Документ подписан электронной подписью.

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Самарский государственный медицинский университет»

Министерства здравоохранения Российской Федерации

«ПРИНЯТО»:	«УТВЕРЖДАЮ»:
Решением	Ректор ФГБОУ ВО СамГМУ
Учёного Совета ФГБОУ ВО	Минздрава России,
СамГМУ Минздрава России	профессор РАН
протокол № 8	А.В. Колсанов
от «30» апреля 2021 г.	Приказ № 148 от «31» мая 2021 г.

ПОЛОЖЕНИЕ
О ПОЛИТИКЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Самара – 2021

Термины, сокращения и обозначения

В настоящем Положении используются следующие сокращения:
ФГБОУ ВО СамГМУ Минздрава России, Университет – Федеральное государственное бюджетное образовательное учреждение высшего образования «Самарский государственный медицинский университет» Министерства здравоохранения Российской Федерации;
ИЦР – Институт цифрового развития;
ЦИБ – Центр 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;
САВЗ - Средство антивирусной защиты информации;
ПДн – Персональные данные;

В настоящем Положении используются следующие определения:
Автоматизированное рабочее место - совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем;
Автоматизированная система – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций;
Авторизация – предоставление субъекту прав на доступ, а также предоставление доступа в соответствии с установленными правами на доступ;
Аутентификация – проверка принадлежности субъекту доступа предъявленного им идентификатора, подтверждение подлинности;
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.

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 Университета;

Информационная система (ИС) – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;

Информационный процесс – процессы сбора, обработки, накопления, хранения, поиска и распространения информации;

Информационный ресурс – 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;

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.

Нормативные ссылки

Настоящее Положение разработано в соответствии с:

- Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи»;
- Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»;
- Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- 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 03.11.1994 № 1253 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти»;
- 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».

1. ОБЩИЕ ПОЛОЖЕНИЯ

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.

1.2. Требования, изложенные в Политике, являются обязательными для выполнения всеми работниками Университета, при этом срочность и важность выполняемых работ не должны являться основанием для нарушения положений настоящей Политики и других документов, регламентирующих в Университете вопросы обеспечения ИБ.

1.3. Ответственность за организацию обработки персональных данных и защищаемой информации, не содержащей сведения, составляющие государственную тайну несет уполномоченное лицо Университета, назначенное приказом ректора.

1.4. Ответственность за организацию обеспечения безопасности персональных данных и защищаемой информации, не содержащей сведения, составляющие государственную тайну несет уполномоченное лицо Университета, назначенное приказом ректора.

1.5. Проректора, руководители структурных подразделений и заведующие кафедр организуют и обеспечивают выполнение требований ИБ в своих структурных подразделениях.

1.6. Работники обязаны соблюдать порядок обращения с конфиденциальными документами, носителями ключевой информации и другой защищаемой информации, соблюдать требования настоящей Политики и других документов по ИБ.

1.7. Актуализация Политики производится в обязательном порядке в следующих случаях:

а) при изменении политики Российской Федерации в области информационной безопасности, указов и законов Российской Федерации в области защиты информации;

б) при изменении внутренних нормативных документов (инструкций, положений, руководств), касающихся ИБ Университета;

в) при выявлении инцидента (инцидентов) по нарушению ИБ, влекущего ущерб для Университета.

2. ЦЕЛЬ ПОЛИТИКИ

2.1. Основной целью, на достижение которой направлены все положения настоящей 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;

2.2. Политика направлена на защиту информационных активов от угроз, исходящих от противоправных действий злоумышленников, уменьшение рисков и снижение потенциального вреда от аварий, непреднамеренных ошибочных действий работников, технических сбоев, неправильных технологических и организационных решений в процессах обработки, передачи и хранения информации и обеспечение нормального функционирования технологических процессов.

3. ЗАДАЧИ ПОЛИТИКИ

3.1. Описание организации системы управления ИБ Университета;

3.2. Определение частных политик ИБ, а именно:

а) политики реализации антивирусной защиты;

б) политики учетных записей;

в) политики предоставления доступа к информационному ресурсу;

г) парольной политики;

д) политики защиты АРМ;

е) политики конфиденциального делопроизводства;

3.3. Определение порядка сопровождения ИС Университета.

4. ОСНОВНЫЕ ПРИНЦИПЫ ОБЕСПЕЧЕНИЕ ИБ

Основными принципами обеспечения ИБ в Университете являются:

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

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

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

г) контроль эффективности принимаемых защитных мер:

д) персонификация и адекватное разделение ролей и ответственности между работниками Университета исходя из принципа персональной и единоличной ответственности за совершаемые операции.

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 ознакомления с настоящей Политикой, а также инструкцией по информационной безопасности.

Правила допуска к работе с информационными ресурсами лиц, не являющихся работниками Университета, определяются на основе договоров, заключенных с этими лицами или с организациями, представителями которых являются эти лица.

