П
11.4-2025

УТВЕРЖДЕН
Приказом № 25 -осн

от 04.02.2025 г.

ПОЛИТИКА

информационной безопасности КГБУЗ «Ачинская МРБ»

Дата введения в действие:

04.02.2025 г.

Ачинск , 2025

СОДЕРЖАНИЕ

1 НАЗНАЧЕНИЕ

Настоящая Политика является обеспечением безопасности объектов, защиты КГБУЗ «Ачинская межрайонная больница» (КГБУЗ «Ачинская МРБ») от всех видов угроз, внешних и внутренних, умышленных и непреднамеренных, минимизация ущерба от возможной реализации угроз безопасности ПДн (УБПДн).

2 ОБЛАСТЬ ПРИМЕНЕНИЯ

Требования настоящей Политики распространяются на всех сотрудников КГБУЗ «Ачинская МРБ» (штатных, временных, работающих по контракту и т.п.), а также всех прочих лиц (подрядчики, аудиторы и т.п.).

3 НОРМАТИВНЫЕ ССЫЛКИ

Настоящая Политика разработана на основании следующих документов:

- ISO/IEC IS 17799-2000. Information Technology. Code of practice for information security management.
- BS 7799-2-2002. Information security management systems. Specification with guidance for use.
- COBIT Control Objectives for Information and related Technology, 3rd Edition, July 2000.
- Федеральный закон от29.07.2004 № 98-ФЗ «О коммерческой тайне».
- Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».

Нормативно-методические документы Федеральной службы по техническому и экспертному контролю Российской Федерации (далее - ФСТЭК России) по обеспечению безопасности ПДн при их обработке в ИСПДн:

– Приказ ФСТЭК России от 18.02.2013 N 21 (ред. от 14.05.2020) «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

4 СПИСОК ТЕРМИНОВ И ОПРЕДЕЛЕНИЙ

Владелец информационного актива – подразделение КГБУЗ «Ачинская МРБ», реализующее полномочия владения, пользования и распоряжения информацией в соответствии со своими функциями и задачами.

Владелец информационного актива определяется на этапе создания соответствующих массивов данных.

Данные – различные виды информации, представленные в электронной форме.

Доступность – обеспечение того, что авторизованные пользователи имеют доступ к информационному активу всегда, когда это необходимо.

Идентификация риска – процесс выявления и классификации рисков.

Информационный актив – различные виды информации (платежной, финансово-аналитической, медицинской, служебной, управляющей, справочной и пр.) на всех этапах ее жизненного цикла, обеспечивающей основную деятельность КГБУЗ «Ачинская МРБ» и представляющей ценность с точки зрения достижения поставленных целей.

Информационная безопасность – состояние и режим эксплуатации средств хранения, доставки и автоматизированной обработки, при котором обеспечивается уровень защиты информационных активов, достаточный для минимизации ущерба, вызванного возможными нарушениями безопасности.

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.

Инцидент информационной безопасности — действительное, предпринимаемое или вероятное нарушение информационной безопасности. Нарушение может быть вызвано ошибками персонала, неправильным функционированием технических средств, природными факторами, преднамеренными злоумышленными действиями, приводящими к нарушению доступности, целостности, конфиденциальности информации.

Коллегиальные органы — в рамках настоящего документа – руководство КГБУЗ «Ачинская МРБ».

Конфиденциальность – обеспечение доступности информации только ограниченному кругу лиц, имеющих соответствующие полномочия.

Критичный информационный актив (критичная информация) – информация, создание, модификация и обработка которой связаны с повышенным риском информационной безопасности.

Критичные операции – операции, связанные с повышенными рисками информационной безопасности.

Критичные процессы/системы – процессы/системы, связанные с использованием критичных информационных активов.

Критичные уязвимости – недостатки и ошибки системного и прикладного программного обеспечения на всех уровнях архитектуры автоматизированных систем, создающие повышенные риски информационной безопасности критичным информационным активам.

Межсетевой экран – локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в информационную систему персональных данных и (или) выходящей из информационной системы.

Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных.

Обезличивание персональных данных – действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных.

Оценка риска – оценка вероятности реализации риска и величины возможных потерь при реализации конкретного вида риска и/или совокупных рисков, принимаемых на себя КГБУЗ «Ачинская МРБ».

Пользователь информационной системы персональных данных – лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования.

Программное (программно-математическое) воздействие – несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ.

Риск – возможность возникновения у КГБУЗ «Ачинская МРБ» финансовых потерь (убытков), незапланированных расходов или возможность снижения планируемых доходов, возможность потери репутации.

Операционный риск – риск, возникающий в результате недостатков в организации деятельности КГБУЗ «Ачинская МРБ», используемых технологиях, функционировании информационных систем, неадекватных действий или ошибок сотрудников, а также в результате внешних событий.

Информационный риск (ИТ - риск, риск автоматизации процессов) – риск, связанный с использованием информационных технологий, неудовлетворительным состоянием автоматизированных систем КГБУЗ «Ачинская МРБ».

Риск информационной безопасности – риск, являющийся составной частью ИТ - риска, возникающий вследствие наличия угроз безопасности информационным активам КГБУЗ «Ачинская МРБ».

