УДК 354.31(477)(004.7+65.012.8) **Кудінов В.А.**

ЗАГАЛЬНА МАТЕМАТИЧНА МОДЕЛЬ ОБ'ЄКТІВ ЗАХИСТУ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНОЇ СИСТЕМИ ОПЕРАТИВНОГО ІНФОРМУВАННЯ МВС УКРАЇНИ

Вступ

В органах і підрозділах внутрішніх справ МВС України функціонує єдина система збирання, опрацювання та подання до Міністерства внутрішніх справ України, головних управлінь (управлінь) МВС України в Автономній Республіці Крим, областях, містах Києві та Севастополі, на залізницях (далі – ГУМВС, УМВС, УМВСЗТ) оперативної інформації про резонансні злочини та інші надзвичайні події, що стались на території країни [1]. Головними цілями функціонування даної системи оперативного інформування (СОІ) є своєчасне інформування керівництва міністерства, зацікавлених інстанцій, держави про реальний стан й динаміку злочинності в цілому у державі та окремих її регіонах для прийняття впливових управлінських рішень на її покращання, а також забезпечення постійного стеження за своєчасністю вирішення й розкриттям резонансних злочинів, ліквідацією наслідків інших надзвичайних подій.

СОІ МВС України функціонує в корпоративній мережі ОВС України, а завдання щодо забезпечення її функціонування покладені на чергові частини ОВС України. Тому питання забезпечення захисту СОІ МВС України безпосередньо пов'язані з розв'язанням проблем захисту функціонування корпоративної мережі та програмно-технічного комплексу чергових частин ОВС України, що знайшло відображення в низці наукових робіт. Так, зокрема, питанням аналізу загальної структури корпоративної мережі ОВС України, а також моделей об'єкта захисту інформації і можливого порушника безпеки мережі, присвячена стаття [2]. У роботі [3] розглянуто проблеми створення комплексної системи захисту корпоративної мережі ОВС України. Методичний підхід до формалізації задачі оцінювання ефективності системи захисту інформаційної системи ОВС України, а також аналіз множини векторів-показників прояву погроз об'єктам захисту цієї інформаційної системи, наведений у статті [4]. В роботі [5] здійснена оцінка коефіцієнта оперативної готовності програмно-апаратних засобів захищеної СОІ МВС України щодо обробки інформації, а в роботі [6] наведена організація їх комплексного захисту від несанкціонованих дій. Подальше удосконалення побудови ефективної комплексної системи захисту інформації та об'єктів з її обробки СОІ МВС України тісно пов'язане з проблемою побудови загальної математичної моделі об'єктів її захисту, що і є ціллю даної статті.

Основна частина

Для побудови загальної математичної моделі інформаційно-телекомунікаційної системи (ІТС) оперативного інформування МВС України, що потребує захисту оперативної інформації та об'єктів з її обробки, скористаємось теоретичними положеннями загальної математичної моделі ІТС, що потребує захисту інформації, яка була розглянута у роботі [2].

ІТС оперативного інформування МВС України представляє собою потужну інформаційно-аналітичну систему, яка поєднує принципи територіально-розподіленої і централізованої топології та побудована у вигляді трирівневої ієрархічної моделі [7]. На кожному її рівні в чергових частинах будуються локальні обчислювальні мережі, що об'єднують автоматизовані робочі місця працівників чергових частин та файл-сервер з інформаційними обліками.

Відомо, що серед інформаційних систем виділяють три ієрархічні класи, вимоги до функціонального складу комплексу засобів захисту яких істотно відрізняються [8]. На кожному структурному рівні СОІ МВС України функціонують інформаційні системи класу «2» (наявність користувачів з різними повноваженнями по доступу і/або технічних засобів, які можуть одночасно здійснювати обробку інформації різних категорій конфіденційності), а

сама СОІ МВС України представляє собою в цілому інформаційну систему класу «3» (істотна відміна від класу «2» – необхідність передачі інформації через незахищене середовище або, в загальному випадку, наявність вузлів, що реалізують різну політику безпеки). З урахуванням вимог до забезпечення певних властивостей оперативної інформації в кожному класі інформаційної системи виділяємо підкласи, в яких підвищені вимоги до забезпечення цілісності, доступності і конфіденційності оброблюваної інформації (підкласи «х.ЦДК»).

