федеральное государственное бюджетное образовательное учреждение высшего образования
«Самарский государственный медицинский университет»
Министерства здравоохранения Российской Федерации (ФГБОУ ВО СамГМУ Минздрава России)

ПРИКАЗ

04.03.2025 № 36

Самара

Об утверждении политики информационной безопасности

В целях исполнения требований Федерального закона «О персональных данных» от 27.07.2006 N 152-ФЗ и Федерального закона «Об информации, информационных технологиях и о защите информации» от 27.07.2006 N 149-ФЗ;

ПРИКАЗЫВАЮ:

1. Считать утратившим силу «Положение о политике информационной безопасности» утверждённый Ректором ФГБОУ ВО СамГМУ Минздрава России от 31.05.2021; Приказ №148.
2. Утвердить «Политику информационной безопасности в ФГБОУ ВО СамГМУ Минздрава России», согласно Приложению к настоящему приказу;
3. Контроль за исполнением настоящего приказа возложить на начальника управления информационной безопасности Института цифрового развития Черникова В.В.

Ректор **А.В. Колсанов**

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Самарский государственный медицинский университет»
Министерства здравоохранения Российской Федерации
(ФГБОУ ВО СамГМУ Минздрава России)

ПОЛИТИКА
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
в ФГБОУ ВО СамГМУ Минздрава России
№ 1П/03-04-2025

Приложение
к приказу ректора
ФГБОУ ВО СамГМУ
Минздрава России
от 04.03.2025 года № 36

Самара 2025

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1 Назначение Политики

1.1.1 Настоящая Политика информационной безопасности (далее - Политика) является локальным нормативным актом ФГБОУ ВО СамГМУ Минздрава России (далее – Университет) и устанавливает общие положения по обеспечению информационной безопасности Университета.

1.1.2 Требования, изложенные в Политике, являются обязательными для выполнения всеми работниками Университета.

1.1.3 Политика вступает в силу с момента ее утверждения Ректором ФГБОУ ВО СамГМУ Минздрава России.

1.1.4 Актуализация Политики производится в обязательном порядке в следующих случаях:

- при изменении политики Российской Федерации в области информационной безопасности, указов и законов Российской Федерации в области защиты информации;
- при изменении внутренних нормативных документов (инструкций, положений, руководств), касающихся информационной безопасности Университета;
- при выявлении инцидента (инцидентов) по нарушению ИБ, влекущего ущерб для Университета.

1.1.5 Политика подлежит опубликованию на официальном сайте ФГБОУ ВО СамГМУ Минздрава России.

1.2 Цели Политики

1.2.1 Целью политики является защита информации от возможного нанесения им материального, физического, морального или иного ущерба, посредством случайного или преднамеренного воздействия на информацию, её носители, процессы обработки и передачи, а также минимизация рисков ИБ;

1.3 Основные понятия

Для целей Политики используются следующие понятия:

Автоматизированное рабочее место - совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем;
Администратор безопасности — это сотрудник, в чьи обязанности входит обеспечение защиты автоматизированной системы от несанкционированного доступа к информации;
Аутентификация – проверка принадлежности субъекту доступа предъявленного им идентификатора; подтверждение подлинности;
Авторизация – предоставление субъекту прав на доступ, а также предоставление доступа в соответствии с установленными правами на доступ;

Безопасность информации – защищённость информации от её нежелательного разглашения (нарушения конфиденциальности), искажения (нарушения целостности), утраты или снижения степени доступности, а также незаконного её тиражирования;
Документ – зафиксированная на материальном носителе информация с реквизитами, позволяющими её идентифицировать;
Доступность информации – состояние, характеризуемое способностью ИС обеспечивать беспрепятственный доступ к информации субъектов, имеющих на это полномочия;
Доменное имя - обозначение символами, предназначенное для адресации сайтов в сети "Интернет" в целях обеспечения доступа к информации, размещенной в сети "Интернет";
Защита информации – деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию и средства доступа к ней;
Идентификация – присвоение субъектам доступа, объектам доступа идентификаторов (уникальных имен) и (или) сравнение предъявленного идентификатора с перечнем присвоенных идентификаторов;
Информация – сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления;
Информационная безопасность (ИБ) – состояние защищённости интересов Учреждения;
Информационная система (ИС) – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;
Информационный процесс (ИП) – процессы сбора, обработки, накопления, хранения, поиска и распространения информации;
Информационный ресурс (ИР)– всё, что имеет ценность и находится в распоряжении Университета;
Инцидент – непредвиденное или нежелательное событие (группа событий) безопасности, которое привело (могут привести) к нарушению функционирования информационной системы или возникновению угроз безопасности информации (нарушению конфиденциальности, целостности, доступности);
Инцидент информационной безопасности – одно или серия нежелательных, или неожиданных событий ИБ, имеющих значительную вероятность нарушения бизнес-процессов или представляющих угрозу ИБ;
Коммерческая тайна – конфиденциальность информации, позволяющая ее обладателю, при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду:

