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

УТВЕРЖДЕНО
Приказом Ректора
член-корреспондента РАН
з.д.н. РФ
А.В. Колсанова

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 7A6B8A5E9CB221443586B1F30109C6F1
Владелец: Колсанов Александр Владимирович
Действителен: с 02.04.2026 до 26.06.2027

ПОЛИТИКА № 1П/08-31-2026
защиты информации
в ФГБОУ ВО СамГМУ Минздрава России

Приложение № 1
к приказу ректора ФГБОУ ВО
СамГМУ Минздрава России
№ 169 от 31.08.2026 г.

Самара 2026

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1 Назначение Политики

1.1.1 Настоящая Политика защиты информации (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 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 информационной безопасности — это сотрудник, в чьи обязанности входит обеспечение защиты автоматизированной системы от несанкционированного доступа к информации;

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;

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

1.3 Термины, сокращения и обозначения

В настоящей 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;
УИБ – Управление информационной безопасности;
АРМ - Автоматизированное рабочее место;
АС - Автоматизированная система;
ДЦТ - Дирекция по цифровой трансформации;
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 разработана в соответствии с:

1. Федеральный закон от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне».
2. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и защите информации».
3. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».
4. Федеральный закон от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи».
5. Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».
6. Указ Президента РФ «Об утверждении перечня сведений конфиденциального характера» от 06 марта 1997 г. № 188.
7. Указ Президента РФ «О дополнительных мерах по обеспечению
8. информационной безопасности Российской Федерации» от 01 мая 2022 г. № 250.
9. Указ Президента РФ «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации» от 30 марта 2022 г. № 166.

10. Постановление Правительства РФ «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» от 01 ноября 2012 г. № 1119.

11. Постановление Правительства РФ «Об утверждении правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений» от 08 февраля 2018 г. № 127.

12. Приказ ФСТЭК РФ «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» от 18 февраля 2013 г. № 21.

13. Приказ ФСТЭК РФ «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» от 25 декабря 2017 г. № 239.

14. Приказ ФСТЭК РФ «Об утверждении требований к оценке вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона «О персональных данных»» от 27 октября 2022 г. № 178.

15. Приказ ФСТЭК РФ «Об утверждении требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений» от 11 апреля 2025 г. № 117.

16. Приказ ФСБ РФ «Об утверждении порядка взаимодействия операторов с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, включая информирование ФСБ России о компьютерных инцидентах, повлекших неправомерную передачу (предоставление, распространение, доступ) персональных данных» от 13 февраля 2023 г. № 77.

17. Приказ ФСБ РФ «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений с использованием шифровальных (криптографических) средств» от 18 марта 2025 г. № 117.

18. Методический документ ФСТЭК РФ от 05.02.2021 «Методика оценки угроз безопасности информации».

19. Методический документ ФСТЭК РФ от 28.10.2022 «Методика тестирования обновлений безопасности программных, программно-аппаратных средств».

20. Письмо ФСТЭК России от 07.10.2025 № 240/92/3228 «О мерах по повышению защищенности информационной инфраструктуры Российской Федерации».

3. ОБЛАСТЬ ДЕЙСТВИЯ ПОЛИТИКИ

3.1 Требования настоящей Политики распространяются на:

– информационные системы университета, включая программные и программно-аппаратные средства, информационные ресурсы и информацию, обрабатываемую в университете, за исключением сведений, составляющих государственную тайну;

– информационно-технологическую инфраструктуру университета, включая сервисы, телекоммуникационное оборудование и каналы связи, обеспечивающие передачу информации между информационными системами и информационное взаимодействие участников информационного обмена;

– системы и подсистемы защиты информации университета, обеспечивающие реализацию и контроль мер информационной безопасности;

– персонал университета, участвующий в процессах сбора, накопления, систематизации, обработки, передачи, хранения и защиты информации.

3.2 Информационные системы на которые распространяется Политика утверждены приказом ректора «Об утверждении перечня информационных систем персональных данных в ФГБОУ ВО СамГМУ Минздрава России» и указаны в Приложении № 1.

3.3 Перечень персональных данных, обрабатываемых в информационных системах персональных данных ФГБОУ ВО СамГМУ Минздрава России на которые распространяется Политика утверждены приказом ректора «Об утверждении перечня персональных данных обрабатываемых в информационных системах персональных данных и на бумажных носителях» и указаны в Приложении № 2.

