1. Цели и задачи информационной безопасности.

Основные цели информационной безопасности:

* Конфиденциальность — предотвращение несанкционированного доступа к информации, обеспечение доступности данных только уполномоченным лицам.
* Целостность — сохранение информации в неизменном виде, недопущение ее искажения или уничтожения, обеспечивающее достоверность данных.
* Доступность — обеспечение своевременного и надежного доступа уполномоченных пользователей к информации и информационным ресурсам.
* Подлинность и неотказуемость — подтверждение авторства и невозможность отрицать участие в информационных операциях.

Задачи информационной безопасности:

* Защита от несанкционированного доступа и утечек информации.
* Обеспечение мониторинга и реагирования на угрозы кибербезопасности.
* Управление информационными рисками и разработка мер по минимизации потенциальных угроз.
* Соблюдение правовых норм и требований национального законодательства.
* Обеспечение защиты персональных данных в соответствии с требованиями 152-ФЗ.
* Защита критической информационной инфраструктуры, обозначенной в законе 187-ФЗ.
* Предотвращение нарушения конституционных прав граждан в сфере информации.

1. Основные положения теории информационной безопасности: информация и информационные отношения.

Основные положения теории информационной безопасности базируются на трех ключевых свойствах информации: конфиденциальности, целостности и доступности. Эти свойства называются триадой CIA (Confidentiality, Integrity, Availability) и являются фундаментом для понимания и построения систем информационной безопасности.

Информация и информационные отношения

* Информация рассматривается как ресурс, который подлежит защите от несанкционированного доступа, искажения и утраты.
* Информационные отношения — это процессы получения, передачи, обработки, хранения и использования информации, в которых участвуют субъекты (люди, системы) и объекты (данные, документы).
* Информационная безопасность направлена на регулирование этих отношений с целью защиты информации и обеспечения надежных условий для ее использования.

1. Основные положения теории информационной безопасности: субъекты информационных отношений, их безопасность.

Субъекты информационных отношений

* Субъектами информационных отношений выступают лица, организации, системы, которые осуществляют действия с информацией или информационными ресурсами.
* Их безопасность подразумевает защиту прав, обязанностей, ответственности и интересов в части использования и обеспечения безопасности информации.
* К субъектам относятся: конечные пользователи, администраторы систем, владельцы информации, разработчики и обслуживающий персонал.

Безопасность субъектов информационных отношений

* Обеспечение безопасности субъектов включает разграничение доступа, контроль действий, аутентификацию и авторизацию.
* Важна персональная ответственность за соблюдение правил информационной безопасности.
* Также применяется принцип минимальных полномочий — предоставление субъектам только необходимых для работы прав и ресурсов.
* Система безопасности предусматривает мониторинг, регистрацию и анализ действий субъектов для предотвращения и выявления нарушений.

1. Три вида возможных нарушений ИС.

* Нарушение конфиденциальности — когда происходит несанкционированный доступ к информации, в результате чего защищаемые данные становятся доступны лицам, не имеющим на это прав. Например, утечки персональных данных или коммерческой тайны.
* Нарушение целостности — действия, приводящие к изменению, искажению или уничтожению информации без разрешения. Это может быть подмена данных, внесение ошибок или удаление важных файлов.
* Нарушение доступности — когда доступ авторизованных пользователей к информационной системе или данным затруднен или полностью блокирован. Пример — атаки типа DDoS, делающие систему недоступной для работы.

1. Определение требований к защищенности информации.

* Основные положения требований к защищенности информации
* Требования направлены на предотвращение неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, распространения и других неправомерных действий с информацией.
* Обеспечение конфиденциальности информации ограниченного доступа, а также реализация права законного доступа к информации.
* Требования охватывают защиту персональных данных, информации, составляющей государственную тайну, и других категорий сведений.
* Важным элементом является необходимость своевременного обнаружения и предупреждения несанкционированного доступа и других инцидентов безопасности.
* Требуется обеспечить возможность восстановления информации, нарушенной вследствие атак или сбоев.
* Требования формируются с учетом класса защищенности информационной системы, уровня значимости обрабатываемой информации и масштаба применения системы (федеральный, региональный, объектовый).
* Средства защиты должны соответствовать установленным стандартам и нормативам, проходить сертификацию (например, ФСТЭК).

1. ГОСТ 34.003-90 «Информационная технология. Комплекс стандартов на автоматизированные системы. Термины и определения».

Стандарт устанавливает унифицированные термины и определения ключевых понятий в области автоматизированных систем (АС), которые используются в различных сферах деятельности, связанных с обработкой информации (управление, проектирование, исследования и др.).

Применение стандарта обязательно для всех документов и литературы, связанных с автоматизированными системами, что способствует единообразию терминологии и понимания в индустрии.

В документе определены виды программного обеспечения АС:

* Общее программное обеспечение — ПО общего назначения, не связанное с конкретной АС, организующее вычислительный процесс и решения типовых задач.
* Специальное программное обеспечение — ПО, разрабатываемое для конкретной АС, управляющее входной, выходной и нормативной информацией.

