Департамент здравоохранения Тюменской области
Государственное бюджетное учреждение здравоохранения
Тюменской области
«Областная больница №14 имени В.Н. Шанаурина» (с.Казанское)

П Р И К А З

13 февраля 2023г. №12 ос

с. Казанское

О проведении мероприятий по защите информации

В целях исполнения Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», **п р и к а з ы в а ю:**

1. Назначить ответственным за защиту информации в ГБУЗ ТО «Областная больница №14 имени В.Н. Шанаурина» (с.Казанское) (далее – Учреждение) заместителя главного врача Учреждения.
2. Утвердить Положение по организации работ по обеспечению информационной безопасности Учреждения согласно приложению к настоящему приказу.
2.1. Определить периодичность мероприятий по обеспечению информационной безопасности Учреждения.
3. Назначить администратором безопасности информации, ответственными за эксплуатацию средств защиты информации– специалиста по защите информации Учреждения.
4. Ознакомить под подпись всех работников Учреждения с Положениями настоящего приказа.
5. Признать утратившими силу приказ ГБУЗ ТО «Областная больница №14 имени В.Н. Шанаурина» (с.Казанское) от 29.12.2017г. № 76 ос «Об организации работ по защите информации, обрабатываемой, в ГБУЗ ТО «Областная больница №14 имени В.Н. Шанаурина» (с. Казанское), в том числе филиале №1 Сладковская районная больница.
6. Контроль за исполнением настоящего приказа оставляю за собой.

Главный врач Д.М. Суворов

Приложение к
приказу ГБУЗ ТО Областная
больница №14 имени В.Н.
Шанаурина» (с.Казанское)
от «13» февраля 2023 г. № 12 ос

Положение
об организации работ по обеспечению безопасности информациив
ГБУЗ ТО Областная больница №14 имени В.Н. Шанаурина» (с.Казанское)

2023год

Термины и определения

Администратор [системный, безопасности] – пользователь, уполномоченный выполнять некоторые действия (имеющий полномочия) по администрированию (управлению) информационной системы (администратор системный) и (или) её системы защиты информации (администратор безопасности) в соответствии с установленной ролью.

Анализ уязвимостей – мероприятия по выявлению, идентификации и оценке уязвимостей информационной системы в интересах определения возможности реализации угроз безопасности информации и способов предотвращения ущерба.

Аутентификационная информация [информация аутентификации] – информация, используемая для установления подлинности (верификации) субъекта доступа в информационной системе.

Аутентификация – проверка принадлежность субъекту доступа предъявленного им идентификатора (подтверждение подлинности субъекта доступа в информационной системе).

Базовый набор мер защиты информации – минимальный набор мер защиты информации, установленный для соответствующего класса защищённости информационной системы.

Виртуализация – технология преобразования формата или параметров программных или сетевых запросов к компьютерным ресурсам с целью обеспечения независимости процессов обработки информации от программной или аппаратной платформы информационной системы.

Виртуальная машина – вычислительная система, эмулируемая с помощью технологии виртуализации, в которую установлена гостевая операционная система и обеспечивается выполнение прикладного программного обеспечения.

Внешняя информационная система – информационная система, взаимодействующая с информационной системой оператора из-за пределов границ информационной системы оператора.

Внешняя информационно-телекоммуникационная сеть – информационно-телекоммуникационная сеть, взаимодействующая с информационной системой оператора из-за пределов границ информационной системы оператора.

Временный файл – файл, создаваемый операционной системой или иным программным обеспечением для сохранения промежуточных результатов в процессе функционирования для передачи данных другому программному обеспечению.

Гипервизор – программа (программное обеспечение), создающая среду функционирования других программ (в т.ч. других гипервизоров) за счёт имитации аппаратных средств вычислительной техники, управления данными средствами и гостевыми операционными системами, функционирующими в данной среде.

Гостевая операционная система – операционная система, установленная на виртуальной машине.

Демилитаризованная зона – экранированный сегмент информационной системы, размещённый не её внешней границе и выполняющий функции «нейтральной зоны» (буферной зоны безопасности) между защищаемой информационной системой оператора и внешней информационной системой или информационно-телекоммуникационной сетью.

Доверенная загрузка – загрузка операционной системы средств вычислительной техники с заранее определённых постоянных машинных носителей при обязательном успешном прохождении процедур проверки целостности программной и аппаратной среды и идентификации и аутентификации.

Доверенный канал – механизм взаимодействия между средствами защиты информационной системы или между средством защиты информации и программным обеспечением информационной системы.

Доверенный маршрут – механизм взаимодействия между субъектом доступа и средством защиты информации информационной системы.

Доступность информации – свойство безопасности информации, при котором субъекты доступа, имеющие права доступа, могут беспрепятственно их реализовать.

Защищённые линии связи – линии (каналы) связи, при передаче информации по которым обеспечивается требуемый уровень её защищённости (конфиденциальность, целостность и (или) доступность информации).

Идентификатор – представление (строка символов), однозначно идентифицирующее субъект и (или) объект доступа в информационной системе.

Идентификация – присвоение субъектам доступа, объектам доступа идентификаторов (уникальных имён) и (или) сравнение предъявленного идентификатора с перечнем присвоенных идентификаторов.

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

Инцидент – непредвиденной или нежелательное событие (группа событий) безопасности, которое привело (могут привести) к нарушению функционирования информационной системы или возникновению угроз безопасности информации (нарушению конфиденциальности, целостности, доступности).

Компонент программного обеспечения – составная часть (программный модуль) программного обеспечения, выполняющий определённую функцию.

Компонент информационной системы – часть информационной системы, включающая некоторую совокупность информации и обеспечивающих её обработку отдельных информационных технологий и технических средств.

Контролируемая зона – пространство (территория, здание, часть здания), в котором исключено неконтролируемое пребывание лиц, а также транспортных, технических и иных средств.

Конфиденциальность информации – свойство безопасности информации, при котором доступ к ней осуществляют только субъекты доступа, имеющие на него право.

Локальный доступ – доступ субъектов доступа к объектам доступа, осуществляемый непосредственно через подключение (доступ) к компоненту информационной системы или через локальную вычислительную сеть (без использования информационно-телекоммуникационной сети).

Многофакторная аутентификация – аутентификация с использованием двух (двухфакторная) или более различных факторов аутентификация.

Мобильный код – несамостоятельное программное обеспечение или компонент программного обеспечения (скрипты, макросы, иные компоненты), получаемые из мест распространения мобильного кода, передаваемые по сети и выполняемые на компонентах информационной системы (в местах использования мобильного кода) без предварительной установки (инсталляции) пользователем для расширения возможностей системного и (или) прикладного программного обеспечения.

Непривилегированная учётная запись – учётная запись пользователя (процесса, выполняемого от его имени) информационной системы.

Объект доступа – единица информационной ресурса информационной системы (файл, техническое средство, узел сети, линия (канал) связи, мобильное устройство, программа, том, каталог, запись, поле записей и иные объекты), доступ к которой регламентируются правилами разграничения доступа и по отношению к которой субъекты доступа выполняют операции.

Оператор информационной системы – гражданин или юридическое лицо, осуществляющее деятельность по эксплуатации информационной системы, в т.ч. по обработке информации, содержащейся в её базах данных.

Отказ в обслуживании – препятствие санкционированному доступу к ресурсам информационной системы или задержка операций и функций операционной системы.

Периметр информационной системы – физическая и (или) логическая граница информационной системы (сегмента информационной системы), в пределах которой оператором обеспечивается защита информации в соответствии с едиными правилами и процедурами, а также контроль за реализованными мерами защиты информации.

Пользователь – лицо, которому разрешено выполнять некоторые действия (операции) по обработке информации в информационной системе или использующее результаты её функционирования.

Потенциал нарушителя – мера усилий, затрачиваемых при реализации угроз безопасности информации в информационной системе.

Привилегированная учётная запись – учётная запись администратора информационной системы.

Программная среда – совокупность программного обеспечения, используемого в информационной системе для решения одной или нескольких задач.

Роль – предопределённая совокупность правил, устанавливающих допустимое взаимодействие между пользователем и информационной системой.

Сегмент информационной системы – совокупность нескольких компонентов информационной системы, использующих общую (в т.ч. разделяемую) среду передачи и объединённых для единства решения функциональных задач.

Событие безопасности (информационной) – идентифицированное возникновение состояния информационной системы (сегмента, компонента информационной системы), сервиса или сети, указывающее на возможное нарушение безопасности информации, или сбой средств защиты информации, или ранее неизвестную ситуацию, которая может быть значимой для безопасности информации.

Субъект доступа – пользователь, процесс, выполняющие операции (действия) над объектами доступа и действия которых регламентируются правилами разграничения доступа.

Техническое средство – аппаратное или программно-аппаратное устройство, осуществляющее формирование, обработку, передачу или приём информации в информационной системе.

Технологии мобильного кода – реализованные в программном обеспечении процессы создания и использования мобильного кода (в частности технологии Java, JavaScript, ActiveX, VBSScript).

Удалённый доступ – процесс получения доступа (через внешнюю сеть) к объектам доступа информационной системы из другой информационной системы (сети) или со средства вычислительной техники, не являющегося постоянно (непосредственно) соединённым физически или логически с информационной системой, к которой он получает доступа.

Управление доступом – ограничение и контроль доступа субъектов доступа к объектам доступа в информационной системе в соответствии с установленными правилами разграничения доступа.

Устройство – конструктивно законченный технический элемент, имеющий определённое функциональное назначение в информационной системе.

Уязвимость информационной системы – недостаток (слабость) информационной системы, который (которая) создаёт потенциальные или реально существующие условия для реализации проявления угроз безопасности информации.

Хостовая операционная система – операционная система, в среде которой функционирует гипервизор.

Целостность информации – свойство безопасности информации, при котором отсутствует любое её изменение либо изменение субъектами доступа, имеющими на него право.

1.Общие положения

1.1. Настоящее Положение определяет основные мероприятия и порядок проведения работ по обеспечению безопасности информации (далее - ОБИ) в ГБУЗ ТО Областная больница №14 имени В.Н. Шанаурина» (с.Казанское)(далее – Учреждения).

1.2. Положение разработано на основании требований законодательства РФ в области информационной безопасности, нормативных и методических документовуполномоченных органов (ФСТЭК России, ФСБ России), а также правовых актов Тюменской области, действующих на момент разработки документа.

1.3. В Положении используются термины и определения, установленные законодательством Российской Федерации, национальными стандартами в области защиты информации.

1.4. В Учреждении обрабатывается общедоступная информация и информация ограниченного доступа, не составляющая государственную тайну, в том числе служебная информация (документы с пометкой «Для служебного пользования» «ДСП») и персональные данные (далее - ПДн).

1.5. Автоматизированная обработка информации осуществляется с использованием средств вычислительной техники (далее - СВТ) и различных информационных систем (далее - ИС) на автоматизированных рабочих местах (далее – АРМ пользователя) и серверах Учреждения.

1.6. Учреждение, как обладатель информации ограниченного доступа, обязан принимать меры по защите информации и ограничивать доступ к информации, если такая обязанность установлена федеральными законами.

1.7. Требования к ОБИ формируются на основании установленных классов защищённости ИС (уровня защищенности ПДн) и перечня актуальных угроз безопасности информации.

1.8. Требования ОБИ реализуются комплексом организационных и технических мер, средств и механизмов защиты информации, определенных в документации системы защиты информации (далее - СЗИ).

1.9. Настоящие Положение обязательно для исполнения всеми работникамиУчреждения (далее – работники).

2. Порядок организации работ по обеспечению безопасности информации

2.1. С целью организации работ по защите информации приказом главного врача Учреждения назначается должностное лицо, ответственное за защиту информации.

2.2. Функции, решаемые задачи и обязанности ответственного за защиту информации определены в Инструкции лица, ответственного за защиту информации, согласно приложению № 1 к настоящему Положению.

2.3. Непосредственное выполнение работ по реализации требований и мер безопасности информации в организации осуществляет администратор

безопасности (далее - АБИ), назначаемый приказом *специалист по защите информации*Учреждения. Функции, решаемые задачи и обязанности АБИ определены инструкцией, согласно приложению № 2 к настоящему Положению.

2.4. Реализация требований ОБИ осуществляется всеми работниками Учреждения (администраторами, пользователями, эксплуатационным персоналом).

2.5. Обязанности и ответственность пользователей по ОБИ при ее обработке определены в Инструкции пользователя согласно приложению № 3 к настоящему Положению.

2.6. Работы по ОБИ в Учреждении осуществляются согласно Плану проведения мероприятий ОБИ Учреждения согласно приложению № 11 к настоящему Положению.

2.1. Все работы ОБИ подлежат учету в Журнале учета мероприятий по ОБИ согласно приложению № 12 к настоящему Положению.

3. Технологический процесс обработки информации

3.1. Технические средства и системы обработки информации (далее - ТС), места их размещения, программное обеспечение, используемое для обработки информации, а также используемые средства защиты информации и их характеристики подлежат учёту в Техническом паспорте объекта информатизации (далее - ОИ). Ответственность за ведение Технического паспорта ОИ и актуализацию сведений в нём возлагается на АБИ.

3.2. Все ТС Учреждения размещены в пределах контролируемой зоны (далее - КЗ). Режим обработки информации многопользовательский с разграничение прав доступа.

3.3. Обработка информации в Учреждении осуществляется в соответствии с Положением о порядке работы с информационными ресурсами согласно приложению № 4 к настоящему Положению.

3.4. Работа с информационными ресурсами Учреждения осуществляется в соответствии с правами разграничения доступа. Правила разграничения доступа назначаются администраторами. Доступ к информационным ресурсам осуществляется при помощи учётных записей пользователей.

3.5. Обработка информации предусматривает следующие действия с данными: сбор, накопление, хранение, использование, уточнение, передача, удаление (уничтожение). Новые данные вводятся вручную, посредством клавиатурного ввода, а также путём считывания в электронном виде.

3.6. Пользователи имеют право постоянного хранения файлов с данными на:

- жёстком диске АРМ пользователя;
- учтённом съёмном носителе информации (USB-накопители, оптические диски, гибкие магнитные диски).

3.7. Доступ к жесткому диску АРМ пользователя разрешен только АБИ. Учтенные съёмные носители информации выдаются пользователю под роспись.

3.8.Доступ к АРМ пользователей производится по идентификатору (логину) и паролю в соответствии с требованиями Инструкция по организации парольной защиты согласно приложению № 5 к настоящему Положению.

3.9. На АРМ пользователей устанавливается лицензионное либо свободно распространяемое общесистемное программное обеспечение (далее – ПО.

3.10.Обработка информации на АРМ пользователей осуществляется с использованием специализированного прикладного ПО и web-браузера.

3.11.Пользователи имеют доступ к ресурсам сети «Интернет» со своих АРМ.

3.12.В качестве вспомогательного средства для разработки документов на АРМ пользователей установлен программный пакет семейства «Мой офис» или «Р7.Офис».

3.13.Копии установленного на АРМ пользователей ПО хранятся у АБИ.

3.14.Обработка служебной информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну (документов с пометкой «для служебного пользования») производится только на учтённых съёмных машинных носителях информации (далее - МНИ). Порядок и условия обработки служебной информации ограниченного доступа на АРМ пользователей определены положением по организации и проведению работ по защите служебной информации ограниченного доступа, несодержащейсведения, составляющие государственную тайну в Учреждении.

4. Система защиты информации

4.1.Перечень объектов доступа

Объектами доступа являются:

- ТС, включая средства отображения информации;
- помещения, в которых размещены ТС;
- носители информации, включая съёмные носители информации и жёсткие магнитные диски (далее – ЖМД);
- базы данных (далее – БД) и каталоги файлов на съёмных носителях информации и ЖМД;
- общесистемное и специальное ПО, предназначенное для обработки информации и разработки документов;
- программные средства, осуществляющие функции по защите информации, а также функции контроля безопасности;
- каналы информационного обмена и телекоммуникации.

4.2.Перечень субъектов доступа

Субъектами доступа к защищаемой информации на ОИ являются:

- администратор безопасности информации;
- системный администратор;
- пользователи, работающие на АРМ;

– процессы, выполняемые от имени АБИ, системного администратора и пользователей при обработке информации и настройке средств защиты информации.

4.3.Штатные средства доступа к информации

В качестве штатных средств доступа на ОИ предусмотрены:

– стандартные средства операционной системыWindows;
– программные из пакета «Мои офис» или «Р7.Офис»;
– система управления базами данных (далее – СУБД)Directum;
– web-браузер;
– программы из пакета антивируса;
– средства настройки и контроля функций СЗИ.

4.4.Объекты защиты организации:

– ТС (в т.ч. СВТ, МНИ, средства и системы связи передачи данных);
– информация, хранящаяся и обрабатываемая на ТС;
– общесистемное, прикладное, специальное ПО;
– средства защиты информации.

4.5.Требования к средствам защиты информации

4.5.1. Все используемые программные и аппаратные СЗИ имеют действующие сертификаты на соответствие требованиям по безопасности информации, установленные Федеральной службой безопасности Российской Федерации и Федеральной службой по техническому и экспортному контролю России.

4.5.2. Класс защищённости применяемых средств защиты информации должен соответствовать классу защищенности средств и систем обработки информации.

4.5.3. При обмене информацией между Учреждением и внешними по отношению к нему информационными системами, а также при передаче данных по кабельным системам, расположенным в пределах КЗ и не защищённым от НСД к информации организационно-техническими мерами, для обеспечения конфиденциальности информации требуется применение средств криптографической защиты информации (далее – СКЗИ).

4.5.4. Установку и настройку СЗИ разрешается проводить только АБИ.

4.5.5. Эксплуатация СЗИ должна осуществляться в строгом соответствии с правилами, установленными в Положении о применении шифровальных (криптографических) средств защиты информации в Учреждении.

4.6.Правила разграничения доступа

4.6.1. средствами СЗИ реализованы правила разграничения доступа, при которых каждый пользователь имеет доступ к:

– средствам ОС, обеспечивающим запуск и функционирование АРМ;
– средствам разработки документов;
– средствам антивирусного контроля;
– прикладному ПО;
– персональному каталогу на ЖМД, предназначенному для хранения информации;

– внешним накопителям данных, предназначенных для хранения информации;

– устройствам и средствам их программной поддержки, необходимым для работы с документами.

4.6.2. Доступ к средствам настройки и изменения полномочий доступа в СЗИ имеет только АБИ. Операции доступа к объектам доступа документируются средствами регистрации и учёта.

5. Средства защиты информации

5.1. Для защиты информации от несанкционированного доступа и воздействия вредоносных программ, на всех ТС Учреждения применяются сертифицированные средства защиты информации от несанкционированного доступа (далее - СЗИ от НСД) и средства антивирусной защиты (далее - САВЗ).

