Приложение № 1 к приказу УОГКУСЗН «ЕОЦСВ» от «\_\_\_» \_\_\_\_\_\_\_\_\_ 20\_\_ года № \_\_\_\_\_\_\_\_

**Политика**

**информационной безопасности**

**УЛЬЯНОВСКОГО ОБЛАСТНОГО ГОСУДАРСТВЕННОГО КАЗЁННОГО УЧРЕЖДЕНИЯ СОЦИАЛЬНОЙ ЗАЩИТЫ НАСЕЛЕНИЯ
«ЕДИНЫЙ ОБЛАСТНОЙ ЦЕНТР СОЦИАЛЬНЫХ ВЫПЛАТ»**

На 26 листах

2020 г.

**Содержание**

[ИСПОЛЬЗУЕМЫЕ СОКРАЩЕНИЯ 3](#_Toc32913194)

[1. Общие положения 4](#_Toc32913195)

[2. цель и задачи СОИБ 6](#_Toc32913196)

[3. Распределение ответственности и ролей 6](#_Toc32913197)

[4. Защищаемые ресурсы 10](#_Toc32913198)

[5. Моделирование угроз ИБ и оценка рисков 11](#_Toc32913199)

[6. Состав мер защиты в СОИБ 12](#_Toc32913200)

[7. Ответственность за соблюдение положений Политики 15](#_Toc32913201)

[8. Порядок внесения изменений 15](#_Toc32913202)

[Приложение 1. Термины и определения 16](#_Toc32913203)

[Приложение 2. нормативно-правовая база 21](#_Toc32913204)

# ИСПОЛЬЗУЕМЫЕ СОКРАЩЕНИЯ

|  |  |
| --- | --- |
| **АРМ** | Автоматизированное рабочее место |
| **АС** | Автоматизированная система |
| **БД** | База данных |
| **ИБ** | Информационная безопасность |
| **ИС** | Информационная система |
| **ИТ** | Информационные технологии |
| **ЛВС** | Локальная вычислительная сеть |
| **НСД** | Несанкционированный доступ |
| **ОС** | Операционная система |
| **ПО** | Программное обеспечение |
| **ПС** | Программное средство |
| **СЗИ НСД** | Средство защиты информации от несанкционированного доступа |
| **СКЗИ** | Средство криптографической защиты информации |
| **СОИБ** | Система обеспечения информационной безопасности |
| **ФСБ России** | Федеральная служба безопасности |
| **ФСТЭК России** | Федеральная служба по техническому и экспортному контролю |
| **ЭЦП** | Электронная цифровая подпись |

## Общие положения

* 1. Настоящая Политика информационной безопасности (далее – Политика ИБ) *-* руководящий документ Ульяновского областного государственного казённого учреждения социальной защиты населения «Единый областной центр социальных выплат» (далее – УОГКУСЗН «ЕОЦСВ»), устанавливающий принципы построения и совершенствования системы обеспечения информационной безопасности (далее – СОИБ) на основе систематизированного изложения целей, процессов и процедур обеспечения информационной безопасности УОГКУСЗН «ЕОЦСВ».
	2. Термины и определения, использующиеся в настоящей Политике ИБ, представлены в Приложении 1.
	3. Настоящая Политика ИБ представляет собой официально принятую руководством УОГКУСЗН «ЕОЦСВ» систему взглядов на проблему обеспечения информационной безопасности.
	4. Руководство УОГКУСЗН «ЕОЦСВ» осознает важность и необходимость развития и совершенствования мер и средств обеспечения информационной безопасности в контексте развития российской, в том числе и отраслевой, нормативно-правовой базы в области защиты информации.
	5. Настоящая Политика ИБ базируется на нормативно-правовых актах, действующих на территории Российской Федерации по обеспечению информационной безопасности. Перечень нормативно-правовых актов представлен в Приложении 2 к настоящей Политике ИБ.
	6. Настоящая Политика ИБ дает общее представление, какие информационные ресурсы УОГКУСЗН «ЕОЦСВ» подлежат защите, почему требуется защита этих ресурсов и каким образом требуется защищать эти ресурсы.
	7. Настоящая Политика ИБ применима ко всей ИТ-инфраструктуре УОГКУСЗН «ЕОЦСВ» (вычислительной технике, серверному и сетевому оборудованию, локальным сетям, приложениям, информационным и операционным системам УОГКУСЗН «ЕОЦСВ»), а также к процессам администрирования, сопровождения и использования информационных систем УОГКУСЗН «ЕОЦСВ».
	8. Настоящая Политика ИБ распространяется на всех сотрудников и временный персонал УОГКУСЗН «ЕОЦСВ», а также сотрудников сторонних организаций, оказывающих УОГКУСЗН «ЕОЦСВ» услуги аутсорсинга, и является обязательной для ознакомления и исполнения.
	9. Настоящая Политика ИБ является основой для:
* внедрения и соблюдения правил в области обеспечения безопасности информации среди сотрудников УОГКУСЗН «ЕОЦСВ»;
* координации деятельности структурных подразделений УОГКУСЗН «ЕОЦСВ» при проведении работ по развитию и модернизации ИТ-инфраструктуры с соблюдением требований по обеспечению безопасности информации;
* разработки предложений по совершенствованию технических и организационных мер защиты информации УОГКУСЗН «ЕОЦСВ».
	1. Документами, детализирующими положения настоящей Политики ИБ применительно к одной или нескольким областям ИБ, видам и технологиям деятельности УОГКУСЗН «ЕОЦСВ», являются внутренние Положения, Частные политики, Инструкции, Регламенты и Процедуры по обеспечению ИБ, которые разрабатываются и согласовываются в соответствии с установленным в УОГКУСЗН «ЕОЦСВ» порядком, и оформляются как отдельные внутренние нормативные документы УОГКУСЗН «ЕОЦСВ».

