МИНИСТЕРСТВО ЗДРАВООХРАНЕНИЯ АЛТАЙСКОГО КРАЯ

КРАЕВОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ ЗДРАВООХРАНЕНИЯ «АЛТАЙСКИЙ КРАЕВОЙ ГОСПИТАЛЬ ДЛЯ ВЕТЕРАНОВ ВОЙН» (КГБУЗ «АКГВВ»)

П Р И К А З

24 июня 2024 г. № 135

г. Барнаул

О защите конфиденциальной информации и персональных данных в КГБУЗ «АКГВВ»

В соответствии с требованиями Федерального закона Российской Федерации от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», от 27.07.2006 № 152-ФЗ «О персональных данных», указа Президента Российской Федерации от 06.03.1997 № 188 «Об утверждении перечня сведений конфиденциального характера», постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», приказа Гостехкомиссии России от 30.08.2002 № 282 «Специальные требования и рекомендации по технической защите конфиденциальной информации» (далее СТР-К), в целях организации работы по защите конфиденциальной информации и персональных данных в краевом государственном бюджетном учреждении здравоохранения «Алтайский краевой госпиталь для ветеранов войн» (далее – КГБУЗ «АКГВВ») п р и к а з ы в а ю:

1. Утвердить прилагаемые:

1.1. Политику информационной безопасности (Приложение № 1);

1.2. Положение о конфиденциальной информации (Приложение № 2);

1.3. Положение о порядке организации проведении работ по защите информации в информационных системах КГБУЗ «АКГВВ» (Приложение № 3);

1.4. Описание технологического процесса обработки информации в информационных системах (Приложение № 4);

1.5. Политика проведения антивирусного контроля (Приложение № 5);

1.6. Порядок работы ответственного за обеспечение безопасности информации в информационных системах (Приложение №6).

1.7. Порядок работы администратора информационных систем (Приложение № 7);

1.8. Порядок работе пользователей в информационных системах (Приложение № 8);

1.9. Перечень сведений конфиденциального характера (Приложение №9);

1.10. Порядок организации работы с материальными носителями защищаемых информационных ресурсов (Приложение №10).

1.11. Порядок работы с электронными носителями конфиденциальной

информации (Приложение № 11);

1.12. Перечень защищаемых информационных ресурсов (Приложение № 12);

1.13. Обязательства о неразглашении сведений конфиденциального характера (Приложение № 13);

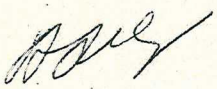
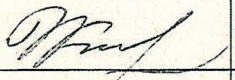
2. Руководителям структурных подразделений ознакомить своих сотрудников, допущенных к сведениям, содержащим конфиденциальную информацию и персональные данные с настоящим приказом.

3. Начальнику отдела кадров Жуковой Ю.Ю. при оформлении на работу новых специалистов ознакомить с настоящим приказом.

4. Контроль за исполнением приказа оставляю за собой.

Начальник КГБУЗ «АКГВВ» О.А. Зубова

СОГЛАСОВАНО

Заместитель начальника КГБУЗ «АКГВВ» по медицинской части		А.Г. Харлова
Начальник отдела информационных технологий		Н.М. Кулеш
Начальник отдела кадров		Ю.Ю. Жукова

СПИСОК ДЛЯ РАССЫЛКИ:
Все отделения
Отдел кадров
Консультативно-поликлиническое отделение
Отдел закупок

Кулеш Наталья Михайловна

Приложение № 1
УТВЕРЖДЕНА
приказом начальника
КГБУЗ «АКГВВ»
от _____

ПОЛИТИКА
информационной безопасности КГБУЗ «АКГВВ»

1. Перечень используемых определений, обозначений и сокращений

АИБ – Администратор информационной безопасности.
АРМ – Автоматизированное рабочее место.
АС – Автоматизированная система.
ИБ – Информационная безопасность.
ИР – Информационные ресурсы.
ИС – Информационная система.
МЭ – Межсетевой экран.
НСД – Несанкционированный доступ.
ОС – Операционная система.
ПБ – Политики безопасности.
ПДн – Персональные данные.
ПО – Программное обеспечение.
СЗИ – Средство защиты информации.
ЭВМ – Электронная – вычислительная машина, персональный компьютер.