5.2. Для защиты информации передаваемой по незащищенным каналам связи за пределы КЗ (во внешние системы) применяются СКЗИ. В установленных случаях могут использоваться средства электронной подписи.

5.3. СКЗИ и их носители подлежат учету в Журнале поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов. При этом программные СКЗИ учитываются совместно с аппаратными средствами, с которыми осуществляется их штатное функционирование.

5.4. В локальной вычислительной сети (далее - ЛВС) Учреждения для обеспечения безопасности периметра ЛВС применяются сертифицированные средства межсетевого экранирования.

5.5. Для контроля защищенности ЛВС используется сетевой сканер безопасности.

5.6. Контроль настройки и работы используемых в Учреждении средств защиты информации осуществляет АБИ.

6. Реализация мер защиты

6.1. Идентификация и аутентификация субъектов доступа и объектов доступа

6.1.1. Применяемые на ОИ меры по идентификации и аутентификации субъектов доступа и объектов доступа обеспечивают присвоение субъектам и объектам доступа уникального признака (идентификатора), сравнение предъявляемого субъектом (объектом) доступа идентификатора с перечнем присвоенных идентификаторов, а также проверку принадлежности субъекту (объекту) доступа предъявленного им идентификатора (подтверждение подлинности).

6.1.2. Идентификация и проверка подлинности субъектов доступа при входе в систему осуществляется СЗИ от НСД с использованием персональных идентификаторов, а также по имени (логину) и паролю условно-постоянного действия длиной не менее шести буквенно-цифровых символов.

6.1.3. СЗИ от НСД не позволяет использовать для входа в систему незарегистрированные идентификаторы.

6.1.4. Правила и требования к парольной защите определены в Инструкции по организации парольной защиты согласно приложению № 5 к настоящему Положению.

6.1.5. Программы, тома, каталоги, файлы, записи, поля записей, терминалы, компьютеры (АРМ), узлы сети, каналы связи, внешние устройства, подключённые к АРМ, идентифицируются по именам при обращении к ним при помощи средств операционной системы и СЗИ. Правильность предоставления доступа в соответствии с установленными правами субъектов по отношению к конкретным объектам (каталогам, устройствам) обеспечивается СЗИ и используемыми на ОИ сетевыми политиками безопасности.

6.2. **Управление доступом субъектов доступа к объектам доступа**

6.2.1. Применяемые меры по управлению доступом субъектов доступа к объектам доступа обеспечивают управление правами и привилегиями субъектов доступа, разграничение доступа субъектов доступа к объектам доступа на основе совокупности установленных на ОИ правил разграничения доступа, а также обеспечивает контроль за соблюдением этих правил.

6.2.2. Управление (заведение, активация, блокирование и уничтожение) учётными записями пользователей на ОИ и выдача (замена) пользовательских персональных идентификаторов для СЗИ от НСД, осуществляется АБИ и системным администратором в соответствии с правилами и процедурами, определёнными в Положении о порядке работы с информационными ресурсами (Приложение № 4).

6.2.3. На ОИ реализован дискреционный метод разграничения доступа. В системе задействована функция блокирования органов управления АРМ при временном оставлении рабочего места. При использовании незарегистрированного пароля, либо пароля, зарегистрированного не для текущего пользователя, разблокировка системы невозможна. В системе применяется ограничение неуспешных попыток входа в систему. При превышении установленного количества неуспешных попыток входа система блокируется.

6.3. **Ограничения программной среды**

6.3.1. Цель принятия мер по ограничению программной среды – обеспечение установки и (или) запуска только разрешённого к использованию в организации программного обеспечения и исключения возможности установки и (или) запуска запрещённого к использованию на ОИ программного обеспечения.

6.3.2. Контроль установки (инсталляции) разрешённого к использованию ПО и (или) его компонентов осуществляется АБИ и системным администратором на основе журналов регистрации событий операционной системы и средств антивирусного контроля АРМ.

6.3.3. Пользователи АРМ не имеют права самостоятельно устанавливать ПО.

6.3.4. Установка ПО на АРМ пользователей производится в соответствии с требованиями и правилами, установленными в Инструкции по модификации технических и программных средств согласно приложению № 6 к настоящему Положению.

6.4. **Защита машинных носителей информации**

6.4.1. Защита машинных носителей информации (средства обработки (хранения) информации, съёмные машинные носители информации) обеспечивается организационно-режимными мероприятиями. Цель принятия мер по защите МНИ – исключение возможности несанкционированного доступа к МНИ и хранящейся на них информации, а также несанкционированное использование съёмных МНИ.

6.4.2. При передаче МНИ межу пользователями или в сторонние организации для ремонта или утилизации производится уничтожение (стирание) информации, а также контроль уничтожения (стирания).

6.4.3. Порядок учёта, хранения и использования съёмных МНИ (ГМД, USB-накопители и т.д.) определён в Положении о порядке работы с информационными ресурсами Учрежденияcогласно приложению № 4 к настоящему Положению.

6.5. **Регистрация событий безопасности**

6.5.1. Принимаемые меры по регистрации событий безопасности позволяют обеспечить сбор, запись, хранение и защиту информации о событиях безопасности, а также возможности просмотра и анализа информации о таких событиях.

6.5.2. Регистрация событий безопасности обеспечивается сертифицированными средствами защиты информации АРМ и серверов.

6.5.3. Регистрация, учёт и порядок реагирования на события безопасности регламентируются Положением о порядке выявления и реагирования на инциденты информационной безопасности согласно приложению № 7 к настоящему Положению.

6.6. **Антивирусная защита**

6.6.1. Целью принятия мер по антивирусной защите является обеспечение обнаружения компьютерных программ либо иной компьютерной информации, предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации СЗИ, а также реагирование на обнаружение этих программ и информации.

6.6.2. САВЗ установлены на всех АРМ и серверах, обрабатывающих информацию.

6.6.3. Применение САВЗ решает следующие задачи:

- автоматическое сканирование АРМ на наличие вирусных программ;

– автоматическое блокирование обнаруженных вирусных программ путём их удаления из программных модулей или уничтожения;

– проведение регулярного сканирования АРМ на наличие вирусов;

– реализация механизма обновления базы данных признаков вредоносных компьютерных программ (вирусов);

– ведение журналов событий безопасности.

6.6.4. Все используемые в организации МНИ подвергаются обязательному контролю на наличие компьютерных вирусов при помощи антивирусной программы. ЖМД находится под контролем антивирусной программы постоянно. При обнаружении вирусного кода он удаляется из программы. АБИ и (или) системным администратором периодически проводится антивирусный контролю ЖМД по расширенному алгоритму.

6.6.5. Обновление БД САВЗ производится по мере выпуска данных обновлений производителем.

6.6.6. Правила и требования, регламентирующие антивирусную политику определены в Инструкции по организации антивирусной защиты согласно приложению № 8 к настоящему Положению.

6.7. **Контроль (анализ) защищённости информации**

6.7.1. Мероприятия, проводимые в целях контроля и анализа защищённости информации, включают в себя:

– контроль состава ТС, ПО и СЗИ;

– выявление, анализ и устранение уязвимостей ПО и СЗИ;

– контроль установки обновлений ПО, включая ПО СЗИ;

– контроль работоспособности, параметров настройки и правильности функционирования ПО и СЗИ;

– контроль правил генерации и смены паролей пользователей, заведения и удаления учётных записей пользователей, реализации полномочий пользователей и правил разграничения доступа пользователей в системе.

6.7.2. Используемые средства регистрации и учёта событий безопасности СЗИ позволяют АБИ контролировать неизменность конфигурации серверов, АРМ, файлов и реестров используемого ПО.

6.7.3. АБИ проводит периодическое обслуживание и тестирование функций СЗИ.

6.7.4. Порядок выполнения работ по выявлению, анализу и устранению уязвимостей ПО и СЗИ определён в Положении по организации контроля эффективности защиты информации согласно приложению № 9 к настоящему Положению.

6.8. **Обеспечение целостности программного обеспечения и информации**

6.8.1. Контроль целостности ПО (в т.ч. ПО СЗИ), установленного на АРМ пользователей и серверах, осуществляется средствами сертифицированных

СЗИ и функциональными возможностями операционной системы (далее – ОС) АРМ и серверов.

6.8.2. В целях обеспечения возможности восстановления ПО, в случае возникновения нештатных ситуаций, организовано хранение:

- дистрибутивов используемого системного и прикладного ПО;
- дистрибутивов с ПО для СЗИ;
- файлов, содержащих конфигурации и настройки СЗИ.

6.8.3. Для обеспечения возможности восстановления информации, содержащейся в файлах, папках и БД, выполняется периодическое резервное копирование критически важных информационных ресурсов на внешние системы хранения данных.

6.9. **Обеспечение доступности информации**

6.9.1. Доступность информации обеспечивается:

- использованием отказоустойчивых ТС;
- выявлением, анализом и устранением уязвимостей ПО;
- резервированием ТС, ПО и каналов передачи информации;
- периодическим резервным копированием информации.

6.9.2. На основе мониторинга и анализа сообщений в электронных журналах учёта событий СЗИ проводится периодическая проверка работоспособности серверного и телекоммуникационного оборудования, каналов связи, средств обработки и защиты информации (в т.ч. направлением текстовых сообщений и принятием «ответов», визуального контроля, контроля трафика, контроля «поведения» системы и иными методами).

6.9.3. В целях восстановления доступности информационных ресурсов после аппаратных или программных сбоев организовано периодическое резервное копирование информации на систему хранения данных.

6.9.4. Контроль за выполнением резервного копирования возложен на АБИ и системного администратора. Восстановление системы и информации осуществляется АБИ и системным администратором.

6.9.5. Реализация мер, направленных на поддержание непрерывности работы средств и систем обработки информации осуществляется в соответствии с Порядком резервирования и восстановления работоспособности ТС, ПО и СЗИсогласно приложению № 10 к настоящему Положению.

6.10.**Защита технических средств**

6.10.1. Помещения, в которых размещены средства и системы обработки информации (ТС), расположены в пределах КЗ. Доступ в помещения имеет ограниченный круг лиц. Реализуемые в организации меры по защите ТС направлены на исключение НСД:

- к стационарным ТС, обрабатывающим информацию;
- к средствам, обеспечивающим функционирование ОИ;
- в помещения, в которых постоянно расположены ТС.

6.10.2. Порядок доступа в помещения организации осуществляется в соответствии с Положении о порядке работы с информационными ресурсами Учрежденияс согласно приложению № 4 к настоящему Положению.

6.11.**Защита средств и систем связи и передачи данных**

6.11.1. Для обеспечения безопасного межсетевого взаимодействия используются сертифицированные средства межсетевого экранирования (далее - СМЭ). СМЭ выполняют фильтрацию входящего и исходящего трафика на различных уровнях стека протоколов, регистрацию и учёт событий системы, а также обеспечивает установление защищённых (шифрованных) соединений между узлами, принадлежащими разным организациям и (или) разным информационным системам.

6.11.2. Для обеспечения защиты информации при передаче по незащищённым каналам связи применяются сертифицированные СКЗИ.

6.11.3. Порядок и правила, определяющие действия пользователей при использовании ресурсов и сервисов сети Интернет, установлены в Инструкции по обеспечению безопасности при работе в сети Интернет (Приложение № 13).

6.11.4. Эксплуатация СКЗИ осуществляется в соответствии с Положением о применении шифровальных (криптографических) средств защиты информации в ГБУЗ ТО Областная больница №14 имени В.Н. Шанаурина» (с.Казанское).

6.12.**Управление конфигурацией систем обработки и защиты информации**

6.12.1. Управление конфигурацией ОИ, а также СЗИ, анализ потенциального воздействия планируемых изменений на обеспечение безопасности информации, а также документирование этих изменений обеспечивается АБИ и системным администратором.

7. Информирование по вопросам обеспечения безопасности информации

7.1.Ознакомление работников с правилами работы с информацией осуществляется:

– путем проведения руководителями структурных подразделений Учреждения первичных инструктажей с вновь принятыми работниками по соблюдению установленных правил обработки и защиты информации;

– путем проведения обучения работников (пользователей средств вычислительной техники) администратором безопасности правилам работы с используемыми средствами защиты информации;

– путем самостоятельного изучения работником документов, регламентирующих вопросы ОБИ в Учреждении.

7.2.Допуск работников к информационным ресурсам Учреждения осуществляется только после прохождения первичного инструктажа и ознакомления с документами по вопросам обеспечения ИБ.

7.3.При проведении первичного инструктажа нового пользователя должны быть разъяснены:

- права и обязанности пользователя при работе с информационными ресурсами Учреждения;
- действия, которые запрещены в отношении информации, составляющей информационные ресурсы Учреждения
- порядок и условия работы с информацией ограниченного доступа;
- возможные последствия и ответственность в случае нарушения правил работы с информационными ресурсами Учреждения (информацией ограниченного доступа).

8. Контроль принятых мер по обеспечению безопасности информации

8.1. Организация контроля выполнения мероприятий информационной безопасности возлагается на ответственного за ОБИ в Учреждении.

8.2. Руководители структурных подразделений Учреждения осуществляют повседневный контроль выполнения требований по ОБИ в своих подразделениях.

8.3. АБИ Учреждения осуществляет текущий контроль выполнения требований по ОБИ в рамках выполнения своих обязанностей.

8.4. Мероприятия по контролю ОБИ в Учреждении проводятся в соответствии с Планом внутренних проверок состояния защиты информации.

8.5. Контроль эффективности принятых мер защиты информации должен осуществляться в соответствии с Положением по организации контроля эффективности защиты информации согласно приложению № 11 к настоящему Положению.

Приложение № 1

к Положению об организации
работ по обеспечению
безопасности информации в
ГБУЗ ТО Областная больница
№14 имени В.Н. Шанаурина»
(с.Казанское)

Инструкция
ответственного за защиту информациив
ГБУЗ ТО Областная больница №14 имени В.Н. Шанаурина»
(с.Казанское)

1. Общие положения

1. Данная Инструкция определяет основные обязанности и права лица, ответственного за обеспечение безопасности информации (далее – ОБИ) в ГБУЗ ТО Областная больница №14 имени В.Н. Шанаурина» (с.Казанское) (далее – Учреждение).
2. Ответственный за ОБИ является штатным работником Учреждения и назначается приказом главного врача Учреждения.
3. Ответственный за ОБИ отвечает за организацию и состояние процесса обработки и обеспечения безопасности информации ограниченного доступа (в том числе служебной информации и персональных данных) в Учреждении.
4. Решение вопросов организации обработки и обеспечения безопасности информации в Учреждении входит в прямые обязанности ответственного за ОБИ.
5. Ответственный за ОБИ отвечает за обеспечение и поддержание требуемого уровня безопасности информации и уполномочен на проведение соответствующих работ.
6. Ответственный за ОБИ в своей работе руководствуется требованиями федеральных законов, указов Президента и постановлений Правительства Российской Федерации, руководящими и нормативными документами уполномоченных органов в области обработки и защиты информации, а также другими нормативно-правовыми актами, действующими на территории, настоящей Инструкцией и иными регламентирующими документами Учреждения.
7. Требования ответственного за ОБИ, связанные с выполнением возложенных на него функций, обязательны для исполнения всеми работниками Учреждения.
8. Ответственный за ОБИ обладает правами доступа к любым носителям информации и информационным ресурсам Учреждения.

2. Обязанности

Ответственный за ОБИ обязан:

1. Обеспечивать выполнение режимных и организационных мероприятий ОБИ, а также следить за выполнением требований по условиям размещения средств вычислительной техники и их сохранностью.
2. Знать и предоставлять администратору безопасности (далее - АБИ) изменения к списку лиц, доступ которых к информации ограниченного доступа необходим для выполнения трудовых обязанностей.
3. Проводить инструктаж и консультации работников Учреждения по вопросам обеспечения безопасности информации в Учреждении.
4. Проверять правильность предоставления в рамках разрешительной системы доступа полномочий пользователям, минимально необходимых им для выполнения трудовых обязанностей.
5. Организовывать периодический контроль пользователей по соблюдению ими режима конфиденциальности, правил работы со съемными машинными носителями информации, выполнению организационных мер по защите информации, а также принимать участие в проведении проверок уполномоченными структурами.
6. Взаимодействовать с АБИ по вопросам обработки в Учреждении информации ограниченного доступа и выполнения требований безопасности информации.
7. Контролировать проведение мероприятий по установке и настройке средств защиты информации.
8. Организовывать работы по плановому контролю работоспособности средств защиты информации и охраны объекта.
9. Контролировать периодическое резервное копирование баз данных и иной защищаемой информации.
10. По указанию руководства своевременно и точно отражать изменения в локальных нормативных правовых актах по управлению системной защиты информации (далее – СЗИ) и по правилам обработки информации ограниченного доступа.
11. Знать перечень и условия обработки в Учреждении информации ограниченного доступа.
12. Знать перечень объектов информатизации (далее – ОИ), их назначение, выполнение на ОИ требований безопасности информации, сроки действия аттестатов соответствия ОИ и сертификатов соответствия установленных средств защиты информации.
13. Обеспечивать соблюдение работниками утвержденного порядка проведения работ по установке и модернизации аппаратных и программных средств компьютеров и серверов из состава ОИ.
14. Осуществлять контроль за порядком учета, хранения и использования машинных носителей информации (далее - МНИ), содержащих защищаемую информацию.

15. При выявлении возможных каналов неправомерного вмешательства в процесс функционирования ОИ и осуществления несанкционированного доступа к защищаемой информации и техническим средствам, сообщать о них главному врачу Учреждения.
16. Инструктировать работников по вопросам обеспечения информационной безопасности и правилам работы со средствами защиты информации.
17. Знать законодательство Российской Федерации в области информационной безопасности (далее - ИБ), следить за изменениями законодательства по ИБ.
18. Проводить разбирательства и составление заключений по фактам несоблюдения условий хранения носителей защищаемой информации, нарушения правил работы с документами, содержащими информацию ограниченного доступа, или по другим нарушениям, которые могут привести к снижению уровня защищенности информации.
19. Выполнять иные мероприятия, требуемые нормативными документами по защите информации.

3. **Права**

Ответственный за ОБИ имеет право:

1. Требовать от всех работников Учреждения выполнения установленной технологии обработки информации ограниченного доступа, инструкций и других нормативных правовых документов по обеспечению безопасности информации.
2. Инициировать блокирование доступа работников к защищаемой информации, если это необходимо для предотвращения нарушения режима защиты информации.
3. Участвовать в разработке мероприятий по совершенствованию СЗИ.
4. Инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения ИБ, несоблюдения условий хранения носителей защищаемой информации, нарушения правил работы с документами, содержащими информацию ограниченного доступа, несанкционированного доступа, утраты, порчи защищаемых носителей информации и технических средств из состава ОИ или по другим нарушениям, которые могут привести к снижению уровня ИБ.
5. Обращаться к руководителю подразделения с предложением о приостановке процесса обработки информации ограниченного доступа или отстранению от работы пользователя в случаях нарушения установленной технологии обработки информации ограниченного доступа или нарушения режима конфиденциальности.
6. Подавать свои предложения по совершенствованию мер защиты информации, разработке и принятии мер по предотвращению возможных опасных последствий нарушений, приводящих к снижению уровня ИБ.

