УДК 004.056.5

МОДЕЛЬ ЗАГРОЗ БЕЗПЕКИ ВІДЕОІНФОРМАЦІЙНОГО РЕСУРСУ СИСТЕМ ВІДЕОКОНФЕРЕНЦЗВ'ЯЗКУ

В. В. Бараннік, д-р техн. наук, проф.; ***А. В. Власов***, ***Р. В. Тарнополов***

Харківський університет Повітряних Сил ім. Івана Кожедуба

Barannik_V_V@mail.ru

У статті розглянуто відеоінформаційний ресурс відеоконференцзв'язку профільних систем управління, який набуває значення державного інформаційного ресурсу. Показано, що для оцінки інформаційної безпеки відеоінформаційних ресурсів, необхідно виконувати аналіз потенційних загроз безпеки і будувати модель загроз. Виконано класифікацію загроз безпеки залежно від джерела їх виникнення та розроблено узагальнену модель загроз безпеки відеоінформаційного ресурсу відеоконференцзв'язку для профільної системи управління.

Ключові слова: відеоконференц зв'язок; відеоінформаційний ресурс; загроза безпеці; модель загроз.

The paper considers that the video information resource management systems videoconferencing profile acquires the importance of state information resource. It is shown that the evaluation of information security video information resource must perform an analysis of potential threats to security threats and build a model. In this context, classification is made security threats depending on their origin and developed a generalized model of video information security threats videoconferencing resource for profile management system.

Keywords: video conferencing, video information resource security threat , threat model.

Вступ

Розвиток інфокомунікаційних технологій, розширене їх упровадження значно впливає на якість функціонування органів державної влади. Головну роль відіграють системи управління та контролю, в тому числі із застосуванням відеоконференц зв'язку (ВКЗ). У цьому випадку відеоінформація, яка використовується в процесі обміну, набуває значення державного інформаційного ресурсу. Отже, актуальним є питання забезпечення безпеки такої інформації.

Для аналізу характеристик безпеки інформації найбільш часто застосовують модель CIA (*confidentiality*, *integrity and availability*) [1; 2]. Згідно з цією моделлю для відеоінформаційного (ВІ) ресурсу ВКС розглядаються три категорії безпеки інформації:

а) конфіденційність ВІ ресурсу — гарантія доступності конкретної відеоінформації тільки авторизованим користувачам;

б) цілісність ВІ ресурсу — здатність зберігати вихідний семантичний зміст відеоінформації, в умовах існуючих характеристик процесів обробки, передачі та зберігання інформації незалежно від територіального розташування її джерел і одержувачів (об'єктів управління і контролю);

в) доступність ВІ ресурсу — здатність забезпечити своєчасний безперешкодний доступ і обмін авторизованих користувачів відеоінформацією, яка за необхідності їх цікавить, установлені часові терміни незалежно від територіального розташування джерел і одержувачів відеоінформації.

Для оцінювання та формування підходів щодо забезпечення інформаційної безпеки ВІ ресурсу ВКЗ потрібно провести аналіз можливих порушень відеоінформації з обов'язковою ідентифікацією джерел загроз, факторів, що сприяють їх прояву і вразливостей [1–4]. Аналіз загроз інформації є одним з найважливіших етапів під час оцінювання реального стану забезпечення інформаційної безпеки (ІБ) в інформаційно-телекомунікаційних системах. Його основою є розробка моделі загроз [3–5].

Під *моделлю загроз* безпеки інформаційних ресурсів розумітемемо абстрактний формалізований або неформалізований опис методів і способів здійснення загроз [1; 4–6]. На підставі моделі загроз формується політика безпеки, в якій висвітлюються питання забезпечення ІБ (захисту від визначених загроз) з урахуванням ризиків їх реалізації.

Моделювання процесів порушення інформаційної безпеки доцільно проводити на основі аналізу взаємодії логічного ланцюжка «загроза — джерело загрози — метод реалізації — вразли-

вість – наслідки» (рис. 1), далі виконувати класифікацію, аналіз і оцінювання джерел загроз, вразливостей (факторів) і формувати вимоги щодо забезпечення інформаційної безпеки.