3.4. Информационно-технологическую инфраструктуру университета, телекоммуникационное оборудование и каналы связи, обеспечивающие передачу информации между информационными системами и информационное взаимодействие участников информационного обмена представлена в Общей схеме комплексной системе защиты информации ФГБОУ ВО СамГМУ Минздрава России в Приложении № 3.

4. ЦЕЛИ, ЗАДАЧИ И МЕРОПРИЯТИЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

4.1. 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;

4.2. Мероприятия и меры по защите информации должны быть направлены на решение следующих задач:

– исключение утечки информации ограниченного доступа и иной конфиденциальной информации;

– предотвращение несанкционированного доступа к информационным активам и содержащейся в них информации, обнаружение фактов несанкционированного доступа и реагирование на них;

– предотвращение несанкционированной модификации информации, обнаружение фактов несанкционированной модификации и реагирование на них;

– предотвращение несанкционированной подмены информации, обнаружение фактов несанкционированной подмены и реагирование на них;

– предотвращение несанкционированного удаления информации и программного обеспечения, обнаружение фактов несанкционированного удаления и реагирование на них;

– исключение или существенное затруднение отказа в обслуживании авторизованным пользователям информационных активов;

– недопущение использования информационных активов и содержащейся в них информации не по назначению;

– исключение или существенное затруднение нарушения функционирования (работоспособности) информационных систем;

– недопущение распространения с использованием информационных активов противоправной информации;

– обеспечение возможности восстановления доступа авторизованных пользователей к информационным активам и содержащейся в них информации, заблокированной вследствие реализации (возникновения) угроз безопасности информации;

– обеспечение возможности восстановления информации, модифицированной или уничтоженной вследствие реализации (возникновения) угроз безопасности информации.

4.3. Для достижения целей и решения задач защиты информации

должны проводиться следующие мероприятия:

– выявление и оценка угроз безопасности информации;

– контроль конфигураций информационных систем;

– управление уязвимостями;

– управление обновлениями;

– обеспечение защиты информации при обработке, хранении и обращении с информацией ограниченного доступа;

– обеспечение защиты информации при применении конечных устройств;

– обеспечение защиты информации при применении мобильных устройств;

– обеспечение защиты информации при удаленном доступе пользователей к информационным системам;

– обеспечение защиты информации при беспроводном доступе пользователей к информационным системам;

– обеспечение защиты информации при предоставлении пользователям привилегированного доступа к информационным активам;

– обеспечение мониторинга информационной безопасности;

– обеспечение разработки безопасного программного обеспечения;

– обеспечение физической защиты информационных систем;

– обеспечение непрерывности функционирования информационных систем при возникновении нештатных ситуаций;

– повышение уровня знаний и информированности пользователей по вопросам защиты информации;

– обеспечение защиты информации при взаимодействии с подрядными организациями;

– обеспечение защиты от компьютерных атак, направленных на отказ в обслуживании;

– обеспечение защиты информации при использовании искусственного интеллекта;

– реализация в информационных системах мер по их защите и защите содержащейся в них информации;

– проведение контроля уровня защищенности информации, содержащейся в информационных системах.

5. ОСНОВНЫЕ ПРИНЦИПЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Университет определяет следующие основные принципы обеспечения информационной безопасности:

- Осведомленность о риске информационной безопасности. Процессы обеспечения информационной безопасности затрагивают каждого сотрудника университета, использующего его информационные активы, и накладывают на него соответствующие обязанности и ограничения.

- Персональная ответственность. Ответственность за нарушения требований информационной безопасности возлагается непосредственно на сотрудников, допустивших нарушения, и руководителя подразделения, в котором нарушения допущены.

- Минимальность полномочий. Любому сотруднику университета доступ к информационным ресурсам предоставляется только в том объеме, который необходим ему для выполнения служебных обязанностей. Все операции по предоставлению доступа или назначению полномочий осуществляются строго в соответствии с установленными процедурами.

- Комплексность защиты. Меры по обеспечению безопасности информационных активов\ресурсов принимаются по всем идентифицированным видам угроз с учетом результатов оценки рисков информационной безопасности.

- Адекватность защиты. Принимаемые меры обеспечения информационной безопасности эффективны и соразмерны имеющим место рискам информационной безопасности.