## цель и задачи СОИБ

* 1. Целью СОИБ УОГКУСЗН «ЕОЦСВ» является реализация и совершенствование мер, необходимых и достаточных для выполнения требований российского законодательства, международных стандартов, требований отраслевых и регулирующих органов к обеспечению защиты информации, в том числе защиты персональных данных сотрудников и клиентов УОГКУСЗН «ЕОЦСВ», защиты банковских платежных технологических процессов и банковских информационных технологических процессов.
	2. Для достижения цели, в рамках СОИБ, решаются следующие задачи:
1. Распределение обязанностей, ответственности и назначение ролей в системе обеспечения информационной безопасности УОГКУСЗН «ЕОЦСВ».
2. Определение и поддержание в актуальном состоянии Перечня защищаемой информации, проведение инвентаризации защищаемых ресурсов (актуальный перечень элементов ИТ-инфраструктуры, где циркулирует защищаемая информация).
3. Моделирование угроз ИБ, анализ и оценка рисков реализации угроз ИБ для защищаемых ресурсов УОГКУСЗН «ЕОЦСВ».
4. Определение, оценка, выбор и реализация организационных и технических мер защиты информации по нейтрализации угроз ИБ для защищаемых ресурсов УОГКУСЗН «ЕОЦСВ», а также разработка и внедрение процедур менеджмента ИБ УОГКУСЗН «ЕОЦСВ».
5. Мониторинг функционирования СОИБ, периодическая оценка соответствия СОИБ требованиям безопасности информации, планирование и реализация мер по совершенствованию СОИБ.

## Распределение ответственности и ролей

* 1. Руководство УОГКУСЗН «ЕОЦСВ».
		1. В рамках организации и осуществления общего руководства текущей деятельностью УОГКУСЗН «ЕОЦСВ», определяет стратегию и программу обеспечения информационной безопасности.
		2. Утверждает политику и процедуры информационной безопасности.
		3. Обеспечивает разработку рекомендаций по осуществлению технической политики УОГКУСЗН «ЕОЦСВ» в области информатизации, эффективному использованию информационных технологий, совершенствованию информационно-технологической инфраструктуры и информационной безопасности УОГКУСЗН «ЕОЦСВ».
		4. Обеспечивает контроль соответствия СОИБ УОГКУСЗН «ЕОЦСВ» принятым решениям, политикам и стандартам, адекватности, эффективности, а также оценку возможности улучшения и изменений СОИБ, в том числе политик и целей информационной безопасности.
	2. Подразделение информационной безопасности (ИБ).
		1. Осуществляет основную деятельность по реализации СОИБ УОГКУСЗН «ЕОЦСВ».
		2. Подготавливает предложения по формированию бюджета, направленного на обеспечение информационной безопасности УОГКУСЗН «ЕОЦСВ».
		3. В рамках своих полномочий разрабатывает частные политики, инструкции, регламенты и процедуры по обеспечению информационной безопасности.
		4. Обеспечивает штатное функционирование комплекса средств информационной безопасности УОГКУСЗН «ЕОЦСВ».
		5. Обеспечивает исполнение требований информационной безопасности, изложенных в настоящей Политике ИБ и других внутренних документах УОГКУСЗН «ЕОЦСВ».
		6. Обеспечивает мониторинг функционирования СОИБ УОГКУСЗН «ЕОЦСВ».
		7. Организует обучение сотрудников УОГКУСЗН «ЕОЦСВ» в области информационной безопасности.
		8. Оценивает риски информационной безопасности.
		9. Контролирует действия пользователей.
		10. Обеспечивает выбор средств и механизмов контроля, управления и обеспечения информационной безопасности УОГКУСЗН «ЕОЦСВ».
		11. Проводит расследование событий, связанных с нарушениями информационной безопасности (инцидентов безопасности).
		12. Оценивает соответствие операций, настроек приложений и систем принятым политикам и стандартам безопасности.
		13. Оценивает стратегию информационной безопасности УОГКУСЗН «ЕОЦСВ» и вносит предложения по ее изменению.
		14. Оценивает состояние информационной безопасности в УОГКУСЗН «ЕОЦСВ».
		15. Информирует руководство УОГКУСЗН «ЕОЦСВ» о состоянии информационной безопасности.
		16. Разрабатывает планы мероприятий по совершенствованию системы информационной безопасности по результатам мониторинга, внутренних и внешних аудитов.
	3. Подразделение информационных технологий (ИТ).
		1. Обеспечивает предоставление доступа пользователям к информационным ресурсам УОГКУСЗН «ЕОЦСВ» в соответствии с авторизованными заявками.
		2. Обеспечивает целостность и доступность (включая архивирование и резервное копирование информации) информационных ресурсов УОГКУСЗН «ЕОЦСВ», конфиденциальность обрабатываемой в них информации (администрирование встроенных механизмов безопасности).
		3. Участвует в эксплуатации средств криптографической защиты информации (СКЗИ) УОГКУСЗН «ЕОЦСВ».
	4. Подразделение по работе с персоналом (кадров).
		1. Обеспечивает ознакомление сотрудников УОГКУСЗН «ЕОЦСВ» с Политикой ИБ.
		2. Обеспечивает наложение на сотрудников УОГКУСЗН «ЕОЦСВ» взысканий в случае нарушения Политики ИБ и правил информационной безопасности.
	5. Сотрудники УОГКУСЗН «ЕОЦСВ»
		1. Выполняют требования информационной безопасности, изложенные в настоящей Политике ИБ и других внутренних документах УОГКУСЗН «ЕОЦСВ».
		2. Обеспечивают исполнение требований информационной безопасности, изложенных в настоящей Политике и других внутренних документах УОГКУСЗН «ЕОЦСВ», третьими лицами, с которыми они контактируют в рамках своих должностных обязанностей, в том числе путем наличия указанных требований в контрактах/ соглашениях/ договорах с третьими лицами.
	6. В целях выполнения задач по обеспечению информационной безопасности УОГКУСЗН «ЕОЦСВ», в рамках СОИБ определены следующие роли:
1. Ответственный за обеспечение информационной безопасности;
2. Администратор информационной безопасности;
3. Администратор ИС;
4. Куратор по вопросам обеспечения ИБ от руководства УОГКУСЗН «ЕОЦСВ».