На рис. наведена схема передачі інформації про резонансний злочин та іншу надзвичайну подію в ІТС оперативного інформування МВС України. Аналіз даної схеми дозволяє виділити найбільш вірогідні об'єкти обробки інформації з порушенням її цілісності, доступності та конфіденційності, а саме:

1) інформаційні системи чергових частин міськрайлінорганів (МРЛО), ГУМВС, УМВС, УМВСЗТ, МВС України;

2) обчислювальна та оргтехніка, носії інформації структурних підрозділів МРЛО, ГУМВС, УМВС, УМВСЗТ;

3) працівники чергових частин МРЛО, ГУМВС, УМВС, УМВСЗТ, МВС України;

4) працівники структурних підрозділів МРЛО, ГУМВС, УМВС, УМВСЗТ;

5) системи електроживлення, зв'язку, теле- та радіомовлення МРЛО, ГУМВС, УМВС, УМВСЗТ, МВС України;

6) передача інформації по локальній мережі МРЛО, ГУМВС, УМВС, УМВСЗТ;

7) передача спецповідомлень по каналам електронної пошти та мережею телеграфного зв'язку між рівнями МРЛО – ГУМВС, УМВС, УМВСЗТ;

8) передача спецповідомлень по каналам електронної пошти та мережею телеграфного зв'язку між рівнями ГУМВС, УМВС, УМВСЗТ – МВС України.

У роботі [9] авторами наведений перелік найбільш поширених носіїв інформації ("інформація не існує сама по собі, вона зберігається на різноманітних носіях" [10]), а саме: 1) папір; 2) пристрої зберігання даних на магнітних носіях (магнітна плівка для запису аудіо- і відеоінформації; гнучкі магнітні диски (дискети); накопичувачі на жорстких магнітних дисках (вінчестери); магнітні стрічкові накопичувачі резервного зберігання даних); 3) пристрої оптичного зберігання даних (CD-ROM, CD-R, CD-RW; DVD, DVD-R, DVD-RW); 4) флеш-пам'ять (зберігання даних в мікросхемі пам'яті); 5) акустичне поле; 6) електричний струм; 7) електричне поле; 8) магнітне поле; 9) електромагнітні хвилі; 10) людина. В деяких роботах всі носії зберігання інформації поділені на три групи: паперові, електронні та людську пам'ять. Зазначені переліки носіїв інформації необхідно також враховувати при деталізації найбільш вірогідних об'єктів обробки оперативної інформації ІТС оперативного інформування МВС України з порушенням її цілісності, доступності та конфіденційності.

Таким чином, ми сформували склад об'єктів захисту $O=\{o(t)\}$ загальної математичної моделі СОІ МВС України, що потребує захисту оперативної інформації. Для повного опису об'єктів захисту необхідно ще сформувати:

1. Набори характеристик об'єктів, що захищаються ($H(o)$).
2. Набори $C=\{c(i,j)\}$, які описують різноманітні зв'язки (взаємодії) між елементами об'єктів ($c(i,j)=1$ для існуючого зв'язку між елементами $o(i)$ і $o(j)$, $c(i,j)=0$ – у протилежному випадку) та їх характеристики ($H(c)$).
3. Перелік зовнішніх об'єктів EO, які взаємодіють із об'єктами, що захищаються, та їх характеристики ($H(EO)$).
4. Перелік зовнішніх зв'язків об'єктів EC та їх характеристики ($H(EC)$).

