де L – кількість смуг.

Після підрахунків за формулами (9 – 13) можна привести такі результати:

ВСШ для розбиття на 5 смуг дорівнює $ВСШ_5$ = 3,907 Вт/Гц; на 13 смуг $ВСШ_{13}$ = 1,461 Вт/Гц; на 20 смуг $ВСШ_{20}$ = 0,984 Вт/Гц; на 22 смуги $ВСШ_{22}$ = 0,895 Вт/Гц.

Висновки з даного дослідження.

Для всіх варіантів вихідних даних отримана лише задовільна якість. Це можна пояснити взятим занадто великим рівнем шумів на передавальній стороні (максимальні санітарні норми). Але й у цих випадках рекомендації ITU-T дозволяють здійснювати передачу повідомлень.

Список літератури

1. Горелов Г.В., Ромашкова О.Н., Чан Туань Ань. Качество управления речевым трафиком в телекоммуникационных сетях – М.:Радио и связь, 2001. – 112 с

2. Вінницький В.П. Термінальне устаткування та передавання інформації в телекомунікаційних системах – К.:ІВЦ "Видавництво «Політехніка»", 2004. – 436 с.

3. Конахович. Г.Ф. Защита информации в телекоммуникационных системах. – К.:"МК-Пресс", 2005. – 288 с.

Надійшла 11.04.2008р.

УДК 354.31(477)(004.7+65.012.8)

В.А.Кудінов

АНАЛІЗ ПРОБЛЕМИ ЗАХИСТУ ВІДКРИТОЇ ОПЕРАТИВНОЇ ІНФОРМАЦІЇ ПРО РЕЗОНАНСНІ ЗЛОЧИНИ ТА ІНШІ НАДЗВИЧАЙНІ ПОДІЇ, ЩО ОБРОБЛЯЄТЬСЯ В СИСТЕМІ ОПЕРАТИВНОГО ІНФОРМУВАННЯ МВС УКРАЇНИ

Вступ

В органах і підрозділах внутрішніх справ, внутрішніх військах та навчальних закладах МВС України функціонує єдина система збирання, опрацювання та подання до Міністерства внутрішніх справ України, головних управлінь (управлінь) МВС України в областях та на транспорті оперативної інформації про резонансні злочини та інші надзвичайні події, що стались на території країни [1, 2]. Ця система оперативного інформування (СОІ) МВС України є невід'ємною частиною завдань, що стоять перед органами і підрозділами внутрішніх справ, внутрішніми військами, навчальними закладами МВС України і спрямовані на підтримання громадського порядку й безпеки громадян на всій території України.

Головними цілями функціонування СОІ МВС України є: 1) 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; 2) 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 (ЧЧ) ОВС України. Тому питання забезпечення захисту СОІ МВС України безпосередньо пов'язані з розв'язанням проблем захисту функціонування корпоративної мережі та програмно-технічного комплексу ЧЧ ОВС України, що знайшло відображення в деяких наукових

роботах. Так, зокрема, питанням аналізу загальної структури корпоративної мережі ОВС України, а також моделей об'єкта захисту інформації і можливого порушника безпеки мережі, присвячена стаття [3]. У роботі [4] 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 [5]. Комплексному дослідженню функціонування системи оперативного інформування МВС України та шляхів її розвитку присвячені статті [6, 7]. У роботі [8] наведений аналіз проблем попередження комп'ютерних злочинів при передачі інформації в корпоративній мережі ОВС України, а в роботі [9] досліджена проблема захисту комп'ютерної інформації у процесі взаємодії ЧЧ ОВС України.

Але при цьому ще залишилась не вирішеною проблема щодо необхідності захисту відкритої оперативної інформації про резонансні злочини та інші надзвичайні події, яка обробляється в системі оперативного інформування МВС України, що і є ціллю статті.

Актуальність даного дослідження пов'язана з суттєвою ознакою СОІ МВС України – можливістю доступу до її оперативної інформації всіх зацікавлених оперативних служб вже з моменту прийняття повідомлення (заяви) про злочин. Це дозволяє проводити їм відповідні заходи щодо розкриття злочинів по "гарячих слідах", негайно реагувати на негативний розвиток подій, залучати можливості інших органів і підрозділів внутрішніх справ, задіяти з цією метою військові формування та спеціальні служби. У більшість інших оперативних баз даних ОВС України надходить інформація тільки з моменту порушення кримінальної справи, надходження офіційних карток тощо, тобто оперативні служби отримують необхідну інформацію із запізненням у 10-30 діб. Тому актуальним є проведення заходів із захисту відкритої оперативної інформації, які повинні забезпечити своєчасність проходження оперативної інформації в СОІ МВС України, її цілісність та доступність.

Структура системи оперативного інформування МВС України

Структурна побудова СОІ МВС України поєднує принципи територіально-розподіленої та централізованої топології і організована у вигляді трьохрівневої ієрархічної моделі:

1. *Центральний рівень* – охоплює інформаційні обліки та автоматизовані робочі місця (АРМ) працівників чергової частини Міністерства внутрішніх справ України.
2. *Обласний (регіональний) рівень* – охоплює інформаційні обліки та АРМ працівників ЧЧ головних управлінь (управлінь) МВС України в областях та на транспорті.
3. *Територіальний рівень* – охоплює інформаційні обліки та АРМ працівників ЧЧ міських, районних та лінійних ОВС. Цей рівень складає основу системи оперативного інформування МВС України.