Контролируемая зона – пространство (территория, здание, часть здания), в котором исключено неконтролируемое пребывание лиц, а также транспортных, технических или иных средств;
Конфиденциальная информация – информация с ограниченным доступом, не содержащая сведений, составляющих государственную тайну, доступ к которой ограничивается в соответствии с законодательством Российской Федерации;
Конфиденциальность информации – состояние защищённости информации, характеризуемое способностью ИС обеспечивать сохранение в тайне информации от субъектов, не имеющих полномочий на ознакомление с ней;
Несанкционированный доступ к информации - доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами;
События информационной безопасности – идентифицированное состояние системы, сервиса или сети, свидетельствующее о возможном нарушении политики безопасности или отсутствии механизмов защиты, либо прежде неизвестная ситуация, которая может иметь отношение к безопасности;
Угроза – опасность, предполагающая возможность потерь (ущерба);
Целостность информации– устойчивость информации к несанкционированному доступу или случайному воздействию на неё в процессе обработки техническими средствами, результатом которого может быть уничтожение и искажение информации;
Электронная подпись —информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию. цифровой аналог собственноручной подписи.

1.4 Термины, сокращения и обозначения

В настоящем Политике используются следующие сокращения:
ФГБОУ ВО СамГМУ Минздрава России, Университет – Федеральное государственное бюджетное образовательное учреждение высшего образования «Самарский государственный медицинский университет» Министерства здравоохранения Российской Федерации;
ФГБОУ ВО СамГМУ Минздрава России, Клиники- Клиники «Самарского государственного медицинского университета» Министерства здравоохранения Российской Федерации;
ИЦР – Институт цифрового развития;
УИБ – Управление информационной безопасности;

АРМ - Автоматизированное рабочее место;
АС - Автоматизированная система;
ИБ - Информационная безопасность;
ИС - Информационная система;
ИР - Информационный ресурс;
ИТ - Информационные технологии;
НСД - Несанкционированный доступ к информации;
ПО - Программное обеспечение;
СКЗИ - Средство криптографической защиты информации;
СЗИ - Средства защиты информации;
ПДн – Персональные данные;
ЭП – Электронная подпись.

2. ПРАВОВЫЕ ОСНОВАНИЯ

Настоящая Политика разработано в соответствии с:

– Конституция Российской Федерации;

– Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи»;

– Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

– Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;

– Указом Президента Российской Федерации от 20.01.1994 № 170 «Об основах государственной политики в сфере информатизации»;

– Указом Президента Российской Федерации от 03.04.1995 № 334 «О мерах по соблюдению законности в области разработки производства, реализации и эксплуатации шифровальных средств, а также предоставления услуг в области шифрования информации"

– Указом Президента Российской Федерации от 06.03.1997 № 188 «Об утверждении Перечня сведений конфиденциального характера»;

– Постановлением Правительства Российской Федерации от 06.07.2015 № 676 «О требованиях к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем, и дальнейшего хранения содержащейся в их базах данных информации»;

– Постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

– Приказом ФСБ России от 10 июля 2014 г. N 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»;

– Приказом ФСТЭК России № 17 от 11 февраля 2013 года «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

– Приказом ФСТЭК России № 21 от 18 февраля 2013 года «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

– Постановление Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

3. ОСНОВНЫЕ ПРИНЦИПЫ ОБЕСПЕЧЕНИЕ ИБ

Основными принципами обеспечения ИБ в Университете являются:

– постоянный и всесторонний анализ информационного пространства Университета с целью выявления уязвимостей информационных ресурсов;

– своевременное обнаружение проблем, потенциально способных повлиять на ИБ Университета, и нарушителя(ей), корректировка моделей угроз;

– разработка и внедрение защитных мер, адекватных характеру выявленных угроз, с учетом затрат на их реализацию;

– контроль эффективности принимаемых защитных мер;

– персонификация и адекватное разделение ролей и ответственности между работниками Университета исходя из принципа персональной и единоличной ответственности за совершаемые операции;

– совместимость в подборе компонентов для обеспечения информационной безопасности способом, гарантирующим их взаимную

системную совместимость на информационном, программном и эксплуатационном уровнях;

– использование компонентов и средств для обеспечения информационной безопасности, соответствующих требованиям по надежности, готовности и обслуживаемости.