При необходимости могут быть определены и другие роли по информационной безопасности. Для исполнения одной роли может привлекаться несколько сотрудников, на одного сотрудника может быть возложено несколько ролей. Назначение сотрудникам УОГКУСЗН «ЕОЦСВ» ролей в рамках СОИБ осуществляется на основании приказа руководителя УОГКУСЗН «ЕОЦСВ».

* 1. Ответственный за обеспечение информационной безопасности отвечает за:
* организацию работ по реализации СОИБ УОГКУСЗН «ЕОЦСВ»;
* анализ состояния, выработку рекомендаций и указаний по совершенствованию СОИБ и контроль их выполнения;
* разработку основных регламентирующих и нормативных документов СОИБ в УОГКУСЗН «ЕОЦСВ» и осуществление контроля выполнения требований указанных документов;
* координацию работ по реализации СОИБ в структурных подразделениях УОГКУСЗН «ЕОЦСВ»;
* контроль выполнения требований по защите информации в ИС УОГКУСЗН «ЕОЦСВ»;
* учет фактов нарушений информационной безопасности, организацию проведения расследований по данным фактам и разработку предложений по устранению недостатков и предупреждению подобного рода нарушений;
* ознакомление сотрудников, которые допущены к работе с защищаемой информацией, с внутренними документами СОИБ.
	1. Ответственный за обеспечение информационной безопасности имеет право:
* представлять куратору по вопросам обеспечения ИБ от руководства УОГКУСЗН «ЕОЦСВ» свои предложения по развитию и повышению эффективности СОИБ УОГКУСЗН «ЕОЦСВ»;
* обращаться к руководителям подразделений УОГКУСЗН «ЕОЦСВ» по вопросам оказания необходимой технической и методологической помощи в своей работе.
	1. Администратор информационной безопасности отвечает за:
* установку, настройку и сопровождение программно-аппаратных средств защиты информации;
* контроль эффективности защиты информации в ИС;
* контроль исполнения пользователями ИС требований информационной безопасности, а именно:
	+ правил парольной политики;
	+ правил работы в сетях общего пользования (Интернет);
	+ правил использования электронной почты;
* контроль соблюдения пользователями ИС требований по учету, использованию и хранению машинных носителей информации;
* контроль соблюдения пользователями ИС правил копирования и передачи информации по каналам связи;
* проверки рабочих станций пользователей ИС с целью недопущения установки, использования, хранения и размножения в ИС программных средств, не связанных с выполнением функциональных задач;
* анализ журналов учета событий, регистрируемых встроенными средствами ИС и средствами защиты информации, с целью выявления фактов несанкционированного доступа в ИС;
* своевременность доклада Ответственному за обеспечение ИБ о выявленных нарушениях информационной безопасности, с изложением факта нарушения, предпринятые и/или рекомендуемые им действия.
	1. Администратор информационной безопасности имеет право:
* требовать от пользователей ИС соблюдения установленных правил и выполнения инструкций по обеспечению безопасности и защите информации;
* инициировать проведение служебных расследований по фактам нарушения установленных требований по обеспечению информационной безопасности, несанкционированного доступа, утраты, порчи защищаемой информации и технических компонентов ИС;
* представлять Ответственному за обеспечение ИБ свои предложения по совершенствованию программно-аппаратных и организационных мер защиты СОИБ;
* обращаться к руководителям подразделений УОГКУСЗН «ЕОЦСВ» по вопросам оказания необходимой технической и методологической помощи в своей работе.
	1. Администратор ИС отвечает за:
* работоспособность элементов ИС и локальной вычислительной сети.
* установку, настройку и своевременное обновление элементов ИС;
* резервирование и восстановление работоспособности программных и аппаратных средств ИС;
* контроль за порядком учета и хранения резервных копий;
* допуск к ИС (заведение учетных записей пользователей и прав доступа), контроль за правильностью использования административных паролей ИС;
* выполнение требований по обеспечению безопасности информации при организации обслуживания технических средств и отправке их в ремонт;
* своевременность принятия мер по реагированию, в случае возникновения внештатных и аварийных ситуаций, с целью ликвидации их последствий.
	1. Администратор ИС имеет право:
* запрещать пользователям ИС устанавливать на своих рабочих станциях нештатное программное и аппаратное обеспечение;
* проводить проверки использования вычислительной техники и информационных ресурсов ИС и пресекать случаи их нецелевого использования;
* информировать Администратора ИБ и Ответственного за обеспечение ИБ о фактах нарушения установленного порядка работ и попытках несанкционированного доступа к информационным ресурсам ИС;
* требовать прекращения обработки информации, как в целом, так и для отдельных пользователей, в случае выявления нарушений установленного порядка работ или нарушения функционирования ИС или средств защиты;
* представлять Ответственному за обеспечение ИБ свои предложения по модификации существующего аппаратно-программного обеспечения с целью повышению эффективности использования ИС.
* обращаться к руководителям подразделений УОГКУСЗН «ЕОЦСВ» по вопросам оказания необходимой технической и методологической помощи в своей работе.
	1. Куратор по вопросам обеспечения ИБ от руководства УОГКУСЗН «ЕОЦСВ» осуществляет общий контроль исполнения мероприятий по реализации СОИБ, а также вносит предложения по финансированию данных мероприятий на утверждение руководителю УОГКУСЗН «ЕОЦСВ».