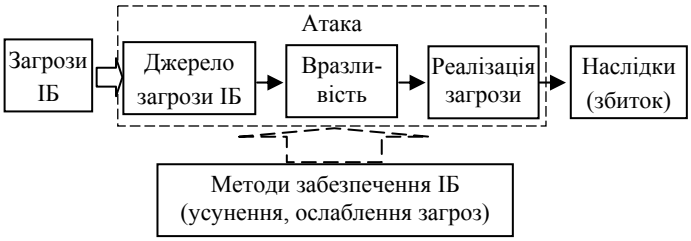

Рис. 1. Загальна модель реалізації загроз інформаційної безпеки

Розглянемо базові поняття. Під *загрозою* безпеки інформаційних ресурсів [1; 4; 5] будемо розуміти можливе порушення безпеки інформації в разі атаки з боку потенційного порушника ІБ (несприятливих для безпеки інформації дій (навмисних і ненавмисних)).

Під *джерелом загроз* інформаційної безпеки [1–5] розуміється носій загрози безпеки (суб'єкт, джерело, обставини), дії якого можуть призвести до порушення безпеки інформації.

Під *вразливістю* інформаційних ресурсів [1–5] розумітимемо причини, що призводять до порушення безпеки інформації і зумовлені недоліками процесу функціонування, властивостями інформаційної системи, технологій обробки і передачі інформації, умовами експлуатації.

Наслідки порушення безпеки інформаційних ресурсів — це можливі реалізації загроз джерелом загрози через наявні вразливості, спрямовані на нанесення збитків інформаційному ресурсу.

На підставі моделі реалізації загроз (рис. 1) виконується аналіз загроз ВІ ресурсу:

– визначаються джерела загроз;

– встановлюються вразливості;

– оцінюється взаємозв'язок загроз, джерел загроз і вразливостей;

– оцінюються можливі наслідки реалізації загроз;

– формується список значущих (актуальних) загроз безпеки інформаційного ресурсу.

Під *значущою (актуальною) загрозою* безпеці ВІ ресурсу розуміється загроза, яка може бути реалізована при здійсненні ВКЗ і становить реальну небезпеку порушення безпеки (окремих її категорій) ВІ ресурсу ВКЗ [1–5].

Результати моделювання процесів порушення інформаційної безпеки ВІ ресурсу ВКЗ можуть бути використані:

а) для оцінки реального стану інформаційної безпеки відеоінформаційного ресурсу;

б) для обґрунтування методів забезпечення інформаційної безпеки.

Вразливості і реалізація загроз безпеки можуть по-різному проявлятися / впливати на безпеку відеоінформаційного ресурсу в різних умовах і режимах функціонування ВКС.

Мета статті — побудова моделі загроз безпеки відеоінформаційного ресурсу при організації ВКЗ для профільних органів управління.

Основна частина

Вихідними даними для побудови моделі загроз та класифікації джерел загроз, вразливостей ВІ ресурсу ВКЗ є [1–4]:

– цільова спрямованість використання ВІ ресурсу в системі управління профільних органів державної влади;

– структура і склад системи управління профільних органів при організації ВКЗ;

– об'єкти і суб'єкти доступу до ВІ ресурсу ВКЗ;

– характеристики безпеки об'єктів доступу;

– апаратні і програмні засоби, що використовуються при організації ВКЗ та режими їх роботи;

– протоколи, які застосовуються в комплексах ВКС при обробці і передачі ВІ ресурсу;

– вимоги до якості ВІ ресурсу;

– зовнішні фактори впливів.

Проведений аналіз процесу організації та функціонування ВКЗ у системах державного управління (на прикладі системи управління ЗС [6–8]), дозволяє класифікувати загрози безпеки ВІ ресурсу ВКЗ на три основні групи залежно від джерела їх виникнення (рис. 2):

I. Загрози, зумовлені діями суб'єктів доступу (антропогенні загрози).

II. Загрози, зумовлені технічними засобами (техногенні загрози).

III. Загрози, спричинені стихійними джерелами (стихійні загрози).

Побудова моделі загроз залежно від джерела їх виникнення дає змогу надалі виконувати аналіз загроз для окремих категорій безпеки (конфіденційність, доступність і цілісність) за логічним ланцюжком взаємодії «загроза — джерело загрози — метод реалізації — вразливість — наслідки» (див. рис. 1).