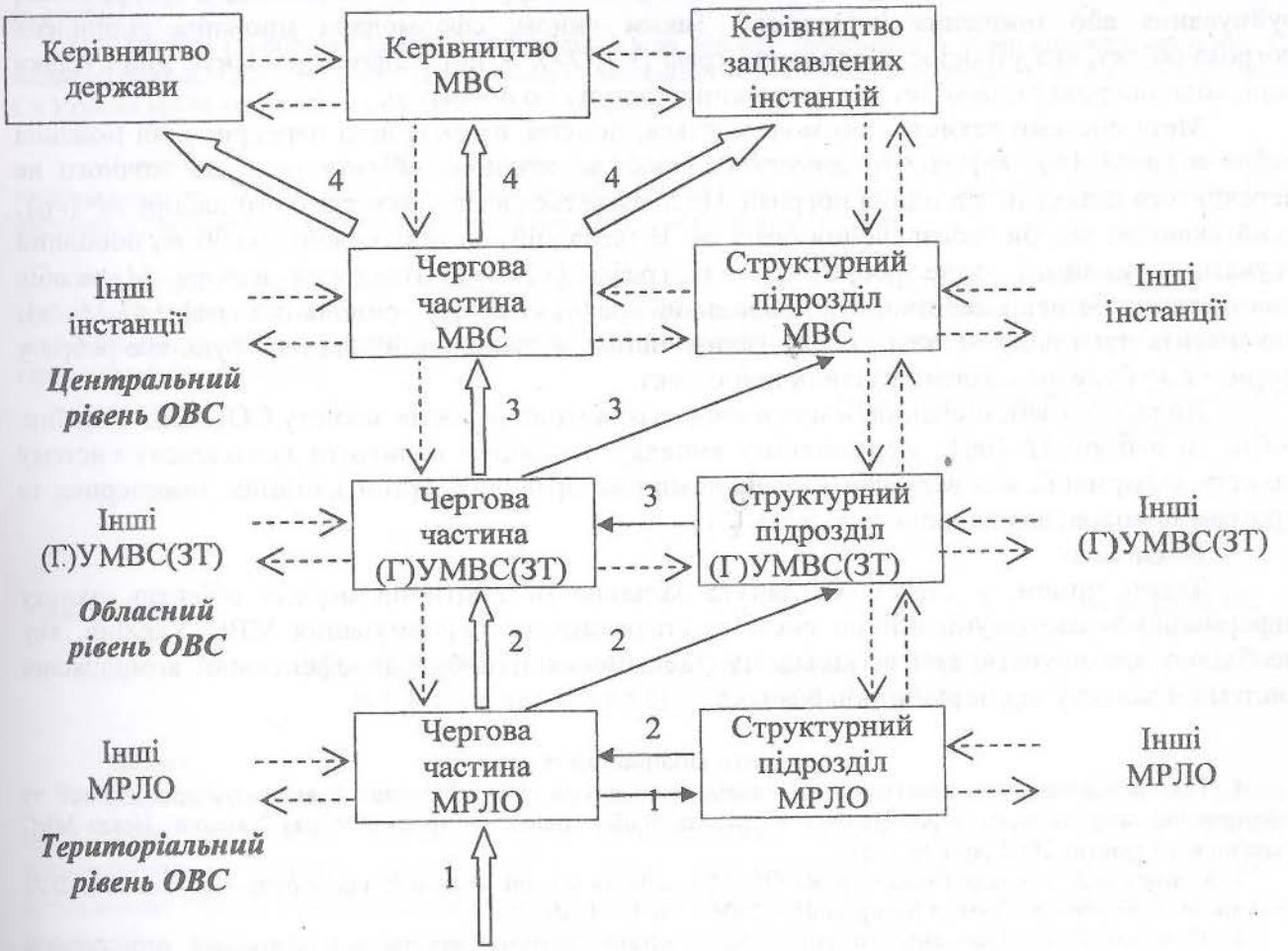

Рис. Схема передачі оперативної інформації в інформаційно-телекомунікаційній СОІ МВС України

Примітки:

а) цифрами позначені спецповідомлення: 1 – первинне; 2 – МРЛО; 3 – ГУМВС, УМВС, УМВСЗТ; 4 – МВС України;

б) (Г)УМВС(ЗТ) – це скорочено ГУМВС, УМВС, УМВСЗТ;

в) безперервними стрілками між різними рівнями ОВС України позначено обмін інформацією з використанням телефонних та телеграфних каналів зв'язку;

г) пунктирними стрілками позначений можливий обмін інформацією.