## Защищаемые ресурсы

* 1. К защищаемой информации УОГКУСЗН «ЕОЦСВ» относится:
1. Информация, составляющая служебную тайну УОГКУСЗН «ЕОЦСВ»;
2. Информация, составляющая коммерческую тайну УОГКУСЗН «ЕОЦСВ»;
3. Персональные данные:
* персональные данные сотрудников;
* персональные данные не сотрудников;
1. Информация о средствах и методах обеспечения информационной безопасности УОГКУСЗН «ЕОЦСВ», в том числе:
* ключевая информация средств криптографической защиты информации, используемая при технологических и производственных процессах;
* информация о конфигурации, автоматизированных систем, программного обеспечения, телекоммуникационного оборудования, используемого для осуществления технологических и производственных процессов;
* информация об учетных записях и паролях пользователей в локальной сети УОГКУСЗН «ЕОЦСВ»;
1. Иная информация, подлежащая защите, в соответствии с законодательством Российской Федерации.
	1. Основными объектами защиты в ИТ-инфраструктуре УОГКУСЗН «ЕОЦСВ» являются:
* защищаемая информация;
* программное обеспечение;
* автоматизированные рабочие места;
* веб-сервера;
* сервера баз данных;
* система хранения данных;
* виртуальные машины;
* система резервного копирования;
* сетевое и коммуникационное оборудование;
* средства защиты информации.
	1. Кроме того, должны учитываться помещения, где расположены элементы ИТ-инфраструктуры, оснащение данных помещений охранными системами (электронные замки, сигнализация), системами видеонаблюдения, системами пожаротушения, кондиционирования, ИБП.
	2. С целью инвентаризации элементов ИТ-инфраструктуры в УОГКУСЗН «ЕОЦСВ» разрабатывается отдельный документ.

## Моделирование угроз ИБ и оценка рисков

* 1. Под угрозами ИБ понимается совокупность условий и факторов, создающих потенциальную или реально существующую опасность, связанную с утечкой защищаемой информации и (или) несанкционированными и (или) непреднамеренными воздействиями на нее.
	2. Угрозы ИБ реализуются источником угрозы, тем или иным способом, используя скрытые или явные уязвимости в ИТ-инфраструктуре информационной системы, в том числе в СОИБ.
	3. Реализация угроз ИБ приводит к нарушению одной или нескольких характеристик безопасности защищаемой информации (конфиденциальность, целостность, доступность), и, как следствие, может привести к негативным последствиям для УОГКУСЗН «ЕОЦСВ» и его клиентов.
	4. Обобщенная схема реализации угроз ИБ представлена на рисунке 1.



Рисунок 1 – Обобщенная схема реализации угроз ИБ

* 1. С целью определения актуальных угроз ИБ для защищаемых ресурсов УОГКУСЗН «ЕОЦСВ» разрабатывается отдельный документ «Модель актуальных угроз ИБ».
	2. В этом же документе определяется оценка степени тяжести последствий (потенциального ущерба для УОГКУСЗН «ЕОЦСВ») от нарушения ИБ в результате реализации актуальных угроз ИБ.
	3. На основании проведенной оценки разрабатывается «План обработки рисков нарушения ИБ», который включает в себя необходимые организационные и технические меры противодействия угрозам ИБ и снижения рисков нарушения ИБ.
	4. На основе «Плана обработки рисков нарушения ИБ» формируются планы развития организационно-распорядительной, инженерно-технической и программно-аппаратной базы СОИБ УОГКУСЗН «ЕОЦСВ».

