ПРОЕКТУВАННЯ КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ ЛЬВІВСЬКОЇ ФІЛІЇ ПрАТ «КИЇВСТАР»

Любов Ігнатюк, Орест Полотай

Львівський державний університет безпеки життєдіяльності, Львів, Україна

Розглядається необхідність створення комплексної системи захисту ПрАТ «Київстар». Показано, з яких основних етапів повинен складатись процес проектування комплексної системи захисту інформації. Розглянуто модель загроз та порушників інформації. Наведено основні методи захисту інформації.

Комплексна система захисту інформації (КСЗІ) є сукупністю організаційних та інженерних заходів, програмно-апаратних засобів, які забезпечують захист інформації в автоматизованих системах (АС) [3].

КСЗІ призначена для забезпечення безпеки критичної інформації та інформаційних ресурсів у процесі функціонування АС. Мета функціонування КСЗІ полягає в підтримці необхідного рівня інформаційної безпеки АС відповідно політиці безпеки, яка визначається її власником.

ПрАТ«Київстар» є лідером галузі телекомунікацій та суспільного життя України та виступає провідником найкращих цінностей з обслуговування абонентів та створення найкращих продуктів. Наявність на досліджуваному об’єкті, інформації з обмеженим доступом, зокрема персональних даних абонентів спонукає до проектування КСЗІ [1].

Створення комплексної системи захисту ПрАТ «Київстар» повинно відштовхуватись від багатьох чинників, таких як:

– детального опису території з прилеглими будівлями, де знаходиться досліджуваний об’єкт;
– вивчення партнерів, конкурентів і клієнтів;
– можливі канали витоку важливої інформації;
– дослідження моделей загроз та порушника;
– рішення, щодо методів захисту інформації;
– правові заходи;
– ціновий чинник.

Основними завданнями такої системи повинен бути захист прав та інтересів підприємства і його співробітників; своєчасне виявлення можливих спрямувань до об’єкта захисту і його співробітників; забезпечення збереження матеріальних цінностей і відомостей, що становлять комерційну таємницю підприємства; фізична і технічна охорона будівель, споруд, території і транспортних засобів; контроль за ефективністю функціонування системи безпеки підприємства.

Серед загроз, які необхідно врахувати при створенні КСЗІ, є навмисні загрози техногенного походження дистанційної та контактної дії, зокрема побічні електромагнітні випромінювання та е-наводи. Також варто звернути увагу на випадкові загрози техногенного походження.

Модель порушника повинна відображати його практичні та потенційні можливості, апріорні знання, час та місце дії тощо. Порушники можуть бути внутрішніми (з числа персоналу або користувачів системи) або зовнішніми (сторонніми особами). Серед внутрішніх порушників найбільш небезпечними виступають керівний персонал та системні адміністратори.

Методи захисту інформації повинні включати організаційні та технічні заходи.

Серед організаційних заходів слід виділити обмеження доступу до найважливіших ділянок і приміщень шляхом запровадження перепусток, на яких вказані персональні дані працівника, встановлення контролю за відвідувачами тощо.

Серед технічних заходів захисту інформації ПрАТ «Київстар» можливе встановлення спеціального обладнання, а саме:

– для захисту телефонних ліній – аналізатори телефонних ліній, прилади активного захисту, скремблери, фільтри, універсальні прилади;

– для захисту від радіо закладок – джерела радіошуму;

– для захисту від лазерного перехвату інформації з віконного скла – вібратор скла;

– для захисту від передачі інформації через лінію електромережі – фільтри, джерела шуму з діапазоном частот 50кГц — ЗООкГц.

Для ефективного функціонування КСЗІ потрібно звернути увагу на відеозахист приміщення та території, там де є найбільш можлива поява зловмисників.

Надійність і ефективність функціонування системи оцінюються, виходячи з таких фактів, як відсутність або своєчасне виявлення спроб несанкціонованого проникнення на об’єкт захисту зі злочинною метою; недопущення фактів витоку інформації, розголошування відомостей; втрати важливих документів, виробів; попередження протиправних і негативних проявів з боку персоналу об’єкта.

До правових заходів відносять діючі в державі закони, накази та положення, систему нормативно-розпорядчих документів підприємства, які регламентують правила поводження з інформацією обмеженого поширення та відповідальність за їхні порушення, запобігаючи у такий засіб несанкціонованому використанню інформації[2].

Література

1. Закон України №2657-XII від 2 жовтня 1992 р. // Бюлетень законодавства і юр. практики України. — 1998. №7. — 272 с.
2. Красилівська О.О. Розробка комплексної системи захисту інформації на об’єкті інформаційної діяльності. [Електронний ресурс]. – Режим доступу з http://o53xo.oj2xg3tbovvwcltdn5wq.nblk.ru/3_SND_2010/Informatica/58042.doc.htm
3. Побудова Комплексних Систем Захисту Інформації [Електронний ресурс]. Режим доступу з http://iqusion.com/ua/sistemi-zakhistu-informatsiji