МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ

АСТРАХАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ИМ. В.Н.ТАТИЩЕВА

Факультет цифровых технологий и кибербезопасности

Кафедра информационных технологий

Форма обучения очная

**ЛАБОРАТОРНАЯ РАБОТА №1**

***Парольная защита***

|  |  |  |
| --- | --- | --- |
| Исполнитель:  студент группы ДПИ-25  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Мартынов В.А.  «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_2025 г.    Преподаватель:  Кафедра информационных технологий  Кандидат технических наук, доцент  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Мартьянова А.Е.  «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_2025 г. |  |  |

Астрахань – 2025

1. **Теоретическая часть**

Под несанкционированным доступом к информации (НСД) согласно руководящим документам Гостехкомиссии будем понимать доступ к информации, нарушающий установленные правила разграничения доступа и осуществляемый с использованием штатных средств, предоставляемых СВТ или АС. НСД может носить случайный или намеренный характер.

Можно выделить несколько обобщенных категорий методов защиты от НСД, в частности:

* организационные;
* технологические;
* правовые.

К первой категории относятся меры и мероприятия, регламентируемые внутренними инструкциями организации, эксплуатирующей информационную систему. Пример такой защиты — присвоение грифов секретности документам и материалам, хранящимся в отдельном помещении, и контроль доступа к ним сотрудников. Вторую категорию составляют механизмы защиты, реализуемые на базе программно-аппаратных средств, например систем идентификации и аутентификации или охранной сигнализации. Последняя категория включает меры контроля за исполнением нормативных актов общегосударственного значения, механизмы разработки и совершенствования нормативной базы, регулирующей вопросы защиты информации. Реализуемые на практике методы, как правило, сочетают в себе элементы нескольких из перечисленных категорий. Так, управление доступом в помещения может представлять собой взаимосвязь организационных (выдача допусков и ключей) и технологических (установку замков и систем сигнализации) способов защиты.

Рассмотрим подробнее такие взаимосвязанные методы защиты от НСД, как идентификация, аутентификация и используемое при их реализации криптографическое преобразование информации.

Идентификация — это присвоение пользователям идентификаторов и проверка предъявляемых идентификаторов по списку присвоенных.

Аутентификация — это проверка принадлежности пользователю предъявленного им идентификатора. Часто аутентификацию также называют подтверждением или проверкой подлинности.

Под безопасностью (стойкостью) системы идентификации и аутентификации будем понимать степень обеспечиваемых ею гарантий того, что злоумышленник не способен пройти аутентификацию от имени другого пользователя, В этом смысле, чем выше стойкость системы аутентификации, тем сложнее злоумышленнику решить указанную задачу. Система идентификации и аутентификации является одним из ключевых элементов инфраструктуры защиты от НСД любой информационной системы.

Различают три группы методов аутентификации, основанных на наличии у каждого пользователя:

* индивидуального объекта заданного типа;
* знаний некоторой известной только ему и проверяющей стороне информации;
* индивидуальных биометрических характеристик.

Кпервой группе относятся методы аутентификации, использующие удостоверения, пропуска, магнитные карты и другие носимые устройства, которые широко применяются для контроля доступа в помещения, а также входят в состав программно-аппаратных комплексов защиты от НСД к средствам вычислительной техники.

Во вторую группу входят методы аутентификации, использующие пароли. По экономическим причинам они включаются в качестве базовых средств защиты во многие

программно-аппаратные комплексы защиты информации. Все современные операционные системы и многие приложения имеют встроенные механизмы парольной защиты.

Последнюю группу составляют методы аутентификации, основанные на применении оборудования для измерения и сравнения с эталоном заданных индивидуальных характеристик пользователя: тембра голоса, отпечатков пальцев, структуры радужной оболочки глаза и др. Такие средства позволяют с высокой точностью аутентифицировать обладателя конкретного биометрического признака, причем "подделать" биометрические параметры практически невозможно. Однако широкое распространение подобных технологий сдерживается высокой стоимостью необходимого оборудования.

Если в процедуре аутентификации участвуют только две стороны, устанавливающие подлинность друг друга, такая процедура называется непосредственной аутентификацией (direct password authentication). Если же в процессе аутентификации участвуют не только эти стороны, но и другие, вспомогательные, говорят об аутентификации с участием доверенной стороны (trusted third party authentication). При этом третью сторону называют сервером аутентификации (authentication server) или арбитром (arbitrator).

Наиболее распространенные методы аутентификации основаны на применении многоразовых или одноразовых паролей. Из-за своего широкого распространения и простоты реализации парольные схемы часто в первую очередь становятся мишенью атак злоумышленников. Эти методы включают следующие разновидности способов аутентификации:

* по хранимой копии пароля или его свёртке (plaintext-equivalent);
* по некоторому проверочному значению (verifier-based);
* без непосредственной передачи информации о пароле проверяющей стороне (zero- knowledge);
* с использованием пароля для получения криптографического ключа (cryptographic). Впервую разновидность способов входят системы аутентификации,

предполагающие наличие у обеих сторон копии пароля или его свертки. Для организации таких систем требуется создать и поддерживать базу данных, содержащую пароли или сверки паролей всех пользователей. Их слабой стороной является то, что получение злоумышленником этой базы данных позволяет ему проходить аутентификацию от имени любого пользователя.

