УТВЕРЖДАЮ

Главный врач \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_

|  |  |
| --- | --- |
| «\_\_» \_\_\_\_\_\_\_ 20\_\_ года | № \_\_\_\_\_ |

**ПРИКАЗ**  
**Об утверждении Положения Об информационных системах,**  
**средствах вычислительной техники и связи, локальной вычислительной сети**  
**и информационной безопасности**

В целях повышения уровня информационной безопасности информационной системы учреждений

ПРИКАЗЫВАЮ:

1. Утвердить

1.1. Положение об информационных системах, средствах вычислительной техники и связи, локальной вычислительной сети и информационной безопасности \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (далее — Положение) (приложение № 1).

1.2. Инструкцию по работе в локальной вычислительной сети и соблюдению правил безопасности при работе с информационными ресурсами \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (далее — Инструкция) (приложение № 2).

1.3. Форму листа ознакомления работников учреждений с Положением и Инструкцией (приложение № 3).

2. Ввести в действие Положение с \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

3. Руководителям подразделений ознакомить работников с Положением и Инструкцией под подпись по утвержденной форме и принять к исполнению.

4. Контроль за исполнением настоящего приказа оставляю за собой.

|  |  |  |
| --- | --- | --- |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (Ф. И. О.) | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (подпись) |

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

**ПОЛОЖЕНИЕ**  
**Об информационных системах, средствах вычислительной техники и связи, локальной вычислительной сети и информационной безопасности \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**1. Основные положения**

1.1. Настоящее положение разработано для повышения уровня информационной безопасности информационной системы \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

1.2. Положение определяет основные принципы формирования информационной системы, группы средств вычислительной техники и связи, объединенных в единую локально-вычислительную сеть, информационной безопасности локальной вычислительной сети \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, а также права, обязанности и ответственность всех участников сети.

1.3. Локальная вычислительная сеть (далее — ЛВС) представляет собой организационно- технологический комплекс, обеспечивающий рабочих процесс, научно-исследовательскую деятельность, функционирование информационно-управленческой системы \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

1.4. Средства вычислительной техники (персональные компьютеры, серверы, вся

информация, хранящаяся на них и вновь создаваемая, оборудование локальной вычислительной сети, коммуникационное оборудование, принтеры и другая оргтехника, программное обеспечение) являются собственностью \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ и предоставляются работникам учреждения для выполнения должностных обязанностей, улучшения условий и качества лечебной деятельности, а также для ведения научной деятельности с согласия руководителей.

1.5. ЛВС является корпоративной сетью передачи данных и выполняет функции объединения подразделений учреждений в единую информационно-коммуникационную систему, способствует формированию единого научно-исследовательского пространства учреждений и его интеграции в мировое информационное пространство.

1.6. ЛВС предоставляет индивидуальным абонентам и коллективным пользователям подразделений услуги сети Интернет.

1.7. Доступ в ЛBC осуществляется на автоматизированной основе, предоставляемой сотрудникам, врачам, ординаторам и докторантам \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, а также организациям и физическим лицам, осуществляющим научно-исследовательскую либо ревизионную деятельность на базе учреждения с согласия руководителя учреждения.

1.8. Целями настоящего Положения являются создание основы регулирования информационных процессов в учреждениях, организация совместной работы подразделений учреждения, индивидуальных абонентов и коллективных пользователей сети.

1.9. Настоящее Положение предназначено для сотрудников учреждения, выполнение должностных обязанностей которых связано с использованием персональных компьютеров, и определяет их полномочия, обязанности и ответственность при использовании информационных ресурсов учреждения и глобальной компьютерной сети Интернет.

1.10. Положение призвано обеспечить надежную и эффективную работу средств вычислительной техники, сети и каналов доступа к сети Интернет.

1.11. Соблюдение данного Положения обязательно для всех пользователей JIBC учреждения.

1.12. Изменения и дополнение в настоящее Положение вносятся в порядке его принятия.

**2. Организационно-правовые основы функционирования ЛВС**

2.1. ЛВС располагается внутри защищенного периметра. Обособлена сертифицированными межсетевыми экранами от внешних сетей. Все внешние подключения в ЛВС осуществляются посредством защищённых каналов связи.

2.2. Функционирование ЛВС осуществляется в соответствии с Федеральными законами Российской Федерации:

* от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
* от 07.07.2003 № 126-ФЗ «О связи» ;
* от 29.07.2004 № 98-ФЗ «О коммерческой тайне»;
* от 27.07.2006 № 152-ФЗ «О персональных данных»;
* от 12.08.1995 № 144-ФЗ «Об оперативно-розыскной деятельности»;
* от 28.12.2010 № 390-ФЗ «О безопасности»;

а также в соответствии с:

* Указом Президента РФ от 06.03.1997 № 188 «Об утверждении перечня сведений конфиденциального характера»;
* Указом Президента РФ от 17.03.2008 № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена»;
* Указом Президента РФ от 01.05.2022 № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации»;
* Кодексом Российской Федерации об административных правонарушениях;
* Уголовным кодексом Российской Федерации.

2.3. Техническое, организационное и оперативное управление ЛВС осуществляет отдел информационных технологий и информационной безопасности.

2.4. В целях осуществления постоянного контроля за соблюдением требований по защите информации приказом руководителя учреждения назначается администратор информационной безопасности (далее администратор ИБ).

2.5. Администратор ИБ осуществляет свою деятельность в соответствии с обязанностями, перечисленными в п. 6 настоящего Положения, и несет за их несоблюдение ответственность в соответствии с действующим законодательством Российской Федерации.

2.6. Пользователи ЛВС должны выполнять Инструкцию по работе в ЛВС и соблюдению правил безопасности при работе с информационными ресурсами, которая утверждается приказом руководителя учреждения.

**3. Структура сети**

3.1 ЛВС объединяет средства вычислительной техники и связи учреждения:

* административно-технический сетевой сегмент;
* серверное оборудование;
* локальные вычислительные сети подразделений учреждения;
* отдельные персональные компьютеры подразделений;
* персональные компьютеры индивидуальных абонентов сети.

