УТВЕРЖДЕНО

приказом ГБУ СО «РЦУП»

от «22» апреля 2011 г. № 24/2-ОД

ИНТЕГРАЦИОННАЯ ШИНА ЭЛЕКТРОННОГО ПРАВИТЕЛЬСТВА САМАРСКОЙ ОБЛАСТИ

КОНЦЕПЦИЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЭЛЕКТРОННОГО ПРАВИТЕЛЬСТВА САМАРСКОЙ ОБЛАСТИ

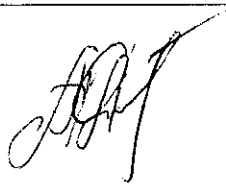
ЛИСТОВ 75

Самара 2011 г.

ЛИСТ СОГЛАСОВАНИЯ

Концепция обеспечения информационной безопасности электронного правительства Самарской области

ГБУ СО РЦУП

Должность	ФИО	Подпись	Дата
Заместитель директора	Д.П.Шевченко		15.04.2011
Начальник управления по развитию и сопровождению информационных систем и ресурсов	А.В.Ягупов		11.04.2011
Главный инженер проекта	С.А.Кузьминов		8.04.2011
Главный инженер проекта	Н.В.Кутузов		08.04.2011

Содержание

Аннотация

Обеспечение информационной безопасности информационно-технологической инфраструктуры является одним из основных направлений, предусмотренных Концепцией развития в Самарской области информационного общества и формирования электронного правительства до 2015 года, утвержденной постановлением Правительства Самарской области от 05.09.2007 №159.

Учитывая значимость развития электронного правительства Самарской области как поставщика информационных услуг, а также специфику информации, обрабатываемой в информационных системах электронного правительства (персональные данные жителей Самарской области), проблема защиты конфиденциальности и целостности критичной информации в этих системах и обеспечения доступности их вычислительных и коммуникационных ресурсов является сложной и необходимой задачей.

Для обеспечения приемлемого уровня защиты информационных ресурсов ЭП СО необходимо создание комплексной системы обеспечения информационной безопасности (СОИБ). СОИБ должна консолидировать правовые, технологические, организационные, технические и физические меры и способы защиты. Она должна иметь продуманную долгосрочную политику, обеспечивающую повышение уровня информационной безопасности в соответствии с появлением новых источников и средств реализации угроз.

Источниками требований к СОИБ являются, во-первых, требования российского законодательства, определяющие обязательность защиты информации ограниченного доступа, в том числе персональных данных. Во-вторых, необходимо обеспечить доверие граждан и организаций к электронному правительству как поставщику информационных услуг и минимизировать риски, связанные с использованием информационных ресурсов – для ЭП как собственника этих ресурсов, ведомств, организаций и граждан как их пользователей.

1. Назначение и задачи Концепции

Концепция представляет собой официально принятую систему взглядов на цели, задачи и направления деятельности по защите информации, обрабатываемой в информационных системах электронного правительства Самарской области, обеспечивающих безопасное использование информационных ресурсов при межведомственном взаимодействии и предоставлении ГУ, оказываемых в электронном виде, населению области в условиях действия возможных угроз информационной безопасности.

Основными задачами Концепции являются:

- определение долгосрочного плана создания, функционирования и развития системы обеспечения информационной безопасности (СОИБ);
- обеспечение выполнения требований законодательства Российской Федерации по защите информации;
- определение требований к информационной безопасности в ЭП СО, обеспечивающих необходимый уровень защиты информационных ресурсов;
- создание основы для проведения единой технической политики в области применения информационных технологий, использования систем безопасности и средств защиты информации.

2. Правовая и нормативно-техническая база обеспечения безопасности информации

Правовую основу обеспечения безопасности конфиденциальной информации и персональных данных в ЭП СО составляют законы, указы, постановления, другие нормативные документы действующего законодательства Российской Федерации:

- Конституция Российской Федерации;
- Гражданский, Уголовный и Трудовой Кодексы Российской Федерации;
- Федеральные законы Российской Федерации: «О безопасности», «Об информации, информационных технологиях и о защите информации», «О персональных данных», «Об электронной цифровой подписи», «Об участии в международном информационном обмене», «О техническом регулировании»;
- Указы Президента Российской Федерации: «Об утверждении перечня сведений конфиденциального характера», «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена»;
- Постановления Правительства Российской Федерации:
- «Об утверждении положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти»;
- «Об утверждении положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных»;
- «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных»;
- другие законодательные акты.

Законодательство Российской Федерации, регламентирующее деятельность в области защиты информации, предусматривает:

- разделение информации на категории свободного и ограниченного доступа;
- правовой режим защиты информации, неправомерное обращение с которой может нанести ущерб ее собственнику, владельцу, пользователю и иному лицу;
- определение прав и обязанностей субъектов в области защиты информации.

Требования законов Российской Федерации детализируются и уточняются в документах Федеральной службы по техническому и экспортному контролю Российской Федерации (ФСТЭК России), ФСБ России и других государственных учреждений, имеющих отношение к обеспечению безопасности информации и безопасному использованию информационных технологий. К этим документам относятся:

- Руководящий документ ФСТЭК (Гостехкомиссии) России «Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)» 2002 г.;
- Приказ ФСБ Российской Федерации № 66 от 09.02.05 г. «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)»;
- Приказ ФСТЭК России, ФСБ России, Мининформсвязи России № 55/86/20 от 13.02.08 г. «Об утверждении Порядка проведения классификации информационных систем персональных данных»;
- «Основные мероприятия по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных», утвержденные ФСТЭК России 15 февраля 2008 г.;

- «Рекомендации по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденные ФСТЭК России 15 февраля 2008 г.;
- «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденные ФСТЭК России 15 февраля 2008 г.;
- «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденные ФСТЭК России 15 февраля 2008 г.;
- «Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации», утвержденные ФСБ России 21 февраля 2008 г. № 149-5/144;
- «Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведения, составляющие государственную тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденные ФСБ России 21 февраля 2008 г. № 149/6/6-622.

Для реализации и контроля требований этих уровней созданы государственные системы сертификации средств защиты и аттестации объектов информатизации. Ответственность за несоблюдение этих требований определена в соответствующих законах и нормативных актах.

3. Основные цели, задачи и направления обеспечения информационной безопасности в электронном правительстве Самарской области

3.1. Цели обеспечения информационной безопасности

Основной целью обеспечения информационной безопасности является защита интересов субъектов информационных отношений, возникающих при межведомственном взаимодействии и предоставлении ГУ, оказываемых в электронном виде, на базе интеграционной платформы электронного правительства Самарской области.

Субъектами информационных отношений при межведомственном взаимодействии и предоставлении ГУ, оказываемых в электронном виде, на базе ИШ ЭП СО являются:

- Правительство Самарской области, как собственник информационных систем и информационных ресурсов;
- должностные лица и сотрудники структурных подразделений Правительства Самарской области, в соответствии с возложенными на них функциями;
- взаимодействующие органы государственной власти и местного самоуправления как поставщики и потребители информационных ресурсов ЭП СО, в соответствии с определенными регламентами взаимодействия;
- юридические и физические лица, сведения о которых накапливаются, хранятся и обрабатываются в информационных системах ЭП СО;
- другие юридические и физические лица, задействованные в процессе создания и функционирования информационных систем

ЭП СО (разработчики компонент ИС, обслуживающий персонал, организации, привлекаемые для оказания услуг в области защиты информации и др.).

Данные субъекты информационных отношений заинтересованы в обеспечении:

- конфиденциальности определенной части информации;
- достоверности (полноты, точности, целостности) информации и защиты от навязывания им ложной (недостоверной, искаженной) информации;
- своевременного доступа (за приемлемое для них время) к необходимой информации;
- разграничения ответственности за нарушения законных прав (интересов) других субъектов информационных отношений и установленных правил обращения с информацией;
- возможности осуществления контроля и управления процессами обработки и передачи информации.

При межведомственном взаимодействии и предоставлении ГУ, оказываемых в электронном виде, на базе ИШ ЭП СО должны в полной мере соблюдаться принципы:

- Гарантированности соблюдения прав граждан и юридических лиц на получение достоверной информации, а также на ограничение доступа (сохранение конфиденциальности) к части информации (персональных данных).
- Создания условий для качественного и эффективного информационного обеспечения граждан, органов власти, организаций на основе создания общедоступных информационных ресурсов и упрощения порядка получения информации из них.

- Объединения и оптимизации структуры разрозненных информационных ресурсов органов государственной власти и местного самоуправления Самарской области с сохранением режимов хранения информации и категорий доступа, непосредственно доступных этим органам, с учетом необходимости устранения дублирования информации в этих информационных ресурсах, преодоления искажений информации, а также восстановления информации в случае ее утраты в одном из ресурсов.
- Обеспечения юридической значимости электронных документов.
- Технологической совместимости с ИТ-инфраструктурой взаимодействующих органов государственной власти и местного самоуправления, в частности для организации юридически значимого документооборота.