Тобто, повний опис всіх вище зазначених об'єктів захисту представляє собою складну багатопараметричну задачу. У найпростішому випадку порушника цілісності (доступності чи конфіденційності) оперативної інформації під час її обробки на об'єктах захисту СОІ МВС України, можна описати за допомогою множини зовнішніх впливів (погроз) $T=\{t_i\}$ з відповідними характеристиками $H(T)=\{h(t)\}$. Для цих об'єктів будуть виконуватись базові вектори показників оцінювання загроз U_{IC}, U_{KM}, $U_{от}$, $U_{сп}$, $U_{еж}$, $U_{вкз}$, $U_{зкз}$, які були розглянуті у роботі [4]. Природно, що в кожному конкретному випадку базова система показників може доповнюватися або скорочуватися експертами, що залучаються для оцінювання рівня загрози СОІ МВС України.

У загальному випадку необхідно розглядати різноманітні типи зовнішніх впливів T_1, T_2,..., T_N, які відповідають різноманітним цілям порушника, наприклад, перекручення, руйнування або знищення інформації. Таким чином, сформована множина відношень погроза-об'єкт, яка утворює дводольний граф $\{<T,O>\}$. У ній ребро $<t,o>$ існує тоді і тільки тоді, коли погроза t є засобом для одержання доступу до об'єкту o.

Мета системи захисту, що моделюється, полягає в тому, щоб перекрити всі можливі ребра в графі $\{<T,O>\}$, тобто домогтися, щоб до жодного об'єкту не було жодного не перекритого шляху ні від однієї погрози. Це досягається введенням третього набору $M=\{m_k\}$, який включає засоби забезпечення безпеки. В ідеальній системі кожний засіб m_k повинний усувати, принаймні, одне ребро $<t,o>$ із графа $\{<T,O>\}$. Введення набору M засобів забезпечення безпеки перетворить дводольний граф $\{<T,O>\}$ у тридольний граф $\{<T,M,O>\}$, що містить дуги виду $<t,m>$ і $<m,o>$. Таким чином, у "захищеній" системі будь-яке ребро у формі $<t,o>$ буде визначати незахищений об'єкт.

До засобів забезпечення безпеки вище зазначених об'єктів захисту СОІ МВС України, тобто до набору $M=\{m_k\}$, у загальному випадку необхідно включити комплексну систему захисту інформації, яка включає до себе комплекс правових, організаційних, інженерних та програмно-апаратних заходів та засобів [11].

Висновки

Таким чином, у статті розглянута загальна математична модель об'єктів захисту інформаційно-телекомунікаційної системи оперативного інформування МВС України, яку необхідно враховувати при подальшому удосконаленні побудови ефективної комплексної системи її захисту від порушників безпеки.

Список використаних джерел

1. Про вдосконалення реагування на повідомлення про злочини, інші правопорушення і події та забезпечення оперативного інформування в органах і підрозділах внутрішніх справ України: Наказ МВС України від 4 жовтня 2003 року № 1155.

2. Кудінов В.А. Корпоративна мережа ОВС України та моделі її захисту від порушників безпеки / В.А. Кудінов, В.О. Хорошко // Захист інформації. – 2004. – № 1. – С. 26-35.

3. Кудинов В.А. Проблемы создания комплексной системы защиты корпоративной сети органов внутренних дел Украины / В.А. Кудинов, В.А. Хорошко // Тр. XIII Межд. научной конф. "Информатизация и информационная безопасность правоохранительных органов" (25-26 мая 2004 г.). – М.: Академия управления МВД России, 2001. – С. 137-140.

4. Кудінов В.А. Методичний підхід до формалізації задачі оцінювання ефективності системи захисту інформаційної системи ОВС України / В.А. Кудінов, В.О. Хорошко // Захист інформації. – 2004. – № 4. – С. 11-18.

5. Кудінов В.А. Оцінка коефіцієнта оперативної готовності програмно-апаратних засобів захищеної автоматизованої системи оперативного інформування МВС України щодо своєчасної та якісної обробки відкритої інформації / В.А. Кудінов, В.О. Хорошко // Вісник Східноукраїнського нац. ун-ту ім. В. Даля. – 2009. – № 6, Ч. 1. – С. 82-85.