4. Действия при обнаружении попыток несанкционированного доступа

1. К попыткам несанкционированного доступа относятся:
   - сеансы работы незарегистрированных пользователей или пользователей, срок действия полномочий которых истек,
   - сеансы работы зарегистрированных пользователей с нарушением прав доступа, превышающих свои полномочия по доступу к данным;
   - действия посторонних лиц, пытающихся получить доступ (или получивших доступ) с использованием учетной записи администратора или другого пользователя, методом подбора пароля или использования пароля, разглашенного владельцем учетной записи, или любым другим методом.
2. При выявлении факта несанкционированного доступа (далее – НСД) Ответственный за ОБИ обязан:
   - по возможности пресечь дальнейший НСД к защищаемой информации;
   - доложить главному врачу Учреждения служебной запиской о факте НСД, его результате (успешный, неуспешный) и предпринятых действиях;
   - известить руководителя структурного подразделения, в котором работает пользователь, от имени учетной записи которого была осуществлена попытка НСД, о факте НСД;
   - известить АБИ о факте НСД.

5. Ответственность

1. Ответственный за ОБИ несет персональную ответственность за:
   - соблюдение требований настоящей Инструкции;
   - правильность и объективность принимаемых решений;
   - качество и своевременность проводимых им работ по обеспечению безопасности информации;
   - за все действия, совершенные от имени его учетной записи на ОИ, если с его стороны не было предпринято необходимых действий для предотвращения несанкционированного использования его учетной записи.
2. Ответственный за ОБИ при нарушении норм, регулирующих получение, обработку и защиту информации ограниченного доступа, несет дисциплинарную, административную, гражданско-правовую и уголовную ответственность в соответствии с законодательством Российской Федерации.

Приложение № 2

к Положению об организации работ по обеспечению безопасности информации в ГБУЗ ТО Областная больница №14 имени В.Н. Шанаурина» (с.Казанское)

Инструкция
администратора безопасности информации
в ГБУЗ ТО Областная больница №14 имени В.Н. Шанаурина»
(с.Казанское)

1. Общие положения

1.1. Данная Инструкция определяет порядок обеспечения безопасности информации при проведении работ администратором безопасности информации (далее – АБИ) в ГБУЗ ТО Областная больница №14 имени В.Н. Шанаурина» (с.Казанское(далее – Учреждение).
1.2. АБИ назначается приказом главного врача Учреждения.
1.3. АБИ осуществляет общее руководство и контроль за обеспечением безопасности информации при работе пользователей объекта информатизации (далее – ОИ) и обслуживающего персонала.
1.4. АБИ осуществляет методическое руководство деятельностью пользователей ОИ в вопросах обеспечения информационной безопасности (далее – ИБ).
1.5. АБИ имеет право вносить предложения по изменению и дополнению данной Инструкции, а также Инструкции пользователя. Изменения и дополнения к данной Инструкции утверждаются в установленном порядке.

2. Обязанности администратора безопасности информации

Администратор безопасности информации обязан:
2.1. Знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций и распоряжений, регламентирующих порядок действий по защите информации. АБИ, не ознакомленный с данной Инструкцией, а также с изменениями и дополнениями к ней, к работе с ресурсами ОИ не допускается.
2.2. Участвовать в установке, настройке и сопровождении средств защиты информации, контроле правильности функционирования, физической сохранности и неизменности их настроек.
2.3. Участвовать в приёмке новых программных и технических средств обработки информации.
2.4. Присутствовать при выполнении технического обслуживания элементов

ОИ сторонними специалистами на территории Учреждения.

2.5. Не допускать установку, использование, хранение и размножение программных и аппаратных средств, не связанных с выполнением функциональных задач.

2.6. Обеспечивать доступ к защищаемой информации пользователям ОИ согласно их правам доступа при получении оформленного соответствующим образом разрешения (заявки).

2.7. Осуществлять учет съемных машинных носителей информации (далее – МНИ), их уничтожение, либо контроль процедуры их уничтожения.

2.8. Вести совместно с системным администратором контроль осуществления резервного копирования информации.

2.9. Разрабатывать планы мероприятий по администрированию и техническому обслуживанию аппаратных и программных средств ОИ.

2.10. Периодически анализировать журнал учёта событий, регистрируемых средствами защиты, с целью контроля действий пользователей и выявления возможных нарушений.

2.11. Осуществлять периодические контрольные проверки автоматизированных рабочих мест (далее – АРМ) пользователей.

2.12. Осуществлять разбирательства и составление заключений по фактам несоблюдения условий хранения носителей информации, нарушения правил работы с техническими и программными средствами ОИ, в том числе с СЗИ, или по другим нарушениям, которые могут привести к снижению уровня информационной безопасности.

2.13. Немедленно реагировать на сообщения пользователей о любых неисправностях в работе основных и вспомогательных средств и систем (далее – ОТСС и ВТСС), системы защиты информации (далее – СЗИ), системного и прикладного программного обеспечения (далее – ПО) ОИ.

2.14. Немедленно ставить в известность ответственного за организацию защиту информации Учреждения обо всех неисправностях аппаратно-программных средств ОИ.

2.15. В случае отказа технических средств (далее – ТС) или ПО элементов ОИ, в том числе СЗИ, принимать меры по их своевременному восстановлению и выявлению причин, приведших к отказу работоспособности.

2.16. Ставить в известность ответственного за защиту информации Учреждения о необходимости проведения работ по администрированию СЗИ.

2.17. Представлять руководству отчёт о состоянии защиты ОИ, нештатных ситуациях и допущенных пользователями нарушений установленных требований по защите информации.

2.18. Принимать участие в проведении работ по оценке соответствия ОИ требованиям безопасности информации (работах по аттестации ОИ).

3. Права администратора безопасности информации

Администратор безопасности информации имеет право:

3.1. Требовать прекращения обработки информации, как в целом, так и для отдельных пользователей, в случае выявления нарушений установленного порядка работ или нарушения функционирования ОИ или СЗИ.

3.2. Давать пользователям обязательные для исполнения указания и рекомендации по вопросам ИБ.

3.3. Проводить внеплановые проверки работоспособности СЗИ и соблюдения пользователями технологии обработки информации ограниченного доступа.

3.4. Инициировать проведение служебных расследований по фактам нарушений установленных требований обеспечения ИБ, несанкционированного доступа (далее – НСД), утраты, порчи защищаемой информации и технических средств ОИ.

3.5. Организовывать и участвовать в любых проверка по использованию пользователями ОИ телекоммуникационных ресурсов.

3.6. Осуществлять контроль информационных потоков, генерируемых пользователями ОИ при работе с электронной почтой, съёмными носителями информации, подсистемой удалённого доступа.

3.7. Запрашивать и получать от руководителей и специалистов структурных подразделений Учреждения информацию и материалы, необходимые для организации своей работы.

3.8. Вносить на рассмотрение руководства предложения по улучшению состояния ИБ в Учреждении.

4. Порядок работы администратора безопасности информации с ресурсами информационной системы

4.1. **Управление (администрирования) системой защиты информации**

В ходе управления (администрирования) системой защиты информации АБИ обязан осуществлять:

4.1.1. заведение и удаление учетных записей пользователей, управление полномочиями пользователей ОИ и поддержание правил разграничения доступа на ОИ;

4.1.2. управление СЗИ, в том числе параметрами настройки ПО, включая программное обеспечение СЗИ, управление учетными записями пользователей, восстановление работоспособности СЗИ, генерацию, смену и восстановление паролей;

4.1.3. изменение аутентификационной информации (средств аутентификации), заданной их производителями и (или) используемой при внедрении СЗИ;

4.1.4. установку обновлений программного обеспечения, включая программное обеспечение СЗИ, выпускаемых разработчиками (производителями) СЗИ или по их поручению;

4.1.5. централизованное управление СЗИ (при необходимости);

4.1.6. регистрацию и анализ событий на ОИ, связанных с защитой информации;
4.1.7. информирование пользователей об угрозах безопасности информации, о правилах эксплуатации СЗИ и отдельных средствах защиты информации, а также их обучение;
4.1.8. сопровождение функционирования СЗИ в ходе ее эксплуатации, включая корректировку эксплуатационной документации на нее и организационно-распорядительных документов по защите информации.

4.2. **Проверка работоспособности и настройка системы доступа к ресурсам ОИ**

АБИ присваивает пользователям идентификационные данные к ресурсам ОИ. При этом должны выполняться следующие требования:

4.2.1. АБИ определяет политику изменения учетных данных пользователей и периодически контролирует ее соблюдение;
4.2.2. АБИ сообщает пользователю его уникальное имя и предоставляет возможность задать пароль, далее кодирует персональный идентификатор (при его наличии) пользователя;
4.2.3. изменение учетных данных пользователя производится АБИ по требованию ответственного за защиту информации Учреждения, а также периодически по утвержденному плану и в случае увольнения работника;
4.2.4. АБИ имеет право в целях тестирования уязвимости системы доступа (выявление простейших паролей) производить попытки взлома паролей пользователей, если попытка взлома была успешной, АБИ обязан потребовать у пользователя изменение пароля.

4.3. **Проверка работоспособности и настройка аппаратных и программных средств защиты информации**

4.3.1. АБИ осуществляет установку, настройку СЗИ и контроль выполнения правил их эксплуатации.
4.3.2. АБИ обязан перед началом работ включить и убедиться в работоспособности аппаратных СЗИ, в случае сбоя – работы прекратить.
4.3.3. В случае сбоя СЗИ, таких, как неправильная идентификация пользователей, АБИ обязан приостановить обработку информации до устранения неисправности. В случае производственной необходимости – отключить СЗИ и лично контролировать проведение работ пользователями.

4.4. **Антивирусная защита ресурсов ОИ**

АБИ разрабатывает и контролирует реализацию антивирусной политики, а именно:

4.4.1. настраивает параметры антивирусной программы;
4.4.2. контролирует работоспособность антивирусной программы;
4.4.3. немедленно реагирует на сообщения пользователей о подозрительном поведении ПО, а также о появлении любых сообщений антивирусной программы и принимает соответствующие меры;
4.4.4. имеет право на проведение внеплановой проверки на наличие вирусов;
4.4.5. периодически (один раз в неделю) контролирует корректность процесса обновления антивирусных баз, а также исполняемых модулей

антивирусной программы.

4.5. **Хранение дистрибутивов программного обеспечения СЗИ**

АБИ должен хранить дистрибутивы программного обеспечения СЗИ и прикладного ПО, установленного на ОИ в месте, исключающем доступ посторонних лиц.

4.6. **Проверка целостности системного и прикладного ПО**

Контролю целостности подлежат файлы ПО с расширениями: *.exe, *.com, *.dll, *.sys, *.vxd,*.drv.

4.7. **Резервное копирование и восстановление информации**

4.7.1. Резервное копирование производится регулярно с заданной периодичностью, а также в случае производственной необходимости. При этом необходимо выполнять следующие требования:

- обязательное резервное копирование производится в случае обнаружения неисправностей в работе ПЭВМ или отчуждаемых МНИ;
- допускается обоснованное внеплановое резервное копирование информации как по инициативе пользователя, так и АБИ, если это не нарушает технологию обработки информации;
- резервные копии пользовательской информации и информации операционной системы хранятся на учтенных внешних МНИ;
- ответственным лицом за хранение резервных копий является АБИ.

4.7.2. По мере устранения неисправностей технических средств АБИ производит восстановление информации с резервных копий.

4.7.3. АБИ разрешаются действия в обход установленных процедур идентификации и аутентификации, необходимые только для восстановления функционирования ОИ в случае сбоев в работе или выходе из строя отдельных технических средств (устройств).

4.8. **Конфигурирование ОИ**

4.8.1. Конфигурационной единицей являются услуги, оборудование, программное обеспечение, здания, люди, документы и пр.

4.8.2. Управление изменениями конфигурации осуществляет ответственный за защиту информации. Планирование реализации и непосредственно реализация необходимых изменений возлагается на АБИ.

4.8.3. В ходе управления конфигурацией ОИ и его системы защиты информации АБИ обязан осуществлять:

- поддержание конфигурации ОИ и его СЗИ (структуры системы защиты информации ОИ, состава, мест установки и параметров настройки СЗИ, ПО и ТС) в соответствии с эксплуатационной документацией на СЗИ (поддержание базовой конфигурации ИС и ее системы защиты информации);
- управление изменениями базовой конфигурации ОИ и его СЗИ, в том числе определение типов возможных изменений базовой конфигурации ОИ и его СЗИ, санкционирование внесения изменений в базовую конфигурацию ОИ и его СЗИ, документирование действий по внесению изменений в базовую конфигурацию ОИ и его СЗИ, сохранение данных об

изменениях базовой конфигурации ОИ и его СЗИ, контроль действий по внесению изменений в базовую конфигурацию ОИ и его СЗИ;

- анализ потенциального воздействия планируемых изменений в базовой конфигурации ОИ и его СЗИ на обеспечение информационной безопасности, возникновение дополнительных угроз безопасности информации и работоспособность ОИ;
- определение параметров настройки ПО, включая программное обеспечение СЗИ, состава и конфигурации ТС и ПО до внесения изменений в базовую конфигурацию ОИ и его СЗИ;
- внесение информации (данных) об изменениях в базовой конфигурации ОИ и его СЗИ в документацию на СЗИ;
- принятие решения по результатам управления конфигурацией о повторной аттестации ОИ или проведении дополнительных аттестационных испытаний.

4.9. Обязанности по управлению изменениями в аппаратном и программном обеспечении и всех элементах документации, которые связаны с работой, поддержкой и сопровождением систем, находящихся в эксплуатации, возлагаются на АБИ. При возникновении необходимости изменения конфигурации ОИ, аттестованного по требованиям безопасности информации, АБИ согласовывает планируемые изменения с предприятием-лицензиатом, проводившим аттестационные испытания.

4.10. **Вывод ресурсов ИС из эксплуатации**

При невозможности ремонта различных ресурсов ОИ АБИ обязан:

- физически уничтожать любые МНИ, независимо от содержащейся на них информации; картриджи принтера, иные комплектующие могут быть использованы за пределами ОИ;
- факт выхода из строя и замены оборудования должен быть отражен в Техническом паспорте на ОИ.

4.11. **Реагирование на сбои при регистрации событий безопасности**

4.11.1. В ходе выявления инцидентов и реагирования на них АБИ обязан осуществлять:

- обнаружение и идентификацию инцидентов, в том числе отказов в обслуживании, сбоев (перезагрузок) в работе технических средств, программного обеспечения и СЗИ, нарушений правил разграничения доступа, неправомерных действий по сбору информации, внедрений вредоносных компьютерных программ (вирусов) и иных событий, приводящих к возникновению инцидентов;
- анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий;
- планирование и принятие мер по устранению инцидентов, в том числе по восстановлению ОИ и его сегментов в случае отказа в обслуживании или после сбоев, устранению последствий нарушения правил разграничения доступа, неправомерных действий по сбору информации, внедрения вредоносных компьютерных программ (вирусов) и иных событий,

приводящих к возникновению инцидентов;

- планирование и принятие мер по предотвращению повторного возникновения инцидентов.

4.11.2. Реагирование на сбои при регистрации событий безопасности осуществляется АБИ путем изменения параметров сбора, записи и хранения информации о событиях безопасности в журналах СЗИ от НСД, в том числе отключение записи информации о событиях безопасности от части компонентов ОИ, запись поверх устаревших хранимых записей событий безопасности.

4.11.3. В случае выявления признаков инцидентов безопасности, АБИ обязан:

- немедленно уведомить руководителя о данном факте;
- по возможности в максимально сжатые сроки установить причину возникновения инцидента и исключить возможность его повторения;
- восстановить работоспособность ОИ;
- по окончании работ по восстановлению работоспособности ОИ произвести запись в соответствующих журналах.

4.12. **Контроль (мониторинг) за обеспечением уровня защищенности информации, содержащейся на ОИ**

В ходе контроля (мониторинга), АБИ обязан осуществлять:

- анализ и оценку функционирования СЗИ, включая выявление, анализ и устранение недостатков в функционировании СЗИ;
- проверку работоспособности и параметров настройки ПО, аппаратных и программных СЗИ;
- проверку состава технических средств, программного обеспечения и СЗИ;
- контроль целостности печатей (пломб, наклеек) ТС, используемых для обработки информации ограниченного доступа;
- еженедельное отслеживание появления новых видов уязвимостей ПО. По необходимости АБИ производит устранение уязвимостей согласно рекомендациям разработчика;
- периодический анализ изменения угроз безопасности информации на ОИ, возникающих в ходе эксплуатации, и принятие мер защиты информации в случае возникновения новых угроз безопасности информации;
- контроль за событиями безопасности и действиями пользователей на ОИ. В частности, АБИ обязан осуществлять постоянный контроль за выполнением пользователями установленного комплекса мероприятий по обеспечению безопасности информации;
- контроль (анализ) защищенности информации, содержащейся на ОИ;
- документирование процедур и результатов контроля (мониторинга) за обеспечением уровня защищенности информации, содержащейся на ОИ;
- принятие решения по результатам контроля (мониторинга) за обеспечением уровня защищенности информации о доработке (модернизации) СЗИ, повторной аттестации ОИ или проведении дополнительных аттестационных испытаний.

5. Ответственность

5.1. АБИ несет персональную ответственность за:

- сохранность носителей информации и содержащейся на них информации в рабочее время;
- несоблюдение требований данной Инструкции и неправомерное использование ресурсов ОИ;
- СЗИ, применяемые в Учреждении;
- качество проводимых работ по обеспечению безопасности информации и за все действия, совершенные от имени учетной записи АБИ на ОИ, если с его стороны не было предпринято необходимых действий для предотвращения несанкционированного использования учетной записи.

5.2. АБИ при нарушении норм, регулирующих получение, обработку и защиту информации ограниченного доступа, несет дисциплинарную, административную, гражданско-правовую и уголовную ответственность в соответствии с законодательством Российской Федерации.