- Эргономичность защиты. Средства защиты должны быть максимально “прозрачными” и удобными для пользователей и администраторов автоматизированных систем.

- Документированность. Документирование обеспечивает закрепление достигнутого текущего состояния системы обеспечения информационной безопасности. Любые изменения этого состояния оформляются документально.

- Непрерывность процессов контроля и совершенствования системы обеспечения информационной безопасности. В университете осуществляется постоянный мониторинг и аудит системы обеспечения информационной безопасности, по результатам которых осуществляется анализ эффективности принятых мер обеспечения информационной безопасности с учетом

изменений среды функционирования информационного актива\ресурса, появления новых угроз, инцидентов и проблем, планируются и внедряются дополнительные меры защиты.

- Контроль со стороны руководства. Руководство на регулярной основе рассматривают отчеты о состоянии информационной безопасности в подразделениях университета и фактах нарушений установленных требований, а также общие и частные вопросы информационной безопасности, связанные с использованием технологий повышенного риска или существенно влияющие на бизнес-процессы.

- Целевое финансирование мероприятий по обеспечению информационной безопасности. Ежегодный бюджет университета предусматривает специальные статьи расходов на обеспечение информационной безопасности.

6. Категории лиц, участвующих в защите информации, их обязанности (функции) и полномочия

6.1. Защиту информации организует ректор или по его решению назначенное ответственное лицо в должности не ниже проректора.

6.2. Ректор либо назначенное ответственное лицо определяет отдельных специалистов из числа сотрудников Управления информационной безопасности, на которых возлагаются обязанности (функции) по защите информации. Назначаются ответственные по защите информации по следующим направлениям:

1) ответственного за организацию обеспечения безопасности защищаемой информации, не содержащей сведения, составляющие государственную тайну
2) ответственного за организацию обеспечения безопасности персональных данных
3) ответственного за организацию работ по криптографической защите информации
4) ответственного за создание и проверку электронной подписи в информационной системе
5) ответственных за обнаружение, предупреждению, ликвидации последствий компьютерных атак и реагированию на компьютерные инциденты
6) Ответственного (Администратор) за безопасность информационных

систем

6.3. Обязанности (функции) и полномочия (права) ответственных лиц по защите информации, управлению защитой информации, организации контроля за данной деятельности и обязанности (функции) и полномочия (права) специалистов по защите информации по проведению мероприятий и принятию мер по защите информации определяются в инструкциях (регламентах). К таким инструкциям (регламентам) относятся:

1) Инструкция по обеспечению информационной безопасности
2) Инструкция ответственного за организацию обработки персональных данных
3) Инструкция администратора безопасности информационных систем
4) Инструкция по организации парольной защиты
5) Инструкция по организации антивирусной защиты
6) Инструкция по организации криптографической защиты информации
7) Регламент взаимодействия с Национальным координационным центром по компьютерным инцидентам и.т.д.

Регламенты могут дополняться и корректироваться при изменении обязанностей и полномочий ответственных лиц по защите информации.

6.4. В целях исполнения требований законодательства по защите информации ректором может утверждаться комиссия, по различным видам деятельности, целью которой является защита информации. Состав комиссии утверждается ректором или ответственным лицом в должности не ниже проректора. В составе комиссии должны присутствовать специалисты из Управления информационной безопасности.

6.5. Специалистами управления информационной безопасности должны применяться программные, программно-аппаратные средства, обеспечивающие выполнение возложенных на них обязанностей (функций) по защите информации, в том числе по выявлению угроз безопасности информации, обнаружению и предотвращению вторжений, проведению контроля уровня защищенности информации, содержащейся в информационных системах, мониторингу информационной безопасности информационных систем, выявлению уязвимостей, контролю настроек и конфигураций информационных систем, а также средства и системы, предназначенные для автоматизации и аналитической поддержки деятельности по защите информации.

6.6. По решению ректора или ответственного лица для проведения

мероприятий и принятия мер по защите информации могут привлекаться организации, имеющие лицензию на деятельность по технической защите конфиденциальной информации. Состав проводимых организациями-лицензиатами мероприятий и принимаемых ими мер по защите информации, используемых при этом программных, программно-аппаратных средств, предназначенных для защиты информации, определяется в договорах или иных документах, на основании которых такие организации-лицензиаты привлекаются к защите информации. Специалисты управления информационной безопасности должны осуществлять контроль проводимых организациями-лицензиатами мероприятий и принимаемых ими мер по защите информации.

