Полотай О.І.
кандидат технічних наук, доцент
Львівський державний університет безпеки життєдіяльності
Рожко Д.К.
курсант
Львівський державний університет безпеки життєдіяльності

ПРИНЦИПИ ТА ПОРЯДОК РОЗРОБЛЕННЯ КОМПЛЕКСНИХ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ

Те, що інформація має цінність, люди усвідомили дуже давно. Її створюють, зберігають, транспортують, продають і купують, а значить - крадуть і підробляють - і, отже, її необхідно захищати. Одним словом, виникнення індустрії обробки інформації призвело до виникнення розробки засобів захисту інформації. Забезпечення безпеки інформації у інформаційно-телекомунікаційних системах здійснюється шляхом створення та впровадження комплексних систем захисту інформації.

Комплексна система захисту інформації – це сукупність організаційних та інженерних заходів, програмно-апаратних засобів, які забезпечують захист інформації від несанкціонованого доступу.

В Законі України «Про захист інформації в інформаційно-телекомунікаційних системах визначено: «Інформація, яка є власністю держави або інформація з обмеженим доступом, вимога щодо якості якої встановлена законом, повинна оброблятися в системі із застосуванням комплексної системи захисту інформації (далі – КСЗІ) з підтвердженою відповідністю».

Роботи зі створення КСЗІ виконуються організацією-власником ІТС. За умови відсутності у неї відповідних ліцензій або дозволу на здійснення окремих видів робіт із захисту інформації до виконання цих робіт залучаються суб’єкти господарювання, які мають такі ліцензії. Дозвіл на проведення робіт з технічного захисту інформації для власних потреб дається Державною службою спеціального зв’язку та захисту інформації.

Процес створення КСЗІ полягає у здійсненні комплексу взаємоузгоджених заходів, спрямованих на розробку і впровадження інформаційної технології, що забезпечує обробку інформації в ІТС згідно з вимогами, встановленими державними стандартами, нормативно-правовими актами та нормативними документами у сфері

захисту інформації. Для створення КСЗІ використовуються засоби захисту інформації, які мають сертифікат відповідності або позитивний експертний висновок за результатами державної експертизи у сфері технічного та криптографічного захисту інформації.

До складу КСЗІ входять заходи та засоби, які реалізують способи, методи, механізми захисту інформації від:

1. Витоку технічними каналами, до яких відносяться канали побічних електромагнітних випромінювань і наведень, акустоелектричні та інші канали;
2. Несанкціонованих дій та несанкціонованого доступу до інформації
3. Спеціального впливу на інформацію, який може здійснюватися шляхом формування полів і сигналів з метою порушення цілісності інформації або руйнування системи захисту.

Створення комплексів технічного захисту інформації від витоку технічними каналами здійснюється, якщо в ІТС обробляється інформація, яка становить державну таємницю або коли необхідність цього визначена власником інформації.

Етапи створення КСЗІ:

1 етап. Обстеження ІТС та підготовка вихідних даних для формування вимог до КСЗІ;

2 етап. Формування політики безпеки;

3 етап. Розробка технічного завдання на створення КСЗІ;

4 етап. Розробка і реалізація проекту КСЗІ в ІТС;

5 етап. Введення КСЗІ в дію;

6 етап. Попередні випробування;

7 етап. Дослідна експлуатація;

8 етап. Державна експертиза КСЗІ;

9 етап. Супровід КСЗІ.

Під політикою безпеки інформації в Системі розуміється набір законів, нормативних документів, вимог, правил, обмежень, інструкцій, рекомендацій, що регламентують порядок обробки інформації і спрямовані на захист інформації від визначених погроз. Програмна політика безпеки – є політикою вищої ланки управління в організації. Об’єктом є організація в цілому, за розробку і здійснення

програмної політики несе відповідальність керівництво організації. Програмна політика визначає стратегічні напрямки забезпечення інформаційної безпеки.

Політика безпеки повинна передбачати комплексне використання правових і морально-етичних норм, організаційних (адміністративних) мір, фізичних, технічних (апаратних і програмних) способів і засобів захисту інформації, а також визначати правила і порядок їхнього застосування в Системі

Методологія розробки політики безпеки містить у собі наступні роботи: розробка концепції безпеки інформації в Системі; аналіз ризиків; визначення вимог до методів і засобів захисту; вибір основних рішень по забезпеченню безпеки інформації; організація виконаних робіт і забезпечення безупинного функціонування Системи; документальне оформлення політики безпеки.

Отже, потрібно чітко розуміти, що будь-які засоби захисту інформації не гарантують абсолютну безпеку і надійність даних, проте вони суттєво мінімізують ризик втрат. При проведенні аналізу та об’єктивної оцінки фахівець з інформаційної безпеки повинен забезпечити найефективніші методи та засоби створення комплексної системи захисту інформації.

Література:

1. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 31.05.2005 року;
2. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі. НД ТЗІ 3.7-003-2005.