3.2. Задачи обеспечения информационной безопасности

Основными задачами обеспечения информационной безопасности в ЭП СО являются:

- защита информационных ресурсов ЭП СО от разглашения, утечки и несанкционированного доступа, обеспечение их целостности и доступности, обеспечение надежного функционирования информационных систем и предоставляемых ими сервисов;
- обеспечение правовой защиты субъектов информационных отношений при использовании информационных ресурсов и систем электронного правительства.

Решение данных задач достигается путем создания комплексной системы обеспечения информационной безопасности и контроля эффективности применяемых мер и средств защиты по всем необходимым направлениям.

3.3. Основные направления обеспечения информационной безопасности

В качестве основных направлений обеспечения безопасности информации в ЭП СО рассматриваются:

- обеспечение информационной безопасности при предоставлении ГУ, оказываемых в электронном виде, населению;
- обеспечение информационной безопасности при межведомственном взаимодействии;
- обеспечение безопасности информации при ее обработке в информационных системах ЭП СО;
- обеспечение безопасности информации при ее передаче по телекоммуникационным системам;
- обеспечение безопасности информации при проведении работ по созданию (модернизации) информационных и технологических подсистем и развитию инфраструктуры ЭП СО.

3.3.1. Обеспечение информационной безопасности при предоставлении населению ГУ, оказываемых в электронном виде

Обеспечение информационной безопасности при предоставлении населению ГУ, оказываемых в электронном виде, предполагает:

- регламентацию процессов оказания услуг, а также разбора конфликтных ситуаций;

- создание надежной системы идентификации, аутентификации и разграничения доступа пользователей ГУ, удаленных терминалов, серверов и информационных ресурсов;
- обеспечение достоверности запрашиваемой в процессе оказания ГУ информации;
- организацию журналирования действий (запросов) пользователей и ответов ИС ЭП СО.

3.3.2. Обеспечение информационной безопасности при межведомственном взаимодействии

Обеспечение информационной безопасности при межведомственном взаимодействии предполагает:

- регламентацию процессов электронного взаимодействия органов власти (организаций), а также разбора конфликтных ситуаций;
- использование технологически совместимых и интегрируемых решений и продуктов обеспечения ИБ электронного правительства Самарской области с продуктами обеспечения ИБ, используемыми в других ведомствах;
- доведение до взаимодействующих организаций требований по правильному использованию средств автоматизации и средств защиты ИС ЭП СО и контроль исполнения данных требований.

3.3.3. Обеспечение безопасности информации при ее обработке в информационных системах ЭП СО

Обеспечение безопасности информации при ее обработке в информационных системах ЭП СО предполагает:

- определение владельцев информационных систем и закрепление

ответственности за санкционированный доступ к ним и их правильное использование;

- разработку правил и рекомендаций по оформлению, категорированию, учету и правилам предоставления доступа к информационным ресурсам;
- создание разграничительной системы допуска сотрудников к информационным ресурсам, системам и сервисам в соответствии с их должностными обязанностями;
- обучение сотрудников принятым нормам и правилам работы с информационными системами и информационными ресурсами;
- регламентацию вопросов обеспечения эксплуатации, технического обслуживания, разделения процессов разработки и использования ПО, внедрения новых систем, модификации ПО, проверки целостности и работоспособности технических и программных средств;
- настройку и администрирование средств защиты в соответствии с принятой политикой безопасности;
- обеспечение физической защиты доступа к серверному, коммуникационному и другому, критичному для функционирования ИТ, оборудованию и программному обеспечению;
- резервирование и обеспечения целостности жизненно важных данных на всех или избранных стадиях их обработки;
- восстановление систем после их отказов, особенно для систем с повышенными требованиями к доступности;
- журналирование значимых событий для целей повседневного контроля или специальных расследований;

- создание системы оперативного реагирования на события нарушений безопасности;
- организацию системы контроля достаточности и эффективности принимаемых мер защиты.

3.3.4. Обеспечение безопасности информации при ее передаче по телекоммуникационным системам

Обеспечение безопасности информации при ее передаче по телекоммуникационным системам предполагает:

- создание надежной системы идентификации и аутентификации удаленных объектов, пользователей, серверов и информационных ресурсов;
- организацию криптографической защиты информации, передаваемой по телекоммуникационным системам, и использования защищенных протоколов;
- создание равнопрочного периметра безопасности телекоммуникационной сети ЭП СО;
- организацию дублирования и резервирования каналов связи, увеличения их пропускной способности и качества, повышение надежности и защищенности системы управления;
- физическую защиту телекоммуникационного оборудования.

3.3.5. Обеспечение безопасности информации при проведении работ по созданию (модернизации) информационных и технологических подсистем и развитию инфраструктуры

Обеспечение безопасности информации при проведении работ по созданию (модернизации) информационных и технологических подсистем и развитию инфраструктуры предполагает:

- разработку процедур управления процессом внесения изменений, технического анализа изменений, вносимых в рабочую среду, ограничений на внесение изменений в пакеты программ и т.д.;
- при постановке задач на разработку функционального прикладного программного обеспечения - необходимость задания в ТЗ требований по безопасности;
- регламентацию процесса документирования разработки, представления и поддержания в актуальном состоянии конструкторской и эксплуатационной документации, исходных текстов программ, эталонных дистрибутивов программ;
- организацию сертификации средств защиты информации, на отсутствие недекларированных возможностей;
- обязательность согласования ТЗ и постановок задач на разработку функционального ПО или внедрения новых систем с информационно-технологическим управлением и отделом безопасности.

4. Объекты защиты

Защите в ЭП СО подлежат:

- Информация в любой форме ее представления:
- персональные данные граждан Самарской области от использования их в целях причинения имущественного и морального вреда гражданам путем возможного создания и распространения недостоверной информации или несанкционированного использования информации в отношении них;
- сведения, составляющие служебную тайну ЭП СО и определенные Перечнем сведений ограниченного доступа ЭП СО;
- иные сведения, составляющие охраняемую действующим законодательством тайну;
- иные сведения, определенные собственником информации (взаимодействующими ведомствами и организациями) при ее передаче в ЭП СО в соответствии с соглашениями о конфиденциальности и/или регламентами взаимодействия.
- информационные ресурсы (файлы, базы данных, электронные документы, и т.д.) содержащие защищаемую информацию. На данном этапе развития к наиболее приоритетным информационным ресурсам следует отнести:
- Регистр населения СО (РН СО), содержащий персональные данные, необходимые для идентификации жителей Самарской области, а также информацию, о принадлежащих им социально значимых документах, как информационная система обработки персональных данных (ИСПДн);
- Реестры, классификаторы и общесистемные справочники,

размещенные на интеграционной шине ЭП СО.

Вводится следующая классификация типов информационных ресурсов ЭП СО:

- внешние ресурсы, доступные всем пользователям услуг электронного правительства (Интернет ресурсы);
- ведомственные ресурсы, доступные сотрудникам правительства Самарской области и взаимодействующих ведомств;
- внутренние ресурсы правительства Самарской области, доступ к которым ограничен определенным перечнем сотрудников правительства Самарской области.
- ГУ, оказываемые в электронном виде, и сервисы, предоставляемые информационными ресурсами ЭП СО, как материальные ресурсы, имеющие стоимость, от их несанкционированного использования и несанкционированного блокирования доступа к ним (нарушения доступности);
- информационная инфраструктура (техническое, программное и информационное обеспечение информационных систем ЭП СО, а также помещения, в которых размещены данные средства), как материальные средства обеспечения бизнес-процессов, от их несанкционированного использования. К защищаемым объектам информационной инфраструктуры следует отнести:
- автоматизированные рабочие места сотрудников, используемые для обработки, хранения и передачи защищаемой информации в рамках ЭП СО;
- автоматизированные рабочие места, установленные во взаимодействующих организациях, объединенные сетью передачи

данных;

- центры обработки данных, серверы ИС ЭП СО;
- каналы информационного обмена и телекоммуникации;
- механизмы обеспечения функционирования телекоммуникационных систем и сетей, в том числе системы и средства защиты информации;
- программные средства (операционные системы, системы управления базами данных, другое общесистемное и прикладное программно-математическое обеспечение), используемые для обработки защищаемой информации;
- помещения, где располагаются АРМы, серверы, устройства ввода/вывода и хранилища носителей информации;
- помещения, предназначенные для обсуждения, обработки и хранения информации, содержащей охраняемые сведения.

Информационные ресурсы и системы, содержащие/обрабатывающие защищаемые сведения, должны быть определены в документе «Перечень информационных ресурсов и систем, содержащих сведения ограниченного доступа», и утверждены в установленном порядке. Эти Перечни должны включать названия информационных систем (подсистем), автоматизированных рабочих мест, баз данных, информационных массивов и пакетов прикладных программ, подлежащих защите.

5. Угрозы безопасности информации

При анализе источников угроз информационной безопасности рассматриваются внутренние и внешние нарушители.