6. Кудінов В.А. Організація комплексного захисту програмно-апаратних засобів інформаційної системи "Зведення" МВС України від несанкціонованих дій / В.А. Кудінов, О.А. Лупало // Спеціальна техніка у правоохоронній діяльності: IV міжнар. наук.-практ. конф., Київ, 26-27 лист. 2009 р.: тези доп. – К.: Київський нац. ун-т внутр. справ, 2009. – С. 175-176.

7. Кудінов В.А. Функціонування системи оперативного інформування МВС України / В.А. Кудінов, П.П. Артеменко, О.В. Золотар та ін.; за ред. В.А. Кудінова // Спеціальна техніка. Загальна частина: посібник. – К.: Київський нац. ун-т внутр. справ, 2007. – С. 156-172.

8. НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу: Наказ Департаменту спеціальних телекомунікаційних систем та захисту інформації СБ України від 28 квітня 1999 року № 22.

9. Носов В.В. Некоторые аспекты организации технической защиты информации в подразделениях правоохранительных органов / В.В. Носов, И.А. Громыко // Спеціальна техніка у правоохоронній діяльності: I міжнар. наук.-практ. конф., Київ, 20-21 квіт. 2004 р.: тези доп. – К.: Нац. акад. внутр. справ України, 2005. – ч. 1. – С. 138–145.

10. До проблеми організації захисту інформації на підприємствах / Г.Б. Жиров, В.Б. Бахвалов, Н.М. Берназ, Є.С. Лєнков // Інформаційна безпека: наук.-практ. конф., Київ, 26-27 бер. 2009 р.: тези доп. – К.: ДУІКТ, 2009. – С. 67–71.

11. НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу: Наказ Департаменту спеціальних телекомунікаційних систем та захисту інформації СБ України від 28 квітня 1999 року № 22.

У статті розглянута загальна математична модель об'єктів захисту інформаційно-телекомунікаційної системи оперативного інформування МВС України, яку необхідно враховувати при подальшому удосконаленні побудови ефективної комплексної системи її захисту від порушників безпеки.

В статье рассмотрена общая математическая модель объектов защиты информационно-телекоммуникационной системы оперативного информирования МВД Украины, которую необходимо учитывать при дальнейшем усовершенствовании построения эффективной комплексной системы ее защиты от нарушителей безопасности.

Рецензент:д.т.н., проф.Хорошко В.О.
Надійшла 12.10.2010

УДК 004.621 **Берназ Н.М.**

МОДЕЛЮВАННЯ ПРОТОКОЛІВ ВЗАЄМОДІЇ В СИСТЕМАХ ЗАХИСТУ ІНФОРМАЦІЇ

Вступ

Системи захисту інформації, що орієнтовані на масове використання у різних прикладних системах, повинні бути мобільними, тобто достатньо легко повинні переноситися з одного середовища на інше, яке підлягає захисту. У зв'язку з цим, є актуальною задача проникнення (занурення) системи захисту в захищуване середовище. Для розв'язання цієї задачі необхідно дослідити інтерфейси взаємодії мобільної системи з користувачем та системою, що підлягає захисту, а також процедури адаптації системи захисту до захищуваного середовища. Крім цього, важливим є визначення параметрів адаптації, основними серед яких можна назвати характеристики і критерії, що задають рівень безпеки об'єкта захисту.

Мобільні системи захисту, на відміну від мобільних операційних систем, повинні вирішувати цілий ряд специфічних задач на етапі їх встановлення в захищувану систему. До таких задач слід віднести наступні задачі:

- визначення інформаційно небезпечних компонент в захищуваній системі;
- визначення необхідного рівня захисту для окремих компонент і системи в цілому;
- встановлення програмного взаємозв'язку між системою захисту та захищуваним середовищем;
- адаптацію інтерфейсу користувача захищуваної системи до вимог мобільної системи захисту;
- формування інтерфейсу системи захисту в рамках функціональних задач захищу ваної системи.

Коротко зупинимося на загальному аналізі приведених задач, які необхідно розв'язувати.

Визначення інформаційно небезпечних компонент захищуваної системи є необхідною умовою впровадження і використання систем захисту. Ця задача принципово відрізняється від відомих задач, які розв'язуються в рамках існуючих систем контролю або перевірки систем захисту. В рамках останнього засобу розглядаються наступні ознаки можливих атак: