УДК 519.7

Рудий Т.В., к.т.н., доцент[1©], **Ганич І.М.,** ст. викладач[1],
Нечепуренко А.В., магістрант[2]
[1]*Львівський державний університет внутрішніх справ*
[2]*Національний лісотехнічний університет України,м. Львів*

ОРГАНІЗАЦІЯ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЙНИХ СИСТЕМ ПІДРОЗДІЛІВ МВС

Розглядаються загальні принципи організації системи захисту інформації в інформаційних системах підрозділів МВС. Обґрунтовано запровадження принципу поетапного здійснення технічного захисту інформації з урахуванням динаміки зміни загроз.

Ключові слова: *інформаційні технології, інформаційна система, захист інформації, інформаційні загрози, технічні заходи.*

Постановка проблеми. Широке впровадження у діяльність підрозділів МВС інформаційних систем (ІС) вимагає забезпечення доступності, цілісності, а також конфіденційності оброблюваної у ІС інформації. Порушення безпеки ІС може істотно ускладнити виконання завдань підрозділами МВС, тому проблема створення ефективної системи захисту інформації (ЗІ) набуває дуже важливого значення. Це пояснюється тим, що при розробленні та удосконаленні таких систем ЗІ є багато недостатньо досліджених аспектів, які можуть негативно вплинути на ефективність і надійність функціонування всієї системи безпеки. Автори вважають, що така система ЗІ повинна бути, у першу чергу, комплексною і адаптивною.

Аналіз останніх досліджень. Проблемам створення і функціонування систем технічного ЗІ присвячено достатньо публікацій як у відкритих, так і закритих літературних джерелах. З доступних для пересічного користувача джерел хочемо відзначити праці таких вчених, як: М.П. Карпінський, А.О. Ботюк, С.Г. Бабичев, В.П. Горбулін, В.В. Домарьов, В.Ю. Захарченко, В.І. Лазуренко, С.А. Петренко, А.В. Бєляєв та ін. Важливість наукового здобутку та внеску у теорію і практику інформаційної безпеки згаданих вчених важко переоцінити.

Аналіз літературних джерел дає підстави стверджувати, що у процесі проектування, створення і експлуатування систем технічного ЗІ є певні недоліки, які знижують ефективність їх функціонування. Як правило, керівники підрозділів МВС розглядають проблему ЗІ в ІС переважно з технічної точки зору. Розв'язання проблеми пов'язують з придбанням та інсталяцією програмно-апаратних засобів ЗІ. Однак, для організації ефективного режиму інформаційної безпеки цього недостатньо. Необхідно, також, обґрунтувати розроблення політики інформаційної безпеки, яка визначає стратегію, тактику системи ЗІ і враховує динаміку зміни загроз інформації.

Вважаємо недоцільним вводити у предметну область даної публікації методи ЗІ які ґрунтуються на системному адмініструванні та математичних методах. Обмежимося розробленням і аналізом організаційно-технічних засобів, які будуть зрозумілими для практичних працівників ОВС.

Мета даної публікації полягає в тому, щоб визначити методи і засоби ЗІ у ІС підрозділів МВС. У результаті нами пропонується набір організаційно-технічних принципів і засобів, які дозволяють створити ефективну систему ЗІ. Разом з тим, варто відзначити, що ці принципи є всього лише одним з аспектів стратегії управління інформаційними технологіями (ІТ) у підрозділах МВС. Неможливо успішно забезпечувати ЗІ в підрозділах МВС при незадовільному управлінні ІТ.

Виклад основного матеріалу. З метою протидії злочинам у сфері ІТ або зменшення збитків від них потрібно фахово вибирати заходи і засоби забезпечення ЗІ від витоку та несанкціонованого доступу (НСД) до неї. Необхідно знати також основні правові положення в цій галузі, організаційні, програмно-технічні та інші заходи забезпечення безпеки інформації [1, 2, 3].

Актуальність даної проблеми пов'язана із зростанням можливостей сучасних ІТ. Розвиток засобів, методів і форм оброблення інформації і масове застосування ІТ роблять інформацію більш уразливою. Основними чинниками, які сприяють підвищенню її уразливості, є:

- лавиноподібне збільшення обсягів інформації, яка накопичується, зберігається та обробляється в ІС;
- зосередження в базах даних інформації різного призначення і різної відомчої приналежності;
- розширення кола користувачів, які мають безпосередній доступ до інформаційних активів ІС та масивів даних;
- ускладнення режимів роботи технічних засобів ІС;
- обмін інформацією в локальних та глобальних комп’ютерних мережах (КМ), у тому числі і віддалений доступ.

У всіх аспектах забезпечення ЗІ основним елементом є аналіз можливих загроз щодо порушення роботи ІС, тобто загроз, що підвищують уразливість інформації, яка обробляється в ІС, призводять до її витоку, випадкового або навмисного модифікування, знищення.