5.1. Внешний нарушитель

Внешний нарушитель не имеет непосредственного доступа к системам и ресурсам, находящимся в пределах контролируемой зоны ЭП СО. Этот нарушитель может осуществлять атаки только с территории, расположенной вне контролируемой зоны и по внешним каналам связи. К нарушителю данного типа можно отнести физических или юридических лиц, осуществляющих атаки с целью добычи конфиденциальной информации, навязывания ложной информации, нарушения работоспособности информационных систем, нарушения целостности информационных ресурсов. К нарушителям данного типа причисляются все субъекты доступа, не имеющие полномочий доступа к ведомственным и внутренним ресурсам ИС ЭП СО и не подпадающие под категорию внутреннего нарушителя.

Предполагается, что субъект доступа данного типа может обладать любыми реально существующими техническими ресурсами для реализации атак. Он может располагать некоторыми фрагментами информации о топологии сети ЭП СО, об используемых коммуникационных протоколах и их сервисах, но не должен (хотя гипотетически может) располагать сетевыми адресами и полной архитектурой сети и системы защиты.

К возможностям внешних нарушителей следует отнести:

- возможность осуществлять НСД через АРМ, подключенные к сетям общего пользования (Интернет);
- возможность осуществлять НСД к информации с использованием вредоносных программ, программных закладок;
- возможность осуществлять НСД через элементы информационной инфраструктуры, которые в процессе своего жизненного цикла оказываются за пределами контролируемой зоны (модернизация, сопровождение, ремонт, утилизация);

- возможность осуществлять НСД через информационные системы взаимодействующих ведомств (организаций, учреждений) при их подключении к ИС ЭП СО.

5.2. Внутренний нарушитель

При разработке моделей нарушителей целесообразно рассматривать следующие категории внутренних нарушителей:

- Сотрудник Правительства Самарской области, не являющийся санкционированным пользователем защищаемых информационных ресурсов, но имеющий доступ в контролируемую зону;
- Санкционированный пользователь информационных ресурсов ЭП СО, осуществляющий ограниченный доступ к ресурсам ЭП СО с рабочего места, в том числе по распределенным информационным системам (абонент удаленного доступа);
- Санкционированный пользователь информационных ресурсов ЭП СО, имеющий полномочия системного администратора ИС ЭП СО или администратора безопасности ИС ЭП СО;
- Программист–разработчик прикладного обеспечения ИС ЭП СО (лицо, осуществляющее сопровождение системы).

По возможным сценариям воздействия внутренние нарушители могут быть классифицированы как злоумышленники, то есть лица, которые целенаправленно стараются преодолеть систему защиты и нанести ущерб, и нарушители, которые совершают несанкционированные действия неумышленно, но эти действия также могут нанести значительный ущерб и должны учитываться при построении системы защиты.

Возможности внутреннего нарушителя существенным образом зависят от действующих в пределах контролируемой зоны ограничительных факторов, из которых основным является реализация комплекса режимных и организационно-технических мер, направленных на предотвращение и пресечение несанкционированных действий, в том числе, по подбору и расстановке кадров, допуску физических лиц внутрь контролируемой зоны, допуску пользователей к ресурсам информационных систем ЭП СО и контролю за порядком проведения работ.

Возможности нарушителей указанных категорий и основные виды угроз безопасности для информационных ресурсов ЭП СО приведены в следующей таблице:

Категория нарушителя	**Возможности нарушителя**	**Виды угроз безопасности**
1. Сотрудник Правительства Самарской области, не являющийся санкционированным пользователем защищаемых информационных ресурсов, но имеющий доступ в контролируемую зону	1.1. Может располагать информацией о топологии ИС и составляющих ее технических средствах; 1.2. Знает имена санкционированных пользователей защищаемой ИС, и может вести деятельность по выявлению парольно-ключевой информации;	– Нарушение установленных ограничений на распространение информации: – разглашение информации об установленной системе доступа и характере конфиденциальной информации; – копирование конфиденциальной информации под видом санкционированного пользователя. – Сканирование сети с целью выявления уязвимостей и изучения возможностей для проведения атаки; – Воздействие на парольно-ключевые

Категория нарушителя	**Возможности нарушителя**	**Виды угроз безопасности**
	1.3. Может иметь доступ к фрагментам защищаемых данных, распространяемых по внутренним каналам связи; 1.4. Может вносить в ИС программные закладки/вирусы, изменять конфигурацию технических средств ИС	системы защиты информационных систем; – Перехват информации в сетях передачи данных и на линиях связи, навязывание ложной информации; – Внедрение вредоносных программ; – Уничтожение, повреждение, разрушение или хищение носителей с конфиденциальной информацией – Физическое нарушение целостности и/или доступности программно-технических средств.
2. Санкционированный пользователь информационных ресурсов ЭП СО	2.1. Обладает всеми возможностями лиц первой категории; 2.2. Знает по крайней мере один набор легальных идентификационных данных; 2.3. Располагает конфиденциальными данными, к которым имеет доступ; 2.4. Располагает информацией о топологии ИС, к которой имеет доступ, и составляющих ее	– Нарушение установленных ограничений на распространение информации: – разглашение защищаемых сведений; – разглашение информации об установленной системе доступа и характере конфиденциальной информации; – разглашение ключевой информации; – пересылка конфиденциальной информации по электронной почте, http и пр.; – копирование конфиденциальной информации на внешние носители. – Внесение недостоверной

Категория нарушителя	**Возможности нарушителя**	**Виды угроз безопасности**
	технических средствах; 2.5. Имеет физический доступ к некоторым техническим средствам.	информации в ИС (не представление или не своевременное представление данных, ввод неверных данных, модификация или удаление данных); – Уничтожение, повреждение, разрушение или хищение носителей с конфиденциальной информацией; – Внедрение вредоносных программ; – Физическое нарушение целостности и/или доступности программно-технических средств.
3. Администратор ИС ЭП СО и администратор безопасности ИС ЭП СО	3.1. Обладает всеми возможностями лиц предыдущих категорий; 3.2. Располагает полной информацией о топологии ИС, к которой имеет доступ, составляющих ее технических средствах, используемом прикладном и системном ПО; 3.3. Имеет физический доступ ко всем техническим	– Нарушение установленных ограничений на распространение информации: – разглашение информации об установленной системе доступа и характере конфиденциальной информации; – копирование конфиденциальной информации, воспользовавшись чужим именем и паролем или создав временное описание пользователя специально для этих целей; – копирование баз данных и файлов с конфиденциальной информацией на файловом уровне при помощи системных утилит и низкоуровневых программ.

Категория нарушителя	**Возможности нарушителя**	**Виды угроз безопасности**
	средствам; 3.4. Имеет возможность конфигурирования некоторых/всех технических средств и средств защиты.	– Преднамеренные ошибки в выполнении своих должностных функций при описании полномочий пользователей при предоставлении доступа к ресурсам, нарушение политик безопасности средств защиты; – Несанкционированное удаление или модификация ПО, несанкционированная установка и запуск системных утилит и программ; – Воздействие на парольно-ключевые системы защиты информационных систем; – Уничтожение, повреждение, разрушение или хищение носителей с конфиденциальной информацией; – Внедрение вредоносных программ; – Физическое нарушение целостности и/или доступности программно-технических средств; – Умышленное блокирование сервисов или информационных ресурсов системы.
4. Программист – разработчик	4.1. Обладает информацией об алгоритмах обработки данных в ИС; 4.2. Может	– Нарушение установленных ограничений на распространение информации: – разглашение информации об установленной системе доступа и характере конфиденциальной

Категория нарушителя	**Возможности нарушителя**	**Виды угроз безопасности**
	располагать информацией о топологии ИС и составляющих ее технических средствах; 4.3. Имеет возможность внесения программных закладок/недекларированных возможностей в ПО ИС на стадиях ее разработки / модернизации / сопровождения	информации; – копирование конфиденциальной информации на этапах модернизации/сопровождения системы. – Воздействие на парольно-ключевые системы защиты информационных систем; – Внедрение вредоносных программ; – Применение инструментальных средств разработки для несанкционированной модификации рабочего ПО; – Включение в ПО вредоносных недекларированных функций; – Преднамеренные ошибки при установке, настройке или модификации ПО.
5. Внешний нарушитель	5.1. Не имеет доступа в контролируемую зону и к ресурсам ИС ЭП СО; 5.2. Может обладать любыми техническими ресурсами для реализации атак; 5.3. Может располагать некоторыми фрагментами	– Сканирование сети с целью выявления уязвимостей и изучения возможностей для проведения атаки; – Перехват информации в сетях передачи данных и на линиях связи, навязывание ложной информации; – Перехват идентификационных данных; – Криптоанализ информации с целью раскрытия ключей шифрования и электронной цифровой подписи; – Внедрение вредоносных программ;

Категория нарушителя	**Возможности нарушителя**	**Виды угроз безопасности**
	информации о топологии сети ЭП СО	– Атаки отказа в обслуживании с целью превышения допустимой нагрузки функционирования сети, операционной системы или приложения.

В соответствии с руководящими документами ФСТЭК России («Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных», «Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)»), при формировании модели угроз безопасности ИС ЭП СО следует также рассматривать возможности реализации угроз утечки защищаемой информации по техническим каналам (ПЭМИН, видовому и акустическому).