6.7. Специалисты управления информационной безопасности должны разрабатывать и представлять ректору или ответственному лицу обоснованные предложения по организационным, материально-техническим и иным обеспечивающим ресурсам, необходимым для проведения мероприятий и принятия мер по защите информации, с указанием сведений о целях защиты информации, на достижение которых требуются ресурсы, и перечня негативных последствий (событий), наступление которых прогнозируется в случае отсутствия ресурсов. Ректор или ответственное лицо на основе представленных предложений и в пределах имеющихся средств предусматривает выделение организационных, материально-технических и иных обеспечивающих ресурсов для проведения мероприятий, и принятия мер по защите информации, привлечения при необходимости дополнительных сил и средств для защиты информации.

7. Организация системы обеспечения информационной безопасности

7.1. Общее руководство системой обеспечения информационной безопасности осуществляет руководство университета по следующим направлениям:

– утверждение и пересмотр политики информационной безопасности университета;

– организация процесса управления информационной безопасностью в университете, включая определение подразделений, ответственных за управление отдельными процессами обеспечения информационной безопасности, утверждение положений о них;

– обеспечение условий и утверждение бюджета для эффективной

реализации политики информационной безопасности;

– анализ отчетов о состоянии информационной безопасности

7.2. Деятельность управления по информационной безопасности должно включать:

а) разработку и планирование мероприятий и мер по защите информации;

б) проведение мероприятий и принятие мер по защите информации;

в) проведение оценки состояния защиты информации;

г) совершенствование мероприятий и мер по защите информации.

7.3. Управление информационной безопасности отвечают за реализацию политики информационной безопасности и управление процессами ее обеспечения в рамках своих компетенций. Для этого управление информационной безопасности:

– разрабатывает нормативные, инструктивные и методические документы университета по обеспечению информационной безопасности;

– разрабатывает требования по защите информационных активов в аспектах целостности и конфиденциальности на основе анализа рисков информационной безопасности;

– осуществляет контроль соответствия требованиям на всех стадиях жизненного цикла автоматизированных систем, от проектирования до снятия с эксплуатации;

– обеспечивает управление ключевыми системами средств криптографической защиты;

– организует проведение единой антивирусной политики в университете;

– осуществляет регистрацию информации об инцидентах, имеющих отношение к информационной безопасности;

– проводит расследования инцидентов и фактов нарушений информационной безопасности и информирует руководство о результатах проведенного расследования;

– обеспечивает выполнение требований информационной безопасности при администрировании автоматизированных информационных систем;

– осуществляет инструментальный контроль и мониторинг текущего состояния информационной безопасности;

– регулярно информирует руководство о состоянии информационной безопасности в университете, в том числе, в составе сводных отчетов;

– обеспечивает взаимодействие с уполномоченными государственными органами по вопросам информационной безопасности;

– осуществляет анализ, оценку и прогноз риска, связанного с нарушением информационной безопасности университета.

– обеспечивает доступность информационных ресурсов;

– организует обучение персонала по вопросам информационной безопасности;

– оценивает риски реализации угроз в информационных системах.

7.4. Все подразделения университета

– обеспечивают выполнение требований и процедур информационной безопасности при работе с информационными системами.

– обеспечивают выполнение требований информационной безопасности при работе со средствами криптографической защиты, в том числе со средствами электронной подписи;

– обеспечивают взаимодействие с ответственными сотрудниками управления информационной безопасности при инцидентах информационной безопасности. инциденты ИБ

8. ВИДЫ ИНЦИДЕНТОВ ИБ

8.1. Инциденты ИБ классифицируются:

8.1.1. По типу нарушения:

– Нарушение конфиденциальности — несанкционированный доступ;

– Нарушение целостности — неправомерное изменение данных или систем;

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

8.1.2. По источнику:

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

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

8.1.3. 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.

8.1.4. По умыслу:

– Умышленные;

– Непреднамеренные.

8.2. Порядок выявления инцидентов ИБ и реагирование на них

8.2.1. 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.

8.2.2. 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.

9. ПРАВИЛА ОБРАЩЕНИЯ С КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИЕЙ

9.1. 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.

9.2. 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.

9.3. 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.