Автоматизированная система – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Администратор информационной безопасности – специалист или группа специалистов организации, осуществляющих контроль за обеспечением защиты информации в ЛВС, а также осуществляющие организацию работ по выявлению и предупреждению возможных каналов утечки информации, потенциальных возможностей осуществления НСД к защищаемой информации.

Доступ к информации – возможность получения информации и ее использования.

Идентификация – присвоение субъектам доступа (пользователям, процессам) и объектам доступа (информационным ресурсам, устройствам) идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Информация – это актив, который, подобно другим активам, имеет ценность и, следовательно, должен быть защищен надлежащим образом.

Информационная безопасность – механизм защиты, обеспечивающий конфиденциальность, целостность, доступность информации; состояние защищенности информационных активов в условиях угроз в информационной сфере. Угрозы могут быть вызваны непреднамеренными ошибками персонала, неправильным функционированием технических средств, стихийными бедствиями или авариями (пожар, наводнение, отключение электроснабжения,

нарушение телекоммуникационных каналов и т.п.), либо преднамеренными злоумышленными действиями, приводящими к нарушению информационных активов.

Информационная система – совокупность программного обеспечения и технических средств, используемых для хранения, обработки и передачи информации, с целью решения задач подразделений КГБУЗ «АКГВВ».

Информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Информационные ресурсы – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий.

Источник угрозы – намерение или метод, нацеленный на умышленное использование уязвимости, либо ситуация или метод, которые могут случайно проявить уязвимость.

Конфиденциальная информация – информация с ограниченным доступом, не содержащая сведений, составляющих государственную тайну, доступ к которой ограничивается в соответствии с законодательством Российской Федерации.

Конфиденциальность – доступ к информации только авторизованных пользователей.

Критичная информация – информация, нарушение доступности, целостности, либо конфиденциальности которой, может оказать негативное влияние на функционирование подразделений КГБУЗ «АКГВВ» или иного вида ущерба.

Локальная вычислительная сеть – группа ЭВМ, а также периферийное оборудование, объединенные одним или несколькими автономными высокоскоростными каналами передачи цифровых данных в пределах одного или нескольких близлежащих зданий.

Межсетевой экран – программно-аппаратный комплекс, используемый для контроля доступа между ЛВС, входящими в состав сети, а также между сетью КГБУЗ «АКГВВ» и внешними сетями (сетью Интернет).

Несанкционированный доступ к информации – доступ к информации, нарушающий правила разграничения уровней полномочий пользователей.

Политика информационной безопасности – комплекс взаимоувязанных руководящих принципов и разработанных на их основе правил, процедур и практических приемов, принятых в КГБУЗ «АКГВВ» для обеспечения его информационной безопасности.

Пользователь локальной вычислительной сети – сотрудник организации (штатный, временный, работающий по контракту и т.п.), а также прочие лица (подрядчики, аудиторы и т.п.), зарегистрированный в сети в установленном порядке и получивший права на доступ к ресурсам сети в соответствии со своими функциональными обязанностями.

Программное обеспечение – совокупность прикладных программ, установленных на сервере или ЭВМ.

Рабочая станция – персональный компьютер, на котором пользователь сети выполняет свои служебные обязанности.

Регистрационная (учетная) запись пользователя – включает в себя имя пользователя и его уникальный цифровой идентификатор, однозначно идентифицирующий данного пользователя в операционной системе (сети, базе данных, приложении и т.п.). Регистрационная запись создается администратором при регистрации пользователя в операционной системе компьютера, в системе управления базами данных, в сетевых доменах, приложениях и т.п. Она также может содержать такие сведения о пользователе, как Ф.И.О., название подразделения, телефоны, E-mail и т.п.

Роль – совокупность полномочий и привилегий на доступ к информационному ресурсу, необходимых для выполнения пользователем определенных функциональных обязанностей.