Руководство – главный врач, заместители главного врача, заведующие структурными подразделениями.

Система обеспечения информационной безопасности – часть общей системы менеджмента КГБУЗ «Ачинская МРБ», предназначенная для создания, реализации, эксплуатации, мониторинга, анализа, поддержки и повышения информационной безопасности КГБУЗ «Ачинская МРБ». Включает структуру, политики, совокупность мероприятий, методов и средств, обеспечивающих требуемый уровень безопасности информационных активов участниками соответствующих процессов.

Съёмные носители - переносное устройство хранения информации, временно подключаемое к компьютерам, ноутбукам, планшетам и т.д. через стандартные разъёмы.

Угроза информационной безопасности – внешний или внутренний фактор, создающий риск информационной безопасности.

Целостность – обеспечение точности и полноты информации и методов ее обработки.

5 СОКРАЩЕНИЯ И ОБОЗНАЧЕНИЯ

В настоящей Политике используются следующие сокращения:

АС - автоматизированная система;

АСУ – автоматизированная система учёта

АВС - антивирусные средства;

АРМ - автоматизированное рабочее место;

БД - база данных;

ВрП - вредоносная программа;

ГМД - гибкий магнитный диск;

ИТ (IT) - информационные технологии;

ИСПДн - информационная система персональных данных;

КГБУЗ «Ачинская МРБ» (Учреждение) – Краевое государственное бюджетное учреждение здравоохранения «Ачинская межрайонная больница»;

ПДн - персональные данные;

НДПДн - несанкционированный доступ к персональным данным;

МЭ - межсетевой экран;

ЛВС - локальная вычислительная сеть;

НСД - несанкционированный доступ;

ПО - программное обеспечение;

СЗИ - средства защиты информации;

СЗПДн - система (подсистема) защиты персональных данных;

СОВ - система обнаружения вторжений;

СУБД - система управления базами данных;

УБПДн - угрозы безопасности персональных данных;

ЭЦП – электронно-цифровая подпись.

6 ОТВЕТСТВЕННОСТЬ

Ответственность за правильность разработки, актуализацию и внедрение Политики информационной безопасности Краевого государственного бюджетного учреждения здравоохранения «Ачинская межрайонная больница», несет начальник отдела АСУ, а также на сотрудников отдела АСУ в соответствии с таблицей 1 «Матрица ответственности».

Таблица 1 – Матрица ответственности

п/п	Наименование подразделения	Должность			
		Руководитель	Медицинский персонал	Административно-управленческий персонал	Прочий персонал
	Отдел АСУ	V	V	V	V

7.ОПИСАНИЕ ПРОЦЕССА

7.1. Система защиты персональных данных

Система защиты персональных данных (СЗПДн), строится на основании - перечня персональных данных, подлежащих защите; — модели угроз безопасности персональных данных; — руководящих документов ФСТЭК и ФСБ России.

На основании этих документов определяется необходимый уровень защищенности ПДн каждой ИСПДн Учреждения. На основании анализа актуальных угроз безопасности ПДн описанного в Модели угроз делается заключение о необходимости использования технических средств и организационных мероприятий для обеспечения безопасности ПДн. Выбранные необходимые мероприятия отражаются в Плане мероприятий по обеспечению защиты ПДн.

Для каждой ИСПДн должен быть составлен список используемых технических средств защиты, а также программного обеспечения участвующего в обработке ПДн, на всех элементах ИСПДн:

- АРМ пользователей;
- сервера приложений;
- СУБД;
- граница ЛВС;
- каналов передачи в сети общего пользования и (или) международного обмена, если по ним передаются ПДн.

В зависимости от уровня защищенности ИСПДн и актуальных угроз, СЗПДн может включать следующие технические средства:

- антивирусные средства для рабочих станций пользователей и серверов;
- средства межсетевого экранирования;

– средства криптографической защиты информации, при передаче защищаемой информации по каналам связи.

Так же в список должны быть включены функции защиты, обеспечиваемые штатными средствами обработки ПДн операционными системами (ОС), прикладным ПО и специальными комплексами, реализующими средства защиты. Список функций защиты может включать:

– управление и разграничение доступа пользователей;
– регистрация и учет действий с информацией;
– обеспечение целостности данных;
– мониторинг обнаружения вторжений.

Список используемых технических средств отражается в Плане мероприятий по обеспечению защиты персональных данных. Список используемых средств должен поддерживаться в актуальном состоянии. При изменении состава технических средств защиты или элементов ИСПДн, соответствующие изменения должны быть внесены в Список и утверждены руководителем Учреждения или лицом, ответственным за обеспечение защиты ПДн.

7.2. Требования к подсистемам СЗПДН

СЗПДн включает в себя следующие подсистемы:
– управления доступом, регистрации и учета;
– обеспечения целостности и доступности;
– антивирусной защиты;
– межсетевого экранирования;
– анализа защищенности;
– обнаружения вторжений;
– криптографической защиты.