**4. Средства вычислительной техники**

4.1. Порядок предоставления средств вычислительной техники

4 1.1. Средства вычислительной техники приобретаются за счет средств учреждения.

4.1.2. Средства вычислительной техники предоставляются работнику на основании заявки, подписанной руководителем структурного подразделения и согласованной руководителем учреждения.

4.1.3. Серверное и сетевое оборудование приобретается учреждением и предоставляется всем сотрудникам в зависимости от их решаемых задач и служебных обязанностей.

4.2. Счет средств вычислительной техники

4.2.1. Средства вычислительной техники подлежат учету. Сотрудник, являющийся материально-ответственным лицом отдела информационных технологий и информационной безопасности, обязан поддерживать электронную базу данных всех средств вычислительной техники в актуальном состоянии. Все изменения (добавление новых средств, передвижения средств внутри подразделения между пользователями, передача средств в другое подразделение, модернизация, списание средств, резерв средств) должны быть зафиксированы в электронной базе данных «БД техники».

4.2.2. По указанию руководителя учреждения база данных вычислительной техники должна быть предоставлена для проверки.

4.2.3. В целях обеспечения целостности и неизменности комплектации, системные блоки персональных компьютеров должны быть опечатаны наклейками, исключающими подделку, с уникальными номерами. Наклейка должна быть расположена так, чтобы вскрытие корпуса системного блока приводило к повреждению наклейки. Сотрудник, являющийся материально-ответственным лицом отдела информационных технологий и информационной безопасности, обязан вести учет наклеек в электронном журнале, фиксировать нарушения целостности наклеек по вине пользователей либо вынужденное нарушение целостности в процессе ремонта и профилактического обслуживания.

4.2.4. По указанию руководителя учреждения журнал учета наклеек предоставляется для проверки и служебного расследования инцидентов.

4.3. Ответственность пользователей средств вычислительной техники

4.3.1. Пользователю запрещается использовать компьютерную и оргтехнику в целях, не связанных с деятельностью учреждения.

4.3.2. Пользователь обязан бережно относиться к средствам вычислительной техники, руководствуясь инструкцией по эксплуатации оборудования.

4.3.3. Пользователю запрещается вскрывать системные блоки компьютеров, убирать установленные устройства и устанавливать новые устройства без согласования с начальником отдела информационных технологий.

4.3.4. Нарушение целостности защитных наклеек влечет за собой служебное расследование и дисциплинарное наказание виновного в нарушении данного Положения.

4.3.5. Запрещено подвергать компьютер и периферийные устройства физическим, термическим и химическим воздействиям.

4.3.6. Запрещается самостоятельно подключать к персональному компьютеру периферийное оборудование (принтеры, колонки), за исключением внешних запоминающих UЅВ-устройств.

4.3.7. При печати на лазерных принтерах и многофункциональных устройствах необходимо использовать бумагу для лазерных принтеров плотностью не ниже 80 г/м2.

4.3.8. Запрещается использовать собственную компьютерную технику без постановки ее на учет в учреждении для доступа к информационным ресурсам учреждения.

4.3.9. Пользователю запрещено самостоятельно устанавливать, удалять, деактивировать и изменять программное обеспечение и сетевые настройки на компьютере.

4.3.10. При увольнении работника — пользователя компьютерной техникой обходной лист подписывает материально-ответственное лицо соответствующего подразделения, убедившись в исправности средств вычислительной техники и целостности защитных наклеек на рабочем месте пользователя.

4.4. Порядок выноса компьютерной и оргтехники

4.4.1. Вынос компьютерной и оргтехники из здания осуществляется при наличии пропуска выноса техники (приложение № 1 к настоящему Положению).

4.4.2. Пропуск вы носа компьютерной и оргтехники оформляется и визируется сотрудником отдела информационным технологий и информационной безопасности.

4.4.3. В пропуске выноса фиксируются название, инвентарный и заводской номер техники. В случае, если техника не является собственностью учреждения, в форме указывается собственник техники.

4.4.4. Пропуск выноса заполняется в двух экземплярах, один экземпляр передается лицу, осуществляющему вынос техники. Второй экземпляр пропуска остается на хранении в отделе информационных технологий и информационной безопасности в течение 1 (одного) года.

4.4.5. Охранник обязан визуально убедиться в соответствии выносимой техники и данных, указанных в пропуске выноса, и подтвердить осмотр подписью в пропуске.

4.4.6. В cлyчае возникновения спорной ситуации, потери либо кражи техники, начальник отдела информационных технологий и информационной безопасности предоставляет пропуск лицам, производящим служебное расследование.

**5. Порядок подключения компьютерной и оргтехники к ЛВС и оказания сетевых услуг**

5.1. Порядок регистрации пользователя ЛВС и предоставления доступа к информационным ресурсам

5.1.1. Регистрация пользователей в ЛВС производится администратором ИБ на основании заявки на доступ к ЛВС (приложение № 2 к настоящему Положению), подписанной руководителем подразделения.

5.1.2. Регистрация нового пользователя ЛВС производится в присутствии самого пользователя после того, как пользователь ознакомится с Инструкцией по работе в ЛВС и соблюдению правил безопасности при работе с информационными ресурсами, утвержденную приказом под подпись.

5.1.3. Работнику, зарегистрированному в качестве нового пользователя системы, под подпись доводится имя соответствующего ему пользователя и начальное значение пароля, которое он обязан сменить при первом же входе в систему.

5.1.4. Уникальное имя (учетная запись пользователя), под которым он регистрируется и осуществляет работу в системе, присваивается каждому пользователю для обеспечения персональной ответственности за свои действия. Использование несколькими работниками при работе в системе одного и того же имени пользователя («группового имени») запрещается.

5.1.5. При изменении должностных обязанностей работника, связанных с переводом в другое подразделение, переводом на другую должность и т.п., учетная запись пользователя на основании заявки руководителя соответствующего структурного подразделения подлежит изменению (корректировке).