Таким чином, СОІ МВС України на кожному рівні будується на базі локальних обчислювальних мереж, які об'єднують АРМ працівників чергових частин з серверами, на яких розміщені інформаційні обліки. На сьогодні існує типове АРМ працівників ЧЧ на центральному та обласному рівнях ОВС України [10, 11]. Для територіального рівня типове АРМ чергового ЧЧ в межах України ще не створено, але, якщо розглянути АРМ працівників ЧЧ міськрайлінорганів в межах деяких областей чи міст України, то можна вважати, що типове АРМ чергового існує і на територіальному рівні.

Розглянемо АРМ працівників ЧЧ центрального рівня МВС України. Воно включає в себе автоматизовану інформаційну систему "Зведення-МВС" (комплекс засобів обчислювальної техніки і спеціального програмного забезпечення, що дозволяє обробляти

документи анкетного виду з формуванням баз даних реляційного типу), а також системи зв'язку по телеграфним ("Телгком") і телефонним ("Електронна пошта") каналам [10].

Таким чином, сучасні інформаційні технології набули широкого застосування в практичній діяльності підрозділів ЧЧ ОВС та забезпечують ефективне функціонування системи оперативного інформування МВС України.

Організація обробки оперативної інформації в СОІ МВС України

Наказом МВС України [12] для органів і підрозділів внутрішніх справ України встановлений єдиний порядок приймання, реєстрації та розгляду заяв і повідомлень про злочини, що вчинені або готуються.

Приймання заяв і повідомлень про злочини, що вчинені або готуються, здійснюється цілодобово оперативним черговим того органу внутрішніх справ, до якого надійшло звернення чи повідомлення. Черговий, прийнявши заяву чи повідомлення про злочин, зобов'язаний діяти згідно з Інструкцією з організації реагування ОВС на повідомлення про злочини [1, 2]. Він з'ясовує характер і обставини того, що сталося. Заяви і повідомлення про злочини реєструються оперативним черговим відразу після їх надходження на персональній електронно-обчислювальній машині шляхом введення до автоматизованої інформаційно-пошукової системи "ФАКТ".

Якщо отримана інформація про злочин (подію) підпадає під Перелік резонансних злочинів та інших надзвичайних подій [1], то начальник структурного підрозділу, на який покладено контроль з розгляду конкретної заяви (повідомлення), вивчає зібрані матеріали, готує проект спецповідомлення та подає його до чергової частини. Після підпису начальником міськрайлінорган, черговий реєструє спецповідомлення в книзі обліку вихідних телеграм і каналами електронної пошти з обов'язковим дублюванням повідомлень мережею телеграфного зв'язку [10] надсилає до чергової частини обласного рівня. Потім аналогічна процедура обробки та направлення спецповідомлення відбувається і на обласному рівні.

Таким чином, оперативна інформація про резонансні злочини та інші надзвичайні події після її обробки на територіальному та обласному рівнях СОІ МВС України повинна надходити у визначений Переліком резонансних злочинів та інших надзвичайних подій термін [1] до автоматизованої інформаційної системи "Зведення-МВС" [13] чергової частини МВС України каналами електронної пошти з обов'язковим його дублюванням мережею телеграфного зв'язку.

Склад оперативної інформації, що обробляється в СОІ МВС України

Оперативна інформація відповідно до Переліку резонансних злочинів та інших надзвичайних подій [1] у вигляді спецповідомлень надсилається до ЧЧ МВС України відкритими або закритими каналами зв'язку.

Як відомо, передача відомчою електронною поштою та мережею телеграфного зв'язку оперативної інформації, що становить державну таємницю, та несекретної інформації обмеженого розповсюдження, заборонена. Відповідальність за зміст телеграми несе виконавець.

В статті ми розглядаємо обробку відкритої оперативної інформації щодо резонансних злочинів та інших надзвичайних подій.

З точки зору безпеки інформація характеризується трьома властивостями [14, 15]: 1) конфіденційність, якщо дотримуються встановлені правила ознайомлення з нею; 2) цілісність, якщо дотримуються встановлені правила її модифікації (видалення); 3) доступність, якщо зберігається можливість ознайомлення з нею або її модифікації відповідно до встановлених правил упродовж будь-якого певного (малого) проміжку часу. А види загроз розрізняють за результатами їх впливу на ці властивості інформації, тобто є загрози конфіденційності, цілісності, доступності інформації.