Ответственный за техническое обеспечение – сотрудник организации, занимающийся сопровождением автоматизированных систем, отвечающий за функционирование локальной сети КГБУЗ «АКГВВ» и ПК.

Угрозы информации – потенциально существующая опасность случайного или преднамеренного разрушения, несанкционированного получения или модификации данных, обусловленная структурой системы обработки, а также условиями обработки и хранения данных, т.е. это потенциальная возможность источника угроз успешно выявить определенную уязвимость системы.

Уязвимость – недостатки или слабые места информационных активов, которые могут привести к нарушению информационной безопасности при реализации угроз в информационной сфере.

Целостность информации – состояние защищенности информации, характеризуемое способностью АС обеспечивать сохранность и неизменность конфиденциальной информации при попытках несанкционированных или случайных воздействий на нее в процессе обработки или хранения.

Электронная подпись – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.

2. Вводные положения

2.1. Введение

Политика ИБ Краевого государственного бюджетного учреждения здравоохранения «Алтайский краевой госпиталь ветеранов войн» (далее - КГБУЗ «АКГВВ») определяет цели и задачи системы обеспечения ИБ и устанавливает совокупность правил, требований и руководящих принципов в области ИБ, которыми руководствуется КГБУЗ «АКГВВ» в своей деятельности.

2.2. Цели

Основными целями политики ИБ являются защита информации КГБУЗ «АКГВВ» от возможного нанесения материального, физического, морального или иного ущерба, посредством случайного или преднамеренного воздействия на информацию, ее носители, процессы обработки и передачи и обеспечение эффективной работы всего информационно-вычислительного комплекса при осуществлении деятельности, указанной в Положении о деятельности КГБУЗ «АКГВВ».

Общее руководство обеспечением ИБ осуществляется начальником КГБУЗ «АКГВВ». Ответственность за организацию мероприятий по обеспечению ИБ и контроль за соблюдением требований ИБ несет Администратор ИБ. Ответственность за функционирование информационных систем КГБУЗ «АКГВВ» несет администратор информационной системы.

Должностные обязанности АИБа и системного администратора закрепляются в соответствующих инструкциях.

Руководители структурных подразделений КГБУЗ «АКГВВ» ответственны за обеспечение выполнения требований ИБ в своих подразделениях.

Сотрудники КГБУЗ «АКГВВ» обязаны соблюдать порядок обращения с конфиденциальными документами, носителями ключевой информации и другой защищаемой информацией, соблюдать требования настоящей Политики и других документов внутренних документов КГБУЗ «АКГВВ» по вопросам обеспечения ИБ.

2.3. Задачи

Политика ИБ направлена на защиту информационных активов от угроз, исходящих от противоправных действий злоумышленников, уменьшение рисков и снижение потенциального вреда от аварий, непреднамеренных ошибочных действий персонала, технических сбоев, неправильных технологических и организационных решений в процессах обработки, передачи и хранения информации и обеспечение нормального функционирования технологических процессов.

Наибольшими возможностями для нанесения ущерба КГБУЗ «АКГВВ» обладает собственный персонал. Действия персонала могут быть мотивированы злым умыслом (при этом злоумышленник может иметь сообщников как внутри, так и вне КГБУЗ «АКГВВ»), либо иметь непреднамеренный ошибочный характер. Категории нарушителей и их возможности определяются в «Модели нарушителя».

На основе вероятностной оценки определяется перечень актуальных угроз безопасности, который отражается в «Модели угроз».

Для противодействия угрозам ИБ в КГБУЗ «АКГВВ» на основе имеющегося опыта составляется прогностическая модель предполагаемых угроз и модель нарушителя. Чем точнее сделан прогноз (составлены модель угроз и модель нарушителя), тем ниже риски нарушения ИБ при минимальных ресурсных затратах.

Разработанная на основе прогноза политика ИБ и в соответствии с ней построенная СУИБ является наиболее правильным и эффективным способом добиться минимизации рисков нарушения ИБ для КГБУЗ «АКГВВ». Необходимо учитывать, что с течением времени меняется характер угроз, поэтому следует своевременно, используя данные мониторинга и аудита, обновлять модели угроз и нарушителя.