5.1.6. По запросу администратора ИБ может быть проведена сверка доступа к информационным ресурсам Администратор ИБ предоставляет руководителям подразделений списки сотрудников, с указанием доступных информационных pecypсов. Руководители подразделений обязаны либо подтвердить имеющийся уровень доступа, либо внести исправления в список.

5.1.7. Оригиналы исполненных заявок хранятся в отделе информационных технологий и информационной безопасности и могут впоследствии использоваться в cледyющиx случаях:

* для восстановления полномочий пользователя после сбоев;
* для контроля правомерности наличия у конкретного пользователя прав доступа к тем или иным ресурсам при разборе конфликтных ситуаций.

5.1.8. При увольнении пользователя ЛВС, администратор ИБ подписывает обходной лист и блокирует учетную запись пользователя с даты увольнения.

5.2. Порядок обмена служебной информацией в ЛВС

5.2.1. Информация, предназначенная для администратора ИБ, отправляется электронной почтой по адресу. При таком способе передачи обеспечиваются минимальные задержки при передаче информации и достигается наибольшая эффективность работы.

5.2.2. Информация, предназначенная для группы пользователей ЛВС, выкладывается владельцем информации на общий сетевой pecypc

5.3. Порядок обработки персональных данных

5 3.1. В ЛВС используется специальная категория персональных данных. Обработка персональных данных осуществляется в целях обеспечения медико-профилактического npoцecca, в целях установления медицинского диагноза, оказания медицинских и медико- социальных услуг при условии. что обработка персональных данных осуществляется лицом, профессионально занимающимся медицинской деятельностью и обязанным в соответствии с законодательством Российской Федерации сохранять врачебную тайну.

5.3.2. Обработка персональных данных допускается лицом, не занимающимся медицинской деятельностью, но обеспечивающим статистическую обработку данных в медицинском учреждении, поэтому также обязанного в соответствии с законодательством Российской Федерации сохранять врачебную тайну.

5.3.3. Обработка персональных данных пациентов и сотрудников регулируется Концепцией информационной безопасности информационных систем персональных данных учреждений, утвержденной в учреждении.

**6. Обязанности администратора ИБ по организации и поддержке ЛВС**

6.1. Администратор ИБ назначается приказом руководителя учреждения.

6.2. В обязанности администратора ИБ входит:

* оперативно-административное руководство сетью;
* решение административных и технических вопросов взаимодействия с пользователями при подключении к ЛВС, изменении предоставляемых услуг и отключении от сети;
* разработка и реализация адресной и маршрутной политики сети;
* проведение исследований, связанных с внедрением новых технологий и развитием сети;
* организация работ по мониторингу сети;
* управление маршрутизаторами и магистралью сети;
* локализация и устранение сбоев в работе сети;
* непрерывный мониторинг и документирование работы каналов, связь с провайдером;
* организация и проведение мероприятий по обеспечению безопасности в сети;
* ведение учета и контроль использования ресурсов информационной системы учреждения;
* контроль за доступом пользователей к ресурсам сети Интернет;
* контроль за соблюдением пользователями настоящего Положения;
* информирование руководителей структурных подразделений о любых нарушениях требований настоящего Положения и других негативных ситуациях, которые могут привести к несанкционированному доступу, модификации, разрушению, удалению информационных ресурсов или сбоям в работе;
* руководство работой по сопровождению технических и программных средств сети;
* оказание консультационной помощи пользователям по вопросам, входящим в его компетенции;
* контроль состояния технических средств магистрали сети, телекоммуникационного узлов, административно-технического сегмента.

6.3. Администратор ИБ обеспечивает для пользователей ЛВС услуги электронной почты, разделения доступа к ресурсам, доступа к глобальной сети Интернет. Указанные услуги реализуются посредством поддержки точек доступа пользователя в ЛВС.

6.4. Администратор ИБ не несет ответственности за

* содержание проходящих по сети данных;
* информацию, находящуюся на компьютерах в ЛВС;
* деятельность, ведущуюся на этих компьютерах.

6.5. Администратор ИБ принимает организационные и технические меры к пресечению попыток несанкционированного доступа на компьютеры из внешних сетей и с компьютеров ЛВС, а также к пресечению передачи информации, распространение которой запрещено действующим законодательством.

6.6. Администратор ИБ несет ответственность за:

* нарушение функционирования ЛВС вследствие некорректного администрирования
* сетевых сервисов и сетевого оборудования;
* несвоевременное уведомление администрации учреждения о случаях злоупотреблений сетью;
* открытие и использование несанкционированных сетевых сервисов.

**7. Безопасность в сети**

7.1. Администратор ИБ обеспечивает информационную безопасность в ЛВС путем реализации организационных, программных и технических мероприятий.

7.2. Организационные мероприятия включают в себя:

* организацию постоянного контроля соблюдения настоящего Положения;
* ограничение доступа сотрудников и посетителей в помещения, в которых установлены серверы и коммутационное оборудование ЛВС;
* контроль структуры сети и пресечение несанкционированного подключения к ЛВС.

7.3. Технические мероприятия включают в себя:

* обязательную регистрацию внутренних пользователей, рабочих мест и ЛВС, с определением уровня разрешенного доступа;
* задание конфигураций и настроек программного, технического и сетевого обеспечения;
* использование различных методов защиты каналов связи при работе в ЛВС; антивирусную защиту почтового трафика, серверов и локальных рабочих станций; резервное копирование и документирование информационных ресурсов;
* обеспечение автоматического обновления и наложение критических исправлений на клиентские рабочие станции;
* регулярную смену сетевых паролей;
* логическое и(или) физическое выделение сегментов сети, в которых передается информация ограниченного доступа;
* отслеживание запуска и пресечение использования программного обеспечения, затрудняющего или нарушающего нормальную работоспособность сети, компьютеров в ней и нарушающего безопасность сети;
* ограничение пропуска сетевых протоколов на маршрутизаторах в соответствии с определенными в утвержденных проектах потребностями отдельных сегментов сети;
* обеспечение автономным питанием наиболее критичных узлов и устройств ЛВС.

