи захисту МР АВК

Із розгляду представлених моделей взаємодії засобів реалізації атак з засобами забезпечення кожної з функціональних властивостей захищеності МР АВК можна зробити висновок про те, що для унеможливлення подолання неавторизованим користувачем системи захисту мережі необхідно застосовувати [11, 12]:

– організаційні заходи (організація зовнішньої охорони, перепускного режиму – унеможливлення проникнення через перепускні пункти, унеможливлення крадіжок матеріальних носіїв даних, зберігання в таємниці ідентифікаторів та паролів користувачів та ін.);

– первинні технічні заходи (блокування витоків інформації чи блокування спеціального впливу на неї технічними каналами, унеможливлення фізичного доступу до ресурсів мережі та до матеріальних носіїв даних, в тому числі через елементи будівельних конструкцій – наявність надійних стін, дверей, віконних ґрат, охоронної сигналізації та ін.);

– основні технічні заходи (засоби адміністрування чи управління доступом, засоби контролю чи контролю та поновлення цілісності та засоби криптографічного захисту інформації у відокремлених терміналах та їх мережах, в тому числі в розподілених мережах).

Розглянуті моделі дозволяють побудувати загальну модель взаємодії атак та засобів захисту ресурсів мережі (рис. 1).

Вона дає можливість отримати, окрім імовірнісних та часових характеристик конфіденційності, цілісності, доступності інформації, узагаль-

Таблиця 5

Вагові коефіцієнти захисних засобів відповідно до ступеня ризику

$K_{СН}$	$K_{ПА}$	$K_{СС}$	$K_{ІП}$	$K_{АЗ}$	$K_{ВБ}$	K_{FW}
низьк.– 0	так – 1	так – 1	низьк.– 0	низьк.– 0	так – 1	так – 1
сер.– 1	ні – 0	ні – 0	сер.– 2	сер.– 3	ні – 0	ні – 0
вис.– 3			вис.– 4	вис.– 5		