Стратегия обеспечения ИБ заключается в использовании заранее разработанных мер противодействия атакам злоумышленников, а также программно-технических и организационных решений, позволяющих свести к

минимуму возможные потери от технических аварий и ошибочных действий персонала.

Задачами настоящей политики являются:

- описание организации системы управления информационной безопасности ;
- определение Политик ИБ;
- определение порядка сопровождения ИС».

2.4. Область действия

Настоящая Политика распространяется на все структурные подразделения КГБУЗ «АКГВВ» и обязательна для исполнения всеми его сотрудниками и должностными лицами. Положения настоящей Политики применимы для использования во внутренних нормативных и методических документах, а также в договорах.

2.5. Период действия и порядок внесения изменений

Настоящая Политика вводится в действие приказом начальника КГБУЗ «АКГВВ».

Политика признается утратившей силу на основании приказа начальника КГБУЗ «АКГВВ».

Изменения в политику вносятся приказом начальника КГБУЗ «АКГВВ».

Инициаторами внесения изменений в политику информационной безопасности являются:

- начальник КГБУЗ «АКГВВ»;
- руководители структурных подразделений КГБУЗ «АКГВВ»;
- администратор информационной безопасности.

Плановая актуализация настоящей политики производится ежегодно и имеет целью приведение в соответствие определенных политикой защитных мер реальным условиям и текущим требованиям к защите информации.

Внеплановая актуализация политики ИБ и производится в обязательном порядке в следующих случаях:

- при изменении политики Российской Федерации в области ИБ, указов и законов Российской Федерации в области защиты информации;
- при изменении внутренних нормативных документов (инструкций, положений, руководств), касающихся ИБ КГБУЗ «АКГВВ»;
- при происшествии и выявлении инцидента (инцидентов) по нарушению ИБ, влекущего ущерб КГБУЗ «АКГВВ».

Ответственными за актуализацию политики ИБ (плановую и внеплановую) несет АИБ.

Контроль за исполнением требований настоящей политики и поддержанием ее в актуальном состоянии возлагается на АИБа.

3. Политики информационной безопасности КГБУЗ «АКГВВ»

3.1. Назначение политик информационной безопасности

Политики ИБ КГБУЗ «АКГВВ» – это совокупность норм, правил и практических рекомендаций, на которых строится управление, защита и распределение информации в КГБУЗ «АКГВВ».

Политики ИБ относятся к административным мерам обеспечения ИБ и определяют стратегию КГБУЗ «АКГВВ» в области ИБ.

Политики ИБ регламентируют эффективную работу СЗИ. Они охватывают все особенности процесса обработки информации, определяя поведение ИС и ее пользователей в различных ситуациях. Политики ИБ реализуются посредством административно-организационных мер, физических и программно-технических средств и определяет архитектуру системы защиты.

Все документально оформленные решения, формирующие Политики, должны быть утверждены начальником КГБУЗ «АКГВВ».

3.2. Основные принципы обеспечения информационной безопасности

Основными принципами обеспечения ИБ являются следующие:

– постоянный и всесторонний анализ информационного пространства КГБУЗ «АКГВВ» с целью выявления уязвимостей информационных активов;

– своевременное обнаружение проблем, потенциально способных повлиять на ИБ КГБУЗ «АКГВВ», корректировка моделей угроз и нарушителя;

– разработка и внедрение защитных мер, адекватных характеру выявленных угроз, с учетом затрат на их реализацию. При этом меры, принимаемые для обеспечения ИБ, не должны усложнять достижение уставных целей КГБУЗ «АКГВВ», а также повышать трудоемкость технологических процессов обработки информации;

– контроль эффективности принимаемых защитных мер;

– персонификация и адекватное разделение ролей и ответственности между сотрудниками КГБУЗ «АКГВВ», исходя из принципа персональной и единоличной ответственности за совершаемые операции.

3.3. Соответствие Политики безопасности действующему законодательству:

Правовую основу политик составляют законы Российской Федерации и другие законодательные акты, определяющие права и ответственность граждан, сотрудников и государства в сфере безопасности, а также нормативные, отраслевые и ведомственные документы, по вопросам безопасности информации, утвержденные органами государственного управления различного уровня в пределах их компетенции.