6. Основные пути и методы противодействия угрозам безопасности

Основные пути и методы противодействия угрозам безопасности информационным ресурсам и системам включают:

6.1. Нормативно-методическое обеспечение

Нормативно-методическое обеспечение инфраструктуры информационной безопасности предполагает создание сбалансированной нормативной правовой базы информационной безопасности, включая:

- регламентацию процессов обработки информации, подлежащей защите;
- закрепление в должностных инструкциях установленного разграничения полномочий в области обеспечения безопасности информации;
- определение ответственности подразделений и сотрудников Правительства Самарской области, а также взаимодействующих организаций, за нарушения в области обеспечения безопасности информации (несанкционированный доступ к информации ИС ЭП СО, ее противоправное копирование, искажение и противозаконное использование, преднамеренное распространение недостоверной информации, противоправное раскрытие конфиденциальной информации).

6.2. Организационное обеспечение

Организационное обеспечение инфраструктуры информационной безопасности предполагает:

- формирование программы работ в области ИБ с учетом жизненного цикла информационных систем ЭП СО, обеспечение ее выполнения

и контроля состояния;

- создание (совершенствование) штатной структуры информационной безопасности;
- организацию системы подготовки (повышения квалификации) специалистов для эксплуатации систем и средств защиты;
- обучение персонала соблюдению принятой политики безопасности и практическим действиям в нештатных ситуациях;
- проведение единой технической политики в области обеспечения информационной безопасности;
- организацию сертификации средств защиты/аттестации информационных систем по требованиям ФСТЭК/ФСБ России;
- разработку и внедрение организационных мер защиты;
- контроль эффективности и достаточности принимаемых мер защиты, организация актуализации регламентов обработки и защиты информации в связи с постоянным развитием ЭП СО и изменяющимися источниками угроз;
- организацию процесса расследования инцидентов безопасности.

6.3. Технологическое обеспечение

Технологическое обеспечение инфраструктуры информационной безопасности предполагает:

- разработку (обоснованный выбор) технологий и средств защиты;
- создание инфраструктурных компонентов системы информационной безопасности;
- оснащение объектов информатизации ЭП СО средствами защиты и системами безопасности.

Средства защиты и системы безопасности, составляющие инфраструктуру информационной безопасности в ЭП СО, а также применяемые организационные мероприятия по защите информации, должны обеспечивать предотвращение или существенное затруднение реализации обозначенных угроз безопасности:

Тип нарушителя	**Характерные методы воздействия**	**Основные способы защиты**
1. Сотрудник Правительства Самарской области, не являющийся санкционированным пользователем защищаемых информационных ресурсов, но имеющий доступ в контролируемую зону	Нарушение установленных ограничений на распространение информации: – разглашение информации об установленной системе доступа и характере конфиденциальной информации; – копирование конфиденциальной информации под видом санкционированного пользователя. Сканирование сети с целью выявления уязвимостей и изучения возможностей для проведения атаки; Воздействие на парольно-ключевые системы защиты информационных систем; Перехват информации в сетях передачи данных и на линиях связи, навязывание ложной информации;	– введение разграничительной системы доступа в помещения, к информационным и вычислительным ресурсам и носителям информации – введение ограничений на подключение внешних носителей – введение ограничений на вывод информации из информационных систем на печать – физическая защита оборудования – антивирусная защита рабочих станций – активный мониторинг событий безопасности – пассивная или активная система обнаружения вторжений (IDS/IPS)

Тип нарушителя	Характерные методы воздействия	Основные способы защиты
	Внедрение вредоносных программ; Уничтожение, повреждение, разрушение или хищение носителей с конфиденциальной информацией Физическое нарушение целостности и/или доступности программно-технических средств.	
2. Санкционированный пользователь информационных ресурсов ЭП СО	Нарушение установленных ограничений на распространение информации: – разглашение защищаемых сведений – разглашение информации об установленной системе доступа и характере конфиденциальной информации – разглашение ключевой информации – пересылка конфиденциальной информации по электронной почте, http, IM, VoIP – копирование конфиденциальной	– введение разграничительной системы доступа в помещения, к информационным и вычислительным ресурсам и носителям информации – контроль целостности программного обеспечения рабочих станций и наличия несанкционированных программ – использование криптографических средств аутентификации пользователей и ресурсов – регистрация действий пользователей в системных журналах – физическая защита оборудования – введение ограничений на подключение внешних

Тип нарушителя	Характерные методы воздействия	Основные способы защиты
	информации на внешние носители Внесение недостоверной информации в ИС ЭП СО (не представление или не своевременное представление данных, ввод неверных данных, модификация или удаление данных) Уничтожение, повреждение, разрушение или хищение носителей с конфиденциальной информацией Внедрение вредоносных программ Физическое нарушение целостности и/или доступности программно-технических средств	носителей – введение ограничений на вывод информации из информационных систем на печать – антивирусная защита рабочих станций – регулярная смена паролей и ключей – физическая защита оборудования – резервное копирование данных – контроль выполнения должностных функций – контроль вносимой в ИС ЭП СО информации
3. Администратор ИС ЭП СО и администратор безопасности ИС ЭП СО	Нарушение установленных ограничений на распространение информации: – разглашение информации об установленной системе доступа и характере конфиденциальной информации – копирование	– разделение полномочий управления системами разграничения доступа между несколькими администраторами систем, передача управления ключевой информацией администраторам безопасности – активный мониторинг и аудит сети – контроль возможности изменения полномочий

Тип нарушителя	Характерные методы воздействия	Основные способы защиты
	конфиденциальной информации, воспользовавшись чужим именем и паролем или создав временное описание пользователя специально для этих целей – копирование баз данных и файлов с конфиденциальной информацией на файловом уровне при помощи системных утилит и низкоуровневых программ Преднамеренные ошибки в выполнении своих должностных функций при описании полномочий пользователей при предоставлении доступа к ресурсам, нарушение политик безопасности средств защиты Несанкционированное удаление или модификация ПО, несанкционированная установка и запуск системных утилит и программ	пользователей только при наличии разрешительного документа от владельца информационного ресурса – защита системных регистрационных журналов от модификации и уничтожения – контроль использования системных утилит – контроль целостности ПО и отсутствия несанкционированных программ – физическая защита оборудования – антивирусная защита рабочих станций и серверов – резервное копирование системных и информационных файлов

Тип нарушителя	Характерные методы воздействия	Основные способы защиты
	Воздействие на парольно-ключевые системы защиты информационных систем Уничтожение, повреждение, разрушение или хищение носителей с конфиденциальной информацией Внедрение вредоносных программ Физическое нарушение целостности и/или доступности программно-технических средств Умышленное блокирование сервисов или информационных ресурсов системы	
4. Программист – разработчик	Нарушение установленных ограничений на распространение информации: – разглашение информации об установленной системе доступа и характере конфиденциальной информации – копирование конфиденциальной информации на этапах	– введение разграничительной системы доступа в помещения, к информационным и вычислительным ресурсам и носителям информации – разделение сред разработки ПО и рабочих сетей – определение формализованных процедур приемки новых систем, модификации и замены рабочего ПО – контроль работоспособности системы и системы защиты после внесения изменений в

Тип нарушителя	Характерные методы воздействия	Основные способы защиты
	модернизации/сопровождения системы Воздействие на парольно-ключевые системы защиты информационных систем Внедрение вредоносных программ Применение инструментальных средств разработки для несанкционированной модификации рабочего ПО Включение в ПО вредоносных недекларированных функций Преднамеренные ошибки при установке, настройке или модификации ПО	рабочее ПО – пользователей в системных журналах – физическая защита оборудования – сертификация разрабатываемого ПО на отсутствие недекларированных возможностей – удаление из рабочих сетей всех средств разработки ПО – хранение и сопровождение всех используемых версий ПО – антивирусная защита рабочих станций – контроль целостности программного обеспечения рабочих станций и наличия несанкционированных программ – регистрация действий пользователей – регулярная смена паролей и ключей – физическая защита оборудования
5. Внешний нарушитель	Сканирование сети с целью выявления уязвимостей и изучения возможностей для проведения атаки Перехват информации в сетях	– использование сканеров безопасности для своевременного обнаружения уязвимостей – отключение неиспользуемых

Тип нарушителя	Характерные методы воздействия	Основные способы защиты
	передачи данных и на линиях связи, навязывание ложной информации Перехват идентификационных данных Криптоанализ информации с целью раскрытия ключей шифрования и электронной цифровой подписи Внедрение вредоносных программ DoS атаки с целью превышения допустимой нагрузки функционирования сети, операционной системы или приложения	сервисов – межсетевое экранирование, NAT – использование VPN – использование защищенных протоколов – использование средств обнаружения и предотвращения вторжений (IDS/IPS) – активный мониторинг внешнего периметра сети – антивирусная защита межсетевых экранов и WWW – серверов – фильтрация электронной почты и Web - ресурсов – использование ЭЦП – использование средств шифрования трафика сети и шифрования электронных документов – регулярная смена паролей и ключей – резервное копирование информации – резервное копирование настроек средств защиты

7. Структура системы обеспечения информационной безопасности в электронном правительстве Самарской области

Система обеспечения безопасности информации в электронном правительстве Самарской области включает четыре основных элемента:

- документационное обеспечение СОИБ (политику безопасности ЭП СО);
- организационно-штатную структуру СОИБ, то есть сотрудников, проводящих политику безопасности в жизнь;
- инженерно-технические и аппаратно-программные средства защиты, системы безопасности и технологии защиты информации. программно-аппаратные средства защиты и технологические системы безопасности, средства аудита и мониторинга информационной безопасности, обеспечивающие защиту информационных ресурсов ЭП СО;
- процедуры планирования, координации деятельности и контроля в области обеспечения информационной безопасности.