Способы, составляющие вторую разновидность, обеспечивают более высокую степень безопасности парольной системы, так как проверочные значения, хотя они и зависят от паролей, не могут быть непосредственно использованы злоумышленником для аутентификации.

Наконец, аутентификация без предоставления проверяющей стороне какой бы то ни было информации о пароле обеспечивает наибольшую степень защиты. Этот способ гарантирует безопасность даже в том случае, если нарушена работа проверяющей стороны (например, в программу регистрации в системе внедрен "троянский конь").

Особым подходом в технологии проверки подлинности являются криптографические протоколы аутентификации. Такие протоколы описывают последовательность действий, которую должны совершить стороны для взаимной аутентификации, кроме того, эти действия, как правило, сочетаются с генерацией и распределением криптографических ключей для шифрования последующего информационного обмена. Корректность протоколов аутентификации вытекает из свойств задействованных в них математических и криптографических преобразований и может быть строго доказана.

Обычные парольные системы проще и дешевле для реализации, но менее безопасны, чем системы с криптографическими протоколами. Последние обеспечивают

более надежную защиту и дополнительно решают задачу распределения ключей. Однако используемые в них технологии могут быть объектом законодательных ограничений.

Для более детального рассмотрения принципов построения парольных систем сформулируем несколько основных определений.

Идентификатор пользователя — некоторое уникальное количество информации, позволяющее различать индивидуальных пользователей парольной системы (проводить их идентификацию). Часто идентификатор также называют именем пользователя или именем учетной записи пользователя.

Пароль пользователя — некоторое секретное количество информации, известное только пользователю и парольной системе, которое может быть запомнено пользователем и предъявлено для прохождения процедуры аутентификации. Одноразовый пароль дает возможность пользователю однократно пройти аутентификацию. Многоразовый пароль может быть использован для проверки подлинности повторно.

Учетная запись пользователя — совокупность его идентификатора и его пароля. База данных пользователей парольной системы содержит учетные записи всех пользователей данной парольной системы.

Под парольной системой будем понимать программно-аппаратный комплекс, реализующий системы идентификации и аутентификации пользователей АС на основе одноразовых или многоразовых паролей. Как правило, такой комплекс функционирует совместно с подсистемами разграничения доступа и регистрации событий. В отдельных случаях парольная система может выполнять ряд дополнительных функций, в частности генерацию и распределение кратковременных (сеансовых) криптографических ключей.

Основными компонентами парольной системы являются:

* интерфейс пользователя;
* интерфейс администратора;
* модуль сопряжения с другими подсистемами безопасности;
* база данных учетных записей.

Парольная система представляет собой "передний край обороны" всей системы безопасности. Некоторые ее элементы (в частности, реализующие интерфейс пользователя) могут быть расположены в местах, открытых для доступа потенциальному злоумышленнику. Поэтому парольная система становится одним из первых объектов атаки при вторжении злоумышленника в защищенную систему.

Ниже перечислены типы угроз безопасности парольных систем:

Разглашение параметров учетной записи через:

* подбор в интерактивном режиме;
* подсматривание;
* преднамеренную передачу пароля его владельцем другому лицу;
* захват базы данных парольной системы (если пароли не хранятся в базе в открытом виде, для их восстановления может потребоваться подбор или дешифрование);
* перехват переданной по сети информации о пароле;
* хранение пароля в доступном месте.

Вмешательство в функционирование компонентов парольной системы через внедрение программных закладок;

* обнаружение и использование ошибок, допущенных на стадии разработки;
* выведение из строя парольной системы.

Некоторые из перечисленных типов угроз связаны с наличием так называемого человеческого фактора, проявляющегося в том, что пользователь может:

* выбрать пароль, который легко запомнить и также легко подобрать;
* записать пароль, который сложно запомнить, и положить запись в доступном месте;
* ввести пароль так, что его смогут увидеть посторонние;
* передать пароль другому лицу намеренно или под влиянием заблуждения.

В дополнение к выше сказанному необходимо отметить существование "парадокса человеческого фактора". Заключается он в том, что пользователь нередко стремится выступать скорее противником парольной системы, как, впрочем, и любой системы безопасности, функционирование которой влияет на его рабочие условия, нежели союзником системы защиты, тем самым ослабляя ее. Защита от указанных угроз основывается на ряде перечисленных ниже организационно-технических мер и мероприятий.