3.4. Ответственность за реализацию политик информационной безопасности:

Ответственность за разработку мер и контроль обеспечения защиты информации несёт АИБ.

Ответственность за реализацию политик возлагается:

– в части, касающейся разработки и актуализации правил внешнего доступа и управления доступом, антивирусной защиты – на АИБа;

– в части, касающейся доведения правил политик до сотрудников КГБУЗ «АКГВВ», а также иных лиц (см. область действия настоящей политики) – на АИБа;

– в части, касающейся исполнения правил политики, – на каждого сотрудника КГБУЗ «АКГВВ», согласно их должностным и функциональным обязанностям, и иных лиц, попадающих под область действия настоящей политики.

3.5. Порядок подготовки персонала по вопросам информационной безопасности и допуска его к работе:

Организация обучения сотрудников КГБУЗ «АКГВВ» в области ИБ возлагается на АИБа. Обучение проводится согласно Плану, утвержденному начальником КГБУЗ «АКГВВ».

Подписи сотрудников об ознакомлении заносятся в «Журнал проведения инструктажа по информационной безопасности».

Допуск персонала к работе с защищаемыми ИР КГБУЗ «АКГВВ» осуществляется только после его ознакомления с настоящими политиками, а также после ознакомления пользователей с «Порядком работы пользователей» КГБУЗ «АКГВВ», а так же иными инструкциями пользователей отдельных ИС. Согласие на соблюдение правил и требований настоящих политик подтверждается подписями сотрудников в «Журнале проведения инструктажа по информационной безопасности».

Допуск персонала к работе с КИ КГБУЗ «АКГВВ» осуществляется после ознакомления с «Порядком организации работы с материальными носителями», «Порядок организации работы с электронными носителями». Правила допуска к работе с ИР лиц, не являющихся сотрудниками КГБУЗ «АКГВВ», определяются на договорной основе с этими лицами или с организациями, представителями которых являются эти лица.

3.6. Защищаемые информационные ресурсы КГБУЗ «АКГВВ»

Защищаемые информационные ресурсы определяются в соответствии с «Перечнем защищаемых ресурсов», утверждаемым соответствующим приказом начальника КГБУЗ «АКГВВ».

4. Политики информационной безопасности

4.1. Политика предоставления доступа к информационному ресурсу

4.1.1. Назначение

Настоящая Политика определяет основные правила предоставления сотрудникам доступа к защищаемым ИР КГБУЗ «АКГВВ».

4.1.2. Положение политики

Положения данной политики определены в «Положении о разрешительной системе допуска», утверждаемом соответствующим приказом начальника КГБУЗ «АКГВВ».

4.2. Политика учетных записей

4.2.1. Назначение:

Настоящая политика определяет основные правила присвоения учетных записей пользователям информационных активов КГБУЗ «АКГВВ».

4.2.2. Положение политики

Регистрационные учетные записи подразделяются на:

– пользовательские – предназначенные для идентификации/аутентификации пользователей информационных активов КГБУЗ «АКГВВ»;
– системные – используемые для нужд операционной системы;
– служебные – предназначенные для обеспечения функционирования отдельных процессов или приложений.

Каждому пользователю информационных активов КГБУЗ «АКГВВ» назначается уникальная пользовательская регистрационная учетная запись.

Допускается привязка более одной пользовательской учетной записи к одному и тому же пользователю (например, имеющих различный уровень полномочий).

В общем случае запрещено создавать и использовать общую пользовательскую учетную запись для группы пользователей. В случаях, когда это необходимо, ввиду особенностей автоматизируемого бизнес-процесса или организации труда (например, посменное дежурство), использование общей учетной записи должно сопровождаться отметкой в журнале учета машинного времени, которая должна однозначно идентифицировать текущего владельца учетной записи в каждый момент времени. Одновременное использование одной общей пользовательской учетной записи разными пользователями запрещено.

Системные регистрационные учетные записи формируются операционной системой и должны использоваться только в случаях, предписанных документацией на операционную систему.