7.3. Подсистемы управления доступом, регистрации и учета

Подсистема управления доступом, регистрации и учета предназначена для реализации следующих функций:

– идентификации и проверка подлинности субъектов доступа при входе в ИСПДн;

– идентификации терминалов, узлов сети, каналов связи, внешних устройств по логическим именам;

– идентификации программ, томов, каталогов, файлов, записей, полей записей по именам;

– регистрации входа (выхода) субъектов доступа в систему (из системы), либо регистрация загрузки и инициализации операционной системы и ее останова.

– регистрации попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам;

– регистрации попыток доступа программных средств к терминалам, каналам связи, программам, томам, каталогам, файлам, записям, полям записей.

Подсистема управления доступом может быть реализована с помощью штатных средств обработки ПДн (операционных систем, приложений и СУБД). Так же может быть внедрено специальное техническое средство или их комплекс осуществляющие дополнительные меры по аутентификации и контролю. Например, применение единых хранилищ учетных записей пользователей и регистрационной информации, использование биометрических и технических (с помощью электронных пропусков) мер аутентификации и других.

7.4. Подсистема обеспечения целостности и доступности

Подсистема обеспечения целостности и доступности предназначена для обеспечения целостности и доступности ПДн, программных и аппаратных средств ИСПДн Учреждения, а также средств защиты, при случайной или намеренной модификации.

Подсистема реализуется с помощью организации резервного копирования обрабатываемых данных, а также резервированием ключевых элементов ИСПДн.

7.5. Подсистема антивирусной защиты

Подсистема антивирусной защиты предназначена для обеспечения антивирусной защиты серверов и АРМ пользователей ИСПДн Учреждения.

Средства антивирусной защиты предназначены для реализации следующих функций:

— резидентный антивирусный мониторинг;

— антивирусное сканирование;

— скрипт-блокирование;

— централизованную/удаленную установку/деинсталляцию антивирусного продукта, настройку, администрирование, просмотр отчетов и статистической информации по работе продукта;

— автоматизированное обновление антивирусных баз;

— ограничение прав пользователя на остановку исполняемых задач и изменения настроек антивирусного программного обеспечения;

— автоматический запуск сразу после загрузки операционной системы.

Подсистема реализуется путем внедрения специального антивирусного программного обеспечения на все элементы ИСПДн.

7.6. Подсистема межсетевого экранирования

Подсистема межсетевого экранирования предназначена для реализации следующих функций:

— фильтрации открытого и зашифрованного (закрытого) IP-трафика по следующим параметрам;

— фиксации во внутренних журналах информации о проходящем открытом и закрытом IP-трафике;

— идентификации и аутентификацию администратора межсетевого экрана при его локальных запросах на доступ;

— регистрации входа (выхода) администратора межсетевого экрана в систему (из системы) либо загрузки и инициализации системы и ее программного останова;

— контроля целостности своей программной и информационной части;

— фильтрации пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств;

— фильтрации с учетом входного и выходного сетевого интерфейса как средство проверки подлинности сетевых адресов;

— регистрации и учета запрашиваемых сервисов прикладного уровня;

— блокирования доступа не идентифицированного объекта или субъекта, подлинность которого при аутентификации не подтвердилась, методами, устойчивыми к перехвату;

— контроля за сетевой активностью приложений и обнаружения сетевых атак.

Подсистема реализуется внедрением программно-аппаратных комплексов межсетевого экранирования на границе ЛСВ, классом не ниже 4.

7.7. Подсистема анализа защищенности

Подсистема анализа защищенности, должна обеспечивать выявления уязвимостей, связанных с ошибками в конфигурации ПО ИСПДн, которые могут быть использованы нарушителем для реализации атаки на систему.

Функционал подсистемы может быть реализован программными и программно-аппаратными средствами.

7.8. Подсистема обнаружения вторжений

Подсистема обнаружения вторжений, должна обеспечивать выявление сетевых атак на элементы ИСПДн подключенные к сетям общего пользования и (или) международного обмена.

Функционал подсистемы может быть реализован программными и программно-аппаратными средствами.

7.9. Подсистема криптографической защиты

Подсистема криптографической защиты предназначена для исключения НСД к защищаемой информации в ИСПДн Учреждения, при ее передаче по каналам связи сетей общего пользования и (или) международного обмена.

Подсистема реализуется внедрения криптографических программно-аппаратных комплексов.

8 ПОЛЬЗОВАТЕЛИ ИСПДН

В Концепции информационной безопасности определены основные категории пользователей. На основании этих категории должна быть произведена типизация пользователей ИСПДн, определен их уровень доступа и возможности.

В ИСПДн Учреждения можно выделить следующие группы пользователей, участвующих в обработке и хранении ПДн:

— администратора ИСПДн;

— администратора безопасности;

— оператора АРМ;

— администратора сети;

— технического специалиста по обслуживанию периферийного оборудования;

— программист-разработчик ИСПДн.

Данные о группах пользователях, уровне их доступа и информированности должен быть отражен в Положение о разграничении прав доступа к обрабатываемым персональным данным.