4. ИНЦИДЕНТЫ ИБ

4.1. Виды инцидентов ИБ

4.1.1. Инциденты ИБ классифицируются:

1. По типу нарушения:

– Нарушение конфиденциальности — несанкционированный доступ;

– Нарушение целостности — неправомерное изменение данных или систем;

– Нарушение доступности — инцидент блокирует доступ к информации или системам.

2. По источнику:

– Внешние угрозы — от лиц, не имеющих прямого доступа к информационной системе;

– Внутренние угрозы — от сотрудников или контрагентов, имеющих доступ к данным.

3. По степени воздействия:

– Низкого уровня — не оказывают существенного влияния на общее функционирование системы;

– Среднего уровня — ведут к временному снижению работоспособности системы;

– Высокого уровня — вызывают серьезный ущерб вплоть до полного отказа системы.

4. По умыслу:

– Умышленные;

– Непреднамеренные.

4.2 Порядок выявления инцидентов ИБ и реагирование на них

4.2.1. В качестве источников информации об инцидентах могут использоваться:

– журналы логирования и оповещения системного и прикладного программного обеспечения информационных систем (log-файлов), обрабатывающих защищаемую информацию, не содержащую сведения,

составляющие государственную тайну;

– журналы логирования и оповещения системы защиты информации (log-файлов);

– оповещения средств обнаружения вторжений;

– информация, получаемая от сотрудников ФГБОУ ВО СамГМУ Минздрава России;

– информация, полученная на основе анализа защищенности ИС и контроля эффективности СЗИ.

4.2.2. При обнаружении инцидента сотрудник, ответственный за выявления инцидентов информационной безопасности должен руководствоваться регламентом выявления инцидентов информационной безопасности и реагирование на них в ФГБОУ ВО СамГМУ Минздрава России утверждённый приказом ректора.

5. ПРАВИЛА ОБРАЩЕНИЯ С КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИЕЙ

5.1. Обучение работников Университета правилам обращения конфиденциальной информацией проводится путем:

а) проведения специалистом по ИБ инструктажа с работниками, принимаемыми на работу в Университет;

б) самостоятельного изучения работниками внутренних нормативных документов Университета.

5.2. Допуск персонала к работе с конфиденциальной информацией Университета осуществляется после подписания в отделе кадров по персоналу подразделений управления, учебного процесса и науки, либо отдела кадров по персоналу клиник «Обязательства о соблюдении конфиденциальности защищаемой информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну» утверждённый приказом ректора.

5.3. Правила допуска к работе с информационными ресурсами лиц, не являющихся работниками Университета, определяются на основе «Соглашений о конфиденциальности» являющихся приложениями к контрактам/договорам, заключенных с этими лицами или с организациями, представителями которых являются эти лица.

6. КОНТРОЛЬ ДОСТУПА

6.2. В качестве основной угрозы безопасности конфиденциальной информации, включая персональные данные, рассматривается нарушение

конфиденциальности путем раскрытия ее содержимого третьим лицам, не допущенным в установленном порядке к работе с этой информацией.

6.3. Защита информации в Университете осуществляется путем исключения неправомерных или неосторожных действий со сведениями, а также с информационными ресурсами, являющимися критичными для обеспечения функционирования процессов Университета.

6.4. Правами наделения полномочий по уровням доступа пользователей обладают ведущие администраторы по обеспечению безопасности информации Управления информационной безопасности ИЦР для сотрудников Университета и ведущие специалисты отдела технического обслуживания и сопровождения пользователей Управления медицинских информационных систем ИЦР для сотрудников Клиник.

6.5. Уровень полномочий каждого пользователя определяется индивидуально, путём добавления прав в Active Directory, согласно служебной записке на имя начальника управления информационной безопасности ИЦР для сотрудников Университета и на имя начальника отдела технического обслуживания и сопровождения пользователей медицинских информационных систем ИЦР для сотрудников Клиник ФГБОУ ВО СамГМУ Минздрава России направленный через HelpDesk или по электронной почте.

6.6. Процессы генерации, получения, хранения, смены и прекращения действия учетной записи в домене, сотрудников ФГБОУ ВО СамГМУ Минздрава России регламентировано «Положением об организации работы сотрудников с информационными ресурсами ФГБОУ ВО СамГМУ Минздрава России».

7. ОРГАНИЗАЦИЯ РАБОТЫ СОТРУДНИКОВ С ИНФОРМАЦИОННЫМИ РЕСУРСАМИ

7.1 При необходимости получения дополнительного доступа к информационным системам Университета, руководитель структурного подразделения оформляет служебную записку на имя директора Института цифрового развития, в которой указывает необходимый доступ к информационным системам Пользователю в соответствии с его должностными обязанностями и направляет через HelpDesk или по электронной почте.