Служебные регистрационные учетные записи используются только для запуска сервисов или приложений.

Использование системных или служебных учетных записей для регистрации пользователей в системе категорически запрещено.

Настоящая Политика определяет основные правила парольной защиты в КГБУЗ «АКГВВ».

Положения политики закрепляются в «Порядке по организации парольной защиты».

4.3. Политика реализации антивирусной защиты

4.3.1. Назначение:

Настоящая Политика определяет основные правила для реализации антивирусной защиты в КГБУЗ «АКГВВ».

Положения политики закрепляются в «Порядке по проведению антивирусного контроля».

4.4. Политика защиты автоматизированного рабочего места

4.4.1. Назначение

Настоящая Политика определяет основные правила и требования по защите автоматизированных рабочих мест КГБУЗ «АКГВВ».

4.5. Политика использования паролей

4.5.1. Назначение:

Настоящая Политика определяет основные правила и требования по защите информации КГБУЗ «АКГВВ» от неавторизованного доступа, утраты или модификации.

4.5.2. Положения политики

Положения данной политики определяются в соответствии с используемым техническим решением.

5. Профилактика нарушений политик информационной безопасности

Под профилактикой нарушений политик ИБ понимается проведение регламентных работ по защите информации, предупреждение возможных нарушений ИБ в КГБУЗ «АКГВВ» и проведение разъяснительной работы по ИБ среди пользователей.

Положения определены документами, утвержденными Приказом «Об обучении сотрудников правилам защиты информации», и «Порядком технического обслуживания средств вычислительной техники».

5.1. Ликвидация последствий нарушения политик информационной безопасности

АИБ, используя данные, полученные в результате применения инструментальных средств контроля (мониторинга) безопасности информации ИС, должен своевременно обнаруживать нарушения ИБ, факты осуществления НСД к защищаемым ИР и предпринимать меры по их локализации и устранению.

В случае обнаружения подсистемой защиты информации факта нарушения ИБ или осуществления НСД к защищаемым ИР ИС рекомендуется уведомить АИБа, и далее следовать их указаниям.

Действия АИБа и администратора информационной системы при признаках нарушения политик информационной безопасности регламентируются следующими внутренними документами:

- политикой информационной безопасности;
- порядком работы пользователей;
- порядка работы администратора информационной безопасности;
- порядок работы ответственного за обеспечение безопасности информации в информационных системах.

После устранения инцидента необходимо составить акт о факте нарушения и принятых мерах по восстановлению работоспособности ИС, а также зарегистрировать факт нарушения в журнале учета нарушений, ликвидации их причин и последствий.

5.2. Ответственность за нарушение Политик безопасности

Ответственность за выполнение правил ПБ несет каждый сотрудник КГБУЗ «АКГВВ» в рамках своих служебных обязанностей и полномочий.

На основании ст. 192 Трудового кодекса Российской Федерации сотрудники, нарушающие требования ПБ КГБУЗ «АКГВВ», могут быть подвергнуты дисциплинарным взысканиям, включая замечание, выговор и увольнение с работы.

Все сотрудники несут персональную (в том числе материальную) ответственность за прямой действительный ущерб, причиненный КГБУЗ «АКГВВ» в результате нарушения ими правил политики ИБ (Ст. 238 Трудового кодекса Российской Федерации).

За неправомерный доступ к компьютерной информации, создание, использование или распространение вредоносных программ, а также нарушение правил эксплуатации ЭВМ, следствием которых явилось нарушение работы ЭВМ (автоматизированной системы обработки информации), уничтожение, блокирование или модификация защищаемой информации, сотрудники КГБУЗ «АКГВВ» несут ответственность в соответствии со статьями 272, 273 и 274 Уголовного кодекса Российской Федерации.

Приложение № 2
УТВЕРЖДЕНО
приказом начальника
КГБУЗ «АКГВВ»
от _____

ПОЛОЖЕНИЕ
о конфиденциальной информации

1. Перечень используемых определений, обозначений и сокращений

НСД — несанкционированный доступ

Допуск к конфиденциальной информации – процедура оформления права работника организации для ознакомления со сведениями, относящимися к конфиденциальным.