7.4. Администратор ИБ использует программные продукты, обеспечивающие централизованную аутентификацию и авторизацию пользователей для доступа к ресурсам ЛВС.

**8. Злоупотребления в сети**

8.1. Возможные злоупотребления

8.1.1. К злоупотреблениям, в первую очередь, относится деятельность, нарушающая действующее законодательство Российской Федерации.

8.1.2. К злоупотреблениям относятся также:

* использование ЛВС в коммерческих целях без согласования с руководителем учреждения;
* доступ к данным и программам лиц, не имеющих на это права, уничтожение и(или) фальсификация данных и программ без разрешения их владельца;
* незапланированная и необоснованная производственной необходимостью загрузка сети или серверных ресурсов.

8.2. Пресечение злоупотреблений

8.2.1. Руководитель подразделения обязан ознакомить работников с настоящим Положением под подпись.

8.2.2. Администратор ИБ при выявлении злоупотреблений должен информировать руководителя учреждения и немедленно принять меры по пресечению злоупотребления.

8.2.3. В случае злоупотребления сетью нарушители частично или полностью отстраняются от пользования сетью и несут ответственность в соответствии с действующим законодательством РФ.

8.2.4. Факты злоупотреблений в J1BC рассматриваются внутренней комиссией учреждений.

Приложение № 2

к приказу \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
от «\_\_» \_\_\_\_\_\_\_ 20\_\_ года № \_\_\_\_\_

**ИНСТРУКЦИЯ**  
**по работе в локальной вычислительной сети**  
**и соблюдению правил безопасности при работе с информационными ресурсами**  
**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**1. Определения**

В настоящей Инструкции установлены следующие сокращения и oпpедeлeния:

**1.1. Средства вычислительной техники и связи** — персональные компьютеры, серверное и сетевое оборудование, а также системное и прикладное программное обеспечение.

**1.2. Информационные ресурсы** — информация, используемая сотрудниками для исполнения своих служебных обязанностей, создаваемая, обрабатываемая и хранимая на средствах вычислительной техники и передаваемая средствами связи.

**1.3. Информационные службы** — совокупность технических и программных средств, предоставляющие пользователям следующие функциональные возможности:

* создание и редактирование электронных документов средствами программного обеспечения, установленного на компьютере;
* централизованное хранение электронных документов на сервере в личных каталогах пользователей и в каталогах групп пользователей;
* обмен электронными документами и данными между пользователями через специализированные каталоги коллективного использования;
* вывод данных на печать;
* обмен сообщениями по электронной почте;
* использование справочно-информационных баз данных;
* доступ к глобальным сетям, в том числе сети Интернет.

**1.4. Информационная система – ИС** — взаимосвязанная совокупность информационным ресурсов, информационных служб, обеспечивающих поддержку производственно-хозяйственной деятельности \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (далее учреждения).

**1.5. Информационная безопасность — ИБ** – комплекс организационно-технических мероприятий, обеспечивающих конфиденциальность, целостность и доступность информации.

**1.6. Служебная информация** — информационные ресурсы, находящиеся в собственности учреждения и предназначенные для использования ее сотрудниками в ходе исполнения служебных обязанностей.

**1.7. Конфиденциальная информация** — документированная информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации и нормативно-правовыми актами учреждения.

**1.8. Пoльзoвaтель информационных ресурсов и служб** — субъект, наделенный правом работы и работающий с информационными ресурсами и службами.

**1.9. Владелец информационной системы** – структурное подразделение, осуществляющее право распоряжения информационной системой в пределах установленных нормативно-правовым актами.

**1.10. Персональные данные** – любая информация, относящаяся к определенному физическому лицу (субъекту персональных данные), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, состояние здоровья, другая информация.

**1.10. Персональный компьютер – ПK**

**1.11. Программное обеспечение – ПО** – ПО вычислительной техники, базы данных.

**1.12. ПО вредоносное** — ПО или изменения в ПО, приводящие к нарушению конфиденциальности, целостности и доступности информации.

**1.13. Трафик** – объем информации, полученной пользователем из глобальной компьютерной сети Интернет.

**1.14. Запрещенные сайты** — сайты, содержащие информацию, распространение которой запрещено в РФ, развлекательные сайты, сайты знакомств, игровые сайты, порнографические сайты, а также любые сайты, которые не относятся к направлению деятельности сотрудника.

**1.15. Трастовые сайты** — сайты, необходимые сотрудникам для исполнения должностных обязанностей и проверенные администратором сети на безопасность, разрешенные для использования в учреждении.

**1.16. chat** – pecypc, предоставляющий возможность вести разговор в реальном времени.

**2. Общие положения**

2.1. Все пользователи, при получении первичного доступа к ресурсам ЛВС, обязаны ознакомиться с требованиями данной Инструкции.

2.2. Предоставление пользователю функциональных возможностей, перечисленных в пункте 1.3 настоящей Инструкции, за исключением доступа к сети Интернет (см. п. 7.1), осуществляется на основании письменной заявки руководителя структурного подразделения, оформляемой в соответствии с порядком, определяемым Положением об информационных системах.

2.3. Информационные системы учреждения могут использоваться пользователем только в служебных целях.

2.4. С целью своевременного устранения несоответствия в уровне доступа пользователей к информационным ресурсам учреждения, руководители структурных подразделений обязаны заблаговременно уведомить отдел информационным технологий, администратора ЛВС об увольнении или должностном перемещении сотрудников, работающих с информационными ресурсами и службами учреждения.

2.5. Каждый пользователь несет персональную ответственность за свои действия и обязан строго соблюдать установленные правила по работе с программными и техническими средствами ЛВС.

2.6. С целью соблюдения принципа персональной ответственности за свои действия каждому пользователю, допущенному к работе с конкретной подсистемой ЛВС, назначается персональное уникальное имя (учетная запись пользователя).