7.1. Документационное обеспечение СОИБ

В рамках пакета документов, фиксирующих и обеспечивающих реализацию требований необходимого уровня безопасности на объектах информатизации ЭП СО, должны быть разработаны:

- документы, регламентирующие работу с информацией и документами в информационных системах;
- инструкции (правила, рекомендации) по оформлению, категорированию, учету и правилам предоставления доступа к информационным ресурсам;

- регламенты взаимодействия с другими организациями (ведомствами) и пользователями предоставляемых в электронном виде ГУ;
- должностные регламенты, устанавливающие ответственность должностных лиц за обеспечение безопасности информации/работу с защищаемой информацией;
- регламенты контроля исполнения требований ИБ, мониторинга текущего состояния и развития СОИБ.

7.2. Штатная структура обеспечения безопасности информации

Штатная структура обеспечения безопасности информации должна предусматривать наличие нескольких уровней организационной структуры.

На первом уровне организационной структуры решаются стратегические вопросы обеспечения безопасности информации в ЭП СО, вопросы технической политики в области средств защиты, принимаются стандарты безопасности, осуществляется координация действий структурных подразделений и контроль эффективности принимаемых мер защиты.

Ко второму уровню относятся сотрудники подразделений, отвечающих за безопасность информации и обеспечивающих разграничительную систему доступа к защищаемым ресурсам информационных подсистем ЭП СО. На втором уровне организационной структуры:

- решаются практические вопросы текущего планирования и управления безопасностью информации;
- осуществляется организация и контроль проведения в жизнь принятой политики безопасности;
- проводится контроль принимаемых защитных мер и расследование случаев нарушения безопасности информации;

- проводятся другие необходимые технические и организационные мероприятия.

К третьему уровню относятся администраторы информационных систем, администраторы безопасности и пользователи информационных систем ЭП СО, имеющие доступ к защищаемым ресурсам. На третьем уровне решаются вопросы:

- администрирования и технического обслуживания конкретных технических средств защиты информации, входящих в СОИБ;
- реализации сотрудниками ЭП СО установленных правил информационной безопасности, определенных в положениях/регламентах по защите информационных ресурсов и должностных инструкциях.

7.3. Концептуальные технические решения по использованию средств защиты информации в ЭП СО

Основными задачами, возлагаемыми на системы и средства защиты СОИБ, являются:

- аутентификация сторон, производящих обмен информацией (подтверждение подлинности отправителя и получателя);
- разграничение прав при доступе к информационным ресурсам ИС ЭП СО, а также при хранении и предоставлении конфиденциальной информации, в том числе защиту от несанкционированного доступа пользователей ведомственных информационных систем к информационным ресурсам ЭП СО;
- возможность доказательства неправомочности действий пользователей и обслуживающего персонала ИС ЭП СО;
- защита сетевой инфраструктуры на основе выделенной локальной

сети либо на основе виртуальной частной сети;

- защита серверов, автоматизированных рабочих мест и телекоммуникационного оборудования информационных систем от несанкционированного доступа к их ресурсам, вредоносного программного обеспечения и сетевых атак, осуществляемых из внешних сетей;
- защита накапливаемой информации от несанкционированного удаления, изменения, ознакомления и копирования;
- защита целостности и конфиденциальности информации при ее передаче по каналам связи;
- обеспечение достоверности и подтверждение авторства информации, размещаемой в информационных ресурсах;
- обеспечение доступности вычислительных и коммуникационных ресурсов, дублирование информации путем создания резервных копий;
- антивирусная защита программного и информационного обеспечения;

- возможность управления именами, идентификационными параметрами и криптографическими ключами;
- применение средств и систем защиты, сертифицированных ФСТЭК или ФСБ России.

Для выполнения данных задач структура комплексной системы безопасности информации ЭП СО должна включать:

- подсистему управления доступом к ресурсам ИС ЭП СО;
- инфраструктуру открытых ключей;

- подсистему криптографической защиты информации;
- подсистему защиты компонентов сетевой инфраструктуры ЭП СО;
- подсистему анализа защищенности;
- подсистему мониторинга и регистрации;
- подсистему антивирусной защиты;
- инженерно-технические системы безопасности.

В качестве интеграционной основы построения системы защиты информационных ресурсов ЭП СО от НСД целесообразно использование технологий инфраструктуры открытых ключей (PKI), цифровых сертификатов, средств шифрования и электронной цифровой подписи.

Развертывание инфраструктуры PKI и централизованное использование средств криптографической защиты информации обеспечит решение вопросов надежной аутентификации пользователей и серверов, защиту конфиденциальной информации при ее передаче по каналам связи, контроль подлинности и целостности электронных документов, обеспечение юридически значимого электронного документооборота. Эта технология обеспечит единые подходы защищенного обмена электронными документами как внутри ЭП СО, между ЭП СО и взаимодействующими ведомствами, так и с внешними пользователями ГУ, оказываемых в электронном виде.

Для создания СОИБ электронного правительства Самарской области целесообразно задействовать уже развернутые в Самарской области решения по обеспечению ИБ. Средства обеспечения ИБ электронного правительства Самарской области должны быть интегрируемы с продуктами обеспечения ИБ, используемыми в других ведомствах (это касается, в частности средств организации инфраструктуры открытых ключей).

При выборе средств обеспечения ИБ в ЭП СО необходимо учитывать необходимость наличия сертификатов соответствия этих средств требованиям безопасности ФСТЭК и/или ФСБ.

7.3.1. Требования к Подсистеме управления доступом

Подсистема управления доступом должна предусматривать:

- индивидуальную идентификацию и аутентификацию пользователей при доступе к информационным ресурсам;
- поддержку различных методов аутентификации, в том числе с использованием сертификатов открытых ключей;
- возможность использования различных ключевых носителей;
- разграничение доступа пользователей к ресурсам рабочих станций, серверов баз данных и прикладных информационных систем;
- эффективное управление правами доступа и идентификацией пользователей информационных систем.

Подсистема управления доступом должна иметь возможность интегрировать:

- сервер аутентификации;
- LDAP-каталог пользователей системы;
- средства управления ключевыми носителями;
- штатные средства управления учетными записями и правами пользователей сетевых операционных систем;
- штатные средства управления учетными записями и правами пользователей систем управления базами данных;
- штатные средства управления учетными записями и правами пользователей используемых прикладных систем;

- дополнительные средства контроля устройств ввода/вывода.

Сервер аутентификации должен обеспечивать:

- возможность аутентификации пользователей на основе сертификатов открытых ключей;
- использование в качестве реестра пользователей единого каталога пользователей системы.

Каталог пользователей системы должен обеспечивать:

- масштабируемое хранилище информации о пользователях, основанное на стандартах LDAP;
- управление всем жизненным циклом информации о пользователях (заведение, изменение и удаление) из единой точки;
- средства автоматической синхронизации информации о пользователях между реестрами различных приложений и операционных систем;
- средства делегирования полномочий по администрированию пользователей;
- средства интеграции с другими системами безопасности, например, с системами контроля доступа в помещения.

Средства управления ключевыми носителями должны позволять с минимальными затратами времени и средств выполнять основные задания по комплексному управлению носителями ключевой информации, в том числе:

- создавать, импортировать, экспортировать, редактировать учётные записи пользователей;
- назначать пользователям ключевые носители;
- записывать в памяти этих устройств сертификаты открытого ключа

и закрытые ключи;

- обновлять, отзывать сертификаты;
- разблокировать устройства;
- управлять полномочиями пользователей.

Носители ключевой информации должны использоваться как единое хранилище сертификатов пользователей для доступа к АРМ и информационным ресурсам, для защиты электронных документов (ЭЦП, шифрование), для установления защищенных соединений (VPN, SSL).

Штатные средства управления учетными записями и правами пользователей операционных систем, СУБД и прикладных систем должны использоваться для разграничения доступа пользователей к ресурсам рабочих станций, серверов и информационных систем.

7.3.2. Требования к Инфраструктуре открытых ключей

Инфраструктура открытых ключей должна обеспечивать централизованное управление криптографическими ключами и цифровыми сертификатами, и может включать Удостоверяющий Центр, центр(ы) регистрации, АРМы генерации закрытых и открытых криптографических ключей, сервер публикации сертификатов открытых ключей, на котором могут находиться сертификаты открытых ключей и списки отозванных сертификатов, серверное и клиентское программное обеспечение, поддерживающее работу с сертификатами открытых ключей.