## Состав мер защиты в СОИБ

* 1. Для достижения и поддержания требуемого уровня защищенности информационной системы УОГКУСЗН «ЕОЦСВ» и противодействия угрозам нарушения ИБ, в СОИБ могут быть задействованы организационно-распорядительные, инженерно-технические и программно-технические меры защиты.
	2. Организационно-распорядительные меры защиты СОИБ
		1. Организационно-распорядительные меры защиты реализуются:
* вводом в действие организационно-распорядительных документов, определяющих требования и/или регламентирующих действия сотрудников по обеспечению ИБ применительно к одной или нескольким областям СОИБ, а также к различным видам деятельности УОГКУСЗН «ЕОЦСВ»;
* выполнением сотрудниками требований и/или предписанных действий по обеспечению ИБ, определенных в организационно-распорядительных документах;
* контролем за выполнением сотрудниками требований и/или предписанных действий по обеспечению ИБ, определенных в организационно-распорядительных документах, со стороны уполномоченных сотрудников УОГКУСЗН «ЕОЦСВ» (ответственных за ИБ, администраторов ИБ и ИС) и руководителей подразделений УОГКУСЗН «ЕОЦСВ» (в соответствии с должностными обязанностями).
	+ 1. Организационно-распорядительная документация, определяющая требования и/или регламентирующая действия сотрудников по обеспечению ИБ (документы СОИБ), в соответствии с рекомендациями УОГКУСЗН «ЕОЦСВ» России, реализуется четырехуровневым комплексом.
		2. К документам СОИБ первого (верхнего) уровня СОИБ относится настоящая Политика ИБ.
		3. К документам второго уровня относятся:
* Положение о конфиденциальной информации, включая Перечень конфиденциальных сведений УОГКУСЗН «ЕОЦСВ»;
* Модель актуальных угроз ИБ, включая Инвентаризацию ИТ-инфраструктуры защищаемых ресурсов, План обработки рисков нарушения ИБ;
* Частные политики ИБ, детализирующие требования по обеспечению ИБ применительно к одной или нескольким областям СОИБ
* другие документы по обеспечению ИБ данного уровня детализации, которые могут разрабатываться и внедряться в УОГКУСЗН «ЕОЦСВ» в соответствии с требованиями российского законодательства и/или отраслевым стандартом СТО БР ИББС.
	+ 1. К документам третьего уровня относятся документы СОИБ, регламентирующие действия сотрудников по обеспечению ИБ применительно к одной или нескольким областям СОИБ, а также к различным видам деятельности УОГКУСЗН «ЕОЦСВ»:
* Регламент предоставления доступа к ресурсам ИС УОГКУСЗН «ЕОЦСВ»;
* Регламент резервного копирования и восстановления ресурсов ИС УОГКУСЗН «ЕОЦСВ»;
* План обеспечения непрерывности и восстановления деятельности УОГКУСЗН «ЕОЦСВ»;
* Процедуры менеджмента СОИБ (обработка инцидентов ИБ, управление записями, управление документами и т.п.)
* Инструкции администраторов ИБ, ИС, пользователей ИС и т.п.
	+ 1. К документам четвертого уровня относятся свидетельства осуществления деятельности СОИБ. Это могут быть и заполненные типовые формы различных журналов учета, отчеты внутренних контрольных проверок, материалы проведенных аудитов ИБ (внутренних и внешних), материалы внутренних расследований инцидентов ИБ, утвержденные планы развития СОИБ, приказы и распоряжения, касающиеся деятельности по СОИБ УОГКУСЗН «ЕОЦСВ» и т.п.
	1. Инженерно-технические и программно-аппаратные меры защиты СОИБ
		1. Инженерно-технические меры защиты должны обеспечивать уменьшение возможности проявления угроз ИБ, обусловленных несанкционированными действиями посторонних лиц и сотрудников УОГКУСЗН «ЕОЦСВ», а также снижение влияния техногенных источников и угроз стихийного характера.
		2. К инженерно-техническим мерам противодействия угрозам ИБ относятся:
* физическая охрана зданий УОГКУСЗН «ЕОЦСВ» (осуществление контрольно-пропускного режима);
* автоматизированные системы контроля доступа в здания и помещения (СКУД);
* системы видеонаблюдения;
* системы пожаротушения;
* средства от утечек информации по ПЭМИН (побочных электромагнитных излучений и наводок);
* средства от утечек информации по акустическим каналам;
* средства от утечек видовой информации;
* средства электрозащиты (источники бесперебойного питания);
* средства грозозащиты оборудования ИС;
* и т.п.
	+ 1. Программно-аппаратные меры защиты реализуются общесистемным программным обеспечением (ОС, СУБД), специальным программным обеспечением сетевых узлов ИС (серверы различного назначения, маршрутизаторы, коммутаторы, концентраторы, межсетевые экраны), а также специальными средствами защиты информации (СЗИ) и должны обеспечивать:
* создание защищенной программной и аппаратной платформ для ИС, использование доверенного ПО и технических средств, гарантирующих целостность и надежность;
* допуск к работе в ИС только авторизованных пользователей и разграничение их полномочий при работе с информационными ресурсами, а также защиту элементов ИС (АРМ, сервер).
* построение защитной оболочки[[1]](#footnote-1) (защищенного периметра) как вокруг ИС, так и вокруг отдельных ее сегментов (при использовании технологии сегментирования), а также ограничения числа точек взаимодействия ИС (точек входа/выхода) с внешними сетями и выделенных сегментов ИС между собой;
* создание доверенных каналов связи между сегментами ИС, ее элементами (АРМ, серверы), а также между ИС головного офиса и ИС дополнительных офисов.
	+ 1. В пределах ИС, в точках её сопряжения с глобальными информационными сетями общего пользования или филиальными ИС, должен быть установлен сервер, обеспечивающий скрытие адресного пространства (топологии) ИС. Адресное пространство ИС должно быть самостоятельным и не может являться подмножеством адресного пространства глобальных информационных сетей общего пользования.
		2. Программно-аппаратные меры, в общем случае, включают в себя:
* средства идентификации и аутентификации;
* средства управления доступом;
* средства межсетевого экранирования;
* средства защиты каналов передачи данных;
* средства антивирусной защиты и антиспама;
* средства обнаружения вторжений;
* средства анализа защищенности;
* средства защиты среды виртуализации (при использовании технологии виртуализации);
* средства криптографической защиты;
* средства контроля содержимого передаваемых данных (web-трафика);
* средства централизованного резервного копирования и восстановления;
* средства мониторинга событий ИБ;
* средства централизованного управления СОИБ.
	1. В целом, комплекс принимаемых мер должен обеспечивать нейтрализацию угроз ИБ и снижение рисков реализации актуальных угроз ИБ. Перечень принимаемых мер должен соответствовать требованиям российского законодательства и регулирующих органов.
	2. В УОГКУСЗН «ЕОЦСВ» должна проводится оценка соответствия СОИБ требованиям безопасности информации. Результаты оценки оформляются в виде Заключения установленной формы.

## Ответственность за соблюдение положений Политики

* 1. Общее руководство обеспечением информационной безопасности УОГКУСЗН «ЕОЦСВ» осуществляет руководитель УОГКУСЗН «ЕОЦСВ».
	2. Ответственность за поддержание положений настоящей Политики ИБ в актуальном состоянии, создание, внедрение, координацию и внесение изменений в процессы системы менеджмента информационной безопасности УОГКУСЗН «ЕОЦСВ» лежит на руководстве подразделения ИБ.
	3. Ответственность сотрудников УОГКУСЗН «ЕОЦСВ» за невыполнение настоящей Политики ИБ определяется соответствующими положениями, включаемыми в трудовые договоры с сотрудниками УОГКУСЗН «ЕОЦСВ», а также положениями внутренних нормативных документов УОГКУСЗН «ЕОЦСВ».