Запрещается использовать чужую учетную запись и/или передавать кому-либо свои учетные данные (имя пользователя и пароль).

2.7. Пользователи не должны разглашать информацию о процедурах и технической реализации защиты информации, принятых в учреждении.

2.8. В случае грубого нарушения пользователем требований настоящей Инструкции, администратор ИБ вправе полностью или частично отключить пользователя от информационным ресурсов и служб учреждения, проинформировав об этом руководителя учреждения.

2.9. Пользователи должны информировать администратора ЛВС обо всех фактах нарушения данной инструкции, недостатках в системе защиты информации и других угрозах информационной безопасности.

2.10. Пользователь, имеющий доступ к персональным данным работников учреждения и пациентов обязан сохранить в тайне информацию, ставшую доступной ему в процессе выполнения служебных обязанностей. За разглашение персональных данных пользователь несет административную ответственность в соответствии с законодательством РФ.

2.11. Контроль за соблюдением пользователей требований настоящей Инструкции осуществляют их непосредственные руководители и администратор ИБ.

**3. Рабочее место пользователя**

3.1. Основным средством доступа к информационным ресурсам является персональный компьютер. Предоставление пользователю персонального компьютера и периферийного оборудования осуществляется на основании письменной заявки установленной формы от руководителя структурного подразделения на имя Главного врача.

3.2. Для доступа к информационным ресурсам ЛВС ПK пользователя подключается к ЛВС установленным порядком. Самовольное подключение к сети строго запрещено!

3.3. На каждом персональном компьютере устанавливается и настраивается базовый комплект программного обеспечения, включающий в себя операционную систему и комплект прикладного программного обеспечения. Программное обеспечение, не входящее в базовый комплект, является дополнительным. Оно устанавливается по согласованию с начальником отдела информационных технологий и информационной безопасности.

3.4. С целью защиты информации от несанкционированного доступа, на компьютеры, не подключенные к ЛВС, специалистами отдела информационных технологий и информационной безопасности устанавливаются пароли на локальных пользователей.

3.5. Пользователь несет ответственность за обеспечение защиты информации, отображаемой на экране своего монитора. Покидая рабочее место или при появлении лиц, имеющих возможность видеть на экране монитора служебную информацию, к которой они не допущены, пользователь должен заблокировать компьютер с помощью стандартных программных средств.

3.6. Ответственность за правильное использование и сохранность предоставленного оборудования возлагается на пользователя.

3.7. Пользователю запрещается самостоятельно (без привлечения специалистов отдела информационных технологий и информационной безопасности):

* обслуживать средства вычислительной техники и связи, вскрывать корпуса системных блоков персональных компьютеров, мониторов, периферийных устройств и т.д.;
* изменять аппаратную конфигурацию персональных компьютеров, подключать или отключать периферийные устройства, использовать не входящие в комплект персональных компьютеров кабели, переходники, заглушки и их комбинации;
* изменять настройки операционной системы (за исключением настроек интерфейса пользователя), удалять системные файлы или файлы, назначение которых пользователю непонятно, отключать программу антивирусного монитора;
* устанавливать, деактивировать, модифицировать и копировать программное обеспечение персональных компьютеров;
* привлекать посторонних лиц для производства ремонта (технического обслуживания);
* предоставлять доступ к закрепленному за ним персональному компьютеру посторонним лицам;
* передавать информацию о паролях другим лицам или оставлять информацию о паролях в общедоступном месте;
* вносить и использовать в рабочих помещениях не принадлежащие учреждению средства вычислительной техники и связи;
* умышленно использовать недокументированные свойства и ошибки в программном обеспечения или в настройках средств защиты. Об обнаружении такого рода ошибках необходимо информировать администратора ИБ;
* осуществлять действия, направленные на преодоление систем безопасности, получение несанкционированного доступа к ресурсам ЛВС, ухудшение рабочих характеристик корпоративных информационным систем, перехват информации, циркулирующей в ЛВС.

3.8. При необходимости обеспечить сохранность важной информации, хранящейся на жестком диске ПK, пользователь должен периодически создавать резервные копии, сохраняя важную информацию в выделенной папке файлового cepвepa. Пользователь обязан не препятствовать действиям специалистов отдела информационных технологий и информационной безопасности по обновлению аппаратного и программного обеспечения на своем персональном компьютере.

3.9. Передача средств вычислительной техники другому сотруднику осуществляется только через отдел информационным технологий и информационной безопасности.

**4. Работа в корпоративной компьютерной сети**

4.1. Для обеспечения совместной работы пользователей, администратором ИБ на серверах учреждений создаются папки общего доступа для обмена информацией внутри структурного подразделения.

4.2. Для хранения рабочих копий служебных документов, по запросу пользователя администратором ИБ может быть создана персональная папка на сервере.

4.3. Дополнительные папки обмена для организации совместной работы пользователей нескольких подразделений учреждений создаются администратором ИБ по письменной заявке руководителей соответствующих подразделений или руководителя рабочей группы на имя начальника отдела. В заявке в обязательном порядке указываются пользователи и лица ответственные за папки обмена и уровни доступа пользователей.

4.4. Пользователь обязан:

* покидая рабочее место, закрыть все программы и открытые документы, активировать процедуру «заставка экрана», защищенную паролем или выполнить блокировку операционной системы;
* по окончанию работы завершить сеанс работы в сети, выключить персональный компьютер и периферийные устройства;
* при работе на компьютере, подключенном к информационно-вычислительной сети учреждения, хранить все служебные документы в специализированных папках на сервере учреждения.

4.5. Пользователю запрещается:

* работать в информационных системах под именами других пользователей и с использованием чужих паролей доступа;
* использовать сетевые каталоги и локальные диски персонального компьютера для хранения данных, не относящихся к служебной деятельности;
* использовать открытые каналы связи для передачи конфиденциальной информации, не защищенной в ycтановленном порядке;
* выполнять с информационными ресурсами операции, не предусмотренные его правами доступа (в том числе несанкционированно копировать, изменять и уничтожать данные).