Определены понятия надежности, живучести и помехоустойчивости АС, важные для оценки качества и устойчивости систем в условиях эксплуатации и внешних воздействий.

Введены понятия жизненного цикла АС, этапов создания, эксплуатации и утилизации, что обеспечивает структурированный подход к проектированию и сопровождению систем.

Особое внимание уделено совместимости систем на техническом, программном, информационном и организационном уровнях для эффективного взаимодействия компонентов комплекса.

Стандарт включает англоязычные эквиваленты терминов, что облегчает международное сотрудничество и обмен информацией.

Не распространяется на системы, предназначенные для обработки физических материалов и энергии.

1. ГОСТ 34.201-89 «Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем».

Стандарт распространяется на автоматизированные системы (АС), используемые в различных сферах (управление, исследование, проектирование и др.), и устанавливает виды, наименование, комплектность и обозначение документов, разрабатываемых на стадиях создания АС, согласно ГОСТ 34.601.

Определяется полный перечень и структура документации, необходимой для каждой стадии жизненного цикла создания автоматизированных систем: от исследовательской стадии и технического задания до эскизного проекта, технического проекта и рабочей документации.

Документы включают пояснительные записки, схемы организационной и функциональной структуры, технические задания на создание специализированных технических средств, описания функций и информационного обеспечения.

Предусмотрена возможность разрабатывать частные технические задания для подсистем, программных и технических комплексов.

Стандарт задает правила обозначения документов, чтобы обеспечить их удобное классифицирование и использование в проектной документации.

В документе раскрывается жизненный цикл создания АС, включающий стадии формирования требований, разработки концепции, проектирования, внедрения и сопровождения.

Документация по программным средствам и техническим средствам также имеет стандартизованное оформление и комплектность, регламентируемую отдельными ГОСТами.

ГОСТ 34.201-89 направлен на упорядочивание и систематизацию процесса создания автоматизированных систем с целью повышения качества, прозрачности и управляемости проектов.

1. ГОСТ 34.601-90 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания».

Стандарт распространяется на автоматизированные системы (АС) различных видов деятельности (исследование, проектирование, управление и др.) и устанавливает стадии и этапы создания АС.

Процесс создания АС рассматривается как совокупность упорядоченных во времени взаимосвязанных работ, объединённых в стадии и этапы, выполнение которых необходимо и достаточно для создания АС, соответствующей заданным требованиям.

Стадии и этапы создания выделяются для рационального планирования и организации работ, каждая стадия завершается конкретным результатом.

Основные стадии создания АС включают:

1. Формирование требований к АС (обследование объекта, формирование требований пользователя);
2. Разработка концепции АС (изучение объекта, проведение научно-исследовательских работ, разработка вариантов концепции);
3. Техническое задание (разработка и утверждение технического задания);
4. Эскизный проект (разработка предварительных проектных решений и документации);
5. Технический проект (детальное проектирование, подготовка документации, задание на проектирование смежных частей);
6. Рабочая документация (разработка полной рабочей документации и программ);
7. Ввод в действие (подготовка объекта автоматизации, монтаж, пусконаладочные работы, испытания);
8. Сопровождение (гарантийное и послегарантийное обслуживание).

В документе допускается изменение структуры стадий и этапов в зависимости от специфики и условий создания конкретной АС, включая объединение этапов, параллельное выполнение работ и исключение некоторых стадий.

Состав и регламентация работ на стадиях определяются договорной и технической документацией организаций, участвующих в создании АС.

Стандарт содержит приложение с подробным содержанием работ для каждого этапа, а также перечень организаций-участников создания АС.

1. ГОСТ 34.602-89 «Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы».

Стандарт распространяется на автоматизированные системы (АС) различных видов деятельности (управление, проектирование, исследование и др.) и определяет состав, содержание и правила оформления документа «Техническое задание (ТЗ) на создание (развитие или модернизацию) АС».

ТЗ является основным документом, формулирующим требования и порядок создания АС, на основании которого ведется её разработка и приемка при вводе в действие.

ТЗ разрабатывается на систему в целом либо на её части (подсистемы, комплексы задач и т.д.).

В документ включаются только конкретизированные требования, дополняющие типовые, содержащиеся в нормативно-технической документации, и отражающие особенности объекта автоматизации.

Стандарт предусматривает изменения ТЗ через дополнения или протоколы согласования между заказчиком и разработчиком.

Типичные разделы технического задания:

* Общие сведения;
* Назначение и цели создания (развития) системы;
* Характеристика объектов автоматизации;
* Требования к системе (функциональные, качественные, эксплуатационные);
* Состав и содержание работ по созданию системы;
* Порядок контроля и приемки системы;
* Требования к подготовке объекта автоматизации к вводу системы в действие;
* Требования к документации;
* Источники разработки.

Указано, что требования в ТЗ не должны ограничивать разработчика в поиске наиболее эффективных технических и экономических решений.

ТЗ разрабатывается на основе исходных данных, включая результаты стадии «Исследование и обоснование создания АС» по ГОСТ 34.601.

Важным аспектом является четкое оформление и согласование технического задания как обязательного управляющего документа в процессе создания автоматизированной системы.