8.1. Администратор ИСПДн

Администратор ИСПДн, сотрудник Учреждения, ответственный за настройку, внедрение и сопровождение ИСПДн. Обеспечивает функционирование подсистемы управления доступом ИСПДн и уполномочен осуществлять предоставление и разграничение доступа конечного пользователя (Оператора АРМ) к элементам, хранящим персональные данные.

Администратор ИСПДн обладает следующим уровнем доступа и знаний:

— обладает полной информацией о системном и прикладном программном обеспечении ИСПДн;

— обладает полной информацией о технических средствах и конфигурации ИСПДн;

— имеет доступ ко всем техническим средствам обработки информации и данным ИСПДн;

— обладает правами конфигурирования и административной настройки технических средств ИСПДн.

8.2. Администратор безопасности

Администратор безопасности, сотрудник Учреждения, ответственный за функционирование СЗПДн, включая обслуживание и настройку административной, серверной и клиентской компонент.

Администратор безопасности обладает следующим уровнем доступа и знаний:

— обладает правами Администратора ИСПДн;

— обладает полной информацией об ИСПДн;

— имеет доступ к средствам защиты информации и протоколирования и к части ключевых элементов ИСПДн;

— не имеет прав доступа к конфигурированию технических средств сети за исключением контрольных (инспекционных).

Администратор безопасности уполномочен:

— реализовывать политики безопасности в части настройки СКЗИ, межсетевых экранов и систем обнаружения атак, в соответствии с которыми пользователь (Оператор АРМ) получает возможность работать с элементами ИСПДн;

— осуществлять аудит средств защиты;

— устанавливать доверительные отношения своей защищенной сети с сетями других Учреждений.

8.3. Оператор АРМ

Оператор АРМ, сотрудник Учреждения, осуществляющий обработку ПДн. Обработка ПДн включает: возможность просмотра ПДн, ручной ввод ПДн в систему ИСПДн, формирование справок и отчетов по информации, полученной из ИСПД. Оператор не имеет полномочий для управления подсистемами обработки данных и СЗПДн.

Оператор ИСПДн обладает следующим уровнем доступа и знаний:

— обладает всеми необходимыми атрибутами (например, паролем), обеспечивающими доступ к некоторому подмножеству ПДн; — располагает конфиденциальными данными, к которым имеет доступ.

8.4. Администратор сети

Администратор сети, сотрудник Учреждения, ответственный за функционирование телекоммуникационной подсистемы ИСПДн.

Администратор сети не имеет полномочий для управления подсистемами обработки данных и безопасности.

Администратор сети обладает следующим уровнем доступа и знаний:

— обладает частью информации о системном и прикладном программном обеспечении ИСПДн;

— обладает частью информации о технических средствах и конфигурации

ИСПДн;

— имеет физический доступ к техническим средствам обработки информации и средствам защиты;

— знает, по меньшей мере, одно легальное имя доступа.

8.5. Технический специалист по обслуживанию периферийного оборудования

Технический специалист по обслуживанию, сотрудник Учреждения, осуществляет обслуживание и настройку периферийного оборудования ИСПДн. Технический специалист по обслуживанию не имеет доступа к ПДн, не имеет полномочий для управления подсистемами обработки данных и безопасности.

Технический специалист по обслуживанию обладает следующим уровнем доступа и знаний:

— обладает частью информации о системном и прикладном программном обеспечении ИСПДн;

— обладает частью информации о технических средствах и конфигурации

ИСПДн; — знает, по меньшей мере, одно легальное имя доступа.

8.6. Программист-разработчик ИСПДн

Программисты-разработчики (поставщики) прикладного программного обеспечения, обеспечивающие его сопровождение на защищаемом объекте. К данной группе могут относиться как сотрудники Учреждения, так и сотрудники сторонних организаций.

Лицо этой категории:

— обладает информацией об алгоритмах и программах обработки информации на ИСПДн;

— обладает возможностями внесения ошибок, недекларированных возможностей, программных закладок, вредоносных программ в программное обеспечение ИСПДн на стадии ее разработки, внедрения и сопровождения;

— может располагать любыми фрагментами информации о топологии ИСПДн и технических средствах обработки и защиты ПДн, обрабатываемых в ИСПДн.

9 ТРЕБОВАНИЯ К ПЕРСОНАЛУ ПО ОБЕСПЕЧЕНИЮ ЗАЩИТЫ ПДн

Все сотрудники КГБУЗ «Ачинская МРБ», являющиеся пользователями ИСПДн, должны четко знать и строго выполнять установленные правила и обязанности по доступу к защищаемым объектам и соблюдению принятого режима безопасности ПДн.

При вступлении в должность нового сотрудника специалист по защите информации, обязан организовать его ознакомление с должностной инструкцией и необходимыми документами, регламентирующими требования по защите ПДн, а также обучение навыкам выполнения процедур, необходимых для санкционированного использования ИСПДн.

Сотрудник должен быть ознакомлен со сведениями настоящей Политики, принятых процедур работы с элементами ИСПДн и СЗПДн.

Сотрудники КГБУЗ «Ачинская МРБ», использующие технические средства аутентификации, должны обеспечивать сохранность идентификаторов (электронных ключей) и не допускать НСД к ним, а также возможность их утери или использования третьими лицами. Пользователи несут персональную ответственность за сохранность идентификаторов.

