Глоссарий

Информационная безопасность — состояние защищенности информационных ресурсов (информационной среды) от внутренних и внешних угроз, способных нанести ущерб интересам личности, общества, государства (национальным интересам).

Безопасность информации — защищенность информации от нежелательного (для соответствующих субъектов информационных отношений) ее разглашения (нарушения конфиденциальности), искажения (нарушения целостности), утраты или снижения степени доступности информации, а также незаконного ее тиражирования.

Информация — сведения (сообщения, данные) независимо от формы их представления.

Информационные технологии — процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Информационная система — совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

Информационно-телекоммуникационная сеть — технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники.

Обладатель информации — лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам.

Доступ к информации — возможность получения информации и ее использования.

Предоставление информации — действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц.

Распространение информации — действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц.

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

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

Защита информации от несанкционированного воздействия — деятельность, направленная на предотвращение воздействия на защищаемую информацию с нарушением установленных прав и (или) правил на изменение информации, приводящего к ее искажению, уничтожению, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

Защита информации от непреднамеренного воздействия — деятельность, 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 мероприятий, приводящих к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

Защита информации от разглашения — деятельность, направленная на предотвращение несанкционированного доведения защищаемой информации до потребителей, не имеющих права доступа к этой информации.

Защита информации от несанкционированного доступа — деятельность, направленная на предотвращение получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации.

Защита информации от разведки — деятельность, направленная на предотвращение получения защищаемой информации разведкой.

Защита информации от технической разведки — деятельность, направленная на предотвращение получения защищаемой информации разведкой с помощью технических средств.

Защита информации от агентурной разведки — деятельность, направленная на предотвращение получения защищаемой информации агентурной разведкой.

Цель защиты информации — заранее намеченный результат защиты информации.

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

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

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

Нормы эффективности защиты информации — значения показателей эффективности защиты информации, установленные нормативными документами.

Организация защиты информации — содержание и порядок действий, направленных на обеспечение 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.

Мероприятие по защите информации — совокупность действий, направленных на разработку и (или) практическое применение способов и средств защиты информации.

Мероприятие по контролю эффективности защиты информации — совокупность действий, направленных на разработку и (или) практическое применение способов и средств контроля эффективности защиты информации.

Техника защиты информации — 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 поставленной целью защиты информации.

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

Категорирование защищаемой информации (объекта защиты) — установление градации важности защищаемой информации (объекта защиты).

Контроль состояния защиты информации — проверка соответствия организации и эффективности защиты информации установленным требованиям и (или) нормам зашиты информации.

Функция защиты — совокупность однородных в функциональном отношении мероприятий, регулярно осуществляемых в информационной системе различными средствами и методами в целях создания, поддержания и обеспечения условий, объективно необходимых для надежной защиты информации.

Программные средства представляют собой программное обеспечение, специально предназначенное для выполнения функций защиты информации

Организационные средства защиты представляют собой организационно-технические и организационно-правовые мероприятия, осуществляемые в процессе создания и эксплуатации аппаратуры телекоммуникаций для обеспечения защиты информации.

Законодательные средства защиты определяются законодательными актами страны, которыми регламентируются правила использования, обработки и передачи информации ограниченного доступа и устанавливаются меры ответственности за нарушение этих правил.

Морально-этические средства защиты реализуются в виде всевозможных норм, которые сложились традиционно или складываются по мере распространения вычислительной техники и средств связи в данной стране или обществе.

Секретность (*конфиденциальность*) информации — субъективно определяемая характеристика информации, указывающая на необходимость введения ограничений на круг субъектов, имеющих доступ к данной информации.

Целостность информации — свойство информации существовать в неискаженном виде.

Доступность информации — свойство системы, в которой циркулирует информация, обеспечивать своевременный беспрепятственный доступ субъектов к интересующей их информации и готовность к обслуживанию поступающих от субъектов запросов всегда, когда в обращении к ним возникает необходимость.

Нарушитель — это лицо, предпринявшее попытку выполнения запрещенных операций (действий) по ошибке, незнанию или осознанно со злым умыслом (из корыстных интересов) или без такового (ради игры или удовольствия, с целью самоутверждения и т. п.) и использующее для этого различные возможности, методы и средства.

Злоумышленник — нарушитель, намеренно идущий на нарушение из корыстных побуждений.

Канал утечки информации — совокупность источника информации, материального носителя или среды распространения несущего указанную информацию сигнала и средства выделения информации из сигнала или носителя.

Алфавит — конечное множество используемых для кодирования информации знаков.

Текст — упорядоченный набор из элементов алфавита.

В *ассиметричных системах (системах с открытым ключом)* используются два ключа — открытый и закрытый, которые математически связаны друг с другом.

Криптостойкостью называется характеристика шифра, определяющая его стойкость к дешифрованию без знания ключа.

Разграничение доступа к информации — разделение информации, циркулирующей в информационной системе, на части, элементы, компоненты, объекты и т. д. и организация системы работы с информацией, предполагающей доступ пользователей к той части (к тем компонентам) информации, которая им необходима для выполнения функциональных обязанностей.

Субъект доступа — активная сущность, которая может изменять состояние системы через порождение процессов над объектами, в том числе порождать новые объекты и инициализировать порождение новых субъектов.

Объект доступа — пассивная сущность, процессы над которой могут в определенных случаях быть источником порождения новых субъектов.

Пользователь — лицо, внешний фактор, аутентифицируемый некоторой информацией и управляющий одним или несколькими субъектами, воспринимающий объекты и получающий информацию о состоянии системы через субъекты, которыми он управляет.