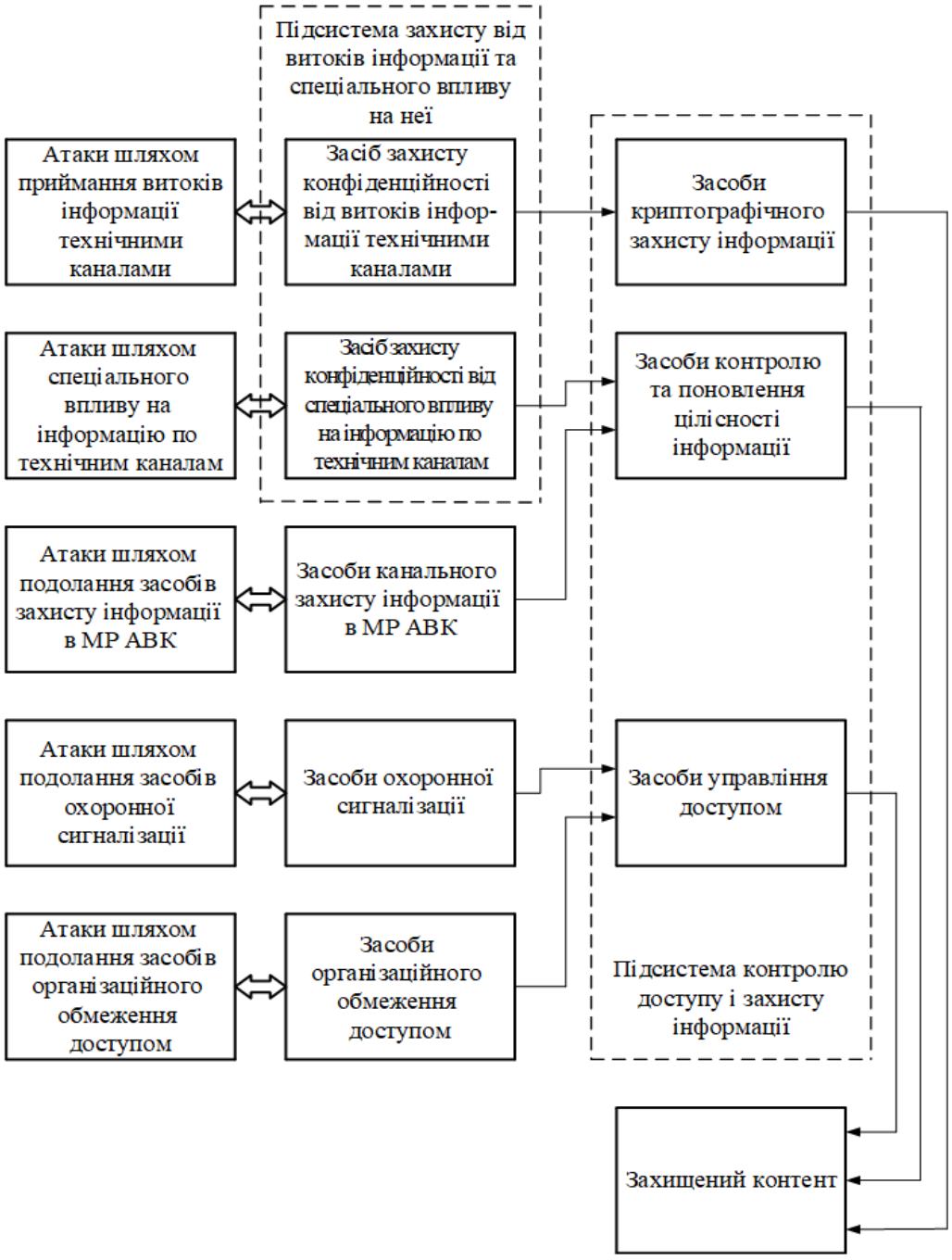

Рис. 1. Загальна модель системи захисту МР АВК

нені кількісні характеристики системи захисту та оцінки тих характеристик чи параметрів відповідних засобів, які впливають на можливість забезпечення функціональних властивостей інформації. Окрім того, ця модель дозволяє визначити ті елементи, через які захищеність інформації у МР АВК є найбільш вразливою для загроз.

При побудові загальної моделі враховано:

– функціональну близькість, схожість, інколи навіть єдність, деяких із засобів захисту, тобто їх здатність виконувати однакові функції захисту, хоча, можливо, і в різних умовах у складі різних моделей забезпечення функціональних властивостей захищеної системи;

– можливість об'єднати в деяких засобах певну множину близьких чи однотипних функцій, наприклад, в засобах управління доступом – функції адміністрування доступом, контролю та поновлення цілісності, фільтрації пакетів, блокування засобів генерації безперервних запитів та ін.;

– здатність інших засобів захисту виконувати функції захисту від однотипних загроз різ-

ним функціональним властивостям захищених ресурсів.

Це надає змогу об'єднувати різні засоби протидії певним загрозам чи, навпаки, відокремлювати окремі з них у відповідні підсистеми, внаслідок чого у складі системи технічного захисту можна вичленити підсистеми, які виконують свої функції в різних середовищах, чи по відношенню до достатньо характерних лише для них загроз, наприклад:

– підсистему контролю доступу і захисту інформації з функціями побудови моделі захищеної системи, побудови і реалізації правил розмежування доступу до ресурсів МР АВК, управління фізичним доступом, контролю та поновлення цілісності, криптографічного захисту інформації, фільтрації пакетів, блокування спроб підбору паролів тощо;

– підсистему захисту інформації від витоків інформації технічними каналами та спеціального впливу на неї.

Слід зазначити, що на рис. 1 не наведено засобів забезпечення спостереженості за подіями в захищеній системі, які є пов'язаними з усіма процесами використання інформації та її захисту. Це не означає приниження їх значення в процесі захисту контенту, а лише ілюструє те, що ці засоби не виконують функцій безпосереднього захисту ресурсів МР АВК. Але відсутність засобів забезпечення спостереженості чи їх подолання порушниками фактично означає наявність змоги доступу цих порушників до ресурсів мережі та, в цьому сенсі, засоби забезпечення спостережності відіграють таку ж роль, як і засоби забезпечення інших властивостей захищеності ресурсів МР АВК.