## Порядок внесения изменений

* 1. Внесение изменений в настоящую Политику осуществляется на периодической и внеплановой основе:
* пересмотр положений настоящей Политики должно осуществляться не реже одного раза в 24 месяца;
* внеплановое внесение изменений в настоящую Политику может производиться по результатам анализа инцидентов информационной безопасности, актуальности, достаточности и эффективности используемых мер обеспечения информационной безопасности, результатам проведения внутренних аудитов информационной безопасности и других контрольных мероприятий, а также при значительных изменениях в законодательных актах Российской Федерации и/или в нормативных актах регулирующих органов (ФСТЭК России, ФСБ России).
	1. Ответственным за внесение изменений в настоящую Политику ИБ является руководитель подразделения ИБ.

## Приложение 1. Термины и определения

| **Термин** | **Определение** | **Источник** |
| --- | --- | --- |
| *Автоматизированная система* | система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций | ГОСТ 34.003-90, ГОСТ Р 51624-00 |
| *Автоматизированное рабочее место* | программно-технический комплекс, предназначенный для автоматизации деятельности определенного вида | ГОСТ 34.003-90 |
| *Аттестация**автоматизированной системы* | процесс комплексной проверки выполнения заданных функций АС по обработке защищаемой информации на соответствие требованиям стандартов и/или нормативных документов в области защиты информации и оформления документов о ее соответствии выполнять функции по обработке защищаемой информации на конкретном объекте информатизации  | ГОСТ Р 51583-00 |
| *Аутентификация* |  проверка принадлежности субъекту доступа предъявленного им идентификатора; подтверждение подлинности | РД. Гостехкомиссия России. «Защита от НСД к информации. Термины и определения.» |
| *Безопасность**информации* | состояние защищенности информации, обрабатываемой средствами вычислительной техники или автоматизированной системы, от внутренних или внешних угроз | РД. Гостехкомиссия России. «Защита от НСД к информации. Термины и определения.» |
| *Защита**информации* | защита информации представляет собой принятие правовых, организационных и технических мер, направленных на:1) обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;2) соблюдение конфиденциальности информации ограниченного доступа;3) реализацию права на доступ к информации. | Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 25.11.2017) "Об информации, информационных технологиях и о защите информации" (с изм. и доп., вступ. в силу с 01.01.2018) |
| *Идентификатор**доступа* | уникальный признак субъекта или объекта доступа | РД. Гостехкомиссия России. «Защита от НСД к информации. Термины и определения.» |
| *Идентификация* | присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов | РД. Гостехкомиссия России. «Защита от НСД к информации. Термины и определения.» |
| *Информационная**система* | совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств | Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 25.11.2017) "Об информации, информационных технологиях и о защите информации" (с изм. и доп., вступ. в силу с 01.01.2018) |
| *Информационная**технология* | приемы, способы и методы применения средств вычислительной техники при выполнении функций хранения, обработки, передачи и использования данных | ГОСТ 34.003-90 |
| *Класс защищенности автоматизированной системы* | определенная совокупность требований по защите АС от НСД к информации | ГОСТ Р 51624-00 |
| *Комплекс**средств защиты* | совокупность программных и технических средств, создаваемая и поддерживаемая для обеспечения защиты средств вычислительной техники или автоматизированных систем от несанкционированного доступа к информации | РД. Гостехкомиссия России. «Защита от НСД к информации. Термины и определения.» |
| *Конфиденциальность* *информации* | обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя | Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 25.11.2017) "Об информации, информационных технологиях и о защите информации" (с изм. и доп., вступ. в силу с 01.01.2018) |
| *Матрица доступа* | таблица, отображающая правила разграничения доступа | РД. Гостехкомиссия России. «Защита от НСД к информации. Термины и определения.» |
| *Метка**конфиденциальности* | элемент информации, который характеризует конфиденциальность информации, содержащейся в объекте | РД. Гостехкомиссия России. «Защита от НСД к информации. Термины и определения.» |
| *Несанкционированный доступ* | получение защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации | ГОСТ Р 50922-96 |
| *Обработка**информации* | совокупность операций сбора, накопления, ввода, вывода, приема, передачи, записи, хранения, регистрации, уничтожения, преобразования, отображения, осуществляемых над информацией | ГОСТ 51583-00 |
| *Операционная**система* | совокупность системных программ, предназначенная для обеспечения определенного уровня эффективности системы обработки информации за счет автоматизированного управления ее работой и предоставляемого пользователю определенного набора услуг | ГОСТ 15971-90 |