Приложение № 3

к Положению об организации
работ по обеспечению
безопасности информации в
ГБУЗ ТО Областная больница
№14 имени В.Н. Шанаурина»
(с. Казанское)

Инструкция пользователя

1. Общие положения

1.1. Настоящая Инструкция определяет порядок обеспечения безопасности информации при ее обработке пользователями на объектах информатизации (далее – ОИ) ГБУЗ ТО Областная больница №14 имени В.Н. Шанаурина» (с.Казанское)(далее – Учреждение).

1.2. Ответственность за функционирование системы защиты информации (далее – СЗИ) возлагается на администратора безопасности (далее – АБИ).

1.3. Ответственность за выполнение установленных Инструкцией требований возлагается на работника Учреждения, производящего обработку информации с использованием средств вычислительной техники на автоматизированном рабочем месте (далее - АРМ пользователя).

1.4. Доступ работников к данным осуществляется в соответствии с Инструкцией по управлению доступом к техническим средствам и информационным ресурсам.

1.5. К работе с защищаемой информацией допускаются только сотрудники, ознакомленные с настоящей Инструкцией под личную подпись в листе ознакомления.

1.6. Вход в помещения, в которых производится автоматизированная обработка защищаемой информации, разрешается постоянно работающим в нём работникам. Лицам, привлекаемым к проведению ремонтных, наладочных и других работ, а также посетителям, вход в помещения разрешается только в сопровождении ответственных лиц.

1.7. По фактам и попыткам несанкционированного доступа (далее – НСД) к защищаемой информации, а также в случаях её утечки и (или) модификации (уничтожения) проводятся служебные расследования.

1.8. Пользователи имеют право письменно вносить предложения по изменению и дополнению настоящей Инструкции. Изменения и дополнения к настоящей Инструкции утверждаются в установленном порядке.

2. Обязанности

Пользователь обязан:

2.1. Знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций и распоряжений, регламентирующих порядок действий по защите информации.

2.2. Знать и соблюдать установленные требования к обработке информации ограниченного доступа, учету и хранению носителей информации, обеспечению информационной безопасности.

2.3. Выполнять только те процедуры, которые определены технологическим процессом обработки информации ограниченного доступа.

2.4. Соблюдать требования парольной политики в соответствии с Инструкцией по организации парольной защиты. Получить уникальное имя и персональный идентификатор (при его наличии) от АБИ. Пользователь обязан помнить и соблюдать в тайне свои имена и пароли, не допускается их запись на каких-либо носителях в целях напоминания. При утере или подозрении на утечку своего имени, пароля и персональных идентификаторов пользователь должен немедленно сообщить об этом АБИ.

2.5. Во время работы располагать экран монитора так, чтобы затруднить посетителям просмотр отображаемой информации.

2.6. При отсутствии визуального контроля за рабочей станцией доступ к компьютеру должен быть немедленно заблокирован. Для этого необходимо нажать одновременно комбинацию клавиш <Ctrl><Alt><Del> и выбрать опцию <Блокировка>.

2.7. При отсутствии пользователя на рабочем месте либо в присутствии лиц, не имеющих допуска к ресурсам ОИ, все документы, содержащие защищаемую информацию, должны быть недоступны для просмотра и иного их использования.

2.8. Немедленно приостановить работы, вызывать АБИ и поставить в известность руководителя структурного подразделения в следующих случаях:

– возникновение подозрения на наличие вредоносного программного обеспечения (частые ошибки в работе программ, появление посторонних графических и звуковых эффектов, искажения данных, неконтролируемое пропадание файлов, появление сообщений о системных ошибках, замедление работы компьютера и т.п.):

– появления информационного окна средства антивирусной защиты, сигнализирующем об обнаружении вредоносного программного обеспечения;

– обнаружения нарушений целостности пломб (наклеек, нарушении или несоответствии номеров печатей) на аппаратных средствах АРМ или иных фактов совершения в его отсутствие попыток несанкционированного доступа к защищаемому АРМ;

– несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств АРМ;

– отклонениях в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию АРМ, выхода из строя или неустойчивого функционирования узлов АРМ или периферийных устройств (дисководов, принтера и т.п.), а также перебоев в системе электроснабжения;

– некорректного функционирования установленных на АРМ средств защиты;

– обнаружения непредусмотренных отводов кабелей и подключенных к АРМ дополнительных устройств;

– обнаружении фактов и попыток НСД;

– нарушения установленного порядка обработки защищаемой информации.

2.9.Принимать меры по реагированию в случае возникновения внештатных ситуаций и аварийных ситуаций с целью ликвидации их последствий в пределах возложенных на него функций.

2.10.Обо всех выявленных нарушениях, связанных с информационной безопасностью Учреждения, а также для получения консультаций по вопросам информационной безопасности, необходимо обратиться к АБИ.

2.11.Пользователям **запрещается**:

– разглашать защищаемую информацию посторонним лицам;

– копировать защищаемую информацию на неучтенные внешние носители;

– самостоятельно устанавливать, тиражировать или модифицировать программное и аппаратное обеспечение, изменять установленный порядок функционирования технических и программных средств;

– производить перемещение технических средств АРМ без согласования с АБИ;

– вскрывать корпуса технических средств АРМ и вносить изменения в схему и конструкцию устройство, производить техническое обслуживание (ремонт) средств вычислительной техники без согласования с АБИ.

– подключать к рабочей станции и корпоративной информационной сети личные внешние носители и мобильные устройства;

– отключать (блокировать) средства защиты информации;

– выполнять на АРМ работы, не предусмотренные технологическим процессом обработки информации;

– использовать компоненты программного и аппаратного обеспечения в неслужебных целях.

– сообщать (или передавать) посторонним лицам параметры своей учетной записи (имя, персональный идентификатор (при его наличии) и пароль);

– оставлять без присмотра и передавать другим лицам персональный идентификатор;

– привлекать посторонних лиц для ремонта или настройки АРМ без согласования с ответственным за защиту информации;

– оставлять без присмотра свое АРМ, не активизировав блокировку доступа, или оставлять свое АРМ включенным по окончании работы;

– умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к нарушению безопасности информации.

3. Организация парольной защиты

3.1. Личные пароли доступа создаются пользователем самостоятельно или выдаются АБИ.

3.2. Полная плановая смена паролей проводится не реже одного раза в квартал.

3.3. Правила формирования пароля:

– пароль должен состоять не менее чем из 6 символов;

– в пароле должны присутствовать символы из числа прописных и строчных букв английского алфавита от A до Z; десятичных цифр (от 0 до 9); символы, не принадлежащие алфавитно-цифровому набору (например, !, $, #, %);

– запрещается использовать в качестве пароля имя учетной записи, простые пароли типа «123», «111», «qwerty» и им подобные, а также имена и даты рождения пользователей ОИ и их родственников, клички домашних животных, номера автомобилей, телефонов и другие пароли, которые можно вычислить, основываясь на информации о пользователе;

– запрещается использовать в качестве пароля один и тот же повторяющийся символ, либо повторяющуюся комбинацию из нескольких символов;

– запрещается использовать в качестве пароля комбинацию символов, набираемых в закономерном порядке на клавиатуре (например, 1234567 и т.п.);

– запрещается выбирать пароли, которые уже использовались ранее.

3.4. Правила ввода пароля:

– ввод пароля должен осуществляться с учетом регистра, в котором он был задан;

– во время ввода паролей необходимо исключить возможность его подсматривания посторонними лицами.

3.5. Правила хранения пароля:

– запрещается записывать пароли на бумаге, в файле и других носителях информации, в том числе на предметах;

– запрещается сообщать другим пользователям личный пароль и/или регистрировать их в системе под своей учетной записью.

3.6. Лица, использующие паролирование, обязаны:

– четко знать и строго выполнять требования настоящей Инструкции и других руководящих документов по паролированию;

– своевременно сообщать АБИ об утере, компрометации, несанкционированном изменении паролей и несанкционированном изменении сроков действия паролей.

4. Ответственность

4.1. Пользователь несет персональную ответственность за:

– сохранность носителей информации и содержащейся на них информации (в рабочее время);

– соблюдение требований данной Инструкции, неправомерное использование информационных ресурсов Учреждения и за все действия, совершенные от имени его учетной записи, если со стороны пользователя не было предпринято действий для предотвращения несанкционированного использования его учетной записи.

4.2. За разглашение информации ограниченного доступа и нарушение порядка работы со средствами обработки информации, работники могут быть привлечены к гражданской, уголовной, административной, дисциплинарной и иной предусмотренной законодательством Российской Федерации ответственности.

Приложение № 4

к Положению об организации работ
по обеспечению безопасности
информации в ГБУЗ ТО Областная
больница №14 имени В.Н.
Шанаурина» (с.Казанское)

Положение
о порядке работы с информационными ресурсами
ГБУЗ ТО Областная больница №14 имени В.Н. Шанаурина» (с.Казанское)

1. Общие положения

1.1. Данное Положение определяет порядок работы с информационными ресурсами (далее – ИР) – ГБУЗ ТО Областная больница №14 имени В.Н. Шанаурина» (с.Казанское)(далее – Учреждение).

1.2. Положение разработано в соответствии с конституцией Российской Федерации, трудовым кодексом Российской Федерации, Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Указом Президента Российской Федерации от 06.03.1997 № 188 «Об утверждении перечня сведений конфиденциального характера».

1.3. К информационным ресурсам относятся документы и отдельные массивы документов, картотеки, записи в журналах, книгах, реестрах, а также базы данных (далее – БД) и информационные системы (далее – ИС), размещённые на технических средствах (далее – ТС) Учреждения, произведенные работниками Учреждения в порядке исполнения служебных обязанностей, созданные за счет бюджетных средств или полученные от других организаций и (или) систем на законных основаниях.

1.4. Перечень информационных ресурсов Учреждения, подлежащих защите и перечень информационных систем и информационных ресурсов сетей связи общего доступа (Интернет), используемых работниками Учреждения для исполнения своих должностных обязанностей, а также Списки работников, имеющих к ним доступ, утверждаются приказом главного врачаУчреждения.

1.5. Информационные ресурсы Учреждения включаются в состав собственности Учреждения, являются объектами отношений физических и юридических лиц, и подлежат защите в соответствии с законодательством Российской Федерации.

2. Документирование информации

2.1. В Учреждении обрабатывается общедоступная информация и информация ограниченного доступа, не составляющая государственную тайну, в том числе служебная информация (документы с пометкой «ДСП») и персональные данные (далее – ПДн).

2.2. Обязательным условием отнесения информации к информационным ресурсам Учреждения является ее документирование на материальных носителях с реквизитами, позволяющими ее идентифицировать (документированная информация). Основными материальными носителями информации являются бумажные и машинные (гибкие и жесткие магнитные диски, оптические, магнитооптические диски, USB-накопители).

2.3. Учреждение создаёт общедоступные информационные ресурсы по вопросам своей деятельности.

2.4. Обработка информации, содержащей ПДн, осуществляется в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» и регламентируется в организационно-распорядительной документации Учреждения.

2.5. Обработка документов с пометкой «ДСП» регламентируется распоряжением Правительства Тюменской области от 25.03.2013 № 400-рп «Об утверждении Положения о порядке работы со служебной информацией ограниченного распространения в исполнительных органах государственной власти Тюменской области».

2.6. Документ, созданный с применением автоматизированных информационных систем, приобретает юридическую силу после его подписания должностным лицом в установленном порядке.

2.7. Юридическая сила документа, хранимого, обрабатываемого и передаваемого с помощью автоматизированных и телекоммуникационных систем, может подтверждаться электронной подписью в установленном порядке в соответствии с федеральным законом Российской Федерации от 06.04.2011 № 63-ФЗ «Об электронной подписи».

3. Порядок хранения и уничтожение информации

3.1. Информационные ресурсы Учреждения в электронном виде хранится на магнитных носителях информации (далее - МНИ) съемных, либо стационарно установленных в технических средствах обработки (АРМ пользователей и серверах) в подразделениях Учреждения, которое осуществляет её обработку.

3.2. Информационные ресурсы на бумажных носителях хранится в подразделениях Учреждения, которое осуществляет её обработку в установленных местах (папках, картотеках, шкафах, сейфах и иных установленных местах).

3.3. Информация в электронном виде может размещаться в локальных и распределённых электронных базах данных компьютерной сети. Доступ к электронным базам данных, обеспечивается системой защиты информации.

3.4. В нерабочее время помещения, где хранятся информационные ресурсы Учреждения, должны закрываться на ключ. В рабочее время, в случае ухода сотрудников, помещение должно быть закрыто на ключ или оставлено под ответственность лиц, назначенных руководителем подразделения.

3.5. Работник Учреждения, имеющий доступ к информации в связи с исполнением трудовых обязанностей, обеспечивает хранение информации, исключающее доступ к ним третьих лиц.

3.6. В отсутствие работника на его рабочем месте не должно быть документов, содержащих информацию Учреждения (соблюдение «политики чистых столов»).

3.7. При отсутствии работника в отпуске, служебной командировке и иных случаях длительного отсутствия на своем рабочем месте, работник обязан передать документы и иные носители информации лицу, на которое приказом (распоряжением) будет возложено исполнение его трудовых обязанностей.

3.8. В случае если такое лицо не назначено, то документы и иные носители информации, по указанию руководителя структурного подразделения, передаются другому работнику, имеющему доступ к данной информации.

3.9. При увольнении работника, имеющего доступ к информации, документы и иные носители, содержащие информацию, по указанию руководителя структурного подразделения передаются другому работнику, имеющему доступ к данной информации.

3.10.Повседневный контроль за выполнением требований по защите информации в подразделении осуществляет руководитель подразделения.

3.11.Периодический контроль эффективности реализации мер защиты информации в подразделениях Учреждения осуществляет ответственный за ОБИ.

3.12.Уничтожение информации на бумажном носителе, либо удаление электронных базах данных, содержащих информацию в электронном виде, осуществляется по истечении установленного срока обработки информации комиссией, назначенной приказом главного врача Учреждения.

4. Порядок обеспечения безопасности информации

4.1. Порядок доступа к информационным ресурсам Учреждения регламентируется Инструкцией по управлению доступом к техническим средствам и информационным ресурсам согласно приложению № 1 к настоящему Положению.

4.2. Порядок учёта, хранения и обращения со съёмными носителями информации регламентируется Инструкцией по порядку учёта, хранения и уничтожения съёмных носителей информации согласно приложению № 2 к настоящему Положению.

Приложение № 1
к Положению о порядке работы с информационными ресурсами ГБУЗ ТО Областная больница №14 имени В.Н. Шанаурина» (с.Казанское)

Инструкция по управлению доступом к техническим средствам, информационным ресурсам и помещениямв ГБУЗ ТО Областная больница №14 имени В.Н. Шанаурина» (с. Казанское)

Общие положения

1.1. Данная Инструкция разработана в целях определения порядка, регламентирующего получение (изменение, лишение полномочий) доступа к техническим средствам (далее – ТС), информационным ресурсам (далее – ИР) и помещениям, в которых ведётся обработка информации ограниченного доступа, объекта информатизации (далее – ОИ) – ГБУЗ ТО Областная больница №14 имени В.Н. Шанаурина» (с.Казанское) (далее –Учреждения).

1.2. Разрешительная система доступа к ОИ представляет собой совокупность процедур оформления прав субъектов на доступ к ТС, ИР и помещениям (объектам доступа) ОИ и прав и обязанностей ответственных лиц, осуществляющих реализацию этих процедур.

1.3. Действие настоящей Инструкции распространяется на все структурные подразделения Учреждения.

1.4. Объектами доступа на ОИ являются:

– ТС, включая средства отображения информации;

– помещения, в которых размещены ТС;

– носители информации, включая съёмные носители информации и жёсткие магнитные диски (далее – ЖМД);

– базы данные (далее – БД) и каталоги файлов на съёмных носителях информации и ЖМД;

– общесистемное и специальное программное обеспечение (далее – ПО), предназначенное для обработки информации и разработки документов;

– программные средства, осуществляющие функции по защите информации, а также функции контроля безопасности (далее – СЗИ);

– каналы информационного обмена и телекоммуникации.

1.5. Субъектами доступа являются:

– администратор безопасности информации (далее – АБИ);

– системный администратор;

– пользователи, работающие на автоматизированных рабочих местах (далее – АРМ пользователя);

– процессы, выполняемые от имени АБИ, системного администратора и пользователей при обработке информации.

1.6. Ответственными лицами, осуществляющими реализацию процедур оформления прав субъектов на доступ к ОИ, являются:

- Главный врачУчреждения;
- руководители структурных подразделений Учреждения;
- администратор безопасности информации;
- системный администратор.

2. Порядок получения доступа к техническим средствами информационным ресурсам

2.1. Доступ к ресурсам ОИ имеют работники, которым данные ресурсы необходимы в связи с исполнением ими трудовых обязанностей.

2.2. Работники допускаются к работе с ресурсами ОИ только после прохождения инструктажа, проводимого АБИ и ознакомление с требованиями Положения об организации работ по обеспечению информационной безопасности, должностной инструкции и иными локальными нормативными актами Учреждения в сфере обеспечения безопасности информации.

2.3. С целью соблюдения принципа персональной ответственности за свои действия каждому работнику Учреждения, допущенному к работе на ОИ, сопоставляется персональное уникальное имя (учётная запись пользователя, логин), под которым он будет регистрироваться и работать в домене локальной вычислительной сети ОИ.

2.4. Для регистрации и работы в информационных системах (далее – ИС), входящих в состав ОИ, работнику могут быть выданы учётные записи пользователя данных информационных систем.

2.5. Некоторым работникам в случае производственной необходимости могут быть сопоставлены несколько уникальных имён (учётных записей).

2.6. Процедура регистрации пользователя (создание учётной записи) для работника и предоставление (изменение) ему прав доступа к ТС (АРМ пользователей, СЗИ) и ИР (информационным системам, файловым хранилищам и т.д.) инициируется Заявкой (Приложение № 1) на доступ (изменение, лишение полномочий доступа) к ТС и ИР (далее – Заявка), направляемой руководителем подразделения работника ответственному за защиту информации.

В Заявке указывается:

- содержание запрашиваемых изменений (регистрация нового пользователя, удаление учётной записи пользователя, расширение или сужение полномочий и прав доступа ранее зарегистрированного пользователя);
- должность (с полным наименованием подразделение), фамилия, имя и отчество работника;
- имя пользователя (учётной записи) данного работника (при наличии);
- полномочия, которые необходимо добавить пользователю или которых необходимо лишить пользователя.

2.7. Ответственный за защиту информации визирует Заявку, утверждая тем самым производственную необходимость допуска (изменения прав доступа) данного работника к ресурсам ОИ и выдаёт задание соответствующим системным (прикладным) администраторам и АБИ на внесение необходимых изменений в списки пользователей ОИ и/или соответствующих ИС.

