**Глоссарий**

**НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ**

**ГОСТ Р 53114-2008
Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения**

**Общие понятия**

* **безопасность информации [данных]:** Состояние защищенности информации [данных], при котором обеспечены ее [их] конфиденциальность, доступность и целостность.
* **безопасность информационной технологии:** Состояние защищенности информационной технологии, при котором обеспечиваются безопасность информации, для обработки которой она применяется, и информационная безопасность информационной системы, в которой она реализована.
* **информационная сфера:** Совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение и использование информации, а также системы регулирования возникающих при этом общественных отношений.
* **информационная инфраструктура:** Совокупность объектов информатизации, обеспечивающая доступ потребителей к информационным ресурсам.
* **объект информатизации:** Совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, а также средств их обеспечения, помещений или объектов (зданий, сооружений, технических средств), в которых эти средства и системы установлены, или помещений и объектов, предназначенных для ведения конфиденциальных переговоров.
* **активы организации:** Все, что имеет ценность для организации в интересах достижения целей деятельности и находится в ее распоряжении.
* **ресурс системы обработки информации:** Средство системы обработки информации, которое может быть выделено процессу обработки данных на определенный интервал времени.
* Примечание - Основными ресурсами являются процессоры, области основной памяти, наборы данных, периферийные устройства, программы.
* **информационный процесс:** Процесс создания, сбора, обработки, накопления, хранения, поиска, распространения и использования информации.
* **информационная технология;** ИТ: Процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.
* **техническое обеспечение автоматизированной системы;** техническое обеспечение АС: Совокупность всех технических средств, используемых при функционировании АС.
* **программное обеспечение автоматизированной системы;** программное обеспечение АС: Совокупность программ на носителях данных и программных документов, предназначенных для отладки, функционирования и проверки работоспособности АС.
* **информационное обеспечение автоматизированной системы;** информационное обеспечение АС: Совокупность форм документов, классификаторов, нормативной базы и реализованных решений по объемам, размещению и формам существования информации, применяемой в АС при ее функционировании.
* **услуга;** *сервис*: Результат деятельности исполнителя по удовлетворению потребности потребителя.
* **услуги информационных технологий**; услуги ИТ: Совокупность функциональных возможностей информационных и, возможно, неинформационных технологий, предоставляемая конечным пользователям в качестве услуги.
* **критически важная система информационной инфраструктуры**; *ключевая система информационной инфраструктуры*; КСИИ: Информационно-управляющая или информационно-телекоммуникационная система, которая осуществляет управление или информационное обеспечение критическим объектом или процессом, или используется для официального информирования общества и граждан, нарушение или прерывание функционирования которой (в результате деструктивных информационных воздействий, а также сбоев или отказов) может привести к чрезвычайной ситуации со значительными негативными последствиями.
* **критический объект**: Объект или процесс, нарушение непрерывности функционирования которого может нанести значительный ущерб.
* Примечание - Ущерб может быть нанесен имуществу физических или юридических лиц, государственному или муниципальному имуществу, окружающей среде, а также выражаться в причинении вреда жизни или здоровью граждан.
* **информационная система персональных данных:** Информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.
* **персональные данные:** Любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.
* **автоматизированная система в защищенном исполнении**; АС в защищенном исполнении: Автоматизированная система, реализующая информационную технологию выполнения установленных функций в соответствии с требованиями стандартов и/или нормативных документов по защите информации.