| *Пароль* | идентификатор субъекта доступа, который является его (субъекта) секретом | РД. Гостехкомиссия России. «Защита от НСД к информации. Термины и определения.» |
| *Политика безопасности*  | совокупность требований (правил), регулирующих управление информационными ресурсами, их защиту и распределение в пределах ИС | ГОСТ Р 15408-99 |
| *Программное**обеспечение* | совокупность программ на носителях данных и программных документов, предназначенная для отладки, функционирования и проверки работоспособности автоматизированной системы | ГОСТ 34.003-90 |
| *Программно-технический**комплекс* | продукция, представляющая собой совокупность средств вычислительной техники, программного обеспечения и средств создания и заполнения машинной информационной базы при вводе системы в действие достаточных для выполнения одной или более задач | ГОСТ 34.003-90 |
| *Система**защиты информации* | совокупность технических, программных и программно-технических средств зашиты информации и средств контроля эффективности защиты информации | ГОСТ Р 51583-00 |
| *Средство**вычислительной**техники* | совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем | ГОСТ Р 50739-95 |
| *Средство**защиты информации* | техническое, программное средство, вещество и/или материал, предназначенные или используемые для защиты информации | ГОСТ Р 50922 |
| *Средство**криптографической* *защиты информации* | средство вычислительной техники, осуществляющее криптографическое преобразование информации для обеспечения ее безопасности. К СКЗИ относятся: а) средства шифрования - аппаратные, программные и аппаратно-программные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты информации при передаче по каналам связи и (или) для защиты информации от несанкционированного доступа при ее обработке и хранении;б) средства имитозащиты - аппаратные, программные и аппаратно-программные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты от навязывания ложной информации;в) средства электронной цифровой подписи - аппаратные, программные и аппаратно-программные средства, обеспечивающие на основе криптографических преобразований реализацию хотя бы одной из следующих функций: создание электронной цифровой подписи с использованием закрытого ключа электронной цифровой подписи, подтверждение с использованием открытого ключа электронной цифровой подписи подлинности электронной цифровой подписи, создание закрытых и открытых ключей электронной цифровой подписи;г) средства кодирования - средства, реализующие алгоритмы криптографического преобразования информации с выполнением части преобразования путем ручных операций или с использованием автоматизированных средств на основе таких операций;д) средства изготовления ключевых документов (независимо от вида носителя ключевой информации);е) ключевые документы (независимо от вида носителя ключевой информации). | РД. Гостехкомиссия России. «Защита от НСД к информации. Термины и определения»Приказ ФСБ России от 9 февраля 2005 года № 66 «Об утверждении положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)» |
| *Средство защиты от несанкционированного доступа* | программное, техническое или программно техническое средство, предназначенное для предотвращения или существенного затруднения несанкционированного доступа | РД. Гостехкомиссия России. «Защита от НСД к информации. Термины и определения.» |
| *Субъект доступа* | лицо или процесс, действия которого регламентируются правилами разграничения доступа | РД. Гостехкомиссия России. «Защита от НСД к информации. Термины и определения.» |
| *Технический проект* | комплект проектных документов на систему, разрабатываемый на стадии «Технический проект», утвержденный в установленном порядке, содержащий основные проектные решения по системе в целом, ее функциям и видам ее обеспечения и достаточный для разработки рабочей документации на систему | ГОСТ 34.003-90 |
| *Техническое задание* | документ, оформленный в установленном порядке и определяющий цели создания автоматизированной системы, требования к системе и основные исходные данные, необходимые для ее разработки, а также план-график создания системы | ГОСТ 34.003-90 |
| *Техническое* *обеспечение* | совокупность всех технических средств, используемых при функционировании автоматизированной системы | ГОСТ 34.003-90 |
| *Управление* | совокупность целенаправленных действий, включающая оценку ситуации и состояния объекта управления, выбор управляющих воздействий и их реализацию | ГОСТ 34.003-90 |
| *Цифровой сертификат электронной цифровой подписи* | документ на бумажном носителе или электронный документ с ЭЦП Удостоверяющего Центра, который включает открытый ключ ЭЦП, и служит для подтверждения подлинности открытого ключа и идентификации его владельца | Федеральный закон «Об электронной цифровой подписи» |
| *Электронная цифровая подпись* | реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе | Федеральный закон «Об электронной цифровой подписи» |