Вибір засобів ЗІ в ІС – складна задача, при розв'язанні якої потрібно враховувати різні імовірні загрози щодо порушення роботи такої системи, вартість реалізування різних засобів ЗІ і наявність численних зацікавлених сторін. При виборі таких засобів важливо знати, що сучасна комп’ютерна наука має в своєму розпорядженні методи, що дозволяють вибрати таку сукупність засобів ЗІ, яка забезпечить максимізування ефекту від впровадження засобів ЗІ за передбачених витратах або мінімізування витрат від впровадження засобів ЗІ при заданому рівні захищеності ІС.

Розглядаючи загальні принципи ЗІ в ІС, доцільно відзначити, що комплексний ЗІ в ІС має в своїй основі використання правових, фізичних, організаційних та програмно-апаратних засобів захисту. Такі засоби повинні

забезпечувати ідентифікування та аутентифікування користувачів, розподіл повноважень доступу до ІС, реєстрацію та облік спроб НСД. Організаційні заходи ЗІ в ІС, як правило, спрямовані на чіткий розподіл відповідальності під час роботи персоналу з інформацією, створення декількох рубежів контролю, запобігання навмисному або випадковому знищенню та модифікуванню інформації.

Об'єктом технічного захисту є інформація, яка становить державну або іншу, передбачену чинним законодавством України таємницю, конфіденційна інформація, яка є державною власністю або передана державі у володіння, користування, розпорядження.

Технічний захист інформації (ТЗІ) здійснюється у кілька етапів: перший етап – визначення і аналіз загроз; другий етап – розроблення системи ЗІ; третій етап – реалізування плану ЗІ; четвертий етап – контроль за функціонуванням та керуванням системою ЗІ.

На першому етапі здійснюється ґрунтовний аналіз об'єктів ТЗІ, ситуаційного плану, умов функціонування ІС, оцінювання ймовірності прояву загроз та очікувані збитки від їх реалізування, підготування даних для побудови виокремленої моделі загроз.

Джерелами загроз може бути діяльність організованих кримінальних структур, а також навмисні або ненавмисні дії юридичних і фізичних осіб. Опис загроз і схематичне подання шляхів їх здійснення формують модель загроз. Загрози можуть здійснюватися:

- технічними каналами, які включають канали побічних електромагнітних випромінювань і наведень (ПЕМВН), акустичні, оптичні, радіо-, радіотехнічні, хімічні та інші канали;
- каналами спеціального впливу шляхом формування полів і сигналів з метою руйнування системи ЗІ або порушення цілісності інформації;
- НСД шляхом під'єднання до апаратури та ліній зв'язку, маскуванням під зареєстрованого користувача, подоланням заходів захисту WEB-ресурсів, застосуванням закладних пристроїв, програм та вкоріненням комп'ютерних вірусів.

На другому етапі ТЗІ розробляється план, який містить організаційні, первинні технічні та основні технічні заходи захисту інформації з обмеженим доступом (ІзОД), визначаються зони безпеки інформації.

Організаційні заходи регламентують порядок інформаційної діяльності (ІД) з урахуванням норм і вимог ТЗІ для всіх періодів життєвого циклу ІД.

Первинні технічні заходи передбачають ЗІ блокуванням загроз без використання засобів ТЗІ.

Основні технічні заходи передбачають ЗІ з використанням засобів ТЗІ.

Заходи захисту інформації повинні:

- бути адекватними до загроз;
- бути розробленими з урахуванням можливих збитків від реалізування загроз і вартості захисних заходів та обмежень, які вносяться ними;
- забезпечувати задану ефективність ЗІ на встановленому рівні протягом часу обмеження доступу до неї або можливості здійснення загроз.

Рівень ЗІ означується системою кількісних та якісних показників, які забезпечують вирішення завдання ЗІ на основі норм та вимог ТЗІ.

Мінімально необхідний рівень ЗІ забезпечують обмежувальними і фрагментарними заходами протидії найнебезпечнішій загрозі.

На третьому етапі ТЗІ слід реалізувати організаційні, первинні технічні та основні технічні заходи захисту ІзОД, установити необхідні зони безпеки інформації, провести атестування технічних засобів забезпечення ІД [4], технічних засобів ЗІ, робочих місць (приміщень) на відповідність вимогам безпеки інформації.

ТЗІ передбачає застосування захищених програм і технічних засобів забезпечення ІД, програмних і технічних засобів ЗІ та контролю ефективності захисту, які мають сертифікат відповідності вимогам нормативних документів або дозвіл на їх використання від уповноваженого Кабінетом Міністрів України органу, а також застосуванням спеціальних інженерно-технічних споруд, засобів і систем.

Засоби ТЗІ можуть функціонувати автономно або сумісно з технічними засобами забезпечення ІД у вигляді окремих пристроїв або вмонтованих у них складових елементів. Склад засобів забезпечення ТЗІ, перелік їх постачальників, а також послуг з інсталювання, налаштування та обслуговування визначаються особами, які володіють, користуються і розпоряджаються ІзОД самостійно або за рекомендаціями фахівців з ТЗІ згідно з нормативними документами системи ТЗІ.