Сотрудники КГБУЗ «Ачинская МРБ» должны следовать установленным процедурам поддержания режима безопасности ПДн при выборе и использовании паролей (если не используются технические средства аутентификации).

Сотрудники КГБУЗ «Ачинская МРБ» должны обеспечивать надлежащую защиту оборудования, оставляемого без присмотра, особенно в тех случаях, когда в помещение имеют доступ посторонние лица. Все пользователи должны знать требования по безопасности ПДн и процедуры защиты оборудования, оставленного без присмотра, а также свои обязанности по обеспечению такой защиты.

Сотрудникам запрещается устанавливать постороннее программное обеспечение, подключать личные мобильные устройства и съёмные носители, а также записывать на них защищаемую информацию.

Сотрудникам запрещается разглашать защищаемую информацию, которая стала им известна при работе с информационными системами КГБУЗ «Ачинская МРБ», третьим лицам.

При работе с ПДн в ИСПДн сотрудники Учреждения обязаны обеспечить отсутствие возможности просмотра ПДн третьими лицами с мониторов АРМ или терминалов.

При завершении работы с ИСПДн сотрудники обязаны защитить АРМ или терминалы с помощью блокировки ключом или эквивалентного средства контроля, например, доступом по паролю, если не используются более сильные средства защиты.

Сотрудники КГБУЗ «АЧИНСКАЯ МРБ» должны быть проинформированы об угрозах нарушения режима безопасности ПДн и ответственности за его нарушение. Они должны быть ознакомлены с утвержденной формальной процедурой наложения дисциплинарных взысканий на сотрудников, которые нарушили принятые политику и процедуры безопасности ПДн.

Сотрудники обязаны без промедления сообщать обо всех наблюдаемых или подозрительных случаях работы ИСПДн, могущих повлечь за собой угрозы безопасности ПДн, а также о выявленных ими событиях, затрагивающих безопасность ПДн, руководству подразделения и лицу, отвечающему за немедленное реагирование на угрозы безопасности ПДн.

9.1. Должностные обязанности пользователей ИСПДн

Должностные обязанности пользователей ИСПДн описаны в следующих документах:

— Инструкция администратора ИСПДн;

— Инструкция администратора безопасности ИСПДн;

— Инструкция пользователя ИСПДн;

— Инструкция пользователя при возникновении внештатных ситуаций.

9.2. Ответственность сотрудников ИСПДн КГБУЗ «Ачинская МРБ»

В соответствии со ст. 24 Федерального закона Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных» лица, виновные в нарушении требований данного Федерального закона, несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

Действующее законодательство РФ позволяет предъявлять требования по обеспечению безопасной работы с защищаемой информацией и предусматривает ответственность за нарушение установленных правил эксплуатации ЭВМ и систем, неправомерный доступ к информации, если эти действия привели к уничтожению, блокированию, модификации информации или нарушению работы ЭВМ или сетей (статьи 272,273 и 274 УК РФ).

Администратор ИСПДн и администратор безопасности несут ответственность за все действия, совершенные от имени их учетных записей или системных учетных записей, если не доказан факт несанкционированного использования учетных записей.

При нарушениях сотрудниками Учреждения – пользователей ИСПДн правил, связанных с безопасностью ПДн, они несут ответственность, установленную действующим законодательством Российской Федерации.

Приведенные выше требования нормативных документов по защите информации должны быть отражены в Положениях о подразделениях, и должностных инструкциях сотрудников Учреждения.

Необходимо внести в Положения о подразделениях Учреждения, осуществляющих обработку ПДн в ИСПДн сведения об ответственности их руководителей и сотрудников за разглашение и несанкционированную модификацию (искажение, фальсификацию) ПДн, а также за неправомерное вмешательство в процессы их автоматизированной обработки.

10 ОРГАНИЗАЦИЯ СИСТЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Общее руководство системой обеспечения информационной безопасности в *КГБУЗ «Ачинская МРБ»* осуществляют главный врач.

10.1. Главный врач:

- утверждает и пересматривает политику информационной безопасности *КГБУЗ «Ачинская МРБ»*;
- организует процесс управления информационной безопасностью в *КГБУЗ «Ачинская МРБ»*, включая определение подразделений, ответственных за управление отдельными процессами обеспечения информационной безопасности, утверждение положений о них;
- обеспечивает условия и утверждает бюджет для эффективной реализации политики информационной безопасности;
- рассматривает информацию и отчеты о состоянии информационной безопасности *КГБУЗ «Ачинская МРБ»*.

Все подразделения *КГБУЗ «Ачинская МРБ»* и их руководители отвечают за реализацию политики информационной безопасности и управление процессами ее обеспечения в рамках своей компетенции.

