**Практическая работа 10. Анализ терминов и определений информационной безопасности**

**Цель работы** проанализировать ГОСТ Р 53114-2008 Защита информации.

**Практическое задание**

1. Изучить ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной

безопасности в организации.

2. Изучить основные термины и определения

3. Составить глоссарий для памятки по информационной безопасности.

**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

**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.

**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.

**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.

**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.

**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 (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 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 организации** - объект или действие, способное вызвать [создать] риск.

**Политика информационной безопасности (организации); политика (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 (организации) -** заранее намеченный результат обеспечения информационной безопасности организации в соответствии с установленными требованиями в политике (организации).



**Система документов по информационной безопасности в организации; система документов по 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.

**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.

**Менеджмент информационной безопасности организации; менеджмент ИБ организации** - скоординированные действия по руководству и управлению организацией в части обеспечения ее информационной безопасности в соответствии с изменяющимися условиями внутренней и внешней среды организации.

**Менеджмент риска информационной безопасности организации; менеджмент риска ИБ организации** - скоординированные действия по руководству и управлению организацией в отношении риска ИБ с целью его минимизации.

**Система менеджмента информационной безопасности; СМИБ** - часть общей системы менеджмента, основанная на использовании методов оценки бизнес-рисков для разработки, внедрения, функционирования, мониторинга, анализа, поддержки и улучшения информационной безопасности.

**Роль информационной безопасности в организации; роль ИБ в организации** - совокупность определенных функций и задач обеспечения информационной безопасности организации, устанавливающих допустимое взаимодействие между субъектом и объектом в организации.

**Служба информационной безопасности организации** - организационно-техническая структура системы менеджмента информационной безопасности организации, реализующая решение определенной задачи, направленной на противодействие угрозам 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.

**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 не криптографическими методами.

**Средство обнаружения вторжений, средство обнаружение 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 - п**рограммное, техническое или программно-техническое средство, предназначенное для предотвращения или существенного затруднения несанкционированного доступа.

**Вывод:**

1. Проанализировав «ГОСТ Р 53114-2008 Защита информации», я изучил обеспечение информационной безопасности в организации, основные термины и определения и Глоссарий.

**Контрольные вопросы**

1. Как называется умышленно искаженная информация?

2. Как называется информация, к которой ограничен доступ?

3. Какими путями может быть получена информация?

4. Как называются компьютерные системы, в которых обеспечивается безопасность информации?

5. Основной документ, на основе которого проводится политика информационной безопасности?

1. Дезинформация

2. Конфиденциальная/частная

3. Покупка информации, хакерские атаки, физическое воздействие на владельца информации, угрозы, вымогательство и т.п.

4. Они называются защищенными.

5. Программа информационной безопасности