Утверждено приказом
Главного врача
Гаськова А.Ю.
От « 18 » ноября 2016 г. № 786-р

Инструкция пользователя информационных систем в ОГБУЗ «Братская городская больница № 2»

г. Братск

2016 год

1. Общие положения

1.1. Пользователями информационных системах согласно перечню, являются сотрудники, допущенные к работе в информационных системах согласно перечню, в соответствии с приказом об утверждении списка лиц, которым необходим доступ к защищаемой информации, обрабатываемой в информационных системах согласно перечню, для выполнения служебных (трудовых) обязанностей.

1.2. Настоящая инструкция определяет задачи, функции, обязанности, права и ответственность пользователей, допущенных к работе в информационных системах согласно перечню.

2. Права и обязанности пользователя

2.1. Работники, получившие доступ к защищаемой информации, обязаны хранить в тайне сведения ограниченного распространения, ставшие им известными во время работы или иным путем и пресекать действия других лиц, которые могут привести к разглашению такой информации. О таких фактах, а также о других причинах или условиях возможной утечки защищаемой информации немедленно информировать администратора информационной безопасности и лицу ответственному за обеспечение информационной безопасности.

2.2. Защищаемая информация (в том числе персональные данные) не подлежат разглашению (распространению). Прекращение доступа к такой информации не освобождает работника от взятых им обязательств по неразглашению сведений ограниченного распространения.

2.3. В случае оставления занимаемой должности работник обязан вернуть все документы и материалы, относящиеся к деятельности подразделения, организации. В том числе: отчеты, инструкции, переписку, списки работников, компьютерные программы, а также все прочие материалы и копии названных

материалов, имеющих какое-либо отношение к деятельности организации, полученные в течение срока работы.

2.4. Пользователь обязан:

– знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций, руководства по защите информации и распоряжений, регламентирующих порядок действий по защите информации;

– знать и соблюдать установленные требования по режиму обработки защищаемой информации, учету, хранению и пересылке носителей информации, обеспечению безопасности данных, а также руководящих и организационно-распорядительных документов;

– соблюдать требования парольной политики (Инструкция по организации парольной защиты винформационных системах согласно перечню;

– соблюдать правила при работе в сетях общего доступа и (или) международного обмена - Интернет и других (Инструкция о порядке работы при подключении к сетям общего пользования и (или) международного обмена винформационных системах согласно перечню;

– соблюдать установленную технологию обработки информации;

– руководствоваться требованиями инструкций по эксплуатации установленных средств вычислительной техники (СВТ) и средств защиты информации (СЗИ);

– экран монитора в помещении располагать во время работы так, чтобы исключалась возможность несанкционированного ознакомления с отображаемой на них информацией посторонними лицами;

– 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>;

– при выходе в течение рабочего дня из помещения, в котором размещается ИС, пользователь обязан:

- блокировать ввод-вывод информации на своем рабочем месте ИС в случаях кратковременного отсутствия (перерыв) или выключать СВТ ИС;
- блокировать вывод информации на монитор рабочих станций.

– немедленно ставить в известность администратора информационной безопасности:

- в случае утери носителя с персональными данными или при подозрении компрометации личных ключей и паролей;
- нарушений целостности пломб (наклеек с защитной и идентификационной информацией, нарушении или несоответствии номеров печатей) на аппаратных средствах рабочих станций или иных фактов совершения в его отсутствие попыток несанкционированного доступа (НСД) к защищенной ИС;
- несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств ИС.

– обо всех выявленных нарушениях, связанных с информационной безопасностью, а так же для получений консультаций по вопросам информационной безопасности, необходимо обратиться к лицу ответственному за обеспечение информационной безопасности ИС;

– для получения консультаций по вопросам работы и настройке элементов ИС необходимо обращаться к администратору информационной безопасности.