**Термины, относящиеся к объекту защиты информации**

* **информационная безопасность организации**; ИБ организации: Состояние защищенности интересов организации в условиях угроз в информационной сфере.
* **объект защиты информации:** Информация или носитель информации, или информационный процесс, которую(ый) необходимо защищать в соответствии с целью защиты информации.
* **защищаемый процесс (информационной технологии):** Процесс, используемый в информационной технологии для обработки защищаемой информации с требуемым уровнем ее защищенности.
* **нарушение информационной безопасности организации;** нарушение ИБ организации: Случайное или преднамеренное неправомерное действие физического лица (субъекта, объекта) в отношении активов организации, следствием которых является нарушение безопасности информации при ее обработке техническими средствами в информационных системах, вызывающее негативные последствия (ущерб/вред) для организации.
* **чрезвычайная ситуация**; *непредвиденная ситуация*; ЧС: Обстановка на определенной территории или акватории, сложившаяся в результате аварии, опасного природного явления, катастрофы, стихийного или иного бедствия, которые могут повлечь или повлекли за собой человеческие жертвы, ущерб здоровью людей или окружающей природной среде, значительные материальные потери и нарушение условий жизнедеятельности людей.
* **опасная ситуация:** Обстоятельства, в которых люди, имущество или окружающая среда подвергаются опасности.
* **инцидент информационной безопасности:** Любое непредвиденное или нежелательное событие, которое может нарушить деятельность или информационную безопасность.
* **событие:** Возникновение или наличие определенной совокупности обстоятельств.
* **риск:** Влияние неопределенностей на процесс достижения поставленных целей.
* **оценка риска:** Процесс, объединяющий идентификацию риска, анализ риска и их количественную оценку.
* **оценка риска информационной безопасности (организации);** оценка риска ИБ (организации): Общий процесс идентификации, анализа и определения приемлемости уровня риска информационной безопасности организации.
* **идентификация риска:** Процесс обнаружения, распознавания и описания рисков.
* **анализ риска:** Систематическое использование информации для определения источников риска и количественной оценки риска.
* **определение приемлемости уровня риска:** Процесс сравнения результатов анализа риска с критериями риска с целью определения приемлемости или допустимости уровня риска.
* **обработка риска информационной безопасности организации;** обработка риска ИБ организации: Процесс разработки и/или отбора и внедрения мер управления рисками информационной безопасности организации.
* **управление рисками:** Координированные действия по направлению и контролю над деятельностью организации в связи с рисками.
* **источник риска информационной безопасности организации;** источник риска ИБ организации: Объект или действие, способное вызвать [создать] риск.
* **политика информационной безопасности (организации);** политика ИБ (организации): Формальное изложение правил поведения, процедур, практических приемов или руководящих принципов в области информационной безопасности, которыми руководствуется организация в своей деятельности.
* **цель информационной безопасности (организации);** цель ИБ (организации): Заранее намеченный результат обеспечения информационной безопасности организации в соответствии с установленными требованиями в политике ИБ (организации).
* **система документов по информационной безопасности в организации;** система документов по ИБ в организации: Объединенная целевой направленностью упорядоченная совокупность документов, взаимосвязанных по признакам происхождения, назначения, вида, сферы деятельности, единых требований к их оформлению и регламентирующих в организации деятельность по обеспечению информационной безопасности.

**Термины, относящиеся к угрозам безопасности информации**

* **угроза информационной безопасности организации;** угроза ИБ организации: Совокупность факторов и условий, создающих опасность нарушения информационной безопасности организации, вызывающую или способную вызвать негативные последствия (ущерб/вред) для организации.
* **угроза (безопасности информации):** Совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации.
* **модель угроз (безопасности информации):** Физическое, математическое, описательное представление свойств или характеристик угроз безопасности информации.
* **уязвимость (информационной системы);** *брешь*: Свойство информационной системы, обусловливающее возможность реализации угроз безопасности обрабатываемой в ней информации.
* **нарушитель информационной безопасности организации;** нарушитель ИБ организации: Физическое лицо или логический объект, случайно или преднамеренно совершивший действие, следствием которого является нарушение информационной безопасности организации.
* **несанкционированный доступ:** Доступ к информации или к ресурсам автоматизированной информационной системы, осуществляемый с нарушением установленных прав и (или) правил доступа.
* **сетевая атака:** Действия с применением программных и (или) технических средств и с использованием сетевого протокола, направленные на реализацию угроз несанкционированного доступа к информации, воздействия на нее или на ресурсы автоматизированной информационной системы.
* **блокирование доступа (к информации):** Прекращение или затруднение доступа к информации лиц, имеющих на это право (законных пользователей).
* **атака «отказ в обслуживании»:** Сетевая атака, приводящая к блокированию информационных процессов в автоматизированной системе.
* **утечка информации:** Неконтролируемое распространение защищаемой информации в результате ее разглашения, несанкционированного доступа к информации и получения защищаемой информации иностранными разведками.
* **разглашение информации:** Несанкционированное доведение защищаемой информации до лиц, не имеющих права доступа к этой информации.
* **перехват (информации):** Неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов.
* **информативный сигнал:** Сигнал, по параметрам которого может быть определена защищаемая информация.
* **недекларированные возможности:** Функциональные возможности средств вычислительной техники и программного обеспечения, не описанные или не соответствующие описанным в документации, которые могут привести к снижению или нарушению свойств безопасности информации.
* **побочные электромагнитные излучения и наводки:** Электромагнитные излучения технических средств обработки информации, возникающие как побочное явление и вызванные электрическими сигналами, действующими в их электрических и магнитных цепях, а также электромагнитные наводки этих сигналов на токопроводящие линии, конструкции и цепи питания.