Звернемо увагу також на те, що до складу кожної з моделей взаємодії атак та засобів захисту ресурсів МР АВК входять засоби захисту відповідних властивостей захищеності контенту. Це означає суттєву вразливість стану захищеності МР АВК як раз через канали обміну інформацією та через їх елементи. Наслідком цього є принаймні відокремлення цих засобів захисту в підсистему захисту інформації в МР АВК. Це дозволяє зробити висновок про актуальність та важливість досліджень та розробок щодо методів та засобів забезпечення властивостей захищеності контенту в мережах, каналах обміну інформацією та їх елементах.

Висновки

1. Розроблено моделі взаємодії засобів реалізації загроз кожній з функціональних характеристик захищеності інформації та засобів протидії цим загрозам, тобто моделі подолання неавторизованим користувачам відповідних елементів систем захисту та отримано вирази для розрахунків величин залишкового ризику, кількісної оцінки захищеності інформації в МР АВК.

2. Визначено можливий склад заходів та засобів для забезпечення кожної з властивостей захищеності МР АВК та розроблено загальну модель взаємодії атак та засобів захисту контенту мережі.

3. Побудована загальна модель взаємодії атак та засобів захисту ресурсів мережі розповсюдження аудіовізуального контенту.

Список літератури:

1. Домарев В.В. Безопасность информационных технологий. Системный подход. Київ, 2004. 992 с.

2. Богуш В.М., Кудін А.М. Моніторинг систем інформаційної безпеки. Київ, 2006. 414 с.

3. Соколов А.В., Шальгин В.Ф. Защита информации в распределяемых корпоративных сетях и системах. Москва, 2002. 656 с.

4. Сірченко Г.А. Задачі забезпечення цілісності та доступності інформаційних об’єктів в комунікаційних мережах. *Захист інформації.* 2010. № 2. С. 49–54.

5. Хорошко В.А. Модель системы защиты информации. *Захист інформації.* 1999. № 1. С. 5–11.

6. Клейнен Дж. Статистические методы в имитационном моделировании. Москва, 1978. 221 с.

7. 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.

8. Яремчук Ю. Є., Павловський П. В., Катаєв В. С., Сінюгін В. В. Комплексні системи захисту інформації : навч. Посібник. Вінниця: ВНТУ, 2017. 120 с.

9. Хорошко В.А., Чекатков А.А. Методы и средства защиты информации. Київ, 2003. 504 с.

10. Конеев И.Р., Беляев А.В. Информационная безопасность предприятия. Санкт-Петербург, 2003. 688 с.

11. Соколов А.В., Шальгин В.Ф. Защита информации в распределяемых корпоративных сетях и системах. Москва, 2002. 656 с.

12. Дмитренко А.П., Сирченко Г.А., Хорошко В.А. Статистическое моделирование для оценки защищенности локальной сети. *Вісник ДУІКТ.* 2010. Т.8. № 1. С. 62–67.

Rozorinov H.M., Sirchenko I.A. MODELING OF INFORMATION SECURITY SYSTEMS FOR AUDIOVISUAL CONTENT DISTRIBUTION NETWORKS

Emphasis is placed on the fact that when modeling secure remote access or secure connection to a remote object in audiovisual content distribution networks, the main thing is to compare the available safeguards and the degree of rigidity of the organization's security policy to control such access and confidentiality unsecured networks. At the same time, it is necessary to take into account the statistics of cases of unauthorized access to the network that took place earlier.

Models are considered secure modem connection, secure router connection, protection of information in audiovisual content distribution networks and secure Internet connection.

From consideration of the presented models of interaction of realization means of attacks with means of providing each of functional properties of networks protection of audiovisual content distribution it is concluded that to prevent overcoming by the unauthorized user of a network protection system it is necessary to apply: organizational measures – external protection; primary technical measures – blocking information leaks or blocking special influence on it through technical channels, preventing physical access to network resources and physical media; basic technical measures – means of administration or management of access, means of control or control and restoration of integrity and means of cryptographic protection of information in separate terminals and their networks.

On the basis of the considered models the general model of interaction of attacks and means of protection of network resources is constructed. It provides an opportunity to obtain, in addition to probabilistic and temporal characteristics of confidentiality, integrity, availability of information, generalized quantitative characteristics of the protection system and evaluation of those characteristics or parameters of appropriate means that affect the functional properties of information. The general model allows us to identify the elements through which the security of information in audiovisual content distribution networks is most vulnerable to threats.

Key words: *remote access, security, content, model, indicator.*