Инфраструктура открытых ключей должна обеспечивать:

- работу ключевой системы;
- генерацию пар закрытого и открытого криптографических ключей для каждого участника информационного обмена;
- формирование электронных сертификатов открытых ключей

пользователей в формате X.509v3 и ключей подписи на основе алгоритма ГОСТ Р 34.10-2001;

- регистрацию пользователей системы, заверение и публикацию цифровых сертификатов с открытыми ключами участников информационного обмена;
- формирование и доставку зарегистрированным пользователям списка отозванных сертификатов открытых ключей пользователей;
- отзыв и выпуск списков отозванных сертификатов;
- криптографическую аутентификацию пользователей и ресурсов по цифровым сертификатам;
- регламент и программно-технические средства разрешения конфликтных ситуаций.

Сервер Удостоверяющего центра (УЦ) должен обеспечивать:

- создание ключей подписи и издание сертификатов уполномоченных лиц УЦ;
- импорт сертификатов Уполномоченных лиц УЦ смежных сетей и головного УЦ;
- создание ключей подписи пользователей и издание соответствующих сертификатов, рассмотрение запросов на издание сертификатов от пользователей сети;
- взаимодействие с Центрами регистрации;
- выполнение операций по отзыву, приостановлению и возобновлению сертификатов, рассылка соответствующих списков отзыва;
- ведение журналов работы и хранение списков изданных сертификатов;

- запись сертификатов и секретных ключей пользователей на аппаратные носители ключей;
- возможность кросс-сертификации с УЦ других производителей, используемых в других ведомствах Самарской области.

Центр регистрации должен обеспечивать:

- регистрацию пользователей защищенной сети и внешних пользователей (держателей ЭЦП);
- формирование секретного ключа подписи пользователя и его запись на аппаратный носитель ключевой информации;
- формирование и отправку в УЦ запроса на сертификацию подписи от своего имени (Уполномоченного лица Центра регистрации), прием и ввод в действие;
- ведение справочника запросов и изданных сертификатов;
- формирование запросов на отзыв, приостановление и возобновление сертификатов зарегистрированных пользователей;
- ведение журналов работы и хранение списков изданных сертификатов;
- ведение журнала событий и действий Уполномоченного лица Центра регистрации;
- импорт учетных записей пользователей из LDAP-каталога.

Сервер публикации сертификатов открытых ключей должен обеспечивать:

- публикацию списков отозванных сертификатов;
- публикацию списков изданных сертификатов пользователей и Уполномоченных лиц;

- обеспечение публикации (экспорта) и импорта сертификатов пользователей через стандартные транспортные протоколы (LDAP, FTP);
- формирование отчетов о публикации сертификатов Уполномоченных лиц для УЦ с целью включения этой информации в сертификаты пользователей.

Цифровые сертификаты, выпускаемые УЦ, могут быть использованы для:

- реализации функций шифрования, формирования ЭЦП;
- обеспечения однократной аутентификации при доступе к домену Windows;
- аутентификации компонент VPN-инфраструктуры.

7.3.3. Требования к Подсистеме криптографической защиты информации

Подсистема криптографической защиты должна предусматривать распределенные программно-технические средства криптографической защиты информации, обеспечивающие:

- возможности шифрования/расшифрования блоков оперативной памяти, файлов, электронных документов, сетевых пакетов или сетевого трафика;
- установку и проверку электронных цифровых подписей под электронными документами и файлами;
- проверку целостности программного и информационного обеспечения на основе использования криптографических методов;
- передачу информации по защищенным протоколам типа TLS и IPSec;

- создание криптографических туннелей между удаленными объектами и пользователями для защиты информации при передаче по каналам связи;
- идентификацию и аутентификацию пользователей и ресурсов ИС ЭП СО на основе использования криптографических способов.

Ключевая система шифрования и подписи должна строиться по принципу открытого распределения ключей. Генерация и управление ключевой информацией должны обеспечиваться инфраструктурой открытых ключей.

Алгоритм шифрования должен быть выполнен в соответствии с требованиями ГОСТ-28147-89 «Системы обработки информации. Защита криптографическая». Цифровая подпись должна быть выполнена в соответствии с требованиями ГОСТ Р 34.10-2001 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи».

Все предлагаемые средства криптографической защиты информации должны иметь сертификаты ФСБ.

7.3.4. Требования к Подсистеме защиты компонентов сетевой инфраструктуры

Подсистема защиты компонентов сетевой инфраструктуры должна обеспечивать:

- сегментирование и защиту сегментов ЛВС ЭП СО от НСД для организации обработки конфиденциальной информации (персональных данных);

- выделение демилитаризованной зоны для размещения серверов, которые должны быть доступны из открытых и внешних телекоммуникационных сетей;
- выявление и предотвращение атак на ресурсы ЭП СО со стороны открытых и внешних телекоммуникационных сетей;
- идентификацию и аутентификацию устройств и служб в сети;
- разграничение доступа пользователей к узлам сети и сервисам;
- централизованное администрирование средств защиты от НСД;
- регистрацию системных событий и попыток НСД к защищаемым ресурсам штатными и наложенными средствами.

Подсистема защиты компонентов сетевой инфраструктуры может включать:

- средства межсетевого экранирования и организации виртуальных частных сетей (VPN);
- средства обнаружения и предотвращения вторжений (IDS/IPS);
- штатные средства разграничения доступа активного коммуникационного оборудования сети.

Средства межсетевого экранирования и организации виртуальных частных сетей должны обеспечивать выполнение следующих функций:

- поддержку межсетевого взаимодействия с удалёнными организациями;
- защиту транзитного трафика между удалёнными пользователями и узлами сети;
- пакетную фильтрацию трафика.

Средства обнаружения и предотвращения вторжений должны обеспечивать выполнение следующих функций:

- мониторинг объектов защиты на сетевом, транспортном и прикладном уровнях;
- мониторинг используемых сетевых сервисов;
- выявление и блокирование атак;
- выдача рекомендаций по изменению конфигурации компонентов защиты при обнаружении неблокируемых атак;
- фиксация описаний выявленных атак;
- информирование администратора безопасности при регистрации в журнале аудита событий, нарушающих политику безопасности компонентов ИС ЭП СО.

Аутентификация и авторизация служб и программных компонент обеспечивается за счет реализации стандартов безопасности передачи данных с использованием цифровых сертификатов.

Разграничение доступа к сервисам обеспечивается расположением компонентов и служб сервиса в отдельном сегменте сети с использованием штатных средств активного коммуникационного оборудования сети и применения технологий VLAN.

Для реализации защищённого входа в сеть может применяться ПО защищённого доступа, обеспечивающее аутентификацию пользователей на компьютере и в сети Windows с помощью носителей ключевой информации и использование цифровых сертификатов X.509 для входа в домен.

7.3.5. Требования к Подсистеме анализа защищенности

Подсистема анализа защищенности должна обеспечивать выполнение следующих функций:

- инвентаризацию элементного состава ИС ЭП СО, который может подвергаться анализу защищенности;
- анализ настроек и выявление уязвимостей объектов сетевой инфраструктуры ЭП СО;
- контроль изменений в конфигурациях элементов ИС;
- контроль целостности программных средств и среды исполнения;
- регистрацию в журнале аудита событий, нарушающих политику безопасности компонентов ИС ЭП СО.

Анализ защищенности должен обеспечиваться специализированными средствами анализа уязвимостей.

Контроль целостности программных средств и среды исполнения должен обеспечиваться средствами автопроверки программных компонентов, проверками контрольных сумм фалов и средствами обеспечения целостности программной среды серверных операционных систем.

7.3.6. Требования к Подсистеме регистрации и мониторинга

Подсистема регистрации и мониторинга должна использоваться для регистрации действий пользователей по доступу к защищаемым ресурсам, и мониторинга состояния элементов технической инфраструктуры, на которых обрабатывается защищаемая информация. Подсистема регистрации и мониторинга должна обеспечивать выполнение следующих функций:

- регистрацию запуска приложений, используемых для обработки защищаемой информации, попыток доступа к защищаемым файлам;
- настройку списка контролируемых событий и уровень детализации записей журнала аудита;
- централизованный сбор событий безопасности и

автоматизированный разбор данных аудита.

Подсистема регистрации и мониторинга должна интегрировать:

- штатные средства операционных систем и систем управления базами данных (регистрация событий доступа, загрузки или останова систем);
- штатные средства используемых прикладных систем (регистрация событий попыток доступа пользователей и программных компонентов к защищаемым ресурсам);
- штатные средства межсетевых экранов, маршрутизаторов и другого коммуникационного оборудования (регистрация событий доступа к ресурсам сети).

Подсистема регистрации и мониторинга должна иметь возможность использовать специализированное ПО активного мониторинга событий ИБ.

7.3.7. Требования к подсистеме резервного копирования и архивирования

Подсистема резервного копирования и архивирования должна соответствовать следующим требованиям:

- резервное копирование и архивирование должно быть организовано для всех информационных ресурсов, указанных в регламентах резервного копирования;
- должно проводиться регулярное тестирование резервных копий.