4.6. Администратор ИБ имеет право в случае обнаружения нарушений и выявления злоупотреблений:

* заблокировать учетную запись пользователя;
* удалять на серверах информацию, не имеющую отношения к производственным процессам.

**5. Работа со съемными носителями информации**

5.1. Пользователю запрещается копировать служебную информацию на съемные носители (дискеты, оптические диски, USB flаsh-диски и т.д.) без разрешения руководителя структурного подразделения, осуществляющего полномочия распоряжения информационной системой в пределах, установленных нормативно-правовыми актами учреждения.

5.2. При извлечении флэш-накопителя или внешнего жесткого диска необходимо использовать «безопасное извлечение устройства». Иначе, это может привести к повреждению информации на извлекаемом устройстве.

5.3. За передачу сторонним лицам и организациям любого рода информации на съемных носителях несет ответственность руководитель структурного подразделения.

5.4. Все съемные носители информации, полученные от сторонних лиц и организаций любого рода, подлежат обязательной проверке пользователем на наличие вирусов средствами установленного на персональном компьютере антивирусного программного обеспечения.

5.5. Во избежание несанкционированного доступа к информации, содержащейся на съемных носителях, категорически запрещается хранение данных носителей информации в местах, доступных для посторонних лиц.

5.6. Для обеспечения безопасности и несанкционированного доступа к информации внутри сети, администратор ИБ имеет право закрыть доступ к портам сменных носителей на ПK.

5.7. В случае отключения портов сменных носителей, доступ пользователя к использованию съемных носителей информации предоставляется при наличии служебной необходимости по заявке установленного образца от руководителя структурного подразделения на имя начальника отдела.

**6. Работа с электронной почтой**

6.1. Отдел информационных технологий и информационной безопасности предоставляет пользователям услуги внутренней электронной почты, предназначенной для безопасной пересылки информации в рамках корпоративной компьютерной сети, а также услуги внешней электронной почты, предназначенной для обмена информацией с внешними информационными системами, в том числе доступными через сеть Интернет.

6.2. Учреждение оставляет за собой право просматривать, контролировать, перехватывать и изымать все сообщения, созданные, полученные или переданные с помощью корпоративной электронной почты. Содержание сообщения электронной почты, даже полученного в рамках выполнения служебных обязанностей, может быть доведено до сведения руководителя учреждения без разрешения пользователя.

6.3. Электронная почта не может использоваться для создания оскорбительных или провокационных сообщений. Таковыми считаются, в том числе сообщения, содержащие сексуальные домогательства, рисовые оскорбления, дискриминацию по половому признаку или другие комментарии, затрагивающие в оскорбительной форме вопросы возраста или сексуальной ориентации, религиозные или политические пристрастия, национальность, состояние здоровья и т.д.

6.4. Электронная почта не может использоваться для агитации и рекламы коммерческих предприятий, пропаганды религиозных или политических идей и для других целей, не связанных с выполнением служебных обязанностей.

6.5. Электронная почта не должна использоваться для передачи или получения материалов, защищенных авторским правом, внутренней финансовой и иной информации или документов лицами, не имеющими соответствующим полномочий.

6.6. Электронное послание не должно использоваться для пересылки секретной и конфиденциальной информации, поскольку является эквивалентом почтовой открытки. Электронная почта не является средством гарантированной доставки отправляемого сообщения до адресата.

6.7. Ответственность за ненадлежащую подготовку информации к передаче по электронной почте несет пользователь.

6.8. Учреждение может разгласить информацию о действиях пользователя уполномоченным на это третьим лицам, включая правоохранительные органы.

6.9. Несмотря на то, что администратор ИБ по требованию руководителя учреждения имеет право извлекать и читать все сообщения электронной почты, такие сообщения должны рассматриваться, как конфиденциальные другими сотрудниками учреждения, и получить к ним доступ может только сотрудник, которому эти сообщения адресованы. Любое исключение из этого правила возможно только при разрешении руководителя учреждения.

6.10. При получении электронных сообщений сомнительного содержания и/или из незнакомого источника не следует открывать файлы, вложенные в сообщение, переходить по указанным в сообщении ссылкам, так как они с большой вероятностью могут содержать вирусы.

6.11. Не следует отвечать на подозрительные письма и, тем более, сообщать любые данные о себе, если Вы не доверяете отправителю письма.

6.12. Не следует выполнять инструкции по установке или настройке программного обеспечения, полученные по электронной почте. При необходимости, письма, отправленные администратором ИБ, будут содержать ссылку на официальные ресурсы ЛВС, с подробными инструкциями.

**7. Работа в сети Интернет**

7.1. Доступ к сети Интернет предоставляется ограниченному перечню ПK учреждения при наличии служебной необходимости на основании мотивированной заявки от руководителя структурного подразделения на имя начальника отдела информационных технологий и информационной безопасности. Заявка согласовывается с главным врачом Учреждения. При этом данному ПK отключается доступ к ресурсам, содержащим персональные данные.

7.2. Доступ к сети Интернет предоставляется пользователю исключительно в целях выполнения пользователем своих служебных обязанностей, требующих непосредственного подключения к внешним информационным ресурсам.

7.3. Доступ к глобальной сети Интернет осуществляется с рабочего ПK пользователя. Ответственность за действия на компьютере другого сотрудника несет пользователь ПK, с которого совершено это действие.

7.4. Действия пользователей в сети Интернет могут контролироваться, протоколироваться и периодически проверяться уполномоченными на эго сотрудниками отдела. Данная информация может служить причиной отключения определенных ресурсов и принятия решений об изменении прав доступа к сети Интернет и, при необходимости может быть представлены руководителю структурного подразделения, а также руководителю учреждения. Нарушители привлекаются к ответственности в установленном порядке.

7.5. Работа пользователей в глобальной компьютерной сети Интернет анализируется по следующим параметрам:

* перечень используемых ресурсов;
* объем трафика.