2.8. На основании Заявки (задания) соответствующими администраторами производятся необходимые операции по созданию (удалению) учётной записи пользователя, присвоению ему начального значения пароля и заявленных прав доступа к ресурсам ОИ, включению его в соответствующие решаемым задачам группы пользователей и другие необходимые действия.

2.9. Настройку и конфигурацию СЗИ на АРМ пользователя для обеспечения необходимого уровня защищённости выполняет АБИ, в соответствии с эксплуатационной документацией на СЗИ.

2.10.Работнику, зарегистрированному в качестве нового пользователя, сообщается имя соответствующего ему пользователя (логин) и начальное значение пароля, которые он обязан сменить при первом же входе в домен.

2.11.Возможность смены первичного пароля в ИС, входящих в состав ОИ, определяется функциональными возможностями конкретной ИС.

2.12.Исполненная Заявка хранится у АБИ. Впоследствии они могут использоваться для:

– восстановления учётных записей и полномочий пользователей после аварии на ОИ;

– контроля правомерности наличия у конкретного пользователя прав доступа к тем или иным ресурсам ОИ при разборе конфликтных ситуаций;

– для проверки правильности настройки средств разграничения доступа к информации ограниченного доступа.

3. Отзыв прав доступа

3.1. При увольнении должностных лиц – пользователей ОИ и/или лишения их прав доступа к ресурсам ОИ руководитель структурного подразделения увольняемого работника в обязательном порядке направляет Заявку в адрес Ответственного за защиту информации.

3.2. Ответственный за защиту информации визирует Заявку, утверждая тем самым лишение прав пользователя на доступ к ИР и ТС ОИ.

3.3. АБИ и системный администратор:

– проводят смену (удаление) соответствующих настроек прав доступа на советующих СЗИ в соответствии с изменившимися полномочиями;

– совместно с непосредственным руководителем работника анализируют целостность данных, к которым имел доступ работник.

3.4. Удаление и сохранение содержимого почтового ящика, личных локальных и сетевых папок согласовывается с руководителем структурного подразделения работника.

3.5. АБИ и системный администратор анализируют АРМ уволенного работника на наличие закладок и вирусов, после чего вся пользовательская информация на дисках АРМ работника уничтожается.

3.6. Все изменения в правах доступа, связанные с увольнением работника, выполняются администраторами не позднее трёх рабочих дней с момента получения ими заявки.

4. Порядок доступа работников в помещения, в которых ведётся обработка информации ограниченного доступа, не составляющей государственную тайну

4.1. Порядок доступа работников Учреждения в помещения, в которых ведётся обработка информации ограниченного доступа, не составляющей государственную тайну, определяет правила доступа в помещения Учреждения, где хранится и обрабатывается информация ограниченного доступа, не составляющая государственную тайну (в т.ч. персональные данные и документы с пометкой «ДСП»), в целях исключения несанкционированного доступа к информации и обеспечения защиты информации от уничтожения, изменения, блокирования, копирования, распространения.

4.2. Список помещений, в которых разрешается обработка информации ограниченного доступа, не составляющей государственную тайну (далее – информация), утверждается *главным врачом* Учреждения (Приложение № 2).

4.3. Доступ в помещения Учреждения, где хранится и обрабатывается информация, осуществляется в соответствии со Списком лиц, допущенных в помещения, предназначенных для обработки информации (далее – Список), утверждаемым *главным врачом* Учреждения (Приложение № 3).

4.4. Нахождение в помещениях, в которых ведётся обработка или хранение информации, лиц, не указанных в Списке, возможно только в сопровождении лица, указанного в Списке.

4.5. Для помещений, в которых хранится и обрабатывается информация, организуется режим обеспечения безопасности, при котором обеспечивается сохранность носителей информации, содержащих информацию, а также исключается возможность неконтролируемого проникновения и пребывания в этих помещениях посторонних лиц. Данный режим должен обеспечивать в том числе:

– запиранием помещения на ключ, в т.ч. при выходе из него в рабочее время;

– закрытием металлических шкафов и сейфов, где хранятся носители информации, во время отсутствия в помещениях работников Учреждения.

4.6. Руководители структурных подразделений Учреждения, в рамках своих полномочий и в соответствии с требованиями, предъявляемыми к защите обрабатываемой информации, обязаны принимать меры организационного характера (организация учёта, контроля и управления физическим доступом в помещения) для обеспечения защиты информации, циркулирующей в помещениях подчинённым их подразделений.

Приложение № 1
к Инструкции по управлению доступом к техническим средствам, информационным ресурсам и помещениям

Заявка
на доступ (изменение, лишение полномочий доступа)
к техническим средствам и информационным ресурсам

Прошу:

1. Зарегистрировать пользователем *(исключить из списка пользователей, изменить/лишить полномочий пользователя)*:

_____
(должность с указанием подразделения)

_____
(фамилия, имя и отчество работника)

2. Предоставить (изменить/запретить) доступ пользователя к АРМ № _____, расположенному в помещении № _____ к следующим информационным системам Учреждения:

№ п/п	Наименование системы

3. Предоставить пользователю доступ к сетевым ресурсам:

_____
и принтерам общего пользования, расположенным в помещениях:

_____
4. Предоставить (ограничить, лишить доступа) доступа к сети Интернет.
5. Создать в домене ЛВС Учреждения почтовый ящик пользователя.

Ответственный за защиту информации _____ _____
(подпись) (ФИО)

_____
(дата)

(ФИО)

Приложение № 2
к Инструкции по управлению доступом к техническим средствам, информационным ресурсам и помещениям

Список помещений, предназначенных для обработки информационных ресурсов Учреждения

№ п/п	№ помещения, размещение	Подразделение организации	Должность ответственного	ФИО ответственного
1.				
2.				
3.				
4.				
5.				
6.				
7.				
8.				
9.				
10.				
11.				
12.				
13.				
14.				
15.				
16.				
17.				
18.				
19.				
20.				
21.				
22.				
23.				
24.				
25.				
26.				
27.				
28.				
29.				
30.				
31.				
32.				

Приложение № 3
к Инструкции по управлению доступом к техническим средствам, информационным ресурсам и помещениям

Перечень должностей, замещение которых предусматривает допуск в помещения, предназначенных для обработки информационных ресурсов Учреждения

№ п/п	Должность	№ помещения, размещение
1.		
2.		
3.		
4.		
5.		
6.		
7.		
8.		
9.		
10.		
11.		
12.		
13.		
14.		
15.		
16.		
17.		
18.		
19.		
20.		
21.		
22.		
23.		
24.		
25.		
26.		
27.		
28.		
29.		

Приложение № 3
к Положению о порядке работы с информационными ресурсами ГБУЗ ТО Областная больница №14 имени В.Н. Шанаурина» (с. Казанское)

Инструкция по порядку учета, хранения и уничтожения съёмных носителей информации в ГБУЗ ТО Областная больница №14 имени В.Н. Шанаурина» (с.Казанское)

1. Общие положения

1.1. Настоящая Инструкция устанавливает порядок использования съёмных машинных носителей информации при работе на объекте информатизации (далее – ОИ) – ГБУЗ ТО Областная больница №14 имени В.Н. Шанаурина» (с.Казанское) (далее – Учреждения).

1.2. Действие настоящей Инструкции распространяется на работников Учреждения, в рамках выполнения своих должностных обязанностей участвующих в обработке информации ограниченного доступа.

1.3. Контроль исполнения требований настоящей Инструкции возлагается на ответственного за защиту информации.

2. Порядок использования носителей информации

2.1. Под использованием носителей информации на ОИ понимается их подключение к инфраструктуре ОИ с целью обработки, приема/передачи информации между ОИ носителями информации.

2.2. На ОИ допускается использование только учтенных носителей информации, которые являются собственностью и подвергаются регулярной ревизии и контролю.

2.3. Носители информации предоставляются работникам по инициативе руководителей структурных подразделений в случаях:

- необходимости выполнения вновь принятым работником своих должностных обязанностей;
- возникновения у работника производственной необходимости.

3. Порядок учета съемных носителей информации

3.1. Все находящиеся на хранении и в обращении съемные носители информации подлежат учёту.

3.2. Каждый съемный носитель с записанной на нем информацией ограниченного доступа должен иметь этикетку, на которой указывается его уникальный учетный номер.

3.3. Учет и выдачу съемных носителей информации осуществляют работники структурных подразделений, на которых возложены функции хранения носителей информации. Факт выдачи съемного носителя фиксируется в журнале учета съемных носителей информации (Приложение № 1) и журнале приема-выдачи защищаемых носителей информации (Приложение № 2).

3.4. Работники получают учтенный съемный носитель от уполномоченного работника для выполнения работ на конкретный срок. При получении делаются соответствующие записи в журнале учета. По окончании работ пользователь сдает съемный носитель для хранения уполномоченному работнику, о чем делается соответствующая запись в журнале учета.

4. Порядок обращения со съёмными носителями информации

4.1. При использовании работниками носителей ПДннеобходимо:

- соблюдать требования настоящей Инструкции;
- использовать носители информации исключительно для выполнения своих служебных обязанностей;
- ставить в известность администратора безопасности информации (далее – АБИ) о любых фактах нарушения требований настоящей Инструкции;
- бережно относится к носителям информации;
- обеспечивать физическую безопасность носителей информации всеми разумными способами;
- извещать администратора безопасности информации о фактах утраты (кражи) носителей информации;

4.2. При использовании носителей информации запрещено:

- использовать носители информации в личных целях;
- передавать носители информации другим лицам (за исключением АБИ и системных администраторов);
- хранить съемные носители с информацией ограниченного доступа вместе с носителями открытой информации, на рабочих столах, либо оставлять их без присмотра или передавать на хранение другим лицам;
- выносить съемные носители с информацией ограниченного доступа из служебных помещений для работы с ними на дому и т. д.

4.3. Любое взаимодействие (обработка, прием/передача информации) инициированное работником между ОИ и неучтенными (личными) носителями информации, рассматривается как несанкционированное (за исключением случаев, оговоренных с АБИ заранее). АБИ оставляет за собой право блокировать или ограничивать использование носителей информации.

4.4. Информация об использовании работником носителей информации на ОИ протоколируется и, при необходимости, может быть предоставлена АБИ.

4.5. В случае выявления фактов несанкционированного и/или нецелевого использовании носителей информации инициализируется служебная проверка, проводимая комиссией, состав которой определяется ответственным за защиту информации.

4.6. По факту выясненных обстоятельств составляется акт расследования инцидента и передается АБИ для принятия мер согласно локальным нормативным актам и действующему законодательству.

4.7. Информация, хранящаяся на носителях информации, подлежит обязательной проверке на отсутствие вредоносного ПО.

4.8. При отправке или передаче информации ограниченного доступа адресатам на съемные носители записываются только предназначенные адресатам данные. Отправка информации ограниченного доступа адресатам на съемных носителях осуществляется в порядке, установленном для документов для служебного пользования.

4.9. Вынос съемных носителей информации для непосредственной передачи адресату осуществляется только с письменного разрешения АБИ.

4.10. В случае утраты или уничтожения съемных носителей информации либо разглашении содержащихся в них сведений немедленно ставится в известность АБИ. На утраченные носители составляется акт. Соответствующие отметки вносятся в журналы учета бумажных и съемных носителей информации.

4.11. Съемные носители информации, пришедшие в негодность, или отслужившие установленный срок, подлежат уничтожению. Уничтожение съемных носителей информации осуществляется уполномоченной комиссией. По результатам уничтожения носителей составляется акт (Приложение № 3).

4.12. В случае увольнения или перевода работника в другое структурное подразделение, предоставленные носители информации изымаются.

5. Ответственность

5.1. Работники, нарушившие требования настоящей Инструкции, несут ответственность в соответствии с действующим законодательством Российской Федерации и локальными нормативными актами.

Приложение № 1
к Инструкции по порядку учета, хранения и уничтожения съёмных носителей информации

Регистрационный №_____

ЖУРНАЛ УЧЕТА
ЗАЩИЩАЕМЫХ НОСИТЕЛЕЙ ИНФОРМАЦИИ

Начат «___» _____20__ г.

Окончен «___» _____20__ г.

На _____листах

_____ _____ _____
(должность руководителя) (подпись) (Фамилия И.О.)

М.П.

№ п/п	Регистрационный номер	Тип защищаемого носителя информации	Дата	Назначение (содержимое) носителя	Сведения об уничтожении носителя	Ответственное должностное лицо (ФИО)
1						
2						
3						
4						
5						
6						
7						
8						
9						
10						
11						

Приложение № 2
к Инструкции по порядку учета, хранения и уничтожения съёмных носителей информации

ЖУРНАЛ ПРИЕМА-ВЫДАЧИ
ЗАЩИЩАЕМЫХ НОСИТЕЛЕЙ ИНФОРМАЦИИ

Начат «___» _____20__ г.

Окончен «___» _____20__ г.

На _____листах

_____ _____ _____
(должность руководителя) (подпись) (Фамилия И.О.)

М.П.

№ п/п	Регистрационный номер/дата	Расписка в получении (ФИО, подпись, дата)	Расписка о возврате (ФИО, подпись, дата)
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			

Приложение № 3
к Инструкции по порядку учета, хранения и уничтожения съёмных носителей информации

Типовая форма акта
об уничтожении носителей информации ограниченного доступа

В связи с достижением цели обработки информации ограниченного доступа к уничтожению отобраны следующие носители информации:

№п/п	Учетный номер носителя	Тип носителя	Цель обработки информации	Дата начала обработки информации	Дата окончания обработки информации
1					
2					
3					
4					
5					
6					

Всего подлежит уничтожению _____ носителей информации.

Проверка правильности включения материальных носителей информации в Акт проведена.

Носители информации полностью уничтожены путем

_____
_____ .

СОГЛАСОВАНО
Ответственный за защиту информации

_____ _____ _____
(ФИО) (подпись) (дата)

ОТМЕТКА О ВЫПОЛНЕНИИ
Ответственный за выполнение

_____ _____ _____
(ФИО, должность) (подпись) (дата)

Приложение № 5

к Положению об организации работ по обеспечению безопасности информации в ГБУЗ ТО Областная больница №14 имени В.Н. Шанаурина» (с. Казанское)

Инструкция по организации парольной защитыв ГБУЗ ТО Областная больница №14 имени В.Н. Шанаурина» (с.Казанское)

1. Общие положения

1.1. Настоящий документ регламентирует организационные и технические вопросы применения парольной защиты на объекте информатизации (далее – ОИ) - ГБУЗ ТО Областная больница №14 имени В.Н. Шанаурина» (с.Казанское)(далее – Учреждения).

1.2. Контроль за действиями исполнителей и обслуживающего персонала системы при работе с паролями возлагается на администратора безопасности информации (далее – АБИ).

1.3. При эксплуатации пользователем на своём автоматизированном рабочем месте (далее – АРМ) внешних информационных систем, оператором которых Учреждение не является, пользователю следует руководствоваться требованиями парольной политики оператора – собственника информационной системы.

2. Правила формирования паролей

2.1. Каждому субъекту доступа (пользователю) ОИ, допущенному в установленном порядке к обработке информации на ОИ, присваиваются персональные идентификаторы (логины, имена пользователей) для доступа к техническим средствами (далее – ТС) и информационным ресурсам ОИ.

2.2. Персональный идентификатор и первичный личный пароль для доступа пользователя в систему создаёт АБИ или системный администратор на основании заявки в соответствии с Инструкцией по управлению доступом к техническим средствам, информационным ресурсам и помещениям.

2.3. Персональные идентификаторы и личные пароли для доступа пользователей в подсистемы ОИ имеют право создавать АБИ, системный администратор, а также уполномоченные лица, осуществляющие техническое сопровождение конкретной подсистемы ОИ.

2.4. Каждому персональному идентификатору пользователя соответствуют определённые полномочия (права доступа) пользователя в информационных подсистемах и пароль, обеспечивающий аутентификацию (проверку подлинности).

2.5. Пользователь несёт ответственность за все действия, совершённые на ОИ и информационных подсистемах с использованием его атрибутов доступа (идентификатора и пароля).

2.6. Первичный пароль – комбинация символов (буквы, цифры, знаки препинания, специальные символы), устанавливаемые системным администратором при создании новой учетной записи.

2.6.1. Установку первичного пароля производит системный администратор при создании новой учетной записи. Ответственность за сохранность временного пароля лежит на системном администраторе.

2.6.2. Временный пароль может содержать несложную комбинацию символов, либо повторяющиеся символы.

2.6.3. При создании временного пароля, системный администратор обязан установить опцию, требующую смену пароля при первом входе в систему, а также уведомить владельца учетной записи о необходимости произвести смену пароля.

2.6.4. Временный пароль так же используется при сбросе забытого пароля на учетную запись.

2.7. Основной пароль – комбинация символов (буквы, цифры, знаки препинания, специальные символы), известная только работнику организации, используемая для подтверждения подлинности владельца учетной записи.

2.7.1. Установку основного пароля производит пользователь при первом входе в систему с новой учетной записью.

2.7.2. При выборе пароля необходимо руководствоваться требованиями сложности пароля, указанными в Приложении № 1 к настоящей Инструкции.

2.8. В случае если формирование личных паролей пользователей осуществляется централизованно, ответственность за правильность их формирования и распределения возлагается на АБИ.

2.9. При настройке парольной политики должны быть учтены следующие требования к характеристикам паролей:

- длина пароля не менее 6 символов;
- алфавит пароля не менее 60 символов;
- максимальное количество неуспешных попыток аутентификации (ввода неправильного пароля) до блокировки от 3 до 10 попыток;
- блокировка программно-технического средства или учетной записи пользователя в случае достижения установленного максимального количества неуспешных попыток аутентификации от 5 до 30 минут;
- смена паролей не реже 1 раза в 120 дней.

3. Ввод пароля

3.1. При вводе пароля пользователю необходимо исключить произнесение его вслух, возможность его просмотра посторонними лицами и техническими средствами (стационарными и встроенными в мобильные телефоны видеокамерами и т.п.).

3.2. Для предотвращения угадывания паролей системный администратор обязан настроить механизм блокировки учетной записи при многократном неправильном вводе пароля.

3.3. Максимальное количество неуспешных попыток аутентификации и время блокировки устанавливаются АБИ или системным администратором для каждой подсистемы индивидуально в зависимости от уровня значимости обрабатываемой информации и масштаба информационной системы.

3.4. Разблокирование учетной записи пользователя осуществляется системным администратором на основании заявки владельца учетной записи или автоматически через продолжительный промежуток времени.

4. Порядок смены личных паролей

4.1. Смена паролей должна проводиться регулярно, не реже одного раза в квартал, самостоятельно каждым пользователем. В случае если по каким-либо причинам, программное обеспечение не позволяет пользователю осуществить самостоятельную смену пароля, пользователь должен обратиться за помощью к АБИ или системному администратору.