2.5. Пользователю **ЗАПРЕЩАЕТСЯ**:

– разглашать защищаемую информацию третьим лицам;

– использовать сведения ограниченного распространения при подготовке

открытых публикаций, докладов, научных работ и т.д.;

– выполнять работы с документами ограниченного распространения на дому, выносить их из служебных помещений, снимать копии или производить выписки из таких документов без разрешения руководителя;

– накапливать ненужные для работы персональные данные;

– передавать или принимать без расписки документы ограниченного распространения;

– оставлять на рабочих столах, в столах и незакрытых сейфах документы ограниченного распространения, а также оставлять незапертыми и не опечатанными после окончания работы сейфы, помещения и хранилища с документами конфиденциального характера;

– осуществлять обработку защищаемой информации (в том числе персональных данных) в присутствии посторонних (не допущенных к данной информации) лиц;

– сообщать устно, письменно или иным способом (показ и т.п.) другим лицам пароли, передавать личные идентификаторы, ключевые дискеты и другие реквизиты доступа к ресурсам ИС;

– подключать к рабочим станциям нештатные устройства;

– записывать и хранить защищаемую информацию на неучтенных носителях информации (гибких магнитных дисках и т.п.);

– не санкционированно открывать общий доступ к папкам на своей рабочей станции;

– отключать (блокировать) средства защиты информации;

– использовать компоненты программного и аппаратного обеспечения ИС подразделения в неслужебных целях;

– оставлять включенной без присмотра свою рабочую станцию (ПЭВМ), не активизировав средства защиты от НСД (временную блокировку экрана и

клавиатуры);

– обрабатывать на АРМ информацию и выполнять другие работы, не предусмотренные перечнем прав пользователя по доступу к ИС;

– самостоятельно вносить изменения в состав, конфигурацию и размещение ИС;

– самостоятельно вносить изменения в состав, конфигурацию и настройку программного обеспечения (ПО), установленного в ИС;

– самостоятельно вносить изменения в размещение, состав и настройку СЗИ ИС;

– умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к возникновению кризисной ситуации. Об обнаружении такого рода ошибок – ставить в известность администратора информационной безопасности;

– привлекать посторонних лиц для производства ремонта или настройки АРМ, без согласования с ответственным за обеспечение защиты данных и/или администратором информационной безопасности;

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

2.6. Пользователь имеет право:

– присутствовать при работах по внесению изменений в аппаратно-программную конфигурацию рабочей станции, закрепленной за ним;

– обращаться к администратору информационной безопасности и/или ответственному за обеспечение безопасности персональных данных с просьбой об оказании технической и методической помощи по обеспечению безопасности обрабатываемой винформационных системах согласно перечнюинформации, а также по вопросам эксплуатации установленных СЗИ;

– обращаться к системному администратору (СА) с просьбой об оказании технической и методической помощи по использованию установленных программных и технических средств ИС;

– обращаться к ответственному за организацию обработки защищаемой информации по вопросам эксплуатации информационных системах согласно перечню(выполнение установленной технологии обработки информации, инструкций и других документов по обеспечению информационной безопасности объекта и защиты информации).

3. Ответственность

3.1. Пользователь несет персональную ответственность:

– за соблюдение режима безопасности защищаемыхданных при их обработке и хранении в информационных системах согласно перечню;

– за правильность понимания и полноту выполнения задач, функций, прав и обязанностей, возложенных на него при работе в информационных системах согласно перечню;

– за соблюдение требований инструкции,нормативных правовых актов, приказов, распоряжений и указаний, определяющих порядок организации работ по информационной безопасности при работе с защищаемой информацией.

3.2. За разглашение информации ограниченного распространения, а также за нарушение порядка работы с документами или машинными носителями, содержащими такую информацию, работники могут быть привлечены к дисциплинарной или иной, предусмотренной законодательством ответственности

3.3. Пользователи, виновные в несоблюдении настоящей инструкции расцениваются как нарушители Федерального закона РФ 27.07.2006 г. N 152-ФЗ «О персональных данных» и несут гражданскую, уголовную,

административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

Разработал

Администратор информационной безопасности_____/_____

«___» _____2016г.

Выдержки из статей Уголовного кодекса РФ.