Доступ к конфиденциальной информации – ознакомление определенных лиц с КИ с согласия ее обладателя или на ином законном основании при условии сохранения конфиденциальности этой информации.

Защита конфиденциальной информации – деятельность, направленная на предотвращение НСД к КИ и (или) её утечки.

Информация – сведения (сообщения, данные) независимо от формы их представления.

Информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Информационная система - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

Информационно-телекоммуникационная сеть – технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники;

Контрагент – сторона гражданско-правового договора, которой обладатель КИ передал эту информацию;

Конфиденциальная информация – документированная информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации.

Конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя;

Обладатель конфиденциальной информации – лицо (физическое или юридическое), которое владеет сведениями, отнесенным к конфиденциальным, на законном основании, ограничило доступ к ним и установило в отношении ее режим конфиденциальности;

Оператор информационной системы – гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных.

Общедоступная информация – общеизвестные сведения и иная информация, доступ к которой не ограничен

Передача конфиденциальной информации – передача сведений, отнесенных к конфиденциальным, и зафиксированных на материальном носителе, ее обладателем контрагенту на основании договора в объеме и на условиях, которые предусмотрены договором, включая условие о принятии контрагентом установленных договором мер по охране ее конфиденциальности.

Предоставление конфиденциальной информации – передача сведений, отнесенных к конфиденциальным, и зафиксированных на материальном носителе, ее обладателем органам государственной власти, иным государственным органам, органам местного самоуправления в целях выполнения их функций.

Разглашение конфиденциальной информации – действие или бездействие, в результате которых сведения, отнесенные к конфиденциальным, в любой возможной форме (устной, письменной, иной форме, в том числе с использованием технических средств) становится известной третьим лицам без согласия обладателя такой информации либо вопреки трудовому или гражданско-правовому договору.

Распространение информации – действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц.

Электронное сообщение – информация, переданная или полученная пользователем информационно-телекоммуникационной сети.

2. Общие положения

2.1. Настоящее Положение о конфиденциальной информации (далее по тексту – Положение) устанавливает общие нормы о сведениях, относящихся к категории конфиденциальных, порядок их защиты, определяет единый для всех работников краевого государственного бюджетного учреждения здравоохранения «Алтайский краевой госпиталь ветеранов войн» (далее – КГБУЗ «АКГВВ») порядок работы со сведениями, конфиденциального характера, порядок допуска к этим сведениям, а также меры ответственности, применяемые за нарушение требований, установленных настоящим Положением.

2.2. Положение разработано на основе действующего законодательства Российской Федерации, в том числе Гражданского, Трудового и Уголовного кодексов Российской Федерации и Федерального закона Российской Федерации № 149 от 27.07.2006 «Об информации, информационных технологиях и о защите информации», а также Указа Президента Российской Федерации от 06.03.1997 № 188 «Об утверждении перечня сведений конфиденциального характера» и других законодательных и нормативно-правовых актов, регулирующих вопросы охраны конфиденциальной информации.

2.3. Положение распространяется на сведения, конфиденциального характера КГБУЗ «АКГВВ» независимо от вида носителя, на котором они зафиксированы.

2.4. Действие Положения распространяется на работников КГБУЗ «АКГВВ», работающих по служебному контракту (трудовому договору),

заключенному с КГБУЗ «АКГВВ», которые дали обязательство о неразглашении конфиденциальной информации, а также на лиц, работающих по гражданско-правовым договорам, заключенным с КГБУЗ «АКГВВ», взявших на себя обязательство о неразглашении конфиденциальной информации), в порядке и на условиях, предусмотренных настоящим Положением.

3. Сведения, относимые к конфиденциальным

3.1. Сведения, относящиеся к конфиденциальной информации, определяются в «Перечне сведений конфиденциального характера», который утверждается начальником КГБУЗ «АКГВВ», принципы отнесения сведений к конфиденциальным определяются в «Порядке организации и проведения работ по защите информации в информационных системах КГБУЗ «АКГВВ».