Резервное копирование общесистемного и прикладного ПО должно обеспечиваться отдельными аппаратными средствами резервного копирования, либо средствами, встроенными в данное ПО.

Резервное копирование БД должно обеспечиваться за счет использования встроенных средств резервного копирования СУБД или аппаратных решений для резервного копирования данных.

7.3.8. Требования к подсистеме антивирусной защиты

Подсистема антивирусной защиты должна обеспечивать надежный контроль над всеми потенциальными источниками проникновения вредоносных программ в ИС ЭП СО, максимально автоматизировать антивирусную защиту компьютеров и локальной сети, а также обеспечить централизованное управление всеми антивирусными продуктами.

Эта подсистема должна соответствовать следующим требованиям. Она должна выполнять:

- антивирусную защиту рабочих станций;
- антивирусную защиту файловых серверов;
- антивирусную защиту электронной почты;
- антивирусную защиту шлюзов Интернет;
- антивирусную защиту Web серверов.

При этом желательно организовать двухуровневую антивирусную защиту с применением антивирусного ПО различных производителей.

Подсистема антивирусной защиты должна обеспечивать:

- централизованное управление сканированием, удалением вирусов и протоколированием вирусной активности;
- централизованную автоматическую инсталляцию клиентского ПО на АРМ пользователей;
- централизованное автоматическое обновление вирусных сигнатур на АРМ пользователей;
- возможность обнаружения и удаления вирусов в режиме реального времени при работе с информационными ресурсами серверов;
- возможность выявления вирусной активности в режиме реального

времени при осуществлении связи с сетями общего пользования по протоколам SMTP, HTTP и FTP;

- ведение журналов вирусной активности в ИС ЭП СО;
- автоматическое уведомление администратора по электронной почте о вирусной активности;
- администрирование всех антивирусных продуктов, установленных в сети.

7.3.9. Решения по использованию инженерно-технических систем безопасности

Инженерно-техническая защита объектов должна обеспечивать:

- разграничение доступа сотрудников на объекты (в здания, помещения и т.п.) в соответствии с назначенными полномочиями;
- предотвращение несанкционированного проникновения на защищаемые объекты злоумышленников и нарушителей (затруднение проникновения, сигнализация о попытках проникновения и прорывах рубежа охраны с локализацией места и времени нарушения);
- пожарную безопасность объектов.

Требуемый уровень защищенности конкретного объекта в общем случае должен определяться важностью (ценностью) защищаемого ресурса и характером значимых угроз его безопасности.

В следующей таблице представлено условное категорирование помещений, подлежащих защите, по важности защищаемых ресурсов, а также технические предложения по используемым средствам инженерно-технической защиты.

Объекты защиты	**Рекомендуемые средства защиты**
- Серверные помещения инфраструктуры ЭП СО - Помещения, предназначенные для генерации криптографических ключей	- Система охранной сигнализации - Система пожарной сигнализации - Система контроля доступа - Возможно оснащение системой видеонаблюдения - Автоматическая система пожаротушения (АСПТ) - Инженерные средства защиты, выполненные из высокоустойчивых к разрушению конструкционных материалов (замки, решетки, жалюзи) - Оборудование сейфами
- Помещения ЛВС, отдельных АРМ, где обрабатывается конфиденциальная информация (рабочие станции) - Помещения, в которых проходят кабельные трассы (стояки, шкафы и т.п.) ЛВС, обрабатывающих конфиденциальную информацию	- Система охранной сигнализации - Система пожарной сигнализации - Система контроля доступа - Возможно оснащение АСПТ - Инженерные средства защиты (решетки, жалюзи) - Оснащение сейфами
- Помещения персонала объектов - Лестницы, коридоры	- Система охранной сигнализации - Система пожарной сигнализации - Система контроля доступа

7.3.10. Решения по защите от утечки информации по техническим каналам

Технические решения должны быть направлены на закрытие каналов утечки информации путем ослабления (снижения) уровня информативных сигналов или уменьшения отношения сигнал/шум в местах возможного размещения портативных средств разведки или их датчиков до величин, обеспечивающих невозможность выделения информативного сигнала средствами разведки, и должны проводиться по возможности с использованием пассивных средств.

К основным организационным мероприятиям по организации защиты объектов информатизации ЭП СО от утечки информации по техническим каналам относятся:

- привлечение к работам по защите информации организаций, имеющих лицензию на деятельность в области технической защиты информации, выданную соответствующими органами;
- привлечение к работам по строительству, реконструкции объектов информатизации, монтажу аппаратуры организаций, имеющих лицензию на деятельность в области технической защиты информации по соответствующим пунктам;
- организация контроля и ограничение доступа на объекты информатизации и в защищаемые помещения;
- размещение объектов защиты на максимальном расстоянии относительно границ контролируемой зоны;
- конструктивные доработки технических средств и помещений, где они расположены, в целях локализации возможных каналов утечки информации;
- размещение понижающих трансформаторных подстанций электропитания и контуров заземления объектов защиты в пределах

контролируемой зоны или применение сетевых фильтров.

Предотвращение утечки обрабатываемой информации за счет побочных электромагнитных излучений и наводок, а также за счет электроакустических преобразований должно реализовываться при необходимости по результатам объектовых исследований путем применения защищенных технических средств, сертифицированных по требованиям безопасности информации, внедрением объектовых мер защиты, в том числе установлением контролируемой зоны вокруг объекта защиты, средств активного противодействия и др.

Конкретные требования к мерам объектовой защиты определяются по результатам специальных исследований технических средств с учетом степени конфиденциальности обрабатываемой информации и условий ее размещения.

7.4. Организационные меры по эксплуатации СОИБ

Эксплуатация СОИБ ЭП СО должна осуществляться в рамках согласованных мероприятий принятой политики безопасности и функционирования комплексной системы безопасности информации ЭП СО на основании разработанных регламентов, должностных инструкций обслуживающего персонала СОИБ и пользователей ЭП СО.

Организационные меры по эксплуатации СОИБ ЭП СО должны охватывать следующие основные направления:

- разработка (совершенствование) системы документов, регламентирующих вопросы эксплуатации СОИБ;
- назначение и подготовку должностных лиц (сотрудников), ответственных за организацию и осуществление практических мероприятий по обеспечению безопасности информации и процессов ее обработки;

- инвентаризация, классификация и учет подлежащих защите ресурсов (информации, задач, каналов связи, серверов, автоматизированных рабочих мест и т.д.);
- организация и контроль процессов присвоения, внесения в систему разграничения доступа СОИБ, модификации и удаления полномочий пользователей по доступу к информационным системам и информации ЭП СО;
- организация процессов изменения настроек средств защиты, в связи с постоянным развитием ЭП СО (подключением новых объектов, пользователей, IP-адресов, внедрением ИС и т.д.);
- организация процессов оперативного контроля за работой средств защиты и разработку мер своевременного реагирования на выявленные факты нарушения информационной безопасности;
- организация периодического контроля работоспособности и технического обслуживания средств защиты;
- организация своевременного копирования и хранения информационных настроек средств защиты с целью возможности быстрого восстановления компонентов СОИБ при сбоях оборудования или возникновении нештатных ситуаций;
- периодический контроль соответствия реальных настроек средств защиты и настроек предписанных политикой безопасности (эталонных настроек);
- организация процессов своевременного обновления программного и информационного обеспечения средств защиты (патчей программного обеспечения, обновления баз данных антивирусных сигнатур и сигнатур сетевых атак, и т.д.);
- организация процесса обучения обслуживающего персонала

правилам эксплуатации и технического обслуживания средств защиты;

- организация процесса обучения пользователей работе со средствами защиты;
- контроль эффективности и достаточности принимаемых мер защиты в связи с постоянным развитием ЭП СО и изменяющимися источниками угроз;
- организация процесса расследования инцидентов и нарушений установленных регламентов и инструкций по обеспечению безопасности;
- организация сертификации средств защиты информации, контроль за использованием лицензионного программного обеспечения.

7.5. Специальные требования по организации защиты информационных систем персональных данных

Специальные мероприятия по обеспечению безопасности персональных данных при их обработке в ИСПДн ЭП СО должны включать:

- определение и документирование перечня персональных данных, обрабатываемых в ИСПДн;
- определение необходимости получения письменных согласий субъектов на обработку их персональных данных в ИС ЭП СО;
- формирование частных моделей угроз ИСПДн на основе Методики определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных и Базовой модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденных ФСТЭК России;

- учет лиц, допущенных к работе с персональными данными в информационной системе;
- разработку регламентов (положений) обработки и защиты персональных данных;
- учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных;
- классификацию ИСПДн в соответствии с Порядком проведения классификации информационных систем персональных данных;
- проведение работ по защите ИСПДн организациями, имеющими лицензию на деятельность в области технической защиты конфиденциальной информации ФСТЭК России;
- описание системы защиты персональных данных;
- организацию аттестации объектов информатизации по требованиям безопасности информации.