7.2 Руководители подразделений обязаны периодически пересматривать права доступа своих сотрудников и других пользователей к соответствующим информационным ресурсам, в соответствии с его должностными обязанностями. В случае изменения должностных обязанностей сотрудника

(или переходу на новую должность), руководитель структурного подразделения оформляет служебную записку на имя директора Института цифрового развития, с указанием ФИО и должности сотрудника на аннулирование прав доступа, которые сотруднику более не нужны, и указывает права, которые понадобятся сотруднику для дальнейшего выполнения новых должностных обязанностей и направляют через HelpDesk или по электронной почте.

8. ОРГАНИЗАЦИЯ РАБОТЫ СОТРУДНИКОВ С ЭП

8.1. Для получения сотрудником Университета ЭП, при организации направления деятельности, выполнения должностных обязанностей, проректор по соответствующему направлению/руководитель структурного подразделения (сотрудников прямого или косвенного подчинения), подготавливает проект приказа «Об организации выпуска усиленной квалифицированной электронной подписи и оформления машиночитаемой доверенности».

8.2. В приказе «Об организации выпуска усиленной квалифицированной электронной подписи и оформления машиночитаемой доверенности» (далее - Приказ), указывается должность и ФИО сотрудника, на которого оформляется УКЭП (далее - Заявитель). Приказ утверждается Ректором Университета или лицом его замещающим (исполняющим обязанности). После регистрации, в отделе документационного обеспечения, Приказ передается в управление информационной безопасности ИЦР для формирования запроса на изготовление ЭП.

8.3. Порядок формирования запроса, получения ЭП, работы с ЭП, аннулирования ЭП и работы с машиночитаемой доверенностью регламентировано «Положением по организации процесса получения усиленной квалифицированной электронной подписи и оформления машиночитаемой доверенности в ФГБОУ ВО СамГМУ Минздрава России».

9. ПАРОЛЬНАЯ ПОЛИТИКА

9.1. В целях обеспечения информационной безопасности в ФГБОУ ВО СамГМУ Минздрава России, для доступа в домен Active Directory и прочие автоматизированные информационные системы, сотрудникам предоставляются учетные записи, защищенные паролем. Не допускается использование учетных записей, не защищенных паролем.

9.2 При вводе пароля Пользователю необходимо исключить возможность получения информации о нем посторонними лицами (человек за спиной, наблюдение человеком за движением пальцев в прямой видимости или в отраженном свете) и техническими средствами (стационарными и встроенными в мобильные телефоны видеокамерами и т.п.).

9.3 Процесс генерации, хранения, смены и прекращения действия паролей, а также контроль за действиями сотрудников ФГБОУ ВО СамГМУ Минздрава России регламентирован «Инструкцией по организации парольной защиты в ФГБОУ ВО СамГМУ Минздрава России».

10. АНТИВИРУСНАЯ ЗАЩИТА

10.1. Основным способом защиты информации от воздействия компьютерных вирусов на АРМ является применение средств антивирусной защиты. К использованию в ФГБОУ ВО СамГМУ Минздрава России допускаются только лицензионные антивирусные средства.

10.2. Антивирусная защита информации в ФГБОУ ВО СамГМУ Минздрава России осуществляется посредством применения организационных мер и средствами антивирусной защиты информации.

20.3. Антивирусная защита информационных ресурсов осуществляется Управлением информационной безопасности ИЦР. Для этой цели используется антивирусное программное обеспечение корпоративного класса, имеющая сервер централизованного администрирования и программы-агенты для установки на сервера и АРМ, обеспечивающие централизованный мониторинг и управление антивирусом. Антивирусному контролю подлежит любая информация, поступающая на АРМ Пользователей, в том числе из Интернета и с внешних носителей.

10.4. Требования к проведению мероприятий по антивирусной защите и ответственность сторон регламентировано «Инструкцией по организации антивирусной защиты в ФГБОУ ВО СамГМУ Минздрава России».

11. ЗАЩИТА ОТ НСД

11.1. Добавления АРМ в сеть ФГБОУ ВО СамГМУ Минздрава России осуществляется специалистами управления информационных технологий, путём добавления уникального имени АРМ в домен. Каждый АРМ, принадлежащий организации, должен находиться в домене ФГБОУ ВО СамГМУ Минздрава России.

11.2. Подключение АРМ к сети ФГБОУ ВО СамГМУ Минздрава России происходит путём добавления MAC-адресов на порты

телекоммуникационного оборудования. Подключение сторонних устройств блокируется автомачески.