**Термины, относящиеся к контролю и оценке информационной безопасности организации**

* **контроль обеспечения информационной безопасности организации;** контроль обеспечения ИБ организации: Проверка соответствия обеспечения информационной безопасности в организации, наличия и содержания документов требованиям нормативных документов, технической, правовой организационно-распорядительной документации в области информационной безопасности.
* **мониторинг информационной безопасности организации;** мониторинг ИБ организации: Постоянное наблюдение за процессом обеспечения информационной безопасности в организации с целью установить его соответствие требованиям по информационной безопасности.
* **аудит информационной безопасности организации;** аудит ИБ организации: Систематический, независимый и документируемый процесс получения свидетельств деятельности организации по обеспечению информационной безопасности и установлению степени выполнения в организации критериев информационной безопасности, а также допускающий возможность формирования профессионального аудиторского суждения о состоянии информационной безопасности организации.
* **свидетельства (доказательства) аудита информационной безопасности организации;** свидетельства аудита ИБ организации: Записи, изложение фактов или другая информация, которые имеют отношение к критериям аудита информационной безопасности организации и могут быть проверены.
* **оценка соответствия информационной безопасности организации установленным требованиям;** оценка соответствия ИБ организации установленным требованиям: Деятельность, связанная с прямым или косвенным определением выполнения или невыполнения в организации установленных требований информационной безопасности.
* **критерий аудита информационной безопасности организации;** критерий аудита ИБ организации: Совокупность принципов, положений, требований и показателей действующих нормативных документов, относящихся к деятельности организации в области информационной безопасности.
* **аттестация автоматизированной системы в защищенном исполнении:** Процесс комплексной проверки выполнения заданных функций автоматизированной системы по обработке защищаемой информации на соответствие требованиям стандартов и/или нормативных документов в области защиты информации и оформления документов о ее соответствии выполнению функции по обработке защищаемой информации на конкретном объекте информатизации.
* **критерий обеспечения информационной безопасности организации;** критерий обеспечения ИБ организации: Показатель, на основании которого оценивается степень достижения цели (целей) информационной безопасности организации.
* **эффективность обеспечения информационной безопасности;** эффективность обеспечения ИБ: Связь между достигнутым результатом и использованными ресурсами для обеспечения заданного уровня информационной безопасности.

**Термины, относящиеся к средствам обеспечения информационной безопасности организации**

* **обеспечение информационной безопасности организации;** обеспечение ИБ организации: Деятельность, направленная на устранение (нейтрализацию, парирование) внутренних и внешних угроз информационной безопасности организации или на минимизацию ущерба от возможной реализации таких угроз.
* **мера безопасности;** *мера обеспечения безопасности*: Сложившаяся практика, процедура или механизм обработки риска.
* **меры обеспечения информационной безопасности;** меры обеспечения ИБ: Совокупность действий, направленных на разработку и/или практическое применение способов и средств обеспечения информационной безопасности.
* **организационные меры обеспечения информационной безопасности;** организационные меры обеспечения ИБ: Меры обеспечения информационной безопасности, предусматривающие установление временных, территориальных, пространственных, правовых, методических и иных ограничений на условия использования и режимы работы объекта информатизации.
* **техническое средство обеспечения информационной безопасности;** техническое средство обеспечения ИБ: Оборудование, используемое для обеспечения информационной безопасности организации некриптографическими методами.
* **средство обнаружения вторжений**, *средство обнаружения атак*: Программное или программно-техническое средство, которое автоматизирует процесс контроля событий, протекающих в компьютерной системе или сети, а также самостоятельно анализирует эти события в поисках признаков инцидента информационной безопасности.
* **средство защиты от несанкционированного доступа:** Программное, техническое или программно-техническое средство, предназначенное для предотвращения или существенного затруднения несанкционированного доступа.