4.2. В случае прекращения полномочий пользователя (увольнение, переход на другую работу и т.п.) должно производиться немедленное удаление его учетной записи сразу после окончания последнего сеанса работы данного пользователя с системой.

4.3. Срочная (внеплановая) полная смена паролей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу и т.п.) ответственного за защиту информации, администратора безопасности информации и других работников, которым по роду работы были предоставлены полномочия по управлению системой парольной защиты.

4.4. Восстановление забытого основного пароля пользователя осуществляется системным администратором путем изменения (сброса) основного пароля пользователя на временный пароль на основании письменной либо электронной заявки пользователя.

4.5. Устная заявка пользователя на изменение пароля не является основанием для проведения таких изменений.

5. Хранение пароля

5.1. Запрещается записывать пароли на бумаге, в файле, электронной записной книжке, мобильном телефоне и любых других предметах и носителях информации.

5.2. Запрещается сообщать свой пароль полностью или частично другим пользователям, запрещается спрашивать или подсматривать пароль других пользователей.

5.3. Запрещается регистрировать других пользователей в ИС со своим личным паролем.

5.4. Запрещается входить в ИС под учетной записью и паролем другого пользователя.

6. Действия в случае утери и компрометации пароля

6.1. В случае утери или компрометации (разглашения, утраты) или подозрения в компрометации пароля пользователю необходимо немедленно

сообщить об этом системному администратору и администратору безопасности информации.

6.2. Системным администратором должна быть немедленно проведена внеплановая процедура смены пароля.

7. Обязанности пользователя

7.1. Помнить свои идентификаторы (логины) и пароли.

7.2. Держать свои пароли в тайне, а именно: не сообщать, не разглашать и любым другим способом не доводить до чьего-либо сведения личные пароли.

7.3. Осуществлять ввод пароля только в условиях, исключающих его просмотр.

7.4. Не хранить записки-памятки с личными идентификаторами и паролями на видном и/или легкодоступном месте: на столе, на мониторе, под клавиатурой и т.п.

7.5. Своевременно сообщать АБИ о факте компрометации пароля.

8. Ответственность

8.1. Каждый пользователь ОИ несет персональную ответственность за соблюдение требований настоящей Инструкции и за все действия, совершенные от имени его учетной записи, если с его стороны не было предпринято необходимых действий для предотвращения компрометации пароля его учетной записи.

8.2. Ответственность за контроль проведения мероприятий по организации парольной защиты в структурных подразделениях Учреждения возлагается на ответственного за защиту информации.

8.3. За разглашение информации ограниченного доступа и нарушение порядка работы со средствами ОИ, обрабатывающими защищаемую информации, работники могут быть привлечены к гражданской, уголовной, административной, дисциплинарной и иной предусмотренной законодательством Российской Федерации ответственности.

Приложение №1
к инструкции по организации парольной защиты

Требования к паролям

Пароли НЕ ДОЛЖНЫ состоять из:

- Вашего имени, отчества или фамилии ни в каком виде (т.е. написаны в строчном, в прописном, в смешанном виде, задом наперед, два раза и т.д.)
- Вашего идентификатора входа (login) ни в каком виде.
- Имен супруга или детей.
- Не используйте какую-либо информацию о себе. Сюда входят: номера телефонов, номера в пропусках и других документах, номер или марка вашего автомобиля, Ваш почтовый адрес и т.д. и т.п.
- Только цифр или одинаковых букв.
- Слов, которые можно найти в словаре (любом, включая иностранные) или в каком-либо списке слов.
- Меньше чем шести символов.

Пароли ДОЛЖНЫ:

- Содержать строчные и прописные буквы.
- Содержать небуквенные символы (т.е. цифры, знаки пунктуации, специальные символы).
- Быть легко запоминаемы, чтобы не было необходимости записывать их.
- Быть составлены так, чтобы Вы могли быстро набрать их на клавиатуре. Это осложнит возможность подглядеть пароль.

Несмотря на такие жесткие требования, есть несколько способов выбора паролей, которые все же соответствуют этим правилам:

- Выберите предложение из песни или стихотворения, и отберите только первые буквы каждого слова (хотя в примере использовано английское предложение, Вы можете воспользоваться и другими языками)

Pretty woman walking down the street становитсяPwwdts.

- Выберите два коротких слова и соедините их с помощью пунктуационных знаков и спецсимволов:

Dog+rain, kid<Goat, TOP^rank

Приложение № 6

к Положению об организации работ по обеспечению безопасности информации в ГБУЗ ТО Областная больница №14 имени В.Н. Шанаурина» (с.Казанское)

Инструкция
по модификации технических и программных средствв
ГБУЗ ТО Областная больница №14 имени В.Н. Шанаурина» (с.Казанское)

1. Общие положения

1.1. Настоящей инструкцией регламентируется взаимодействие подразделений и работников ГБУЗ ТО Областная больница №14 имени В.Н. Шанаурина» (с.Казанское) (далее – Учреждение) при проведении модификаций программного обеспечения (далее – ПО), технического обслуживания и ремонта средств вычислительной техники, а также при возникновении нештатных ситуаций в работе защиты объекта информатизации (далее – ОИ).

1.2. Право внесения изменений в конфигурацию аппаратно-программных средств (автоматизированных рабочих мест (далее – АРМ пользователя) и серверов) и телекоммуникационного оборудования ОИ предоставляется:

- в отношении системных и прикладных программных средств, а также в отношении аппаратных средств – системному администратору ОИ;
- в отношении программно-аппаратных средств защиты информации – администратору безопасности информации (далее – АБИ);
- в отношении программно-аппаратных средств телекоммуникаций – системному администратору и АБИ.

1.3. Изменение конфигурации аппаратно-программных средств рабочих станций и серверов кем-либо, кроме указанных лиц, запрещено.

2. Порядок внесения изменений в программное обеспечение и аппаратные средства

2.1. Основанием для внесения изменений в программное обеспечение и состав технических средств является Заявка (Приложение № 1), направляемая начальником структурного подразделения на имя АБИ.

2.2. В заявке могут быть указаны следующие виды изменений:

- установка в подразделении нового АРМ пользователя;
- замена АРМ пользователя;
- изъятие АРМ пользователя;
- перенос АРМ пользователя в другое помещение;
- добавление устройства в состав конкретного АРМ пользователя;
- замена устройства в составе конкретного АРМ пользователя;

– изъятие устройства из состава конкретного АРМ пользователя;

– установка (развертывание) программных средств, необходимых для решения определенной задачи (добавление возможности, решения новой задачи) на конкретном АРМ пользователя;

– обновление (замена) программных средств на конкретном АРМ пользователя;

– удаление программных средств с конкретного АРМ пользователя.

2.3. В Заявке указываются условные наименования АРМ пользователя в соответствии с Техническим паспортом ОИ.

2.4. При согласовании Заявки учитывается:

– техническая возможность осуществления затребованных изменений;

– возможность совмещения затребованных изменений с требованиями по безопасности.

2.5. После согласования Заявка передаётся системному администратору и/или АБИ для непосредственного исполнения работ по внесению изменений в конфигурацию ОИ.

2.6. Все добавляемые программные и аппаратные компоненты предварительно проверяются на работоспособность и отсутствие опасных функций.

2.7. Установка и обновление подсистем ОИ проводится в строгом соответствии с технологией проведения модификаций программных комплексов данных подсистем.

2.8. Установка, снятие и внесение необходимых изменений в настройки средств защиты информации (далее – СЗИ) и средства контроля целостности файлов на АРМ и серверах осуществляется АБИ.

2.9. Подготовка модификаций, установка, изменение (обновление) и удаление системных и прикладных программных средств на АРМ пользователей и серверах производится системным администратором.

2.10. Модификация ПО на серверах осуществляется системным администратором при участии АБИ.

2.11. Установка и обновление общего ПО (системного, офисного, тестового и т.п.) на рабочие станции и сервера производится с оригинальных лицензионных дистрибутивных носителей (компакт дисков и т.п.), полученных установленным порядком, а прикладного ПО – с эталонных копий программных средств, полученных из сетевого архива эталонных дистрибутивов программ. При необходимости (в случае установки части компонент на дисках сетевых серверов) к работам привлекаются администраторы сети (серверов) и администраторы баз данных.

2.12. После установки (обновления) ПО системный администратор и АБИ производят настройку средств управления доступом к данному программному продукту, проверяют его работоспособность, а также проверяют работоспособность и правильность настройки СЗИ.

2.13. После проведения модификации ПО на АРМ пользователей и серверах АБИ проводит антивирусный контроль.

2.14. После завершения работ по внесению изменений в состав аппаратных средств АРМ пользователей, его системный блок закрывается и опечатывается

(защищается специальной наклейкой) с возможностью постоянного визуального контроля за её целостностью.

2.15. Уполномоченные исполнители работ производят соответствующую запись в Журнале учёта фактов вскрытия и опечатывания АРМ пользователей и серверов (Приложение № 2).

2.16. АБИ проводит периодический контроль за опечатываем АРМ пользователей и серверов.

2.17. При изъятии АРМ пользователя или сервера из состава ОИ ее передача на склад, в ремонт или в другое структурное подразделение для решения иных задач осуществляется только после того, как АБИ снимет с данного технического средства СЗИ и предпримет необходимые меры для затирания защищаемой информации, которая хранилась на дисках компьютера. Факт уничтожения данных, находившихся на диске компьютера, оформляется актом за подписью ответственного за информационную безопасность в подразделении.

2.18. После выполнения всех работ системных администратором и/или АБИ на Заявке делается отметка о даты выполнения работ и подпись исполнителя. Исполненная Заявка передаётся АБИ для хранения.

2.19. Оригиналы документов, на основании которых производились изменения в составе технических или программных средств АРМ и серверов, хранятся у АБИ. Они могут использоваться для:

- отражения АБИ выполненных изменений в Техническом паспорте ОИ;
- восстановления конфигураций АРМ пользователей и серверов после аварий;
- контроля правомерности установки на АРМ пользователя или сервере средств для решения соответствующих задач при разборе конфликтных ситуаций;
- проверки правильности установки и настройки СЗИ АРМ пользователей и серверов.

2.20. Работы по внесению изменений в аппаратные и программные средства ОИ и СЗИ могут проводится системным администратором и АБИ на основании устного распоряжения начальника структурного подразделения Учреждения, ответственного за защиту информации в следующих случаях:

- сбой программных и/или аппаратных средств ОИ и/или средств СЗИ на ОИ, не позволяющий продолжить работу и требующий безотлагательного вмешательства (оперативный ремонт и восстановление работоспособности подсистем ОИ, серверов, АРМ пользователей), а также в других нештатных ситуациях;
- централизованные плановые мероприятия по обновлению системного и прикладного ПО на ОИ.

2.21. Факт модификации ПО и корректировки настроек системы защиты фиксируется в Журнале учета мероприятий по обеспечению информационной безопасности.

2.22. Модификация технических и программных средств, входящих в состав систем, аттестованных по требованиям безопасности информации, производится по согласованию изменений с организацией, проводившей аттестацию, которая

принимает решение о необходимости проведения контроля эффективности аттестованного объекта информатизации.

2.23. Все изменения конфигурации технических и программных средств АРМ пользователей и серверов, входящих в аттестованные по требованиям безопасности информации, отражаются в Техническом паспорте объекта информатизации.

Приложение № 7

к Положению об организации работ по обеспечению безопасности информации в ГБУЗ ТО Областная больница №14 имени В.Н. Шанаурина» (с. Казанское)

Положение о порядке выявления и реагирования на инциденты информационной безопасности в ГБУЗ ТО Областная больница №14 имени В.Н. Шанаурина» (с. Казанское)

1. Общие положения

1.1 Настоящее Положение устанавливает порядок управления инцидентами (одним событием или группой событий), способными привести к сбоям или нарушению функционирования объекта информатизации (далее – ОИ) – ГБУЗ ТО Областная больница №14 имени В.Н. Шанаурина» (с. Казанское) (далее – Учреждение) и (или) возникновению угроз безопасности конфиденциальной информации Учреждения (далее – инциденты ИБ), а также регулирует порядок проведения служебного расследования нарушений режима коммерческой тайны (далее – служебное расследование) в Учреждения.

1.2 Процесс управления инцидентами ИБ включает:

- учет и регистрацию инцидентов ИБ;
- оповещение ответственного лица о возникновении инцидентов ИБ;
- расследование обнаруженных инцидентов ИБ;
- устранение причин и последствий инцидентов ИБ;
- определение плана корректирующих и превентивных мероприятий.

1.3 Требования настоящего Положения являются обязательными для выполнения всеми работниками Учреждения.

2. Учет и регистрация инцидентов информационной безопасности

2.1 Для выявления инцидентов ИБ должны использоваться встроенные механизмы регистрации и учета событий безопасности операционных систем, систем управления базами данных, прикладного программного обеспечения и средств защиты информации, а также специализированные средства анализа защищенности информационных систем Учреждения.

2.2 В обязательном порядке должны регистрироваться следующие события безопасности:

- попытки входа (выхода) пользователей в операционную систему (из операционной системы);
- загрузка и инициализация операционной системы и ее программного останова для рабочих станций и серверов;

- попытка доступа к средствам виртуализации;
- факт изменения конфигурации средств виртуализации;
- запуск и остановка служб (системных сервисов) средств виртуализации;
- попытки подключения к рабочим станциям и серверам мобильных устройств и внешних носителей информации.

2.3 В параметрах регистрации событий безопасности в обязательном порядке должны указываться следующие параметры:

- тип события;
- дата и время события;
- результат события;
- источник события;
- идентификатор пользователя информационной системы, предъявленный при попытке доступа.

2.4 Хранение информации об инцидентах ИБ должно осуществляться в течение срока, достаточного для проведения служебного расследования.

2.5 Учет инцидентов ИБ осуществляется администратором безопасности информации (далее – АБИ), назначенным приказом *главного врача* Учреждения. Допускается ведение учета инцидентов ИБ в электронном виде.

2.6 При обнаружении инцидента ИБ АБИ проводит его классификацию в соответствии с Приложением № 1 к настоящему Положению. Инциденты ИБ и их последствия классифицируются по значимости на текущие, значимые и имеющие признаки преступления.

3. Порядок оповещения ответственного лица о возникновении инцидентов информационной безопасности

3.1 Применяемые методы и способы регистрации событий безопасности на ОИ должны обеспечивать возможность информирования АБИ о критических событиях безопасности на ОИ в масштабе времени, близком к реальному.

3.2 Если зафиксированный инцидент ИБ классифицируется как «текущее нарушение», АБИ самостоятельно проводит анализ, выяснение и устранение причин, приведших к возникновению инцидента ИБ.

3.3 В случае, если зафиксированный инцидент ИБ был классифицирован как «значимый» или «имеющий признаки компьютерного преступления», АБИ обязан незамедлительно сообщить о выявленном инциденте ИБ ответственному за защиту информации по электронной почте или иному средству связи.

3.4 Ответственный за защиту информации должен провести внеплановый анализ выявленного инцидента ИБ и, в случае необходимости, инициировать процедуру служебного расследования в соответствии с порядком, установленным данным Положением.

4. Порядок расследования обнаруженных инцидентов информационной безопасности

4.1 Проведение служебного расследования инициируется приказом Учреждения на основании распоряжения лица, ответственного за защиту информации. В этом же приказе устанавливается состав Комиссии для проведения служебного расследования (далее – Комиссия).

4.2 Служебное расследование может быть возбуждено:

– по решению лица, ответственного за защиту информации в Учреждении;

– по инициативе любого работника Учреждения на основании служебной записки в произвольной форме на ответственного за защиту информации в Учреждении;

– по устному докладу администратора безопасности информации лицу, ответственному за защиту информации в Учреждении.

4.3 В состав Комиссии входят следующие работника Учреждения:

4.3.1 В обязательном порядке:

– Председатель Комиссии – ответственный за защиту информации;

– АБИ.

4.3.2 В случае необходимости Комиссия вправе привлекать к расследованию:

– системного (прикладного) администратора;

– администратора информационной системы Учреждении;

– руководителя структурного подразделения, в котором произошел инцидент ИБ;

– непосредственного руководителя работника, в отношении которого проводится служебное расследование;

– экспертов из других структурных подразделений и, при необходимости, представителей сторонних организаций.

4.4 Комиссия для проведения служебного расследования в рабочем порядке в максимально короткие сроки, привлекая все необходимые ресурсы, проводит служебное расследование.

4.5 Результаты работы Комиссии оформляются в виде аналитического экспертного заключения на имя главного врача Учреждения, с предложениями:

– по внесению изменений в организационные и (или) технические меры по защите информации;

– по внесению изменений и улучшений в комплект организационно-распорядительной документации Учреждения;

– по расширению или дополнению списка инцидентов ИБ, установленного данным Положением, если это необходимо.

4.6 В аналитическом экспертном заключении должен быть приведен перечень ответственных за выполнение запланированных работ и сроки выполнения запланированных работ.

4.7 Материалы служебного расследования, его выводы и заключения могут быть использованы как основание для реализации уголовной, гражданской,

административной или дисциплинарной ответственности, в порядке, определяемом действующим законодательством и локальными правовыми актами Учреждения.

5. Устранение причин и последствий инцидентов информационной безопасности

5.1 Для инициирования работ по устранению причин и последствий инцидента ИБ, лицо, ответственное за руководство работами по защите информации в Учреждении, даёт распоряжение ответственным лицам на выполнение запланированных работ в соответствии со сроками, указанными в аналитическом экспертном заключении.

5.2 После реализации запланированных работ ответственное лицо должно направить по электронной почте ответственному за защиту информации подтверждение выполнения работ, не позднее срока реализации, установленного в экспертном заключении.

5.3 Оценку результативности предпринятых мер осуществляет ответственный за защиту информации ежемесячно на основании анализа информации, предоставляемой АБИ.

5.4 О результативности предпринятых корректирующих и превентивных мер свидетельствует отсутствие повторных инцидентов ИБ.

6. Определение плана корректирующих и превентивных мероприятий

6.1 Ежемесячно администратор безопасности информации готовит сводный отчет по инцидентам ИБ, предоставляемый ответственному за защиту информации Учреждения.

6.2 В сводном отчете АБИ должен провести анализ выявленных инцидентов ИБ, в качестве приложения к отчету должен быть предложен перечень корректирующих и превентивных мероприятий, направленных на устранение причин и последствий инцидентов ИБ и на предотвращение подобных нарушений в будущем. Данный перечень должен устанавливать сроки реализации и ответственных за проведение указанных мероприятий.

6.3 После согласования указанного перечня с ответственным за защиту информации, данная информация доводится администратором ИБ до всех работников, назначенных ответственными за проведение корректирующих и превентивных мероприятий.