У головному штабі МВС України розроблений склад типової форми спецповідомлення при поданні відкритої оперативної інформації [1, 9], а саме:

1. Дата й час надходження заяви (повідомлення).
2. Орган внутрішніх справ, до якого надійшла заява.
3. Дані на особу (заявника, підозрюваного тощо).
4. Зміст заяви (обставини події): дата і час скоєння; місце скоєння; що вчинено (скоїлося); що викрадено, наслідки події, спричинені збитки.
5. Заходи, що вжиті ОВС для розшуку й затримання підозрюваних осіб (ліквідації наслідків надзвичайної події).
6. Про розкриті злочини – дані на затриманих чи осіб, які розшукуються за підозрою у вчиненні злочину.
7. Дані про вилучені речі, знаряддя злочину, речові докази.
8. Початкові слідчі дії, організаційні заходи щодо ліквідації наслідків події.

Якщо врахувати склад типової форми спецповідомлення та важливість її оперативної інформації для ефективної діяльності оперативних служб ОВС України, то виникає питання щодо необхідності здійснення заходів із захисту відкритої оперативної інформації СОІ МВС України від загроз порушення її цілісності та доступності.

Цей висновок також підтверджує такий принцип формування і проведення державної політики у сфері технічного захисту інформації, як: "обов'язковість захисту інженерно-технічними заходами інформації, яка становить державну та іншу передбачену законом таємницю, конфіденційної інформації, що є власністю держави, відкритої інформації, важливої для держави, незалежно від того, де зазначена інформація циркулює, а також відкритої інформації, важливої для особи та суспільства, якщо ця інформація циркулює в державних органах, підприємствах, установах і організаціях" [16].

Висновки

Таким чином, враховуючи важливість оперативної інформації в СОІ МВС України для ефективної діяльності оперативних служб ОВС України, особливості її обробки, склад типової форми спецповідомлення, вимоги нормативно-правових документів з питань технічного захисту інформації, можна зробити висновок щодо необхідності здійснення заходів із захисту відкритої оперативної інформації системи оперативного інформування МВС України від загроз порушення її цілісності, доступності на кожному з трьох рівнів СОІ МВС України та під час її передачі каналами зв'язку.

Список літератури

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. *Про внесення* змін та доповнень до наказу МВС України від 4 жовтня 2003 року № 1155: Наказ МВС України від 10 жовтня 2005 року № 860.

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

4. *Хорошко В.А., Кудинов В.А.* Проблемы создания комплексной системы защиты корпоративной сети органов внутренних дел Украины // 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.

5. *Хорошко В.О., Кудінов В.А.* Методичний підхід до формалізації задачі оцінювання ефективності системи захисту інформаційної системи ОВС України //

Науково-технічний журнал "Захист інформації". – 2004. – № 4. – С. 11-18.

6. *Кудінов В.А.* Функціонування системи оперативного інформування МВС України // Спеціальна техніка. Загальна частина. – К.: Київський нац. ун-т внутр. справ, 2007. – С. 156-172.

7. *Кудінов В.А.* Шляхи удосконалення системи оперативного інформування МВС України // Науково-технічний вісник "Безпека дорожнього руху України". – 2003. – № 3-4(16). – С. 27-36.

8. *Кудінов В.А.* Проблема попередження комп'ютерних злочинів при передачі інформації в корпоративній мережі ОВС України // Злочини у сфері використання комп'ютерної техніки: проблеми кваліфікації, розслідування і попередження: Вісник ЛАВС МВС імені 10-річчя незалежності України. Спеціальний випуск. – Луганськ: РВВ ЛАВС, 2005. – С. 48-51.

9. *Кудінов В.А.* Проблеми захисту комп'ютерної інформації у процесі взаємодії чергових частин МВС-УМВС(УМВСТ) // Тр. Міжвуз. наук.-практ. конф. "Правові основи захисту комп'ютерної інформації від протиправних посягань" (22 грудня 2000 р.). – Донецьк: Донецький інститут внутрішніх справ, 2001. – С. 187-190.

10. *Кудинов В.А., Рыбалко Т.В.* Автоматизированное рабочее место дежурного дежурной части МВД-УМВД(УМВДТ): Метод. рекомендации. – К.: РИО МВД Украины, 1996. – 100 с.

11. *Кудінов В.А.* Проблеми функціонування автоматизованого робочого місця чергового чергової частини в ОВС України // Матер. Міжв. наук.-практ. конф. "Сучасні проблеми інформатизації органів внутрішніх справ України" (15 березня 2001 р.). – К.: НАВСУ. – 2002. – С. 47-51.

12. *Про порядок* приймання, реєстрації та розгляду в органах і підрозділах внутрішніх справ України заяв і повідомлень про злочини, що вчинені або готуються: Наказ МВС України від 14 квітня 2004 року № 400.

13. *Кудінов В.А.* Структура бази даних автоматизованої інформаційної системи "Зведення" з обліку злочинів та надзвичайних подій, які взяті на контроль МВС України // Науково-технічний вісник "Безпека дорожнього руху України". – 2003. – № 1-2(15). – С. 57-62.

14. *Загальні* положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу (НД ТЗІ-1.1-002-99). – К.: ДСТСЗІ СБ України, 1999. – 31 с.

15. *Класифікація* автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу (НД ТЗІ-2.5-005-99). – К.: ДСТСЗІ СБ України, 1999. – 23 с.

16. Концепція технічного захисту інформації в Україні: Постанова КМУ від 08.10.1997 № 1126.

Надійшла 19.03.2008р.