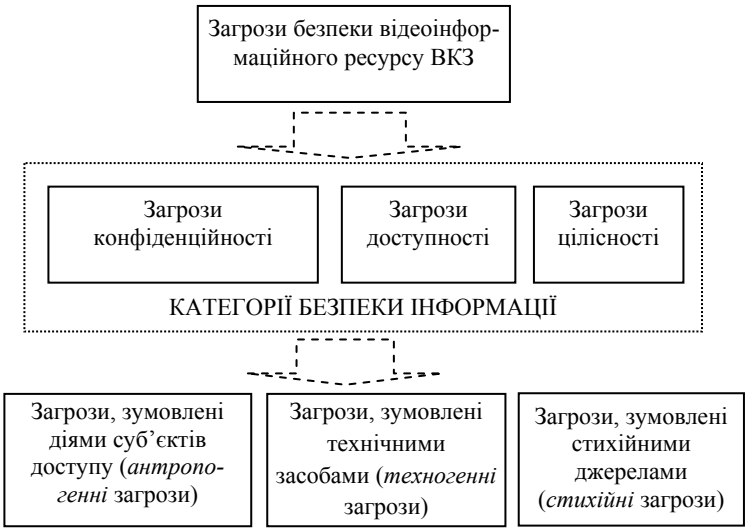

Рис. 2. Модель класифікації загроз безпеки відеоінформаційного ресурсу ВКЗ

Розглянемо модель загроз безпеки відеоінформаційного ресурсу ВКЗ.

До першої групи належать загрози, що виникають унаслідок дій суб'єктів доступу. Методи забезпечення ІБ (протидії) цим загрозам керовані і безпосередньо залежать від повноти оцінки і прогнозу. Суб'єкти, дії яких можуть призвести до порушення безпеки інформації в системі управління ЗС (в умовах мирного часу), можуть бути як *зовнішніми* відносно до системи управління, так і *внутрішніми*.

Зовнішні загрози, зумовлені діями:

– протидіючих структур (розвідувальні органи інших країн);

– контролюючих структур;

– конкуруючих структур (промислове шпигунство).

Внутрішні загрози, зумовлені діями:

– персоналу об'єктів управління;

– персоналу об'єктів контролю.

Аналіз застосування ВКЗ у системі управління профільних органів управління [7] дає змогу виділити такі антропогенні загрози, зумовлені діями суб'єктів доступу:

1. Крадіжка:

а) технічних засобів;

б) носіїв інформації (будь-якого виду);

в) інформації (читання і несанкціоноване копіювання);

г) засобів доступу (ключі, паролі, ключова документація та ін.).

2. Підміна (модифікація):

а) операційних систем;

б) серверів сховищ відеоінформації;

в) прикладних програм;

г) інформації (даних), заперечення факту відправлення відеоповідомлень;

д) паролів і правил доступу.

3. Знищення (руйнування):

а) технічних засобів;

б) носіїв інформації (будь-якого виду);

в) програмного забезпечення (комплексів ВКЗ, серверів сховищ відеоінформації);

г) інформації (файлів, даних);

д) паролів і ключової інформації.

4. Порушення нормальної роботи (переривання):

а) швидкості обробки інформації;

б) пропускної здатності каналів зв'язку;

в) маршрутизації передачі інформації;

г) збільшення обсягів необхідної інформації;

д) електроживлення технічних засобів.

5. Помилки:

а) при інсталяції програмного забезпечення (комплексів ВКЗ, серверів сховищ відеоінформації);

б) при розробці прикладного програмного забезпечення;

в) при передачі інформації;

г) при кодуванні / декодуванні інформації;

ж) при експлуатації програмного забезпечення;

е) при експлуатації технічних засобів.

6. Перехоплення інформації (несанкціоноване):

а) за рахунок електромагнітного випромінювання від технічних засобів;

б) за рахунок використання програмного забезпечення іноземних виробників (кодеків та ін.) в комплексах ВКЗ, серверах сховищ відеоінформації;

в) за рахунок наведень по лініях електроживлення;

г) за рахунок наведень по сторонніх провідниках;

д) по акустичному каналу від засобів виведення;

е) по акустичному каналу при проведенні нарад, обговоренні питань;

ж) при підключенні до каналів передачі інформації;

з) за рахунок порушення встановлених правил доступу (злом).

У другій групі загроз розглянемо менш прогнозовані загрози, але більш залежні від властивостей апаратури. Потенційні загрози безпеці ВІ ресурсу ВКЗ, зумовлені технічними засобами, так само можуть бути зовнішніми і внутрішніми.

До *зовнішніх* загроз другої групи (*техногенні* загрози) віднесемо загрози, зумовлені:

– функціонуванням апаратних засобів зв'язку;

– технологічно небезпечними виробництвами, розташованими в територіальній близькості від об'єктів управління і контролю;

– експлуатацією мереж інженерних комунікацій (енерго-, водопостачання, каналізації);

– транспортом.

Внутрішні загрози, зумовлені невідповідністю технологій і технічних засобів вимогам забезпечення безпеки, а саме:

– технологій обробки відеоінформації;

– програмних засобів комплексів ВКЗ;

– технічних засобів обробки і передачі відеоінформації;

– допоміжних відеозасобів (охорони, сигналізації, телефонії);

– інших технічних засобів.

Таким чином, *техногенними* загрозами безпеці відеоінформації ВКЗ можуть бути:

1. Порушення нормальних умов функціонування:

а) непрацездатність системи обробки відеоінформації;

б) непрацездатність єдиної інфокомунікаційної системи;

в) невідповідність (за технічними характеристиками) каналів обміну і засобів обробки інформації потрібним обсягам відеоінформації;

г) недотримання встановлених правил доступу;

д) електромагнітний вплив на технічні засоби.

2. Знищення (руйнування):

а) комплексів ВКЗ, серверів сховищ відеоінформації (програмні збої);

б) засобів обробки інформації (стрибки напруг, протікання);

в) приміщень;

г) інформації (розмагнічування, радіація, витік і ін.);

д) персоналу.

3. Модифікація (зміна):

а) програмного забезпечення комплексів ВКЗ, серверів сховищ відеоінформації;

б) відеоінформації при передачі в єдиній інфокомунікаційній системі.

Третю групу складають загрози, які зумовлені стихійними джерелами (факторами). Такі потенційні загрози безпеки ВІ ресурсу ВКЗ, як правило, є зовнішніми відносно ВКЗ. Як стихійні джерела виникнення загроз розглядаються:

– пожежі;

– землетруси;

– повені;

– урагани;

– інші обставини.

Стихійні загрози безпеки ВІ ресурсу ВКЗ завдають шкоди всім елементам системи управління ЗС. Під *стихійними* загрозами безпеці будемо розглядати:

1. Знищення (руйнування):

а) технічних засобів обробки і передачі відеоінформації;

б) носіїв відеоінформації;

в) апаратно-програмного забезпечення комплексів ВКЗ, серверів сховищ відеоінформації;

г) відеоінформаційних ресурсів;

д) приміщень;

е) персоналу.

2. Зникнення (руйнування, пошкодження):

а) ВІ ресурсу в засобах обробки (серверах сховищ відеоінформації);

б) ВІ ресурсу при передачі по каналах обміну;

в) носіїв відеоінформації;

г) персоналу.

У загальному вигляді модель загроз безпеки відеоінформаційного ресурсу ВКЗ у системі управління ЗС графічно пропонується подавати таким чином (рис. 3).

Для кожної складової ВКЗ при обробці і передачі ВІ ресурсу в системі управління ЗС розглянуті загрози за наведеною вище моделлю загроз: римська цифра позначає класифікаційну групу загроз, арабська цифра — порядковий номер загрози в групі загроз (див. рис. 2), а буква відповідне її найменування.

Як приклад розглянемо загрози безпеки ВІ ресурсу ВКС для складової — «виділені канали» (рис. 3). Визначено такі загрози:

– для І групи: 1, б, г; 2, а, б, в, г; 3, б, г, д; 4, а, б, в, г; 6, б, е, ж;

– для ІІ групи: 1, б, д; 2, б, г, 3, б;

– для ІІІ групи: 1, г; 2, б.

Погрозами, що виникають унаслідок дій суб'єктів доступу (*антропогенні* загрози) є:

1. Крадіжка:

а) носіїв інформації (будь-якого виду);

б) засобів доступу (ключі, паролі, ключова документація та ін.).

2. Підміна (модифікація):

а) операційних систем;

б) серверів сховищ відеоінформації; в) прикладних програм;

г) інформації (даних), заперечення факту відправлення відеоповідомлень. б) інформації (файлів, даних);

в) паролів і ключової інформації.

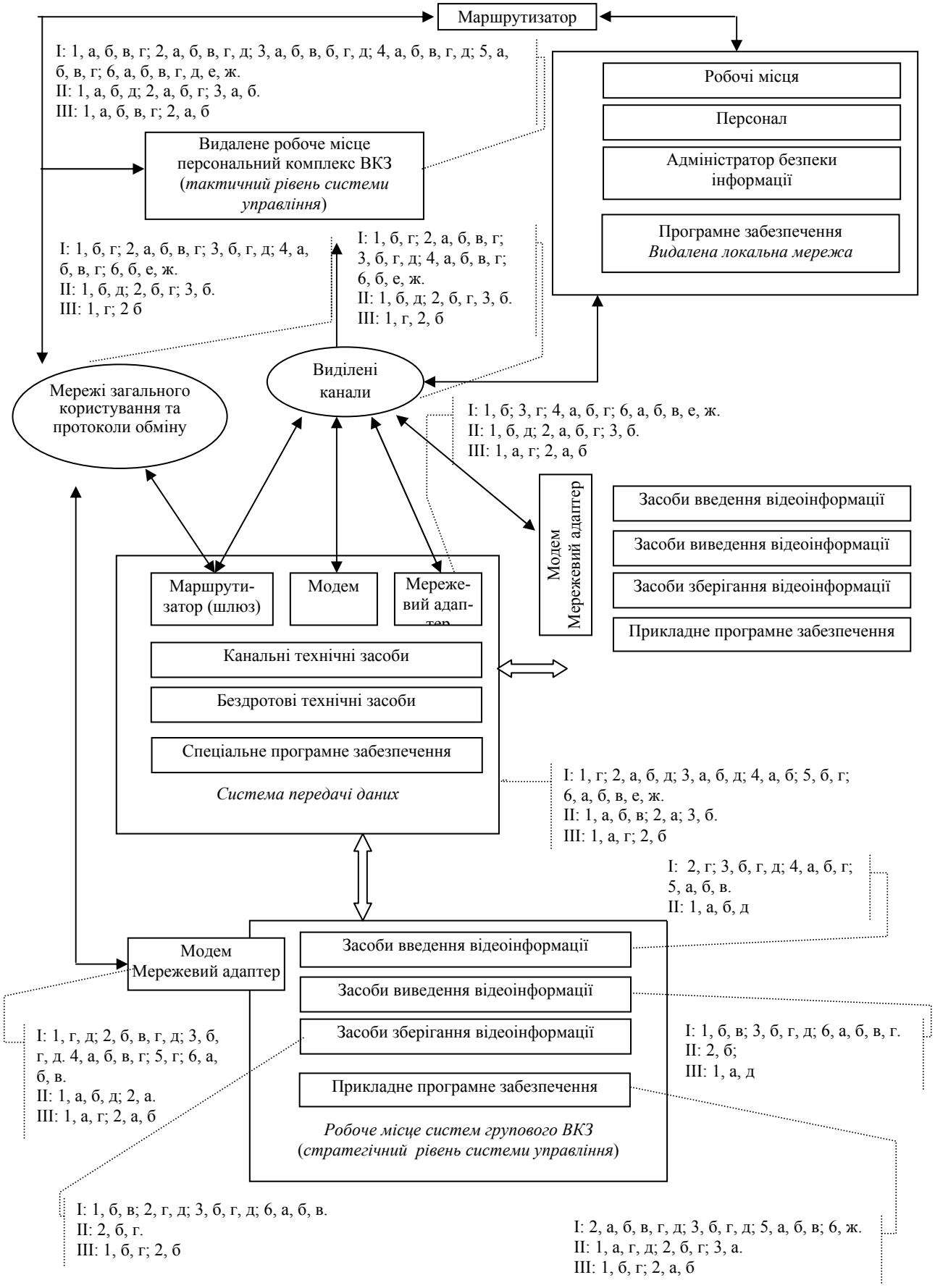

Рис. 3. Загальна модель загроз безпеки відеоінформаційного ресурсу ВКС у профільній системі управління (системі управління ЗС)

3. Знищення (руйнування):

а) носіїв інформації (будь-якого виду);

4. Порушення нормальної роботи (переривання):

а) швидкості обробки інформації;

б) пропускної здатності каналів зв'язку;

в) маршрутизації передачі інформації;

г) збільшення обсягів необхідної інформації;

д) електроживлення технічних засобів;

5. Перехоплення відеоінформації (несанкціоноване):

а) за рахунок використання програмного забезпечення іноземних виробників (кодеків і ін.) із впровадженими програмними закладками;

б) по акустичному каналу при проведенні нарад, обговоренні питань;

в) при підключенні до каналів передачі інформації.

Техногенними загрозами є:

1. Порушення нормальної роботи:

а) порушення працездатності єдиної інфокомунікаційної системи;

б) електромагнітний вплив на технічні засоби.

2. Знищення (руйнування):

а) засобів обробки інформації (кидки напруг, протікання);

б) інформації (розмагнічування, радіація, протікання і ін.).

3. Модифікація (зміна):

а) відеоінформації при передачі в єдиній інфокомунікаційній системі.

Погрозами, зумовленими діями *стихійних* факторів, є:

1. Знищення (руйнування):

а) інформації.

2. Зникнення (пошкодження, руйнування):

а) ВІ ресурсу при передачі по каналах обміну.

Аналіз наведеної моделі загроз дозволяє формувати перелік загроз безпеки ВІ ресурсу ВКЗ для кожної конкретної категорії ІБ — конфіденційності, цілісності, доступності.

Для визначення вразливостей ВІ ресурсу ВКЗ на етапах обробки і доставки в системі управління ЗС необхідно виконати:

– аналіз характеристик та вимог до відеоінформаційного ресурсу ВКЗ;

– аналіз характеристик телекомунікаційних технологій і каналів обміну інформацією;

– оцінювання граничних значень параметрів з обробки і доставки відеоінформаційного ресурсу;

– оцінювання взаємозв'язку та відповідності знайдених характеристик з необхідними параметрами та обсягами.

Більш докладне визначення загроз безпеці відеоінформаційного ресурсу ВКС виконується на підставі аналізу взаємодії логічного ланцюжка «загроза — джерело загрози — вразливість — метод реалізації — наслідки».

Таким чином, існує необхідність визначення вразливостей ВКЗ і вибору (обґрунтування) актуальних (найбільш значущих) загроз порушення безпеки відеоінформаційного ресурсу ВКЗ для конкретних її категорій, що і є завданням подальших досліджень.

Висновок

1. Розроблено модель загроз безпеки ВІ ресурсу ВКЗ для профільної системи управління, яка дозволяє враховувати структуру і склад системи при організації ВКЗ, цільове призначення ВІ ресурсу, об'єкти і суб'єкти доступу до ВІ ресурсу і джерела виникнення загроз.

2. Розроблена модель загроз безпеки ВІ ресурсу ВКЗ дозволяє виконувати аналіз вразливостей і реалізації загроз безпеці в профільних системах управління при різних умовах і режимах функціонування ВКЗ.

3. Аналіз запропонованої моделі загроз безпеки ВІ ресурсу ВКЗ за ланцюжком «загроза — джерело загрози — вразливість — метод реалізації» дозволяє визначати значущі (актуальні) загрози безпеки для конкретної категорії безпеки (конфіденційність, доступність і цілісність) ВІ ресурсу ВКЗ.

ЛІТЕРАТУРА

1. *Богуш В. М.* Інформаційна безпека держави / В. М. Богуш, О. К. Юдин. — К. : МК-Прес, 2005. — 432 с.

2. *Perrin*, Chad. The CIA Triad and Engineering Principles for Information Technology Security. Retrieved 31 May 2012.

3. *Рекомендации* по стандартизации «Информационные технологии. Основные термины и определения в области технической защиты информации» (Р 50.1.053-2005).

4. *Международный* стандарт ISO/IEC 15408-1-99 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель».

5. *Юдін О. К.* Інформаційна безпека. Нормативно-правове забезпечення: підруч. / О. К. Юдін. — К. : НАУ, 2011. — 640 с.

6. *Юдін О. К.* Концептуальний аналіз уразливості державних інформаційних ресурсів / О. К. Юдін, С. С. Бучик // Наукоємні технології. — 2013. — № 3 (19). — С. 299–304.

7. *Власов А. В.* Анализ особенностей применения видеоконференцсвязи в интересах профильных органов государственного управления / А. В. Власов, В. В. Баранник // Сучасна спеціальна техніка. — 2014. — Вип. 1. — С. 22–32.

8. *Власов А. В.* Кодирование информационных ресурсов систем видеоконференцсвязи для повышения их безопасности. / А. В. Власов, В. В. Лукин // Радиоэлектроника и информатика. — 2013. — № 2. — С. 65–73.

Стаття надійшла до редакції 12.02.2014