10.2. Специалист по защиты информации:

- проводит первичные и внеплановые инструктажи по информационной безопасности
- разрабатывает нормативные, инструктивные и методические документы

КГБУЗ «Ачинская МРБ» по обеспечению информационной безопасности;

- разрабатывает требования по защите информационных активов в аспектах целостности и конфиденциальности на основе анализа рисков информационной безопасности;
- осуществляет контроль соответствия требованиям на всех стадиях жизненного цикла автоматизированных систем, от проектирования до снятия с эксплуатации;
- обеспечивает управление ключевыми системами средств криптографической защиты;
- организует проведение единой антивирусной политики в *КГБУЗ «Ачинская МРБ»*;
- проводит аудит подразделений по выполнению данной политики
- проводит расследования инцидентов и фактов нарушений информационной безопасности и информирует руководство *КГБУЗ «Ачинская МРБ»* о результатах проведенного расследования;
- организует обучение персонала *КГБУЗ «Ачинская МРБ»* по вопросам информационной безопасности;
- осуществляет инструментальный контроль и мониторинг текущего состояния информационной безопасности, информирует руководство *КГБУЗ «Ачинская МРБ»* об инцидентах информационной безопасности;
- осуществляет регистрацию инцидентов, имеющих отношение к информационной безопасности;
- регулярно (не реже одного раза в полгода) информирует руководство *КГБУЗ «Ачинская МРБ»* о состоянии информационной безопасности в больнице, в том числе, в составе сводных отчетов;
- обеспечивает взаимодействие с уполномоченными государственными органами по вопросам лицензирования и сертификации;
- взаимодействует с удостоверяющими центрами сторонних организаций;
- осуществляет анализ, оценку и прогноз риска, связанного с нарушением информационной безопасности *КГБУЗ «Ачинская МРБ»* и составляет совместно с отделом

АСУ список мер по уменьшению этих рисков

10.3. Отдел автоматизированных системы учёта:

- обеспечивает выполнение требований информационной безопасности при подключении и администрировании коммуникационного оборудования, операционных систем, СУБД и систем доставки;
- проводит обновление системного ПО, связанное с устранением критичных уязвимостей;
- обеспечивает доступность информационных активов в условиях отказов и других неблагоприятных событий в части

коммуникационного оборудования, операционных систем, СУБД и систем доставки.

- обеспечивает выполнение требований информационной безопасности при администрировании автоматизированных систем;
- ведет Фонд программ и документации *КГБУЗ «Ачинская МРБ»*;
- обеспечивает доступность информационных активов в условиях отказов и других неблагоприятных событий в части автоматизированных систем.
- обеспечивает реализацию требований информационной безопасности в разрабатываемых и находящихся на сопровождении АС.
- разрабатывает требования в области информационных технологий, участвует в формировании решений, связанных с организацией технологических процессов, разрабатывает предложения по использованию современных информационных технологий с учетом требований по обеспечению информационной безопасности.

10.4. Подразделения КГБУЗ «Ачинская МРБ»

- совместно со отделом АСУ проводят категорирование информационных активов, владельцами которых они являются, и определяют те из них, которые являются критичными;
- совместно со отделом АСУ участвуют в оценке рисков реализации угроз их информационным активам;
- устанавливают в пределах своей компетенции режим и порядок доступа, правила работы с информационными активами, владельцами которых они являются;
- разрабатывают нормативные и инструктивные документы с учетом требований информационной безопасности;
- обеспечивают выполнение требований и процедур информационной безопасности при работе сотрудников с информационными активами *КГБУЗ «Ачинская МРБ»*.

Ознакомление с данной политикой проводит специалист по защите информации во время первичного инструктажа по информационной безопасности. Данный инструктаж должен проводиться при приеме на работу нового сотрудника.

11 ОБЩИЕ ТРЕБОВАНИЯ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КГБУЗ «АЧИНСКАЯ МРБ»

В основе процессов управления информационной безопасностью КГБУЗ «Ачинская МРБ» лежат следующие общие требования:

11.1. Назначение и распределение ролей, и обеспечение доверия к персоналу

—Ролевое управление является основным механизмом управления полномочиями пользователей и администраторов в автоматизированных системах. Роли формируются с учетом принципа минимальности полномочий.

Роли пользователю назначаются администратором ИСПДн в момент создания ему логина и пароля.

Ни одна роль не должна позволять пользователю проводить единолично критичные операции.

Критичные технологические процессы должны быть защищены от ошибочных и несанкционированных действий администраторов. Штатные процедуры администрирования, диагностики и восстановления должны выполняться через специальные роли в автоматизированных системах без непосредственного доступа к данным.

В критичных системах по решению владельца информационного актива может вводиться роль администратора информационной безопасности АС, в функции которого входит подтверждение прав и полномочий пользователей, заведенных в системе ее администратором.

Должностные обязанности сотрудников и трудовые договоры предусматривают обязанности персонала по выполнению требований по обеспечению информационной безопасности, включая обязательства по неразглашению информации, составляющей персональные данные и коммерческую тайну КГБУЗ «Ачинская МРБ».

Приказы и распоряжения, актуальная информация по вопросам обеспечения информационной безопасности, в том числе по выявленным нарушениям, доводятся до всех сотрудников КГБУЗ «Ачинская МРБ» под роспись.

Реализуются программы обучения персонала КГБУЗ «Ачинская МРБ» и информирования в вопросах обеспечения информационной безопасности. Периодически проверяется и оценивается уровень компетентности персонала в этих вопросах.