8. Список используемых сокращений

АРМ	Автоматизированное рабочее место
ГУ	Государственная услуга
ИБ	Информационная безопасность
ИС	Информационная система
ИСПДн	Информационная система персональных данных
ИШ ЭП СО	Интеграционная шина электронного правительства Самарской области
НСД	Несанкционированный доступ
ПДн	Персональные данные
ПО	Программное обеспечение
ПЭМИН	Побочные электромагнитные излучения и наводки
СКЗИ	Средства криптографической защиты информации
СОИБ	Система обеспечения информационной безопасности
ТЗ	Техническое задание
ФСТЭК России	Федеральная служба по техническому и экспертному контролю
ЭП СО	Электронное правительство Самарской области
PKI	Public Key Infrastructure - Инфраструктура открытых ключей
VLAN	Virtual Local Area Network - Виртуальная локальная сеть
VPN	Virtual Private Network — Виртуальная частная сеть

9. Глоссарий

Аттестация объектов информатизации	Комплекс организационно-технических мероприятий, в результате которых специальным документом - Аттестатом соответствия подтверждается, что объект соответствует требованиям стандартов или иных нормативно-технических документов по безопасности информации, утвержденных ФСТЭК России.
Безопасность информации	Состояние защищенности информации, характеризуемое способностью персонала, технических средств и информационных технологий обеспечивать конфиденциальность, т.е. сохранение в тайне от субъектов, не имеющих полномочий на ознакомление с ней, целостность и доступность информации при ее обработке техническими средствами. (СТР-К).
Документированная информация (документ)	Зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать. (ФЗ «Об информации, информатизации и защите информации»).
Доступ к информации (доступ)	1) получение субъектом возможности ознакомления с информацией, в том числе с помощью технических средств; 2) ознакомление с информацией, ее обработка, в частности, копирование, модификация или уничтожение информации (ГОСТ Р 50922-2006).

Доступность информации	Состояние информации, характеризуемое способностью АС обеспечивать беспрепятственный доступ к информации субъектов, имеющих на это полномочия (СТР-К).
Защита информации (ЗИ)	Деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию (ГОСТ Р 50922-2006).
Защита информации от НСД	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. Примечание. Заинтересованным субъектом, осуществляющим несанкционированный доступ к защищаемой информации, может быть: государство; юридическое лицо; группа физических лиц, в том числе общественная организация, отдельное физическое лицо. (ГОСТ Р 50922-2006).
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 (ГОСТ Р 50922-2006).

Информационная безопасность	Состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государства. (Федеральный закон «Об участии в международном информационном обмене»).
Информационная система	Организационно упорядоченная совокупность документов (массивов документов) и информационных технологий, в том числе с использованием средств вычислительной техники и связи, реализующих информационные процессы. (Федеральный закон «Об информации, информатизации и защите информации»).
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 (ФЗ 152)
Информационная технология	Приемы, способы и методы применения средств вычислительной техники при выполнении функций хранения, обработки, передачи и использования данных (ГОСТ 34.003-90).
Информационные услуги	Действия субъектов (собственников и владельцев) по обеспечению пользователей информационными продуктами. (Федеральный закон «Об участии в международном информационном обмене»).

Информационные ресурсы	Отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных, других информационных системах) (Федеральный закон «Об информации, информатизации и защите информации»).
Информация	Сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления. (Федеральный закон «Об информации, информатизации и защите информации»).
Коммерческая тайна	1) информация составляет служебную или коммерческую тайну в случае, когда информация имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к ней нет свободного доступа на законном основании и обладатель информации принимает меры к охране ее конфиденциальности; 2) сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с Гражданским кодексом Российской Федерации; («Гражданский кодекс Российской Федерации», Перечень сведений конфиденциального характера: Утвержден Указом Президента Российской Федерации №188 от 6 марта 1997 г).

Конфиденциальная информация	Информация с ограниченным доступом, не содержащая сведений, составляющих государственную тайну, доступ к которой ограничивается в соответствии с законодательством Российской Федерации (СТР-К).
Конфиденциальность персональных данных	Обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания (ФЗ 152)
Концепция	Определенный способ понимания трактовки какого-либо предмета, явления, процесса, основная точка зрения на предмет или явление, руководящая идея их систематического освещения (система взглядов на то или иное понимание явлений, процессов, единый определяющий замысел, ведущая мысль).
Мероприятие по защите информации	Совокупность действий по разработке и/или практическому применению способов и средств защиты информации (ГОСТ Р 50992-96).

Нарушитель или злоумышленник	Лицо (субъект), которое предприняло (пыталось предпринять) попытку несанкционированного доступа к ресурсам информационно-коммуникационной системы (попытку выполнения запрещенных ему действий с данным ресурсом) по ошибке, незнанию или осознанно со злым умыслом (из корыстных интересов) или без такового (ради игры или с целью самоутверждения и т.п.) и использовавшее для этого различные возможности, методы и средства (чисто агентурные методы получения сведений, технические средства перехвата без модификации компонентов системы, штатные средства и недостатки систем защиты, подключение к каналам передачи данных, внедрение программных закладок и использование специальных инструментальных и технологических программ и т.п.).
Недекларированные возможности	Функциональные возможности программного обеспечения, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации (РД Гостехкомиссии России).
Несанкционированный доступ к информации	Доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами (ОСТ 45.127-99).

Носитель информации	Физическое лицо или материальный объект, в том числе физические поля, в которых информация находит свое отображение в виде символов, образов, сигналов, технических решений и процессов (ГОСТ Р 50922-2006).
Обработка персональных данных	Действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных (ФЗ 152)
Объект защиты информации	Информация, носитель информации, информационный процесс, система и т.п., в отношении которых необходимо обеспечивать защиту в соответствии с поставленной целью защиты информации (ГОСТ Р 50922-2006).
Объект информатизации	Совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, средств обеспечения объекта информатизации, помещений или объектов (зданий, сооружений, технических средств), в которых они установлены, или помещения и объекты, предназначенные для ведения конфиденциальных переговоров (ГОСТ Р 51275-99).

Оператор персональных данных	Государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных (ФЗ 152)
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 (ФЗ 152)
Политика безопасности организации, обрабатывающей информацию	Совокупность документированных управленческих решений, направленных на защиту информации и связанных с ней ресурсов.
Пользователь (потребитель) информации	Субъект, обращающийся к информационной системе или посреднику за получением необходимой ему информации и пользующийся ею (Федеральный закон «Об информации, информатизации и защите информации»).
Регламент функционирования удостоверяющего центра	- основной руководящий документ удостоверяющего центра, отражающий обязанности пользователей и членов группы администраторов, протоколы работы, принятые форматы данных, а также основные организационно-технические мероприятия, необходимые для безопасного функционирования УЦ.

Собственник информационных ресурсов, информационных систем, технологий и средств их обеспечения	Субъект, в полном объеме реализующий полномочия владения, пользования, распоряжения указанными объектами (Федеральный закон «Об информации, информатизации и защите информации»).
Специальные исследования	Выявление с использованием контрольно-измерительной аппаратуры возможных технических каналов утечки защищаемой информации от основных и вспомогательных технических средств и систем и оценка соответствия защиты информации требованиям нормативных документов по защите информации (ГОСТ Р 51624-00).
Средства защиты информации	Технические, криптографические, программные и другие средства, предназначенные для защиты информации, а также средства контроля эффективности защиты информации. (Федеральный закон «О государственной тайне», Положение о сертификации средств защиты информации.: Утверждено Постановлением Правительства Российской Федерации № 608 от 26 июня 1995 г).
Средства криптографической защиты информации (шифровальные средства)	Средства защиты информации, реализованные с использованием криптографических алгоритмов, ключевые документы к ним, средства изготовления и распределения ключевых документов.

Средство электронной цифровой подписи	Совокупность программных и технических средств, реализующих функцию выработки и проверки электронно-цифровой подписи (закон "Об электронной цифровой подписи").
Удостоверяющий Центр (УЦ)	Организация, обладающая необходимым комплексом технических средств, материальными и финансовыми возможностями, реализующая систему организационно-технических мероприятий и обеспечивающая выполнение целевых функций согласно ст.9 Федерального закона «Об электронной цифровой подписи».
Угроза безопасности информации	Совокупность условий и факторов, создающих потенциальную или реально существующую опасность, связанную с утечкой информации и/или несанкционированными и/или непреднамеренными воздействиями на нее. (ГОСТ Р 51624-00).
Целостность информации	Состояние защищенности информации, характеризуемое способностью АС обеспечивать сохранность и неизменность конфиденциальной информации при попытках несанкционированных или случайных воздействий на нее в процессе обработки или хранения (СТР-К).

Электронная цифровая подпись	Последовательность символов, полученная в результате криптографического преобразования исходной информации с использованием закрытого ключа электронной цифровой подписи, которая позволяет лицу, владеющему открытым ключом электронной цифровой подписи, установить целостность и неизменность этой информации, а также владельца закрытого ключа электронной цифровой подписи. (Закон «Об электронной цифровой подписи»).

ЛИСТ ИЗМЕНЕНИЙ

№ п/п	Дата	Автор	Содержание изменения