Тема 5.1 Цели совершения преступления. Уровни и меры по защите информации.

Целью совершения любого преступления является удовлетворение корыстных целей человека или группы людей, как то материальных, моральных, психических и так далее. Преступления в информационной сфере затрагивают различные аспекты: это и получение информации нелегальным путем (в том числе и с использованием детей), распространения в Интернете материалов порнографического типа (в том числе и детской), мошенничество в Интернете и т.д.

Основные понятия в области защиты информации от разрушения и несанкционированного доступа рассмотрим исходя из **ГОСТ Р 50922-2006.** Настоящий стандарт устанавливает основные термины с соответствующими определениями, применяемые при проведении работ по стандартизации в области защиты информации. Термины данного стандарта, рекомендуется использовать в правовой, нормативной, технической и организационно-распорядительной документации, научной, учебной и справочной литературе.

Защищаемая информация - информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Примечание: собственниками информации могут быть - государство, юридическое лицо, группа физических лиц, отдельное физическое лицо.

Защита информации - деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

Защита информации от утечки – защита информации, направленная на предотвращение неконтролируемого распространения защищаемой информации в результате ее разглашения и несанкционированного доступа к ней, а также на исключение (затруднение) получения защищаемой информации [иностранными] разведками и другими заинтересованными субъектами.

Примечание – заинтересованными субъектами могут быть: государство, юридическое лицо, группа физических лиц, отдельное физическое лицо.

Защита информации от несанкционированного воздействия - защита информации, направленная на предотвращение несанкционированного доступа и воздействия на защищаемую информацию с нарушением установленных прав и (или) правил на изменение информации, приводящих к разрушению, уничтожению, искажению, сбою в работе, незаконному перехвату и копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

Защита информации от непреднамеренного воздействия - защита информации, направленная на предотвращение воздействия на защищаемую информацию ошибок ее пользователя, сбоя технических и программных средств информационных систем, природных явлений или иных нецеленаправленных на изменение информации событий, приводящих к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

Защита информации от разглашения - защита информации, направленная на предотвращение несанкционированного доведения защищаемой информации до заинтересованных субъектов (потребителей), не имеющих права доступа к этой информации.

Защита информации от несанкционированного доступа - защита информации, направленная на предотвращение получения защищаемой информации заинтересованными субъектами с нарушением установленных нормативными и правовыми документами (актами) или обладателями информации прав или правил разграничения доступа к защищаемой информации.

Примечание - заинтересованными субъектами, осуществляющими несанкционированный доступ к защищаемой информации, могут быть: государство, юридическое лицо, группа физических лиц, в том числе общественная организация, отдельное физическое лицо.

Цель защиты информации: Заранее намеченный результат защиты информации.

Примечание - результатом защиты информации может быть предотвращение ущерба обладателю информации из-за возможной утечки информации и (или) несанкционированного и непреднамеренного воздействия на информацию.

Эффективность защиты информации - степень соответствия результатов защиты информации цели защиты информации.

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

Норма эффективности защиты информации - значение показателя эффективности защиты информации, установленное нормативными и правовыми документами.

Замысел защиты информации - основная идея, раскрывающая состав, содержание, взаимосвязь и последовательность осуществления технических и организационных мероприятий, необходимых для достижения цели защиты информации.

Система защиты информации - совокупность органов и (или) исполнителей, используемой ими техники защиты информации, а также объектов защиты информации, организованная и функционирующая по правилам и нормам, установленным соответствующими документами в области защиты информации.

Техника защиты информации - средства защиты информации, в том числе средства физической защиты информации, криптографические средства защиты информации, средства контроля эффективности защиты информации, средства и системы управления, предназначенные для обеспечения защиты информации.

Объект защиты информации - информация или носитель информации, или информационный процесс, которые необходимо защищать в соответствии с целью защиты информации.

Способ защиты информации - порядок и правила применения определенных принципов и средств защиты информации.

Оценка соответствия требованиям по защите информации - прямое или косвенное определение степени соблюдения требований по защите информации, предъявляемых к объекту защиты информации.

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

Средство контроля эффективности защиты информации - средство защиты информации, предназначенное или используемое для контроля эффективности защиты информации.

В связи с тем, что информация является предметом собственности (государства, коллектива, отдельного лица (субъекта)), то неизбежно возникает проблема угрозы безопасности этой информации, заключающейся в неконтролируемом ее распространении, в хищении, несанкционированном уничтожении, искажении, передаче, копировании, блокировании доступа к информации. Следовательно, возникает проблема защиты информации от утечки и несанкционированных воздействий на информацию и ее носители, а также предотвращения других форм незаконного вмешательства в информационные ресурсы и информационные системы. В связи с чем, понятие ***«Защита информации»*** становится основополагающим (ключевым) понятием и рассматривается как деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию. Значимость защиты информации увеличивается в связи с возрастанием возможностей иностранных разведок за счет совершенствования технических средств разведки, приближения этих средств к объектам разведки (носителям информации) вследствие развертывания инспекционной деятельности, создания совместных предприятий и производств, сокращения закрытых для иностранцев зон и городов.

Определившись с терминологией защиты информации, переходим на рассмотрение уровней и мер защиты информации. Можно выделить три основных уровня защиты информации. Например, применительно к общеобразовательному учреждению они выглядят следующим образом:

- защита информации на уровне рабочего места ученика и учителя;
- защита информации на уровне компьютерного класса;
- защита информации на уровне образовательного учреждения.

Защита информации на этих различных уровнях будет иметь как общие способы, так и специальные способы, зависящие от уровня.

Одним из способов (мер) по защите информации являются программные средства защиты. В настоящее время создано большое количество операционных систем, систем управления базами данных, сетевых пакетов и пакетов прикладных программ, уже включающих в себя разнообразные средства защиты информации.

С помощью программных средств защиты решаются следующие задачи информационной безопасности:

- контроль загрузки и входа в систему с помощью персональных идентификаторов (имя, код, пароль и т.п.);
- разграничение и контроль доступа субъектов к ресурсам и компонентам системы, внешним ресурсам;
- изоляция программ процесса, выполняемого в интересах конкретного субъекта, от других субъектов (обеспечение работы каждого пользователя в индивидуальной среде);
- управление потоками конфиденциальной информации с целью предотвращения записи на носители данных несоответствующего уровня (грифа) секретности;
- защита информации от компьютерных вирусов;
- стирание остаточной конфиденциальной информации в разблокированных после выполнения запросов полях оперативной памяти компьютера;
- обеспечение целостности информации путем введения избыточности данных;
- автоматический контроль над работой пользователей системы на базе результатов протоколирования и подготовка отчетов по данным записей в системном регистрационном журнале.

Методы обеспечения защиты информации могут быть разные, но основные из них следующие:

- препятствие;
- управление доступом;
- маскировка;
- регламентация;
- принуждение и побуждение.