## Выбор паролей

В большинстве систем пользователи имеют возможность самостоятельно выбирать пароли или получают их от системных администраторов. При этом для уменьшения деструктивного влияния описанного выше человеческого фактора необходимо реализовать ряд требований к выбору и использованию паролей.

Таблица 1 – требования к выбору пароля

|  |  |
| --- | --- |
| **Требование к выбору пароля** | **Получаемый эффект** |
| Установление минимальной длины пароля | Усложняет задачу злоумышленника при попытке подсмотреть пароль или подобрать пароль методом «тотального опробования» |
| Использование в пароле различных групп символов | Усложняет задачу злоумышленника при попытке подобрать пароль методом «тотального опробования» |
| Проверка и отбраковка пароля по словарю | Усложняет задачу злоумышленника при попытке подобрать пароль по словарю |
| Установление максимального срока действия пароля | Усложняет задачу злоумышленника при попытке подобрать пароль методом «тотального опробования», в том числе без непосредственного обращения к системе защиты (режим off-line) |
| Установление минимального срока действия пароля | Препятствует попыткам пользователя заменить пароль на старый после его смены по предыдущему требованию |
| Ведение журнала истории паролей | Обеспечивает дополнительную степень защиты по предыдущему требованию |
| Применение эвристического алгоритма, бракующего пароли на основании данных журнала истории | Усложняет задачу злоумышленника при попытке подобрать пароль по словарю или с использованием эвристического алгоритма |
| Ограничение числа попыток ввода пароля | Препятствует интерактивному подбору паролей злоумышленником |
| Поддержка режима принудительной смены пароля пользователя | Обеспечивает эффективность требования, ограничивающего максимальный срок действия пароля |
| Использование задержки при вводе неправильного пароля | Препятствует интерактивному подбору паролей злоумышленником |
| Запрет на выбор пароля самими пользователями и автоматическая генерация паролей | Исключает возможность подобрать пароль по словарю. Если алгоритм генерации паролей не известен злоумышленнику, последний может подбирать пароли только методом «тотального опробования» |
| Принудительная смена пароля при первой регистрации пользователя в системе | Защищает от неправомерных действия системного администратора, имеющего доступ к паролю в момент создания учетной записи |

1. **Практическая часть**

1. Определить время перебора всех паролей с параметрами. Алфавит состоит из n символов. Длина пароля символов **k**. Скорость перебора **S** паролей в секунду. После каждого из **m** неправильно введенных паролей идет пауза в **V** секунд.

Таблица 2 – Вариант для задания 1

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| вариант | n | k | s | m | v |
| 10 | 500 | 5 | 1000 | 10 | 10 |

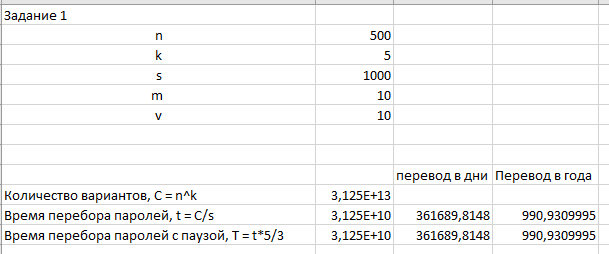


Рисунок 1 – Расчёт времени перебора паролей с параметрами

Таким образом, с заданными параметрами перебор паролей составит приблизительно **991 год.**

2. Определить минимальную длину пароля, алфавит которого состоит из **n** символов, время перебора которого было не меньше **t** лет. Скорость перебора **S** паролей в секунду.

Таблица 3 – Вариант для задания 2

|  |  |  |  |
| --- | --- | --- | --- |
| вариант | n | t | s |
| 10 | 500 | 50 | 1000 |

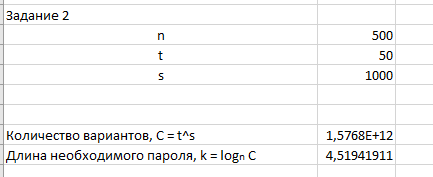


Рисунок 2 – Определение минимальной длины пароля

Таким образом, минимальная длина пароля, согласно варианту, составляет не менее **5 символов.**

3. Определить количество символов алфавита, пароль состоит из k символов, время перебора которого было не меньше t лет. Скорость перебора s паролей в секунду.

Таблица 4 – Вариант для задания 3

|  |  |  |  |
| --- | --- | --- | --- |
| вариант | k | t | s |
| 10 | 50 | 50 | 1000 |

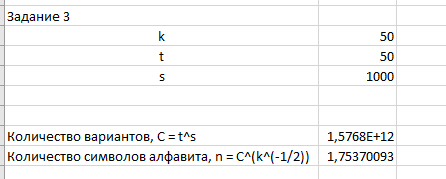


Рисунок 3 – Определение количества символов алфавита

Таким образом, для решения данной задачи достаточно алфавита, в котором содержится всего **2 символа.**

1. **Ответы на контрольные вопросы**
2. 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.

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.