11.2. Управление доступом к информационным активам и регистрация

Все информационные активы идентифицируются, категорируются и имеют своих владельцев.

Не предоставляется доступ к информационной сети КГБУЗ «Ачинская МРБ» электронно-вычислительных устройствам не прошедших сетевую идентификацию по доменному имени

Пользователям ИСПДн запрещается самостоятельно подключать сетевое оборудование (WI-Fi роутеры, планшеты, сотовые телефоны и т.д.)

Не корпоративное сетевое оборудование не будет иметь доступа к информационной сети КГБУЗ «Ачинская МРБ».

Доступ ко всем информационным активам *КГБУЗ «Ачинская МРБ»* осуществляется только после авторизации пользователя. Средством авторизации (аутентификации является) является доменная учетная запись.

Пароль учетной записи должен отвечать минимальным требованиям сложности, а именно:

- пароль не может содержать имя учетной записи пользователя или какую-либо его часть;
- пароль должен состоять не менее чем из шести символов;
- в пароле должны присутствовать символы трех категорий из числа следующих четырех:

а) прописные буквы английского алфавита от A до Z;

б) строчные буквы английского алфавита от a до z;

в) десятичные цифры (от 0 до 9);

г) неалфавитные символы (например, !, $, #, %).

Смена пароля учетной записи должна производится не реже 1 раза в 90 календарных дней.

Запрещается разглашать пароль от своей учетной записи другим сотрудникам, каждый пользователь ИСПДн должен работать, используя исключительно свою учетную запись.

Блокировка учетной записи пользователя производится:

- автоматически при неправильном вводе пароля более 5 раз (на 15 мин, после чего блокировка снимается)
- при увольнении сотрудника в момент отметки обходного листа администратором учетной безопасности
- по распоряжению главного врача КГБУЗ
- при возникновении угрозы НДПДниз - под данной учетной записи

Доступ к информационным ресурсам всем сотрудникам *КГБУЗ «Ачинская МРБ»* предоставляется только на основании документально оформленных заявок, согласованных с их владельцами. По умолчанию определяется отсутствие доступа.

Правила сетевого файлообмена в КГБУЗ «Ачинская МРБ» регулируется на основании стандарта «ГОСТ Р 54471-2011 Системы электронного документооборота. Управление документацией. Информация, сохраняемая в электронном виде. Рекомендации по обеспечению достоверности и надежности».

Проводится периодический (для наиболее критичных систем - не реже одного раза в год) формальный контроль соответствия согласованных и реальных прав доступа к информационным активам текущему статусу пользователя.

Работа пользователей с базами данных осуществляется исключительно через экранные формы автоматизированных систем. Прямой доступ пользователей к базам данных не предоставляется.

Журналы аудита действий пользователей и администраторов автоматизированных систем должны быть информативны, защищены от модификации и храниться в течение срока, потенциально необходимого для использования при расследовании возможных инцидентов, связанных с нарушением информационной безопасности.

11.3. Управление жизненным циклом автоматизированных систем

Процедуры по обеспечению информационной безопасности предусматриваются на всех стадиях жизненного цикла автоматизированных систем: при разработке (приобретении), эксплуатации, модернизации, снятии с эксплуатации.

Разработка, тестирование автоматизированных систем отделяются от эксплуатации:

- разработка и тестирование программного обеспечения проводятся на выделенных физически или логически средствах вычислительной техники (виртуальные серверы), не использующихся для промышленной эксплуатации автоматизированных систем. Хорошей практикой является выделение рабочих станций и серверов, предназначенных для разработки и тестирования программного обеспечения, в отдельный сегмент ЛВС, доступ из которого к промышленным системам ограничивается.

В контрактах со сторонними разработчиками на поставку систем предусматривается их ответственность за наличие в системах скрытых недокументированных возможностей, ведущих к финансовому и репутационному ущербу *КГБУЗ «Ачинская МРБ»*, а также соблюдение условий конфиденциальности.

Системы сторонней разработки проверяются на соответствие требованиям информационной безопасности, предъявляемым *КГБУЗ «Ачинская МРБ»*. При несоответствии текущей версии системы требованиям *КГБУЗ «Ачинская МРБ»* по информационной безопасности, указанные требования включаются в контракт на поставку и приобретается доработанная версия.

Все изменения, вносимые в автоматизированные системы, контролируются и документируются. Дистрибутивные комплекты и исходные тексты систем собственной разработки, а также дистрибутивные комплекты приобретаемых систем хранятся в отделе АСУ.

Ввод автоматизированных систем в эксплуатацию производится только после их аттестации на соответствие предъявленным требованиям по информационной безопасности. Не допускается эксплуатация автоматизированных систем, не прошедших аттестации или имеющих не устранённые критичные замечания.

При выводе АС из эксплуатации или замене входящего в ее состав оборудования осуществляется принудительное удаление конфиденциальной информации с соответствующих машинных носителей и из памяти компьютеров за исключением ведущихся в установленном порядке контрольных архивов электронных документов.