6.4 Контроль за своевременным и качественным выполнением работ по проведению корректирующих и превентивных мероприятий осуществляет ответственный за защиту информации.

7. Ответственность

7.1 Ответственность за проведение служебного расследования и за контроль своевременного и качественного выполнения работ по проведению корректирующих и превентивных мероприятий несет ответственный за защиту информации.

7.2 Ответственность за обеспечение своевременной регистрации инцидентов ИБ несет администратор безопасности информации.

7.3 Ответственность за выделение требуемых ресурсов (в том числе финансовых и трудовых) для реализации положений настоящего документа несет ответственный за защиту информации.

Приложение №1
к Положению о порядке выявления и реагирования
на инциденты информационной безопасности

ПЕРЕЧЕНЬ
инцидентов информационной безопасности

№ п/п	Описание инцидента информационной безопасности
1	2
1.Текущие нарушения	
1.1.	Ошибка при регистрации в информационной системе: ввод неправильных персональных регистрационных данных (пароля, имени пользователя и т.п.) более трех раз подряд (однократная)
1.2.	Периодические попытки неудачного доступа к объектам: компьютерам, принтерам, файлам, документам
1.3.	Несанкционированный перевод времени на рабочей станции либо на других элементах информационной инфраструктуры Учреждения
1.4.	Выполнение производственных обязанностей с использованием компьютерного оборудования в нерабочее время
1.5.	Оставление работающего (включенного) компьютерного оборудования без запущенного хранителя экрана в нерабочее время
1.6.	Перезагрузка рабочей станции при сбоях в работе (однократная), в том числе аварийная перезагрузка путем нажатия кнопки горячей перезагрузки или полного отключения питания
1.7.	Нецелевое использование элементов информационной инфраструктуры Учреждения (печать, сервисы сети Интернет, электронная почта, и т.п.)
2.Значимые нарушения	
2.1.	Ошибка при регистрации в информационной системе: ввод неправильных персональных регистрационных данных (пароля, имени пользователя и т.п.) более трех раз подряд (многократная)
2.2.	Неоднократное оставление работающего (включенного) компьютерного оборудования без запущенного хранителя экрана в нерабочее время
2.3.	Утрата учтенного магнитного, оптического или иного носителя конфиденциальной информации
2.4.	Утрата носителя информации с резервной копией

1	2
2.5.	Неудачная попытка регистрации в информационной системе под чужими регистрационными данными (именем пользователя, паролем и т.п.) (многократная)
2.6.	Удачная попытка регистрации в информационной системе под чужими регистрационными данными (именем пользователя, паролем и т.п.)
2.7.	Нерегламентированная очистка журналов событий безопасности информационных систем Учреждения
2.8.	Нерегламентированное подключение неучтенных внутренних и (или) периферийных устройств и носителей информации
2.9.	Нерегламентированное изменение аппаратной конфигурации компьютерного оборудования
2.10.	Нерегламентированное копирование информации (файлов) на флеш-накопители или иные внешние носители информации, а также нерегламентированная передача подобной информации с использованием сервисов электронной почты, мгновенных сообщений (ICQ и т.п.) и других сервисов сети Интернет
2.11.	Нерегламентированная установка (удаление) прикладного программного обеспечения, не разрешенного к использованию на рабочих станциях и серверах Учреждения
2.12.	Попытка получения привилегированного доступа к рабочей станции или к другим ресурсам информационных систем Учреждения (повышение уровня прав доступа, получение прав на отладку программ и т.п.)
2.13.	Заражение программного обеспечения рабочих станций и серверов вредоносным кодом (непреднамеренное)
2.14.	Нерегламентированное использование сканирующего (на различные уязвимости) программного обеспечения
2.15.	Нерегламентированное использование анализаторов протоколов (снифферов)
2.16.	Нерегламентированный просмотр, вывод на печать, передача третьим лицам сведений, содержащих конфиденциальные данные (информацию, подлежащую защите)
2.17.	Несанкционированное проведение обновления версий системного и прикладного программного обеспечения
3.Нарушения, имеющие признаки преступления	
3.1.	Несанкционированное получение привилегированного доступа к любым элементам информационной инфраструктуры Учреждения
3.2.	Несанкционированное изменение конфигурации элементов информационной инфраструктуры Учреждения

1	2
3.3.	Утрата резервных копий
3.4.	Утечка конфиденциальной информации (баз данных информационных систем и др.)
3.5.	Подозрение в умышленном нарушении работоспособности информационной сети Учреждения, элементов информационной инфраструктуры Учреждения, системного и прикладного программного обеспечения
3.6.	Юридически необоснованная передача (распространение) конфиденциальной информации
3.7.	Несанкционированное внесение изменений в базы данных информационных систем Учреждения
3.8.	Несанкционированное уничтожение конфиденциальной информации
3.9.	Проведение обновления версии информационных систем Учреждения (равно как и другого программного обеспечения), повлекшее за собой потерю конфиденциальной информации
3.10.	Намеренное заражение информационных систем Учреждения вредоносным кодом

Приложение № 8

к Положению об организации
работ по обеспечению
безопасности информации в ГБУЗ
ТО Областная больница №14
имени В.Н. Шанаурина»
(с.Казанское)

Инструкция по организации антивирусной защиты в ГБУЗ ТО Областная больница №14 имени В.Н. Шанаурина» (с. Казанское)

2. Общие положения

2.1. Настоящая Инструкция определяет требования к организации антивирусной защиты на объекте информатизации (далее – ОИ) – Наименование организацииГБУЗ ТО Областная больница №14 имени В.Н. Шанаурина» (с. Казанское) (далее – Учреждения).

2.2. Настоящая Инструкция предназначена для работников, выполняющих функции администратора безопасности информации (далее – АБИ), системного администратора и пользователей, осуществляющих обработку информации на автоматизированных рабочих местах (далее – АРМ пользователей).

2.3. Действие настоящей Инструкции распространяется на все структурные подразделения Учреждения.

2.4. В целях обеспечения защиты от деструктивных воздействий компьютерных вредоносных программ производится антивирусный контроль. Обязательному антивирусному контролю подлежит любая информация, поступающая на средства вычислительной техники (далее – СВТ), в т.ч. получаемая на внешних носителях из сторонних организаций.

2.5. Объектами защиты от воздействия вредоносных программ являются информационные массивы, содержащиеся в информационных подсистемах (информационные ресурсы), технические средства (в т.ч. СВТ, машинные носители информации, средства и системы связи передачи данных, технические средства обработки буквенно-цифровой, графической, видео- и речевой информации), общесистемное, прикладное, специальное программное обеспечение (далее – ПО), информационные технологии, а также средства защиты информации (далее – СЗИ).

2.6. Вредоносная программ – программа, предназначенная для осуществления несанкционированного доступа и/или воздействия на ресурсы ОИ.

Вредоносная программа способна выполнять ряд функций, в т.ч.:

– скрывать признаки своего присутствия в программной среде СВТ;

– обладать способностью к самодублированию, ассоциированию себя с другими программами и/или переносу своих фрагментов в иные области оперативной или внешней памяти;

– разрушать (искажать произвольным образом) код программ в оперативной памяти;

– сохранять фрагменты информации из оперативной памяти в некоторых областях внешней памяти прямого доступа (локальных или удаленных);

– искажать произвольным образом, блокировать и/или подменять выводимый во внешнюю память или в канал связи массив информации, образовавшийся в результате работы прикладных программ, или уже находящиеся во внешней памяти массивы данных.

2.7. Основными задачами системы обеспечения антивирусной защиты являются:

– исключение или существенное затруднение противоправных действий в отношении ОИ;

– обеспечение условий для устойчивой бесперебойной работы информационных объектов и сетей передачи данных.

2.8. Обеспечение антивирусной защиты включает:

– регулярные профилактические работы;

– анализ ситуации проявления вредоносных программ и причины их появления;

– уничтожение вредоносных программ на СВТ;

– принятие мер по предотвращению причин появления вредоносных программ.

2.9. Для выполнения требований по антивирусной защите объектов защиты используется специализированное ПО – средство антивирусной защиты (далее – САВЗ), обеспечивающее надёжную ежедневную автоматическую антивирусную защиту и контроль чистоты информационных массивов данных от вредоносных программ.

2.10. Все процессы производятся в автоматическом режиме без участия пользователей и без помех для работы основного и специального ПО. Процесс плановой полной проверки файловой системы рабочих станций пользователей и серверов ОИ проводится во время наименьшей нагрузки оборудования пользовательскими задачами.

2.11. Организация работ по антивирусной защите и ответственность за сопровождение системы антивирусной защиты возлагается на ответственного за защиту информации.

2.12. Периодический контроль и ответственность за состояние защиты ОИ возлагается на работников, выполняющих функции АБИ и системного администратора.

2.13. АБИ и системный администратор имеют полноправный доступ ко всем АРМ, серверам и другому оборудованию ОИ.

2.14. АБИ и системный администратор обладают необходимыми практическими навыками и теоретическими знаниями в области

информационной безопасности. В их основные обязанности по антивирусной защите входит:

- проведение периодического анализа и оценки ситуации по обеспечению антивирусной безопасности для контроля степени защищенности ОИ и выработка предложений по изменению и улучшению состояния дел;
- проверка соблюдения порядка обновления средств и баз данных САВЗ;
- осуществление контроля за состоянием САВЗ на СВТ;
- осуществление контроля за соблюдением работниками требований по обеспечению антивирусной защиты;
- обеспечение контроля за соблюдением требований при работе с сетью Интернет, а также за характером и объёмом трафика, получаемого из сети Интернет, и его соответствия служебной необходимости;
- проведение служебных расследований по фактам обнаружения вредоносных программ, повлекших неустойчивую работу и/или полную остановку функционирования ОИ;
- организацию мероприятий по улучшению антивирусной защиты ОИ.

2.15. Устанавливаемое (изменяемое) ПО на ОИ предварительно проверяется на отсутствие вредоносных программ. Непосредственно после установки (изменения) ПО АБИ или системный администратор выполняет антивирусную проверку на СВТ.

2.16. При возникновении подозрения на наличие вредоносных программ (частые ошибки в работе программ, нетипичная работа программ, появление посторонних графических и звуковых эффектов, искажения данных, неконтролируемое пропадание файлов, появление сообщений о системных ошибках, замедление работы компьютера и т.п.) совместно с АБИ или системных администратором проводит внеочередной антивирусный контроль своего АРМ.

2.17. Для пользователей АРМ запрещена возможность изменения настроек и параметров САВЗ на своём АРМ. Эти действия производит АБИ или системный администратор с помощью средств централизованного управления или вручную.

2.18. По факту появления и проникновения вредоносных программ, повлекших неустойчивую работу и/или полную остановку функционирования ОИ проводится служебное расследование.

2.19. Результаты расследования причин появления и последствий воздействия вредоносных программ на ОИ докладываются лицу, ответственному за защиту информации с предложениями по принятию мер, предотвращающих в будущем повторения подобных фактов.

3. Применение средств антивирусного контроля

Используемое на ОИ лицензионное САВЗ должно:

3.1. Иметь сертификат на соответствие требованиям безопасности информации ФСТЭК России.

3.2. Обеспечивать возможность обнаружения как можно большего числа известных вредоносных программ, в т.ч. вирусов, деструктивного кода (макро-вирусы, объектов ActiveX, апплетов языка Java и т.п.), а также быть максимально подготовлено для быстрого реагирования на появление новых видов вирусных угроз.

3.3. Поддерживать исчерпывающий список защищаемых точек (почтовые серверы, файловые серверы, АРМ и т.д.) возможного проникновения вредоносных программ.

3.4. Обеспечивать возможность получения обновлений, консультаций и других форм сопровождения поставщиком антивирусного ПО.

3.5. Обеспечивать автоматическое распространение обновлений антивирусных баз на каждое СВТ.

3.6. Соответствовать платформам, характеристикам и комплектации СВТ.

3.7. Обеспечивать надёжность и работоспособность САВЗ в любом из предусмотренных режимов работы.

3.8. Иметь эксплуатационную документацию, необходимую для практического применения и освоения САВЗ.

4. Мероприятия по штатному управлению средствами антивирусного контроля

4.1. В штатном режиме работы системы антивирусной защиты АБИ и системный администратор выполняют:

- установку САВЗ на все объекты антивирусной защиты в порядке, описанном в эксплуатационной документации;
- контроль наличия связи между серверов администрирования и защищаемыми объектами;
- необходимые обновления версий САВЗ на объектах антивирусной защиты;
- контроль над выполнением задач постоянно защиты;
- настройку автоматических проверок объектов антивирусной защиты не реже одного раза в неделю с целью профилактики;
- контроль актуальных версий антивирусных баз и модулей сканирования ПО сервера администрирования;
- непрерывный мониторинг информационного обмена в СЗИ с целью выявления проявлений программно-математических воздействий;
- обработку сведений, поступающих от САВЗ;
- анализ сводных отчётов о работе САВЗ и инцидентах.

4.2. Процесс управления системой антивирусной защиты включает в себя следующие действия АБИ и системного администратора:

- внесение изменений в политику антивирусной защиты;
- управление САВЗ защиты, входящих в состав системы антивирусной защиты;
- мониторинг событий, информация о которых поступает от САВЗ с объектов защиты;

– анализ результатов работы САВЗ.

5. Мероприятия по нештатному управлению средствами антивирусного контроля

5.1. В случае заражения СВТ вредоносными программами АБИ совместно с системным администратором выполняет следующие действия:

– централизованно обновляет антивирусные базы сервера администрирования и всех объектов антивирусной защиты;

– проверяет состояние всех объектов антивирусной защиты, наличие заражённые АРМ пользователей в случае обнаружения заражённых узлов;

– оперативно принимает меры по предотвращению распространения заражения вредоносными программами и при необходимости отключает от сети заражённое СВТ;

– проводит действия, направленные на устранения вредоносной программы на всех заражённых узлах ОИ;

– по завершении мероприятий по устранению последствий заражения работоспособность АРМ пользователя и передаёт его ответственному пользователю.

6. Уничтожение вредоносных программ

6.1. Уничтожение вредоносных программ выполняется АБИ и/или системным администратором.

6.2. Если вредоносная программа поразила какие-либо программы, то уничтожение вредоносной программы выполняется путём уничтожения программы на жёстком диске либо на ином носителе. После уничтожения заражённой программы восстанавливают программу, используя её резервную копию.

6.3. Если вредоносная программа поразила файлы, то вредоносная программа уничтожается либо путём стирания этих файлов, либо путём использования специального «лечащего» режима САВЗ. Использование «лечащего» режима не даёт полной гарантии восстановления файла, поэтому после «лечения» необходима проверка восстановления данного файла. «Лечащие» программы используются лишь в тех случаях, когда отсутствует резервная копия заражённой программы или файла с данными, либо восстановление уничтоженного файла с помощью резервной копии очень трудоёмко.

6.4. После уничтожения вредоносных программ и восстановления заражённых программ и файлов с данными ещё раз выполняется проверка наличия вредоносных программ, используя САВЗ с установленными последними обновлениями. Перед повторной проверкой производится перезагрузка СВТ через выключение и последующее включение.

7. Ответственность

7.1. Организация мероприятий по централизованной антивирусной защите ОИ возлагается на АБИ и системного администратора.

7.2. АБИ и системный администратор несут ответственность за формирование политики антивирусной защиты, организацию своевременной инсталляции САВЗ и централизованное обновление баз данных вирусных описаний на комплексе программно-технических средств ОИ.

7.3. Выполнение технических мероприятий по централизованной антивирусной защите на ОИ производится непосредственно АБИ и/или системным администратором.

7.4. Непосредственную ответственность за соблюдение в повседневной деятельности установленных норм обеспечения антивирусной защиты информации и требований настоящей Инструкции несут пользователи, за которыми закреплены соответствующие АРМ.

Приложение № 9

к Положению об организации работ по обеспечению безопасности информации в ГБУЗ ТО Областная больница №14 имени В.Н. Шанаурина» (с. Казанское)

Положение по организации контроля эффективности защиты информации в ГБУЗ ТО Областная больница №14 имени В.Н. Шанаурина» (с. Казанское)

1. Общие положения

1.1. Настоящее Положение разработано в целях контроля реализации принятых мер по обеспечению безопасности информации на объекте информатизации (далее – ОИ) ГБУЗ ТО Областная больница №14 имени В.Н. Шанаурина» (с. Казанское)(далее – Учреждения).

2. Общий порядок организации контроля эффективности мер защиты информации

2.1. Ответственным за контроль эффективности защиты информации является ответственный за защиту информации.

2.2. Администратор безопасности информации Учреждения (далее – АБИ) осуществляет постоянный контроль выполнения требований по обеспечению безопасности информации в рамках выполнения своих обязанностей.

2.3. Мероприятия по контролю эффективности принятых мер по обеспечению безопасности информации при ее обработке в информационной системе Учреждения должны включать:

- создание комиссии по контролю исполнения мероприятий по защите информации;
- установление порядка проведения внутренних проверок состояния защиты информации;
- контроль (анализ) защищённости информации.

2.4.Состав комиссии по контролю состояния защиты информации утверждается ответственным за защиту информации.

3. Порядок проведения внутренних плановых проверок состояния защиты информации

3.1.Внутренние проверки состояния защиты информации при ее обработке на ОИ проводятся в соответствии с Планом внутренних проверок состояния защиты информации (Приложение № 1).

3.2.План внутренних проверок состояния защиты информации составляется на год ответственным за защиту информации и утверждается *главным врачом* Учреждения.

3.3.Руководители подразделений, работники которых осуществляют обработку информации ограниченного доступа, должны обеспечивать возможность проведения внутренних проверок состояния защиты информации.

3.4.При проведении внутренних проверок состояния защиты информации должен присутствовать представитель проверяемого подразделения.

3.5.Необходимыми видами внутренних проверок состояния защиты информации являются проверки выполнения требований к организации:

- системы допуска и учета лиц, допущенных к работе с информацией ограниченного доступа;
- системы защиты межсетевого взаимодействия;
- режима безопасности помещений, в которых осуществляется обработка информации ограниченного доступа;
- безопасного хранения и уничтожения материальных носителей информации;
- защиты от вредоносного кода;
- парольной защиты;
- управления инцидентами информационной безопасности и реагирование на них;
- управления конфигурацией ОИ и системы защиты информации;
- системы криптографической защиты информации;
- системы резервного копирования и восстановления;
- системы обучения по вопросам обеспечения безопасности информации.

3.6.По результатам проведения проверки каждого подразделения комиссией по контролю состояния защиты информации составляется Отчет по результатам проведения проверки (Приложение № 2). Отчет по результатам проведения проверки согласуется с руководителем проверяемого структурного подразделения Учреждения и предоставляется на утверждение *главному врачу*Учреждения ответственным за защиту информации.