10. КОНТРОЛЬ ДОСТУПА

10.1. 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.

10.2. 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.

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

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

10.5. 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».

11. ОРГАНИЗАЦИЯ РАБОТЫ СОТРУДНИКОВ С ИНФОРМАЦИОННЫМИ РЕСУРСАМИ

11.1 При необходимости получения дополнительного доступа к

информационным системам Университета, руководитель структурного подразделения оформляет служебную записку на имя директора Дирекции по цифровой трансформации, в которой указывает необходимый доступ к информационным системам Пользователю в соответствии с его должностными обязанностями и направляет через HelpDesk или по электронной почте.

11.2 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 Дирекции по цифровой трансформации, 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.

12. ОРГАНИЗАЦИЯ РАБОТЫ СОТРУДНИКОВ С ЭП

12.1. 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».

12.2. 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 ДЦТ для формирования запроса на изготовление ЭП.

12.3. 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».

13. ПАРОЛЬНАЯ ПОЛИТИКА

13.1. 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.

13.2 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.).

13.3 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».

14. АНТИВИРУСНАЯ ЗАЩИТА

14.1. 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.

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

14.3. Антивирусная защита информационных ресурсов осуществляется Управлением информационной безопасности ДЦТ. Для этой цели используется антивирусное программное обеспечение корпоративного класса, имеющее 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.

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

15. ЗАЩИТА ОТ НСД

15.1. 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.

15.2. Подключение АРМ к сети ФГБОУ ВО СамГМУ Минздрава России происходит путём добавления MAC-адресов на порты телекоммуникационного оборудования. Подключение сторонних устройств блокируется автоматически.

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

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

15.5. 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.

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

15.7. 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;

15.8. 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.

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

15.10. 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».

16. ПРОФИЛАКТИКА НАРУШЕНИЙ ПОЛИТИКИ

16.1. 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.

16.2. 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.

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

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

17. ОЦЕНКА ВРЕДА

17.1 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.

17.2 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.

17.3 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.

18. ЛИКВИДАЦИЯ ПОСЛЕДСТВИЙ НАРУШЕНИЯ ПОЛИТИКИ

18.1. 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.

18.2. 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/).

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

19 ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ ПОЛИТИКИ

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

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

19.3 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 информационных технологий ДЦТ.

Приложение к политике № 1
от «___» _____2026 г. № ____

Список информационных систем в которых осуществляется защита информации:

1. 1С: Предприятие;
2. Электронная информационно-образовательная среда (ЭИОС);
3. PACS «Луч-С»;
4. Автоматизированная система управления учебным процессом «ТАНДЕМ. УНИВЕРСИТЕТ;
5. Система контроля управления доступом (СКУД);
6. Цифровая экосистема (Единая точка входа);
7. Инновационная инфраструктура СамГМУ.

Приложение к политике № 2
от «___» _____2026 г. № ____

Перечень персональных данных, обрабатываемых в информационных системах персональных данных и государственных информационных системах ФГБОУ ВО СамГМУ Минздрава России

№ п/п	Содержание сведений	Категория персональных данных	Условия обработки	Срок хранения
Цель обработки персональных данных: ведение бухгалтерского и кадрового учета (**«1С: Предприятие»)**				
1.	*Сотрудники, обучающиеся, субъекты не являющиеся сотрудниками оператора:* ФИО; дата рождения; пол; адрес проживания; контактные телефоны; данные документа, удостоверяющего личность; ИНН; должность; реквизиты трудового договора; номер расчетного счета; стаж работы; сведения о трудовой деятельности; сведения о составе семьи; сведения о воинском учете; сведения о повышении квалификации; сведения о наградах (поощрениях); размер оклада; сведения о наличии (отсутствии) судимости; медицинские сведения.	*Специальные, иные*	*Условия обработки ПДн:* - обработка персональных данных необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем, по которому является субъект персональных данных, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем; - обработка персональных данных необходима для достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения возложенных законодательством Российской Федерации на ФГБОУ ВО СамГМУ Минздрава России функций, полномочий и обязанностей; - обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных.	По достижению целей обработки
Цель обработки персональных данных: Обеспечение доступа к информационным и образовательным ресурсам «Электронная информационно-образовательная среда» (**«ЭИОС»**)				
2.	*Сотрудники, обучающиеся:* ФИО; электронная почта.	*Иные*	*Условия обработки ПДн:* - обработка персональных данных необходима для достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения возложенных законодательством Российской	По достижению целей обработки