4. Порядок отнесения сведений к категории конфиденциальных

4.1. Порядок отнесения сведений к категории конфиденциальных определен в «Порядке организации и проведения работ по защите информации в информационных системах КГБУЗ «АКГВВ».

5. Порядок оформления допуска к сведениям, конфиденциального характера

5.1. Порядок оформления допуска к сведениям, конфиденциального характера определен в «Порядке организации и проведения работ по защите информации в информационных системах КГБУЗ «АКГВВ».

6. Меры по защите конфиденциальной информации

6.1. Меры по защите сведений, конфиденциального характера, определены в «Порядке организации и проведения работ по защите информации в информационных системах КГБУЗ «АКГВВ».

6.2. Требования к обеспечению рабочих мест пользователей и порядок работы пользователей определены в приложениях к «Порядке организации и проведения работ по защите информации в информационных системах КГБУЗ «АКГВВ».

7. Ответственность за нарушение конфиденциальности информации

7.1. В случае разглашения сведений, конфиденциального характера, ставших известными работнику в связи с исполнением им трудовых обязанностей, трудовой договор с работником может быть расторгнут по инициативе работодателя в соответствие с трудовым законодательством.

7.2. Сбор сведений, составляющих конфиденциальную информацию, путем похищения документов, подкупа или угроз, а равно иным незаконным способом влечет уголовную ответственность в соответствие законом.

7.3. Разглашение конфиденциальной информации (за исключением случаев, когда разглашение такой информации влечет уголовную ответственность), лицом, получившим доступ к такой информации в связи с исполнением служебных или профессиональных обязанностей, влечет дисциплинарную и (или) материальную ответственность.

7.4. Возмещение ущерба, причиненного КГБУЗ «АКГВВ» в связи с нарушением прав КГБУЗ «АКГВВ» на его конфиденциальную информацию, производится в установленном законом порядке, организациями и лицами (в том числе работниками КГБУЗ «АКГВВ»), нарушившими действующее законодательство и указанные права.

7.5. Ответственность, в соответствии с действующим законодательством, несут также работники и должностные лица КГБУЗ «АКГВВ», не выполнившие или не обеспечившие выполнение требований настоящего положения и тем самым способствовавшие нарушению, а также не принимавшие необходимых и достаточных мер по пресечению ставших им известными фактов нарушения прав КГБУЗ «АКГВВ».

8. Заключительные положения

8.1. Настоящее положение утверждается и изменяется начальником КГБУЗ «АКГВВ».

8.2. Настоящее положение уточняется и изменяется в соответствии с изменением действующего законодательства.

Приложение № 3
УТВЕРЖДЕН
приказом начальника
КГБУЗ «АКГВВ»
от _____ № ____

ПОЛОЖЕНИЕ
о порядке организации и проведения работ по защите информации в информационных системах КГБУЗ «АКГВВ»

1. Перечень используемых определений, обозначений и сокращений

АРМ – автоматизированное рабочее место.
АС – автоматизированная система.
АТС – автоматическая телефонная станция.
ГИС – государственная информационная система.
ИСПДн – информационная система персональных данных.
КЗ – контролируемая зона.
КИ – конфиденциальная информация.
ЛВС – локальная вычислительная сеть.
НСД – несанкционированный доступ.
РФ – Российская Федерация.
СВТ – средства вычислительной техники.

Автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники.

Блокирование персональных данных – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

Государственные информационные системы – федеральные информационные системы и региональные информационные системы, созданные на основании соответственно федеральных законов, законов субъектов Российской Федерации, на основании правовых актов государственных органов.

Документированная информация – зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель.

Допуск к конфиденциальной информации – процедура оформления права работника Краевого государственного бюджетного учреждения здравоохранения «Алтайский краевой госпиталь ветеранов войн» для ознакомления со сведениями, относящимися к конфиденциальным.

Доступ к информации – возможность получения информации и ее использования.

Доступ к конфиденциальной информации – ознакомление определенных лиц с КИ с согласия ее обладателя или на ином законном основании при условии сохранения конфиденциальности этой информации.