11.3. Использование личных АРМ в сети ФГБОУ ВО СамГМУ Минздрава России запрещено.

11.4. Запрещено самостоятельно разбирать АРМ и все его комплектующие. При возникновении неисправностей необходимо обратиться в управление информационных технологий.

11.5. По завершению рабочего дня АРМ нужно выключить, но по требованию специалистов управление информационных технологий АРМ может быть оставлен включенным для проведения профилактических работ в нерабочее время.

11.6. Запрещено подвергать АРМ и периферийные устройства физическим, термическим и химическим воздействиям

11.7. Во время работы с конфиденциальной информацией пользователь должен не допускать просмотр информации к лицам, не допущенным к ней. Пользователь должен принимать все необходимые меры по защите информации и контролю прав доступа к ней;

11.8. Если есть подозрения что, какие-либо нужные документы уничтожены или повреждены, необходимо полностью прекратить работу с АРМ или сетевым ресурсом и незамедлительно обратиться в управление информационных технологий.

11.9. На всех АРМ подлежащих аттестации по работе с ИСПДн в ФГБОУ ВО СамГМУ Минздрава России сотрудниками УИБ устанавливаются средства защиты информации от НСД.

11.10. Администраторы безопасности должны обеспечивать правильное функционирование и поддерживать работоспособность средств защиты информации от НСД в пределах, возложенных на него функций. Основные функции, обязанности и права Администратора безопасности регламентированы «Инструкцией администратора безопасности информационных систем».

12. ПРОФИЛАКТИКА НАРУШЕНИЙ ПОЛИТИКИ

12.1. Под профилактикой нарушений политики понимается проведение регламентных работ по защите информации, предупреждение возможных нарушений ИБ в Университете и проведение разъяснительной работы по ИБ среди пользователей. Проведение в ИС Университета регламентных работ по

защите информации предполагает выполнение процедур контрольного тестирования (проверки) функций СЗИ, что гарантирует ее работоспособность.

12.2. Задача предупреждения в ИС Университета возможных нарушений информационной безопасности решается по мере наступления следующих событий:

а) включение в состав ИС Университета новых программных и технических средств (новых рабочих станций, серверного или коммуникационного оборудования и др.) при условии появления уязвимых мест в СЗИ ИС Университета;

б) изменение конфигурации программных и технических средств ИС (изменение конфигурации программного обеспечения рабочих станций, серверного или коммуникационного оборудования и др.) при условии появления уязвимых мест в СЗИ ИС Университета, при появлении сведений о выявленных уязвимых местах в составе операционных систем и/или программного обеспечения технических средств, используемых в ИС Университета.

12.3. Администратор ИБ собирает и анализирует информацию о выявленных уязвимых местах в составе операционных систем и/или программного обеспечения относительно ИС Университета.

12.4 Для решения задач контроля защищенности ИС используются инструментальные средства для тестирования реализованных в составе СЗИ ИС Университета средств и функций защиты.

13. ОЦЕНКА ВРЕДА

13.1 Вред субъекту персональных данных возникает в результате неправомерного или случайного доступа к персональным данным, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении конфиденциальной информации, в том числе персональных данных.

13.2 Оценка вреда осуществляется согласно «Правилам оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных» утверждённый приказом ректора.

13.3 По результатам оценки вреда комиссией по уничтожению персональных данных составляется Акт оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных.

14. ЛИКВИДАЦИЯ ПОСЛЕДСТВИЙ НАРУШЕНИЯ ПОЛИТИКИ

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

14.2. В случае обнаружения подсистемой защиты информации факта нарушения ИБ или осуществления НСД к защищаемым информационным ресурсам ИС необходимо поставить в известность администратора ИБ и начальника Управления информационной безопасности (телефон: 8 (846) 374-00-66 (вн.: 4729, 4732, 4745, 4719, 6005), эл. почта: cib@samsmu.ru, через систему Helpdesk https://helpdesk.samsmu.ru/).

14.3 Порядок действий по управлению инцидентами информационной безопасности описан в «Регламенте выявления инцидентов информационной безопасности и реагирование на них в ФГБОУ ВО СамГМУ Минздрава России».

15 ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ ПОЛИТИКИ

15.1 Ответственность за выполнение правил Политик безопасности в рамках своих служебных обязанностей несет каждый пользователь ИС.

15.2 Ответственность за разработку мер и контроль обеспечения защиты информации несет администратор ИБ.

15.3 Ответственность за реализацию Политики в части, касающейся разработки и актуализации правил внешнего доступа и управления доступом, антивирусной защиты - возлагается на управление информационной безопасности и на управление информационные технологий ИЦР.