№ п/п	Содержание сведений	Категория персональных данных	Условия обработки	Срок хранения
			Федерации на ФГБОУ ВО СамГМУ Минздрава России функций, полномочий и обязанностей; - обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных; - обработка персональных данных, разрешенных субъектом персональных данных для распространения, осуществляется с соблюдением запретов и условий, предусмотренных статьей 10.1 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».	
Цель обработки персональных данных: оказание медицинских услуг **(«PACS луч-с»)**				
3.	*Пациенты:* ФИО; дата рождения; пол; сведения о состоянии здоровья; медицинские снимки	*Специальные, иные*	*Условия обработки ПДн:* - обработка персональных данных необходима для достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения возложенных законодательством Российской Федерации на ФГБОУ ВО СамГМУ Минздрава России функций, полномочий и обязанностей; - обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных.	По достижению целей обработки
Цель обработки персональных данных: Электронный документооборот **(«Тандем»)**				
4.	*Сотрудники:* ФИО; адрес проживания; контактные телефоны (или иной вид связи); данные документа, удостоверяющего личность; сведения об образовании; должность *Обучающиеся:* ФИО; дата рождения;	*Специальные* *Иные*	*Условия обработки ПДн:* - обработка персональных данных необходима для достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения возложенных законодательством Российской Федерации на ФГБОУ ВО СамГМУ Минздрава России функций,	По достижению целей обработки

№ п/п	Содержание сведений	Категория персональных данных	Условия обработки	Срок хранения
	данные документа, удостоверяющего личность; номер расчетного счета; сведения об образовании; сведения о сдаче квалификационного экзамена; результаты ЕГЭ; сведения о наличии инвалидности		полномочий и обязанностей; - обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных;	
Цель обработки персональных данных: Организация пропускного режима Система контроля и управления доступом (**«СКУД»**)				
5.	*Сотрудники:* ФИО; Фотография, используется для установления личности; *Обучающиеся:* ФИО*;* Фотография, используется для установления личности *Пациенты:* ФИО; Фотография, используется для установления личности	*Иные,* *Биометрические*	*Условия обработки ПДн:* - обработка персональных данных необходима для достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения возложенных законодательством Российской Федерации на ФГБОУ ВО СамГМУ Минздрава России функций, полномочий и обязанностей; - обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных;	
Цель обработки персональных данных: оказание медицинских и иных услуг населению **Инновационная инфраструктура СамГМУ**				
6.	*Пациенты:* ФИО; дата рождения; возраст; место рождения; пол; гражданство; адрес регистрации; дата регистрации по месту жительства; данные документа, удостоверяющего личность; СНИЛС; Полис ОМС; сведения о состоянии здоровья; сведения о заболевании; сведения о наличии инвалидности; медицинские снимки; категория льготы;	*Специальные* *Иные*	*Условия обработки ПДн:* - обработка персональных данных осуществляется в медико-профилактических целях, 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; - обработка персональных данных	В соответствии с номенклатурой дел

№ п/п	Содержание сведений	Категория персональных данных	Условия обработки	Срок хранения
	иные сведения, необходимые в целях оказания медицинских услуг; иные сведения, необходимые в соответствии с законодательством в сфере здравоохранения		осуществляется с согласия субъекта персональных данных на обработку его персональных данных.	
Цель обработки персональных данных: Цифровая экосистема (Единая точка входа);				
7.	*Сотрудники* *Обучающиеся* *Лица, не являющиеся сотрудниками:* ФИО; e-mail; дата рождения; пол; адрес регистрации; контактный телефон; данные документа, удостоверяющего личность; СНИЛС; должность; реквизиты трудового договора; стаж работы; сведения о воинском учете; сведения о повышении квалификации; сведения о наградах (поощрениях); сведения об образовании; сведения о сдаче квалификационного экзамена;	*Иные*	*Условия обработки ПДн:* - обработка персональных данных необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем, по которому является субъект персональных данных, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем; - обработка персональных данных необходима для достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения возложенных законодательством Российской Федерации на ФГБОУ ВО СамГМУ Минздрава России функций, полномочий и обязанностей; - обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных.	По достижению целей обработки