7.6. Администратор ИБ может разгласить информацию о действиях пользователя уполномоченным на это третьим лицам, включая правоохранительные органы. Использование ресурсов означает согласие пользователя с тем, что за его деятельностью осуществляется контроль.

7.7. При использовании ресурсов Интернет в личных целях сообщения пользователя должны включать ссылку о том, что выраженная точка зрения — его личная

7.8. При использовании сети Интернет запрещено:

* осуществлять действия, запрещенные законодательством РФ;
* осуществлять неавторизованные попытки получить доступ к сети интернет;
* осуществлять действия, направленные на «взлом» любых компьютеров, находящихся как в локальной сети организации, так и за его пределами;
* использовать предоставленный доступ в сеть Интернет в коммерческих целях, за исключением случаев, когда это входит в служебные обязанности;
* публиковать, загружать и распространять материалы содержащие:

|  |  |
| --- | --- |
|  | * конфиденциальную информацию, а также информацию, составляющую коммерческую тайну, за исключением случаев, когда это входит в служебные обязанности и способ передачи является безопасным, согласованным с администратором ЛВС заранее; * персональные данные пациентов и сотрудников; * информацию, полностью или частично, защищенную авторскими или другим правами, без разрешения владельца; * вредоносное ПО, предназначенное для нарушения, уничтожения либо ограничения функциональности любых аппаратных и программных средств, для осуществления несанкционированного доступа, а также серийные номера к коммерческому ПО, пароли и прочие средства для получения несанкционированного доступа к платным Интернет-ресурсам, а также ссылки на вышеуказанную информацию; * угрожающую, клеветническую, непристойную информацию, а также информацию, оскорбляющую честь и достоинство других лиц, материалы, способствующие разжиганию национальной розни, подстрекающие к насилию, призывающие к совершению противоправной деятельности и т.д. |

* создавать и посещать сайты, содержание информацию, запрещенную к распространению в Российской Федерации (эротико-порнографические ресурсы, нацистские или националистические ресурсы, ресурсы, призывающие к насилию, ресурсы, содержание оскорбительную или провокационную информацию), посещать игровые, развлекательные и прочие сайты, не имеющие отношения к деятельности организации и деятельности пользователя;
* посещать ресурсы трансляции потокового видео и аудио (веб-камеры. трансляция ТВ- и музыкальных программ в Интернете), создающих большую загрузку сети и мешающих нормальной работе остальных пользователей;
* получать из сети Интернет большой объема информации (свыше l00мб) без согласования с отделом;
* использовать рабочее время и ресурсы сети Интернет в личных целях; использовать интернет-пейджеры (ICQ, IRC и т.п.);
* регистрироваться в Интернет-рассылках, конференциях, форумах с использованием имени регистрации и пароля, совпадающих с используемыми для доступа к информационным системам Учреждения
* использовать Интернет для несанкционированной передачи (выгрузки) или получения (загрузки) материалов, защищенных авторским правом;
* использовать несанкционированную нагрузку программ из сети Интернет и запуск их, поскольку они могут содержать вирусы и программы-трояны;
* подключаться к ресурсам Интернета, используя сотовый телефон, модем и другие устройства.

7.9. Пользователи несут ответственность за содержание сознательно принимаемой и передаваемой информации.

7.10. Содержание Интернет-ресурсов, а также файлы, загружаемые из сети Интернет, подлежат обязательной проверке на отсутствие вредоносного ПО.

7.11. Обслуживание каналов связи, контроль за их работоспособностью, оперативную связь с провайдерами и устранение сбоев, ввод в действие резервного канала осуществляет администратор ИБ.

7.12. Администратор ИБ имеет право:

* при обнаружении доступа к Интернет-ресурсам, содержание и направленность которых запрещены Российским законодательством, а так же к развлекательным сайтам, блокировать доступ к сайту без предварительного предупреждения;
* ограничить доступ к ресурсам сети Интернет, содержание которых не имеет отношения к исполнению служебных обязанностей;
* при обнаружении использования пользователем программных продуктов, которые могут привести к несанкционированному доступу, модификации, разрушению, удалению информационным ресурсов или сбоям в работе сети, запретить доступ к сети Интернет.

7.13. Система контроля Интернет-доступа в учреждении предусматривает следующие автоматические ограничения:

* запрет входа на определенные сайты (приложение 6 к настоящей инструкции).
* антивирусную проверку Интернет-трафика, с автоматическим отказом принимать вирусный файл.
* отключение пользователя и/или групп пользователей при достижения ими лимита 10 Гб, в cлyчae злоупотреблений.

7.14. При подозрении пользователя в нецелевом использовании сети Интернет администратором ИБ информация об использованном трафике и список посещаемых ресурсов передается руководителю структурного подразделения для принятия решения по дальнейшему предоставлению доступа к сети Интернет.

7.15. В случае возникновения претензий или вопросов, касающихся конкретного запрещенного сайта, невозможности продолжения работы в сети Интернет, пользователь обращаются к администратору ЛВС. Если претензию не удается решить двум сторонам, тогда вопрос рассматривает руководство учреждения.

**8. Требования при работе с персональными паролями**

8.1. При первичной регистрации в информационным системах учреждений пользователь обязан самостоятельно определить персональный пароль с учетом следующих требований:

* длина пароля должна быть не менее 6 символов;
* пароль не должен быть тривиальным (11111, 12345, QWERTY и т.п.);
* в числе символов пароля должны присутствовать буквы в верхнем и нижнем регистрах, цифры или специальные символы (@, #, $, &, ’. % и т.п.);

8.2. При использовании паролей запрещается:

* использовать в качестве пароля «пустой» пароль, имя пользователя;
* использовать в качестве пароля легко вычисляемые сочетания символов (имена, фамилии, общепринятые сокращения);
* записывать пароль на неучтенных бумажных носителях информации;
* сообщать кому-либо, даже администратору ИБ, свой пароль для доступа к информационным ресурсам ЛВС.