3.7.Обо всех существенных нарушениях, выявленных в ходе проведения внутренних проверок состояния защиты информации, незамедлительно сообщается *главному врачу* Учреждения.

3.8.По фактам выявленных нарушений проводятся служебные расследования в соответствии с порядком, определенном в Положении о выявлении и реагировании на инциденты информационно безопасности.

3.9.Обязанности по проведению разбирательств по выявленным фактам несоблюдения требований по информационной безопасности, которые могут привести к снижению уровня защищенности информации, возложены на АБИ.

3.10. Проведенные внутренние проверки должны учитываться в Журнале учета проводимых внутренних проверок ответственным за защиту информации (Приложение № 3).

4. Требования к мерам по анализу защищённости ОИ

4.1.Меры по контролю (анализу) защищённости информации должны обеспечивать контроль уровня защищённости информации, содержащейся на ОИ, путём проведения мероприятий по анализу защищённости ОИ и тестирования его системы защиты информации (далее – СЗИ).

4.2.Меры по контролю (анализу) защищённости информации включают:

- выявление, анализ уязвимостей ОИ и оперативное устранение вновь выявленных уязвимостей;
- контроль установки обновлений программного обеспечения (далее – ПО), включая обновление ПО СЗИ;
- контроль работоспособности, параметров настройки и правильности функционирования ПО и СЗИ;
- контроль состава технических средств (далее – ТС), ПО и СЗИ;
- контроль правил генерации и семы паролей пользователей, заведения и удаления учётных записей пользователей, реализация правил разграничения доступа, полномочий пользователей на ОИ.

4.3.При выявлении (поиске), анализе и устранения уязвимостей на ОИ должны проводиться:

- выявление (поиск) уязвимостей, связанных с ошибками кода в программном (микропрограммном) обеспечении (общесистемном, прикладном, специальном), а также ПО СЗИ, правильностью установки и настройки СЗИ, ТС и ПО, а также корректностью работы СЗИ при их взаимодействии с ТС и ПО;
- разработка по результатам выявления (поиска) уязвимостей отчётов с описанием выявленных уязвимостей и планом мероприятий по их устранению;
- анализ отчётов с результатами поиска уязвимостей и оценки достаточности реализованных мер защиты информации;
- устранение выявленных уязвимостей, в т.ч. путём установки обновлений ПО СЗИ, общесистемного ПО, прикладного ПО или микропрограммного обеспечения ТС;
- информирование заинтересованных лиц Учреждения (пользователей, администраторов и т.д.) о результатах поиска уязвимостей и оценки достаточности реализованных мер защиты информации.

4.4.В качестве источников информации об уязвимостях используются опубликованные данные разработчиков СЗИ, общесистемного, прикладного и специального ПО, ТС, а также другие базы данных уязвимостей.

4.5.В случае невозможности устранения выявленных уязвимостей путём установки обновлений ПО СЗИ, общесистемного ПО, прикладного ПО или микропрограммного обеспечения ТС, АБИ и/или системный администратор должны предпринять действия (изменение настроек СЗИ, изменение режима и порядка работы на ОИ и/или его подсистемах и т.п.), направленные на устранение возможности использования выявленных уязвимостей.

5. Требования к средствам анализа защищённости

5.1.Для поиска уязвимостей в сервисах, предлагаемых операционными системами, межсетевыми экранами, маршрутизаторами и другими сетевыми компонентами могут использоваться как стандартные средства тестирования и

сбора информации и конфигурации и функционирования сети, так и специализированные средства.

5.2.Используемые специализированные средства анализа защищённости должны быть сертифицированы ФСТЭК России.

6. Ответственность

6.1.Работы по контролю над установленным уровнем защищённости ОИ, анализ и устранение уязвимостей ОИ проводятся АБИ и системным администратором Учреждения.

6.2.Работы по анализу защищённости и обнаружению уязвимостей на ОИ с использованием специализированных средств (сканеров безопасности и т.п.), а также их периодичность и порядок проведения определяются ответственным за обеспечения информационной безопасности Учреждения.

Приложение №1
к Положению об организации
контроля эффективности

ФОРМА

Плана внутренних проверок состояния защиты конфиденциальной информации
на 20__ г.

№ п/п	Структурное подразделение	Период проведения внутренних проверок
1.		
2.		
3.		
	….	

Главный врач Д.М. Суворов

(м.п.)

«___» _____20_ г.

Приложение №2
к Положению об организации контроля эффективности

ФОРМА

Отчета о проведении проверки контроля эффективности защиты информации

Для оценки выполнения требований по защите конфиденциальной информации в период _____
была проведена проверка отдела _____.

Результаты внутренней проверки состояния защиты конфиденциальной информации приведены в таблице:

№ п/п	Вид внутренней проверки	Выявленные нарушения	Корректирующие меры
1	Организация системы допуска и учета лиц, допущенных к конфиденциальной информации		
2	Организация системы защиты межсетевого взаимодействия		
3	Организация режима безопасности помещений информационных систем		
4	Организация безопасного хранения и уничтожения материальных носителей информации		
5	Организация защиты от вредоносного кода		
6	Организация парольной защиты		
7	Организация управления инцидентами информационной безопасности и реагирование на них		
8	Организация управления конфигурацией информационных систем Учреждения и системы защиты конфиденциальной информации		

№ п/п	Вид внутренней проверки	Выявленные нарушения	Корректирующие меры
9	Организация системы криптографической защиты информации		
10	Организация системы резервного копирования и восстановления		
11	Организация централизованного управления системой защиты информации		
12	Организация системы обучения по вопросам обеспечения безопасности информации		

Руководителю отдела _____
в срок до _____ устранить выявленные в ходе проверки недочеты и составить отчет по итогам работы на имя главного врача .

Ответственный за обеспечение безопасности
конфиденциальной информации _____/_____/
«____» _____ 20___г.

ОЗНАКОМЛЕН
Руководитель проверяемого отдела_____/_____/
«____» _____ 20___г.

Приложение №3
к Положению об организации
контроля эффективности

ЖУРНАЛ УЧЕТА ПРОВОДИМЫХ ВНУТРЕННИХ ПРОВЕРОК

Начат «___»_____20__ г.

Окончен «___»_____20__ г.

На _____листах

_____ _____ _____
(должность руководителя) (подпись) (Фамилия И.О.)
М.П.

№ п/п	Наименование внутренней проверки	Краткое описание	Дата проведения проверки	Подпись ответственного за контроль эффективности мер по защите информации	Примечание
1	2	3	4	5	6

Приложение № 10

к Положению об организации работ по обеспечению безопасности информации в ГБУЗ ТО Областная больница №14 имени В.Н. Шанаурина» (с. Казанское)

Порядок резервирования и восстановления работоспособности технических средств, программного обеспечения, баз данных и средств защиты информации в ГБУЗ ТО Областная больница №14 имени В.Н. Шанаурина» (с. Казанское)

1. Общие положения

1. Настоящий Порядок определяет меры и средства поддержания непрерывной работы и восстановления работоспособности объекта информатизации (далее – ОИ) – ИТ-инфраструктуры ГБУЗ ТО Областная больница №14 имени В.Н. Шанаурина» (с. Казанское) (далее – Учреждение).
2. Порядок определяет:
   - меры защиты от потери информации;
   - мероприятия и порядок действий в случае потери информации.
3. Действие настоящего документа распространяется на всех работников Учреждения, имеющих доступ к информационным ресурсам, техническим средствам (далее – ТС) и основным систем обеспечения непрерывности работы и восстановления ресурсов при возникновении аварийных ситуаций.
4. Ответственными работниками за реагирования на инциденты безопасности, приводящие к потере защищаемой информации, являются администратор безопасности информации (далее – АБИ) и системный администратор.
5. Ответственным работником за контроль обеспечения мероприятий по предотвращению инцидентов безопасности, приводящих к потере защищаемой информации, является ответственный за защиту информации в Учреждения.

2. Меры обеспечения непрерывности работы и восстановления ресурсов при возникновении инцидентов

1. В настоящем документе под инцидентом понимается некоторое происшествие, связанное со сбоев в функционировании элементов ОИ, предоставляемых пользователям ОИ, а также потерей защищаемой информации.
2. Происшествие, вызывающее инцидент, может произойти:
   - в результате непреднамеренных действий пользователей;

- в результате преднамеренных действий пользователей;
- в результате нарушения правил эксплуатации технических средств ОИ;
- в результате возникновения внештатных ситуаций и обстоятельств непреодолимой силы.

1. В кратчайшие сроки, ответственные за реагирование работники Учреждения (АБИ, системный администратор) предпринимают меры по восстановлению работоспособности, согласованные с руководством Учреждения.
2. К техническим мерам обеспечения непрерывной работы и восстановления относятся программные, аппаратные и технические средства и системы, используемые для предотвращения возникновения инцидентов, такие как:
   - системы обеспечения отказоустойчивости;
   - системы резервного копирования и хранения данных.
5. Все критические помещения Учреждения (помещения, в которых размещаются элементы ОИ и средства защиты) должны быть оборудованы средства пожарной сигнализации и пожаротушения.
6. Для выполнения требований по эксплуатации (температура, относительная влажность воздуха) программно-аппаратных средств ОИ в помещениях, где они установлены, должны применяться системы вентиляции и кондиционирования воздуха.
7. Для предотвращения потерь информации при кратковременном отключении электроэнергии все ключевые элементы ОИ, сетевое и коммуникационное оборудование, а также наиболее критичные автоматизированные рабочие места должны подключаться к сети электропитания через источники бесперебойного питания.
8. Для обеспечений отказоустойчивости критичных компонентов ОИ при сбое в работе оборудования и их автоматической замены без простоев могут быть использованы методы кластеризации.
9. Для защиты от отказов отдельных дисков серверов, осуществляющих обработку и хранение защищаемой информации, должны использоваться технологии RAID, которые применяют дублирование данных, хранимых на дисках. Система резервного копирования и хранения данных должна обеспечивать сохранение защищаемой информации на твёрдый носитель.

3. Порядок резервного копирования

1. Состав и объем копируемых данных, периодичность проведения резервного копирования определяется Перечнем резервируемых данных (Приложение № 1). Максимальный срок хранения резервных копий 3 (три) месяца.
2. Система резервного копирования должна обеспечивать производительность, достаточную для сохранения информации, указанной в Перечне, в установленные сроки и с заданной периодичностью.
3. О выявленных попытках несанкционированного доступа к резервируемой информации, а также иных нарушениях информационной безопасности, произошедших в процессе резервного копирования, должно быть

немедленно сообщено АБИ, либо ответственному за защиту информации Учреждения.

4. Методика резервного копирования

1. Для организации системы резервного копирования используются стандартные средства операционной системы и специализированное ПО.
2. Резервное копирование и хранение данных осуществляется на периодической основе:
   - для обрабатываемых данных – не реже раза в неделю;
   - для технологической информации – не реже раза в месяц;
   - эталонные копии ПО (операционные системы, штатное и специальное ПО, программные СЗИ), с которых осуществляется установка на элементы ОИ – не реже раза в месяц, и каждый раз при внесении изменений в эталонные копии (выход новых версий).
3. Для резервирования информации, хранимой в базах данных ОИ, в качестве промежуточного звена автоматизации используются средства конфигурирования информационной системы и архиваторы. В результате работы промежуточного звена автоматизации формируется каталог с резервной копией данных информационной системы.
4. Носители, на которые произведено резервное копирование, должны быть учтены с проставлением даты проведения резервного копирования.
5. Носители должны храниться в несгораемом шкафу или помещении, оборудованном системой пожаротушения.

5. Контроль результатов резервного копирования

1. Контроль результатов всех процедур резервного копирования осуществляется АБИ.
2. На протяжении периода времени, когда система резервного копирования находится в аварийном состоянии, должно осуществляться ежедневное копирование информации, подлежащей резервированию, с использованием средств файловых систем серверов, располагающих необходимыми объемами дискового пространства для ее хранения.

6. Ротация носителей резервной копии

1. Система резервного копирования должна обеспечивать возможность периодической замены (выгрузки) резервных носителей без потерь информации на них, а также обеспечивать восстановление текущей информации информационной системы в случае отказа любого из устройств резервного копирования. Все процедуры по загрузке, выгрузке носителей из системы резервного копирования, а также их перемещение, осуществляются АБИ. В качестве новых носителей допускается повторно использовать те, у которых срок хранения содержащейся информации истек.
2. Носители, которые перестали использоваться в системе резервного копирования, должны стираться (форматироваться) с использованием

специального программного обеспечения.

3. Носители, используемые в системе резервного копирования, должны быть учтены в Журнале учета отчуждаемых носителей информации резервного копирования (Приложение № 2).

7. Восстановление информации из резервной копии

1. Восстановление данных из резервных копий производится на основании заявки пользователя ОИ администратору безопасности информации или в случае необходимости восстановления утерянной или поврежденной информации, подлежащей резервированию.
2. После поступления заявки, восстановление данных осуществляется в максимально сжатые сроки, ограниченные техническими возможностями системы, но не более одного рабочего дня.
3. В процессе восстановления резервной копии следует руководствоваться инструкциями по восстановлению информации из резервных копий, описанных в документации, прилагающейся к средствам резервного копирования.

Приложение 1 к Порядку резервного копирования данных

Перечень информации для резервного копирования

Копируемый ресурс	Метод копирования	Тип копирования	Место размещения		Расписание копирования	Временные характеристики		Примечание
			Тип носителя	Периодичность смены		Срок хранения	Периодичность тестирования копий	

Приложение 2 к Порядку резервного копирования данных

Журнал учета отчуждаемых носителей информации резервного копирования

Носитель копии	Передача на хранение			Выдача с хранения		
	Дата и время	Ответственное лицо, передавшее носитель		Дата и время	Ответственное лицо	
		ФИО	Подпись		ФИО	Подпись

Приложение № 11

к Положению об организации работ по обеспечению безопасности информации в ГБУЗ ТО Областная больница №14 имени В.Н. Шанаурина» (с. Казанское)

План проведения мероприятий по обеспечению информационной безопасности в ГБУЗ ТО Областная больница №14 имени В.Н. Шанаурина» (с. Казанское)

Мероприятие	Периодичность	Исполнитель/ Ответственный
Организационные мероприятия		
Определение состава объектов информатизации и защищаемых ресурсов	Разовое срок до	
Определение круга лиц, участвующих в обработке информации ограниченного доступа	Разовое срок до	
Назначение прав доступа пользователей, необходимых для выполнения должностных обязанностей	Разовое срок до	
Назначение ответственного за защиту информации, администраторов безопасности	Разовое срок до	
Первичный анализ угроз безопасности информации	Разовое срок до	
Установление контролируемой зоны	Разовое срок до	
Определение помещений для организации обработки информации ограниченного доступа	Разовое срок до	
Организация режима и контроля доступа (охраны) в помещения ограниченного доступа	Разовое срок до	
Организация резервного копирования данных, порядка восстановления работоспособности технических средств, программного обеспечения и баз данных	Разовое срок до	
Введение в действие организационной-распорядительной документации информационной безопасности	Разовое срок до	

Мероприятие	Периодичность	Исполнитель/ Ответственный
Информирование сотрудников о правилах обработки и защиты информации ограниченного доступа	Разовое срок до	
Физические мероприятия		
Организация постов охраны для пропуска в контролируемую зону	Разовое срок до	
Установка жалюзи на окнах помещения с размещенными средствами обработки информации	Разовое срок до	
Установка решеток на окнах помещений с размещенными средствами обработки информациина первом и последнем этажах зданий	Разовое срок до	
Установка систем бесперебойного питания для средств обработки информации	Разовое срок до	
Установка системы пожаротушения в помещениях с размещенными средствами обработки информации	Разовое срок до	
Установка систем кондиционирования в помещениях с размещенными средствами обработки информации	Разовое срок до	
Внедрение технической системы контроля доступа к техническим средствам обработки информации (доступ в помещения по электронным картам, токенам и т.п.)	Разовое срок до	
Технические (аппаратные и программные) мероприятия		
Установка и настройкасредств защиты информации от НСД	Разовое срок до	
Внедрение единого хранилища зарегистрированных действий пользователей	Разовое срок до	
Внедрение резервных (дублирующих) технических средств обработки информации	Разовое срок до	
Контролирующие мероприятия		
Контроль над соблюдением режима обработки и защиты информации ограниченного доступа	Еженедельно	
Контроль над выполнением антивирусной защиты	Еженедельно	

Мероприятие	Периодичность	Исполнитель/ Ответственный
Контроль подключений к сетям связи общего пользования и (или) международного обмена	Еженедельно	
Контроль состава и обновлений применяемого программного обеспечения	Еженедельно	
Контроль за обеспечением резервного копирования	Ежемесячно	
Контроль за разработкой и внесением изменений в программное обеспечение собственными разработчиками или сотрудниками сторонних организаций	Ежемесячно	
Поддержание в актуальном состоянии нормативно-организационных документов	Ежемесячно	
Создание и поддержание в актуальном состоянии Журнала внутренних проверок	Ежемесячно	
Проведение внутренних проверок на предмет выявления изменений в режиме обработки и защиты информации	Ежегодно	
Анализ и пересмотр (при необходимости) актуальных угроз безопасности информации	Ежегодно	
Контроль эффективности принятых мер безопасности информации	Ежегодно	

Приложение № 12

к Положению об организации
работ по обеспечению
безопасности информации в ГБУЗ
ТО Областная больница №14
имени В.Н. Шанаурина»
(с. Казанское)

Типовой журнал

учета мероприятий по обеспечению безопасности информации

Начат _____

Окончен _____

№ п/п	Наименование мероприятия[1]	Краткое описание	Цель проводимого мероприятия	Основания для проведения мероприятия (номер и дата приказа/ распоряжения)	Дата проведения мероприятия	Фамилия И.О. проводившего мероприятия	Подпись лица, проводившего мероприятие	Фамилии И.О. участников мероприятия	Приме-чание
1	2	3	4	5	6	7	8	9	10

ЛИСТ ОЗНАКОМЛЕНИЯ

с приказом ГБУЗ ТО «Областная больница № 14 имени В.Н.Шанаурина» (с.Казанское)

«О проведении мероприятий по защите информации»

от_________________ №______

ГБУЗ ТО «Областная больница № 14 имени В.Н.Шанаурина» (с.Казанское)

№ п/п	Ф.И.О.	Должность	Подпись	Дата

ЛИСТ ОЗНАКОМЛЕНИЯ
с приказом ГБУЗ ТО «Областная больница № 14 имени В.Н.Шанаурина» (с.Казанское)

«О проведении мероприятий по защите информации»

от____________________ №_____

Филиал №1 Сладковская районная больница:

№ п/п	Ф.И.О.	Должность	Подпись	Дата