# Приложение 2. нормативно-правовая база

1. Конституция Российской Федерации.
2. Гражданский Кодекс Российской Федерации, часть I, 1994 г.
3. Гражданский Кодекс Российской Федерации, часть II, 1995 г.
4. Трудовой кодекс РФ
5. Уголовный Кодекс Российской Федерации, 1996 г.
6. Уголовно-Процессуальный Кодекс Российской Федерации, 2001 г.
7. Доктрина информационной безопасности Российской Федерации от 9 сентября 2000 г. № Пр-1895;
8. Федеральный закон от 28 декабря 2010 г. № 390-ФЗ «О безопасности»;
9. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
10. Федеральный закон от 06 апреля 2011 г. № 63-ФЗ «Об электронной подписи»;
11. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;
12. Федеральный закон от 04 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности»;
13. Федеральный закон от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне»;
14. Указ Президента Российской Федерации № 260 от 22 мая 2015 года «О некоторых вопросах информационной безопасности Российской Федерации».
15. Указ Президента Российской Федерации № 537 от 12 мая 2009 года «О стратегии национальной безопасности Российской Федерации до 2020 года»;
16. Указ Президента Российской Федерации № 1576 от 01 ноября 2008 года «О совете при Президенте Российской Федерации по развитию информационного общества в Российской Федерации»;
17. Указ Президента Российской Федерации № 188 от 6 марта 1997 года «Об утверждении перечня сведений конфиденциального характера» (в ред. Указов Президента РФ от 23.09.2005 № 1111, от 13.07.2015 № 357);
18. Указ Президента РФ № 351 от 17.03.2008 г. «О мерах по обеспечению информационной безопасности РФ при использовании информационно-телекоммуникационных сетей международного информационного обмена»;
19. Постановление Правительства Российской Федерации от 16 ноября 2015 г. № 1236 «Об установлении запрета на допуск программного обеспечения происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд»
20. Постановление Правительства Российской Федерации от 21 марта 2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»;
21. Постановление Правительства Российской Федерации от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
22. Постановление Правительства Российской Федерации от 26 июня 1995 г. № 608 «О сертификации средств защиты информации»;
23. Постановление Правительства Российской Федерации от 03 ноября 1994 г. № 1233 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти»;
24. Приказ ФСБ России № 416, ФСТЭК № 489 от 31 августа 2010 г. «Об утверждении требований о защите информации, содержащейся в информационных системах общего пользования»;
25. Приказ ФСБ России от 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических средств защиты информации (Положение ПКЗ-2005))» (в ред. Приказа ФСБ РФ от 12.04.2010 №173);
26. Приказ ФСБ России от 10 июля 2014 г. N 378 "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности";
27. Методические рекомендации по обеспечению с помощью шифровальных (криптографических) средств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации, утверждены 8 Центром ФСБ России 21 февраля 2008 г. № 149/54-144;
28. Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну, в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных, утверждены 8 Центром ФСБ России 21 февраля 2008 г. № 149/6/6-622;
29. Инструкция об организации и обеспечении безопасности хранении, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну. Утверждена приказом ФАПСИ от 13 июня 2001 г. № 152;
30. Требования ФСБ России к шифровальным (криптографическим) средствам, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну», в/ч 43753, 2007 г.;
31. Требования ФСБ России к средствам электронной подписи, утверждена приказом директора ФСБ № 796 от 27.12.2011 г.;
32. Приказ ФСТЭК России от 14 марта 2014 г. № 31 «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды»;
33. Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
34. Приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;
35. ФСТЭК России. Методический документ «Меры защиты информации в государственных информационных системах» (утв. Федеральной службой по техническому и экспортному контролю 11 февраля 2014 г.);
36. ФСТЭК России. «Базовая Модель угроз безопасности персональных данных при обработке в информационных системах персональных данных» (выписка) (утв. Заместителем директора ФСТЭК России 15 февраля 2008 г.);
37. ФСТЭК России. «Положение по аттестации объектов информатизации по требованиям безопасности информации» (утв. Председателем ГТК при Президенте РФ 25 ноября 1994 г.);
38. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). Утверждены приказом Гостехкомиссии России от 30.08.2002 № 282;
39. Руководящий документ «Автоматизированные системы. Защиты от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации», Гостехкомиссия России, 1992 год;
40. Руководящий документ «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации». Утверждены решением председателя Гостехкомиссии России от 30.03.1992;
41. Руководящий документ «Безопасность информационных технологий. Критерии оценки безопасности информационных технологий», утверждена Приказом Гостехкомиссии России № 187 от 19.06.2002 г.;
42. Руководящий документ «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации», утверждены Председателем Гостехкомиссии России от 30 марта 1992 г.
43. Руководящий документ «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей», введен в действие Приказом Председателя Гостехкомиссии России № 114 от 04.06.1999 г.;
44. «Требования к средствам антивирусной защиты», утверждены приказом ФСТЭК России от 20.03.2012 г. № 28 (рег. в Минюсте России от 03.05.2012г. №24045);
45. «Требование к системам обнаружения вторжений», утверждены приказом ФСТЭК России от 06.12.2011г., № 638 (зарегистрированы в Минюсте России 1.02.2012 № 23088);
46. Приказ ФСТЭК России от 9 февраля 2016 г. N 9 (зарегистрирован Минюстом России 25 марта 2016 г., регистрационный N 41564) «Требования к межсетевым экранам»;
47. ГОСТ.34.201-89. ИТ. Комплекс стандартов на АС. Виды, комплектность и обозначение документов при создании АС.
48. ГОСТ 34.602-89. ИТ. Комплекс стандартов на АС. Техническое задание на создание АС.
49. ГОСТ 34.003-90. ИТ. Комплекс стандартов на АС. Термины и определения.
50. ГОСТ 29339-92. ИТ. Защита информации от утечки за счет ПЭМИН при ее обработке СВТ. Общие технические требования.
51. ГОСТ Р 50752-95. ИТ. Защита информации от утечки за счет ПЭМИН при ее обработке СВТ. Методы испытаний.
52. ГОСТ Р 50739-95. СВТ. Защита от несанкционированного доступа к информации.
53. ГОСТ Р 50922-96. ЗИ. Основные термины и определения.
54. ГОСТ Р 51188-98. ЗИ. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство.
55. ГОСТ Р 51275-99. ЗИ. Объект информатизации. Факторы, воздействующие на информацию. Общие положения.
56. ГОСТ Р ИСО 7498-1-99. ИТ. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 1. Базовая модель.
57. ГОСТ Р ИСО 7498-2-99. ИТ. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 1. Архитектура защиты информации.
58. ГОСТ Р ИСО/МЭК 15408-1-2002. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель.
59. ГОСТ Р ИСО/МЭК 15408-2-2002. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности.
60. ГОСТ Р ИСО/МЭК 15408-3-2002. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности.
61. ГОСТ Р 51583-00. ЗИ. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения.
62. ГОСТ Р 51624-00. ЗИ. Автоматизированные системы в защищенном исполнении. Общие требования.
63. ГОСТ Р ИСО/МЭК 27001-2006. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования.
64. ГОСТ Р ИСО/МЭК 27002-2012. Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента безопасности.
65. ГОСТ Р ИСО/МЭК 27003-2012. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Руководство по реализации системы менеджмента информационной безопасности.

**ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| №изменения | Номера страниц | Всегостраниц | Дата | Подпись лица, вносившего изменения |
| изменен­ных | замененных | аннулиро­ванных | новых |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

**Лист ознакомления**

|  |  |  |  |
| --- | --- | --- | --- |
| **№ п/п** | **Фамилия, инициалы сотрудника** | **Дата ознакомления** | **Расписка сотрудника в ознакомлении** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

1. Под **защитной оболочкой** в контексте настоящего документа понимается совокупность мер и средств, обеспечивающих выполнение основных защитных функций, предусматривающих защиту от НСД к информации, контроль за межсетевыми и межсегментными потоками данных, а также разграничение доступа внешних пользователей к внутренним ресурсам ИС. [↑](#footnote-ref-1)