8.3. Пользователи не должны хранить свои пароли в общедоступных местах (записывать пароли на мониторе, клавиатуре, бумаге и т.д.). Пароли не должны храниться на диске в открытом виде и использоваться в процедурах с автоматической подстановкой пароля.

8.4. Смена пароля производится в следующих случаях:

* по истечению установленного срока жизни пароля:
* длительное отсутствие пользователя на рабочем месте (например, по причине болезни, ухода в отпуск);
* подозрение на компрометацию пароля.

8.5. Последовательность символов, назначаемая пользователем в качестве нового пароля, не должна совпадать с паролями, используемыми им ранее.

8.6. В случае длительного отсутствия (отпуск, длительная командировка, болезнь, декретный отпуск и т.д ), пользователь или его непосредственный руководитель должен поставить в известность отдел информационных технологий и информационной безопасности о предполагаемых сроках отсутствия с целью блокировки сетевого пароля пользователя на этот срок.

**9. Порядок действий при возникновении нештатных ситуаций**

9.1. При возникновении любых сбоев в работе аппаратных средств и программного обеспечения, пользователям следует обращаться за консультациями к специалистам отдела Информационных технологий.

9.2. В случае утери одного их своих паролей или в случае невозможности зарегистрироваться в информационных системах учреждения необходимо сообщить об этом администратору ИБ.

9.3. При получении предупреждений об обнаружении на персональном компьютере программ-вирусов, пользователь обязан приостановить работу и сообщить об этом в отдел.

**10. Права**

10.1. Пользователь имеет право получать консультации по вопросам обеспечения безопасности при работе с информационными ресурсами в отделе информационных технологий и информационной безопасности.

10.2. Пользователь имеет право обращаться в отдел информационных технологий и информационной безопасности за технической поддержкой, а также по вопросам поиска информации в глобальной сети Интернет.

10.3. Пользователь имеет право в любое время (с соблюдением требований, описанных в пп. 8.1, 8.4 настоящей Инструкции) изменять свои пароли доступа к информационным ресурсам и службам.

**11. Ответственность**

11.1. За разглашение персональных данных работников и пациентов Учреждения пользователь несет ответственность в соответствии с действующим законодательством РФ.

11.2. Пользователь несет персональную ответственность за соблюдение им требований безопасности при работе с информационными ресурсами и службами учреждений.

11.3. Неисполнение либо ненадлежащее исполнение пользователем требований безопасности при работе с информационными ресурсами и службами учреждений расценивается как нарушение трудовой дисциплины.

11.4. За неисполнение либо ненадлежащее исполнение требований безопасности при работе с информационными ресурсами и службами учреждений, повлекшее за собой ущерб, пользователь несет дисциплинарную, материальную и уголовную ответственность в соответствии с действующим законодательством РФ.

Приложение № 3

к приказу \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
от «\_\_» \_\_\_\_\_\_\_ 20\_\_ года № \_\_\_\_\_

**Форма листа ознакомления работников**  
**с Положением «Об информационных системах, средствах вычислительной техники и связи, локальной вычислительной сети и информационной безопасности» и Инструкцией по работе в локальной вычислительной сети**  
**и соблюдению правил безопасности при работе с информационными ресурсами \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

С Положением «Об информационных системах, средствах вычислительной техники и связи, локальной вычислительной сети и информационной безопасности» и Инструкцией по работе в локальной вычислительной сети и соблюдению правил безопасности при работе с информационными ресурсами \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, утвержденных приказом от «\_\_» \_\_\_\_\_\_\_ 20\_\_ года № \_\_\_\_\_ ознакомлен.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **№** | **Ф. И. О.** | **Отделение** | **Дата** | **Подпись** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Приложение № 1

к Положению  
«Об информационных системах, средствах вычислительной техники и связи, локальной вычислительной сети и информационной безопасности›

**Пропуск выноса компьютерной и оргтехники из здания**  
**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Название выносимого оборудования** | **Подразделение** | **Дата вноса** | **Дата выноса** | **Инвентаризационный** **№** | **Завод** № | **Ф. И. О.**  **Подпись** **сопровождающего** |
|  |  |  |  |  |  |  |

|  |  |
| --- | --- |
| **Цель вноса:** |  |
|  |  |
|  |  |
|  |  |
|  |  |
| **Подпись сотрудника ОИТ:** |  |
|  |  |
| **Цель выноса:** |  |
|  |  |
|  |  |
|  |  |
|  |  |
| **Подпись охранника при выносе:** |  |

**Пропуск выноса компьютерной и оргтехники из здания**  
**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Название выносимого оборудования** | **Подразделение** | **Дата** **выноса** | **Дата** **выноса** | **Инвентаризационный** **№** | **Завод** **№** | **Ф. И. О.**  **Подпись** **сопровождающего** |
|  |  |  |  |  |  |  |

|  |  |
| --- | --- |
| **Цель выноса:** |  |
|  |  |
|  |  |
|  |  |
|  |  |
| **Подпись сотрудника ОИТ:** |  |
|  |  |
| **Подпись охранника при выносе:** |  |

Приложение № 2

К положению  
«Об информационных системах, средствах вычислительной техники и связи, локальной вычислительной сети и информационной безопасности»

**Заявка на доступ к ЛВС**

|  |  |  |  |
| --- | --- | --- | --- |
| **Наименование** **подразделения** | **Ф. И. О.** **пользователя**  **Должность,** **специальность** | **Список информационных** **ресурсов, требующих предоставления доступа** | **Уровень доступа** **только чтение \** **полный доступ** |
|  |  |  |  |

|  |  |  |
| --- | --- | --- |
| Руководитель подразделения | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (Ф. И. О.) | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (подпись) |
|  |  |  |
| Доступ предоставлен (отметка ставится администратором ИБ): | | |
| \_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (Ф. И. О.) | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (подпись) |

«\_\_» \_\_\_\_\_\_\_ 20\_\_ года