Практическая работа №1

ОСНОВЫ ЗАЩИТЫ ИНФОРМАЦИИ

Цель работы. Изучить основные понятия защиты информации и уяснить связи между ними.

Краткие сведения из теории

Существует множество понятий в сфере информационной безопасности, наиболее значимые из которых сформулированы в государственных стандартах и законах, посвященных тематике защиты информации.

К ним, например, относятся:

– государственный стандарт Республики Беларусь 50922-2000 «Защита информации. Основные термины и определения»;

– закон Республики Беларусь № 455-З «Об информации, информатизации и защите информации»;

– Концепция Национальной безопасности Республики Беларусь;

– Концепция информационной безопасности Республики Беларусь.

На рисунке 1 представлена схема связи между понятиями, определенными в государственном стандарте Республики Беларусь 50922-2000 «Защита информации. Основные термины и определения».

Информационная безопасность – состояние защищенности сбалансированных интересов личности, общества и государства от внешних и внутренних угроз в информационной сфере.

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником (государство, юридическое лицо, группа физических лиц или отдельное физическое лицо) информации.

Защита информации (ЗИ) – комплекс правовых, организационных и технических мер, направленных на обеспечение конфиденциальности, целостности, подлинности, доступности и сохранности информации.

Нарушение защиты информации происходит в результате:

– утечки защищаемой информации;

– несанкционированных воздействий на защищаемую информацию;

– непреднамеренных воздействий на защищаемую информацию.

Защита информации от утечки – деятельность, направленная на предотвращение неконтролируемого распространения защищаемой информации в результате ее разглашения, несанкционированного доступа (НСД) к информации и получения защищаемой информации разведками.

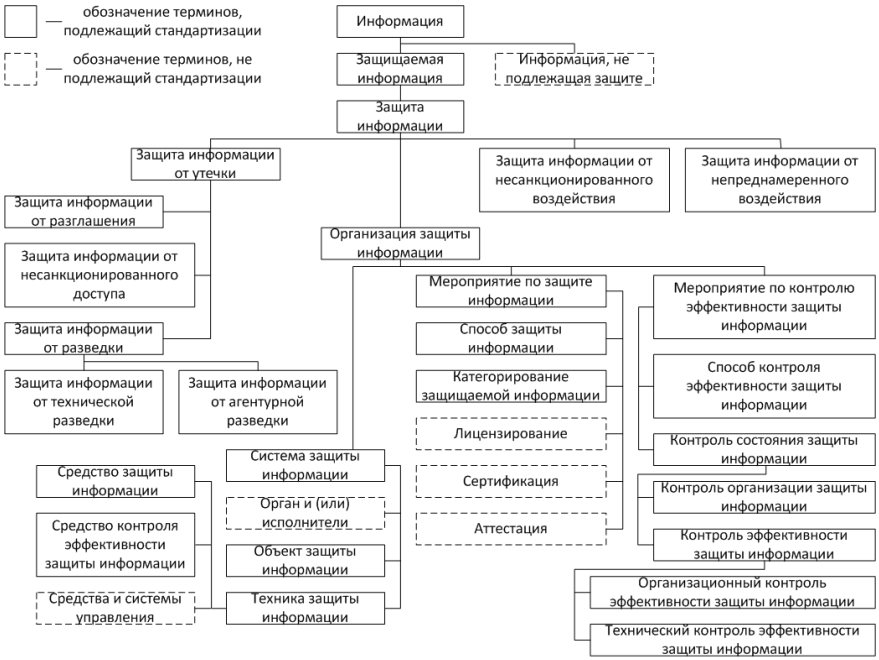

Рисунок 1 – Схема связи между понятиями, определенными в ГОСТ 50922-200.

Защита информации от несанкционированного доступа (НСД) – деятельность, направленная на предотвращение получения защищаемой информации заинтересованным субъектом (государство, юридическое лицо, группа физических лиц, в том числе общественная организация, отдельное физическое лицо) с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации.

Защита информации должна быть эффективной.

Эффективность защиты информации – степень соответствия результатов защиты информации поставленной цели.

Показатель эффективности защиты информации – мера или характеристика для оценки эффективности защиты информации.

В качестве технических мер, направленных на защиту информации, используются средства и системы защиты информации.

Система защиты информации – совокупность органов и (или) исполнителей, используемой ими техники защиты информации, а также объектов защиты, организованная и функционирующая по правилам, установленным соответствующими правовыми, организационно-распорядительными и

нормативными документами в области защиты информации.

Средство защиты информации – техническое, программное средство, вещество и (или) материал, предназначенные или используемые для защиты информации.

Порядок выполнения работы

1 Организовать группы из числа студентов в составе не менее 6 студентов каждая.

2 В каждой из групп организовать три следующие бригады, каждая не менее чем из 2-х студентов:

- Бригада «Источник информации»;
- Бригада «Приемник информации»;
- Бригада «Нарушители».

3 Бригада «Источник информации», получив от преподавателя «Сообщение», должна произвести его шифрование и подготовить два экземпляра шифротекста. Одно необходимо для передачи бригаде «Приемник информации» (имитация процесса передачи зашифрованной информации по каналам связи), а второе – бригаде «Нарушители» (имитация незащищенных каналов связи). Использование незащищенных каналов связи потенциально дает доступ нарушителям ко всей передаваемой информации.

4 Обе бригады, получившие шифротекст, должны попытаться его расшифровать и получить исходное «Сообщение». Действовать они должны независимо и втайне друг от друга.

5 Бригада «Источник информации» может оказывать содействие бригаде «Приемник информации» в процессе расшифровки, но их действия должны иметь открытый характер, позволяя студентам из бригады «Нарушители» получать к ним доступ.

6 Запрещается в процессе передачи информации между бригадами использовать технические средства, препятствовать студентам из бригады «Нарушители» получать доступ к передаваемой информации.

Содержание отчета

1 Цель работы.

2 Сообщение, полученное от преподавателя.

3 Шифротекст, созданный бригадой «Источник информации», и способ его получения.

4 Краткое описание результата работы бригады «Приемник информации», трудности и особенности расшифровки.

5 Краткое описание результата работы бригады «Нарушители», трудности и особенности расшифровки.

6 Вывод по работе.

Контрольные вопросы

1 Дайте понятие информационной безопасности.
2 Какая информация подлежит защите?
3 Что такое защита информации?
4 В результате чего может произойти нарушение защиты информации?
5 Что такое несанкционированный доступ к информации?
6 Что означает эффективная защита информации?
7 В чем отличия системы и средства защиты информации?