На четвертому етапі здійснюється контроль за функціонуванням системи ТЗІ на об’єктах ІД з метою визначення й удосконалення стану ТЗІ в ІС, виявлення та запобігання порушенням системи ЗІ.

Контроль стану ТЗІ в ІС організовується відповідно до планів, затверджених керівниками підрозділів, шляхом проведення перевірок.

Контрольно-інспекційна робота з питань ТЗІ включає планування та проведення перевірок стану ТЗІ в ІС, щодо яких здійснюється ТЗІ, проведення аналізу та надання рекомендацій з вдосконалення заходів з ТЗІ.

Перевірки поділяються на комплексні, цільові (тематичні) та контрольні.

Під час комплексної перевірки вивчається та оцінюється стан ЗІ у ІС, щодо яких здійснюється ТЗІ.

Під час цільової (тематичної) перевірки вивчаються окремі напрямки ТЗІ, перевіряється виконання рішень (розпоряджень, наказів, вказівок) органів державної влади з питань ТЗІ в ІС, щодо яких здійснюється ТЗІ, виконання завдань або провадження діяльності в галузі ТЗІ за відповідними дозволами та ліцензіями суб'єктами системи ТЗІ.

Під час контрольної перевірки перевіряється усунення недоліків, які були виявлені під час проведення попередньої комплексної або цільової перевірки. Зазначені перевірки можуть бути планові та позапланові, з попередженням та раптові.

Позапланова перевірка здійснюється за вказівкою керівництва підрозділу МВС у разі виникнення потреби визначення повноти та достатності заходів з ТЗІ

за наявності відомостей щодо порушень виконання вимог нормативно-правових актів з питань ТЗІ.

Перевірки здійснюються комісіями на які покладено виконання завдань здійснення контролю за функціонуванням системи ТЗІ.

При проведенні перевірки стану ТЗІ контролю підлягають організаційні, організаційно-технічні, технічні заходи з ТЗІ у виділених приміщеннях, ІС і КМ, повнота та достатність робіт з атестування виділених приміщень.

Керування системою ЗІ полягає в адаптуванні заходів ТЗІ до поточного завдання ЗІ. За фактами зміни умов здійснення або виявлення нових загроз заходи ТЗІ реалізовуються у найкоротший термін.

Контроль організаційних заходів з ТЗІ в ІС включає перевірку:

• переліку відомостей, які підлягають ТЗІ;

• окремої моделі загроз для ІС або КМ;

• плану контрольованої зони підрозділу, щодо якого здійснюється ТЗІ;

• переліку виділених приміщень підрозділу, щодо якого здійснюється ТЗІ, ІС та КМ;

• проведення категоріювання виділених приміщень та об'єктів.

Висновки. Контроль за організаційно-технічними заходами з ТЗІ у виділених приміщеннях, ІС та КМ, повнотою та достатністю робіт з атестування виділених приміщень повинен включати перевірку відповідності виконання цих заходів нормативно-правовим актам з питань ТЗІ.

Організаційно-технічні заходи ТЗІ у виділених приміщеннях, ІС та КМ, роботи з атестування виділених приміщень виконуються власними силами або передається на аутсорсинг суб'єктам підприємницької діяльності в галузі ТЗІ, які мають дозвіл і ліцензію від уповноваженого Кабінетом Міністрів України органу.

Керівник підрозділу зобов'язаний ужити невідкладних заходів щодо усунення недоліків і реалізування пропозицій комісії відповідно до вимог нормативно-правових актів з питань ТЗІ.

Література

1. Тихонов В.А., Райх В.В. Информационная безопасность: концептуальные, правовые, организационные и технические аспекты: Учебное пособие. – М. – Гелиос АРВ, 2006. – 528 с.

2. Петренко С.А., Курбатов В.А. Политики информационной безопасности – М.: Компания Ай Ти, 2006. – 400 с.

3. Щеглов А.Ю. Защита компьютерной информации от несанкционированного доступа.– СПб: Наука и Техника, 2004. –384 с.

4. Когут В.В., Рудий Т.В., Кулешник Я.Ф. Порядок атестування систем технічного захисту інформації. Проблеми діяльності кримінальної міліції в умовах розбудови правової держави // Матеріали науково-звітної конференції факультету кримінальної міліції Львівського державного університету внутрішніх справ 12 березня 2010 р. – Львів: ЛьвДУВС. 2010. - С. 90-97.

Summary

Rudij T.V.[1], Ganich I.M.[2], Nechepurenko A.V.[3]
[1]Lviv state university of internal affairs under the Ministry of internal affairs of Ukraine
[2] National Forest-technical University, Lviv

ORGANIZATION THE TECHNICAL PROTECTION OF INFORMATION SYSTEM IN SUBUNIT IN MIA

In the article conducted main principles of organization systems of technical protection of information in informational systems of subunit in Ministry of internal affairs.

Стаття надійшла до редакції 14.04.2011 р.