- **Статья 183.** Незаконное получение и разглашение сведений, составляющих коммерческую или банковскую тайну.

1. Собирание сведений, составляющих коммерческую или банковскую тайну, путем похищения документов, подкупа или угроз, а равно иным незаконным способом в целях разглашения либо незаконного использования этих сведений - наказываются штрафов в размере от ста до двухсот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от одного до двух месяцев либо лишением свободы на срок до двух лет.

2. Незаконные разглашение или использование сведений, составляющих коммерческую или банковскую тайну, без согласия их владельцев, совершенные из корыстной или иной личной заинтересованности и причинившие крупный ущерб, - наказывается штрафом в размере от двухсот до пятисот минимальных окладов оплаты труда или в размере заработной платы или иного дохода осужденного за период от двух до пяти месяцев либо лишением свободы на срок до трех лет со штрафом в размере до пятидесяти минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период до одного месяца либо без такового.

- **Статья 272.** Неправомерный доступ к компьютерной информации

1. Неправомерный доступ к охраняемой законом компьютерной информации, то есть информации на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети, - наказываются штрафом в размере от двухсот до пятисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от двух до пяти месяцев, либо исправительными работами на срок от шести месяцев до одного года, либо лишением свободы на срок до двух лет.

2. То же деяние, совершенное группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, а равно имеющим доступ к ЭВМ, системе ЭВМ или их сети, - наказываются штрафом в

размере от пятисот до восьмисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от пяти до восьми месяцев, либо исправительным работам на срок от одного года до двух лет, либо арестом на срок от трех до шести месяцев, либо лишением свободы на срок до пяти лет.

- **Статья 273.** Создание, использование и распространение вредоносных программ для ЭВМ

1. Создание программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сетей, а равно использование либо распространение таких программ или машинных носителей с такими программами - наказываются лишением свободы на срок до трех лет со штрафом в размере от двухсот до пятисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от двух до пяти месяцев.

2. Те же деяния, повлекшие по неосторожности тяжкие последствия, - наказывается лишением свободы на срок от трех до семи лет.

- **Статья 274.** Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети

1. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети лицом, имеющим доступ к ЭВМ, системе ЭВМ или их сети, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ, если это деяние причинило существенный вред, - наказывается лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет, либо обязательными работами на срок от ста восьмидесяти до двухсот сорока часов, либо ограничением свободы на срок до двух лет.

2. То же деяние, повлекшее по неосторожности тяжкие последствия, - наказывается лишением свободы на срок до четырех лет.

- **Статья 283.** Разглашение государственной тайны

1. Разглашение сведений, составляющих государственную тайну, лицом, которому она была доверена или стала известна по службе или работе, если эти сведения стали

достоянием других лиц, при отсутствии признаков государственной измены - наказывается арестом на срок от четырех до шести месяцев либо лишением свободы на срок до четырех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.

- **Статья 284.** Утрата документов, содержащих государственную тайну

Нарушение лицом, имеющим допуск к государственной тайне, установленных правил обращения с содержащими государственную тайну документами, а равно с предметами, сведения о которых составляют государственную тайну, если это повлекло по неосторожности их утрату и наступление тяжких последствий, - наказывается ограничением свободы на срок до трех лет, либо арестом на срок от четырех до шести месяцев, либо лишением свободы на срок до трех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.

- **Статья 293.** Халатность

Халатность, то есть неисполнение или ненадлежащее исполнение должностным лицом своих обязанностей вследствие недобросовестного или небрежного отношения к службе, если это повлекло существенное нарушение прав и законных интересов граждан или организаций либо охраняемых законом интересов общества или государства, - наказывается штрафом в размере от ста до двухсот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от одного до двух месяцев, либо обязательными работами на срок от ста двадцати до ста восьмидесяти часов, либо исправительными работами на срок от шести месяцев до одного года, либо арестом на срок до трех месяцев.

Выдержки из статей Кодекс Российской Федерации об административных правонарушениях (КоАП РФ).