11.4. Антивирусная защита

Каждый сотрудник *КГБУЗ «Ачинская МРБ»* обязан выполнять правила эксплуатации антивирусного ПО и требования антивирусной безопасности в отношении внешних источников и съёмных носителей, а также сети Интернет, немедленно прекращать работу и информировать службы автоматизации и безопасности при подозрениях на вирусное заражение.

Для снижения влияния человеческого фактора, исключения возможности отключения или не обновления антивирусных средств, контроль и управление антивирусным программным обеспечением, а также устранение выявленных уязвимостей в системном программном обеспечении производится централизованно в автоматизированном режиме. При этом обеспечивается минимально возможный период обновления с учетом обязательного предварительного тестирования на совместимость с системным и прикладным ПО.

11.5. Использование ресурсов Интернет

Использование ресурсов Интернет в подразделениях *КГБУЗ «Ачинская МРБ»* разрешается исключительно в производственных целях.

Доступ к сайтам информационной сети интернет, посещение которых может угрожать безопасности информационной сети КГБУЗ «Ачинская МРБ» запрещен.

Предоставление услуг клиентам КГБУЗ «Ачинская МРБ» и взаимодействие с партнерами по сети Интернет осуществляется с использованием специализированных систем и средств защиты, аттестованных на соответствие требованиям информационной безопасности.

Прямое подключение к рабочим станциям ЛВС КГБУЗ «Ачинская МРБ» мобильных телефонов, беспроводных (радио) интерфейсов, модемов и прочего оборудования, позволяющего выходить в Интернет, запрещается.

Порядок публикации информации в сети Интернет определяется отдельными регламентами.

Запрещается передача не обезличенных ПДн через сеть интернет.

На узлах доступа в сеть Интернет принимаются необходимые меры для противодействия хакерским атакам и распространению спама.

11.6. Использование средств криптографической защиты информации

Применение средств криптографической защиты информации для обеспечения безопасности информационных активов *КГБУЗ «Ачинская МРБ»* и взаимодействия с клиентами производится в соответствии с порядком, установленным государственными уполномоченными органами.

Использование средств ЭП обеспечивает целостность электронного документа и подтверждение авторства подписавшей его стороны и является лучшей практикой организации электронного документооборота при взаимодействии с партнерами.

Использование иных аналогов собственноручной подписи (кодов аутентификации, PIN-кодов и пр.) при взаимодействии с партнерами допускается в технически и экономически обоснованных случаях.

Во внутренних системах КГБУЗ «Ачинская МРБ» электронная подпись и/или другие механизмы криптографического контроля целостности используются в зависимости от результатов оценки рисков информационной безопасности, а также в случаях, когда необходимо строго разделить ответственность между подразделениями или сотрудниками КГБУЗ «Ачинская МРБ».

Конфиденциальность информации при передаче по публичным сетям и внешним каналам связи обеспечивается обязательным применением шифрования. В обоснованных случаях информация, составляющая коммерческую тайну *КГБУЗ «Ачинская МРБ»* и персональные данные, может также шифроваться при ее передаче в ЛВС и хранении на средствах вычислительной техники.

Риски, связанные с возможной компрометацией криптографических ключей или доступом к защищаемой информации в обход средств криптографической защиты, должны минимизироваться специальными техническими и организационными мерами.

Ключи электронной подписи, предназначенные для защиты финансового электронного документооборота *КГБУЗ «Ачинская МРБ»* со сторонними организациями, изготавливаются самостоятельно *КГБУЗ «Ачинская МРБ»*.

11.7. Обеспечение непрерывности бизнеса и восстановления после сбоев

Непрерывность критичных рабочих процессов при наступлении отказов и сбоев обеспечивается резервированием оборудования, каналов связи, резервным копированием информации, регулярной проверкой их работоспособности и адекватности. Процедуры восстановления после сбоев документируются в соответствующих регламентах и планах.

11.8. Обеспечение физической безопасности

Помещения *КГБУЗ «Ачинская МРБ»* категорируются в зависимости от критичности размещаемых в них информационных активов. В соответствии с категорией обеспечивается техническая укрепленность помещений, оснащение средствами видеоконтроля, контроля доступа, пожаротушения и сигнализации.

12 ВНЕСЕНИЕ ИЗМЕНЕНИЙ

Предложения по внесению изменений в содержание настоящей Политики может внести любой сотрудник. Предложения передаются начальнику отдела АСУ.

Внесение изменений в подлинник настоящего стандарта производит начальник отдела АСУ, совместно с менеджером отдела СМК.

13 ХРАНЕНИЕ

Подлинник настоящей Политики хранится в отделе СМК.

Срок хранения подлинника – до минования надобности.

Электронная версия утвержденной Политики располагается на сетевых ресурсах КГБУЗ «Ачинская МРБ»:

- Share//ИНФОРМАЦИЯ\СМК\Раздел 11. Безопасность среды\П 11.4-2025 Политика информационной безопасности КГБУЗ «Ачинская МРБ».

ЛИСТ ОЗНАКОМЛЕНИЯ С ПОЛИТИКОЙ

Структурное подразделение: ____
____

Фамилия, инициалы	**Должность**	**Подпись**	**Дата**