- **Статья 13.11.** Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных)

Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных) - влечет предупреждение или наложение административного штрафа на граждан в размере от трех до пяти минимальных размеров оплаты труда; на должностных лиц - от пяти до десяти минимальных размеров оплаты труда; на юридических лиц - от пятидесяти до ста минимальных размеров оплаты труда.

- **Статья 13.12.** Нарушение правил защиты информации

1. Нарушение условий, предусмотренных лицензией на осуществление деятельности в области защиты информации (за исключением информации, составляющей государственную тайну), - влечет наложение административного штрафа на граждан в размере от трех до пяти минимальных размеров оплаты труда; на должностных лиц – от пяти до десяти минимальных размеров оплаты труда; на юридических лиц – от пятидесяти до ста минимальных размеров оплаты труда.

2. Использование несертифицированных информационных систем, баз и банков данных, а также несертифицированных средств защиты информации, если они подлежат обязательной сертификации (за исключением средств защиты информации, составляющей государственную тайну), - влечет наложение административного штрафа на граждан в размере от пяти до десяти минимальных размеров оплаты труда с конфискацией несертифицированных средств защиты информации или без таковой; на должностных лиц - от десяти до двадцати минимальных размеров оплаты труда; на юридических лиц - от ста до двухсот минимальных размеров оплаты труда с конфискацией несертифицированных средств защиты информации или без таковой.

3. Нарушение условий, предусмотренных лицензией на проведение работ, связанных с использованием и защитой информации, составляющей государственную тайну, созданием средств, предназначенных для защиты информации, составляющей государственную тайну, осуществлением мероприятий и (или) оказанием услуг по защите информации, составляющей государственную тайну, - влечет наложение административного штрафа на должностных лиц в размере от двадцати до тридцати

минимальных размеров оплаты труда; на юридических лиц - от ста пятидесяти до двухсот минимальных размеров оплаты труда.

4. Использование несертифицированных средств, предназначенных для защиты информации, составляющей государственную тайну, - влечет наложение административного штрафа на должностных лиц в размере от тридцати до сорока минимальных размеров оплаты труда; на юридических лиц - от двухсот до трехсот минимальных размеров оплаты труда с конфискацией несертифицированных средств, предназначенных для защиты информации, составляющей государственную тайну, или без таковой.

- **Статья 13.13.** Незаконная деятельность в области защиты информации

1. Занятие видами деятельности в области защиты информации (за исключением информации, составляющей государственную тайну) без получения в установленном порядке специального разрешения (лицензии), если такое разрешение (такая лицензия) в соответствии с федеральным законом обязательно (обязательна), - влечет наложение административного штрафа на граждан в размере от пяти до десяти минимальных размеров оплаты труда с конфискацией средств защиты информации или без таковой; на должностных лиц - от двадцати до тридцати минимальных размеров оплаты труда с конфискацией средств защиты информации или без таковой; на юридических лиц - от ста до двухсот минимальных размеров оплаты труда с конфискацией средств защиты информации или без таковой.

2. Занятие видами деятельности, связанной с использованием и защитой информации, составляющей государственную тайну, созданием средств, предназначенных для защиты информации, составляющей государственную тайну, осуществлением мероприятий и (или) оказанием услуг по защите информации, составляющей государственную тайну без лицензии, - влечет наложение административного штрафа на должностных лиц в размере от сорока до пятидесяти минимальных размеров оплаты труда; на юридических лиц - от трехсот до четырехсот минимальных размеров оплаты труда с конфискацией созданных без лицензии средств защиты информации, составляющей государственную тайну, или без таковой.

- **Статья 13.14.** Разглашение информации с ограниченным доступом

Разглашение информации, доступ к которой ограничен федеральным законом (за исключением случаев, если разглашение такой информации влечет уголовную ответственность), лицом, получившим доступ к такой информации в связи с исполнением служебных или профессиональных обязанностей, - влечет наложение административного штрафа на граждан в размере от пяти до десяти минимальных размеров оплаты труда; на должностных лиц – от сорока до пятидесяти минимальных размеров оплаты труда.