6. ЗАЩИЩАЕМЫЕ ИНФОРМАЦИОННЫЕ РЕСУРСЫ УНИВЕРСИТЕТА

6.1. Различаются следующие категории информационных ресурсов, подлежащих защите в Университете:

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

6.1.2. Открытая информация - информация, полученная от физических или юридических лиц, запрет на распространение и обработку которой был ими официально снят; информация, сформированная в результате деятельности Университета, которую запрещено относить к конфиденциальной на основании законодательства Российской Федерации; информация, представляемая в публичный доступ, используемая в хозяйственной деятельности Университета.

6.1.3. Информация ограниченного доступа - не содержащая сведений, составляющих государственную тайну (конфиденциальная информация) – это информация, доступ к которой ограничен федеральными законами.

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.

Для этого в Университете выполняются следующие мероприятия:

а) определяется порядок работы с документами, образцами, изделиями и другими источниками данных;

б) устанавливается круг лиц и порядок доступа к информации;

в) вырабатываются меры по контролю обращения с документами, содержащими конфиденциальные данные;

г) с работниками заключаются соглашения о неразглашении конфиденциальных сведений.

6.4. Защита конфиденциальной информации, принадлежащей третьей стороне, осуществляется на основании договоров, заключаемых Университетом с данными лицами и организациями.

7. ОРГАНИЗАЦИЯ СИСТЕМЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ УНИВЕРСИТЕТА

7.1. Система управления информационной безопасностью Университета предназначена для создания, реализации, эксплуатации, мониторинга, анализа, поддержки и повышения ИБ Университета.

Для успешного функционирования Системы ИБ Университета должны быть реализованы следующие процессы:

а) определение и уточнение области действия Системы ИБ и выбор подхода к оценке рисков ИБ (определение и уточнение области действия Системы ИБ должно осуществляться на основе результатов оценки рисков, связанных с основной деятельностью Университета, а также оценки правовых рисков деятельности Университета);

б) анализ и оценка рисков ИБ, варианты обработки рисков ИБ для наиболее критичных информационных активов;

в) выбор и уточнение целей ИБ и защитных мер и их обоснование для минимизации рисков ИБ;

г) реализация системы управления ИБ.

7.2. В зависимости от специфики процесса его реализация осуществляется с соблюдением следующих этапов:

а) на этапе планирования определяется политика и методология управления рисками, а также выполняется оценка рисков, включающая в себя инвентаризацию активов, составление профилей угроз и уязвимостей, оценку эффективности контрмер и потенциального ущерба, определение допустимого уровня остаточных рисков;

б) на этапе реализации производится обработка рисков и внедрение механизмов контроля, предназначенных для их минимизации; Университетом принимается одно из четырех решений по каждому идентифицированному риску: проигнорировать, избежать, передать внешней стороне, минимизировать: после этого разрабатывается и внедряется план обработки рисков.

в) на этапе проверки отслеживается функционирование механизмов контроля, контролируются изменения факторов риска (активов, угроз, уязвимостей), проводятся аудиты и выполняются различные контролирующие

процедуры.

г) на этапе действия по результатам непрерывного мониторинга и проводимых проверок выполняются необходимые корректирующие мероприятия, которые могут включать в себя, в частности, переоценку величины рисков, корректировку политики и методологии управления рисками, а также плана обработки рисков.

8. ОЦЕНКА ИНФОРМАЦИОННЫХ РИСКОВ

8.1. Оценка информационных рисков Университета выполняется по следующим основным принципам:

а) идентификация и количественная оценка информационных ресурсов, значимых для работы Университета;

б) оценивание возможных угроз;

в) оценка существующих уязвимостей;

г) оценка эффективности средств обеспечения информационной безопасности.

При этом информационные риски зависят от:

а) показателей ценности информационных ресурсов:

б) вероятности реализации угроз для ресурсов;

в) эффективности существующих или планируемых средств обеспечения информационной безопасности.

8.2. Цель оценки рисков состоит в определении характеристик рисков информационной системы и ее ресурсов.

8.3. В результате оценки рисков становится возможным выбрать средства, обеспечивающие желаемый уровень информационной безопасности Университета.

9. ЧАСТНАЯ ПОЛИТИКА ПРЕДОСТАВЛЕНИЯ ДОСТУПА К ИНФОРМАЦИОННЫМ РЕСУРСАМ

9.1. Частная политика предоставления доступа к информационному ресурсу определяет основные правила предоставления работникам доступа к защищаемым информационным ресурсам Университета.

9.2. Права на информационные ресурсы, разработанные работниками в соответствии с трудовыми функциями, подрядчиками и иными контрагентами, если данное условие закреплено в договоре, принадлежат Университету.

Любое размещение таких информационных ресурсов в сетях общего пользования, в том числе Интернет, без письменного согласования с ректором Университета или уполномоченным им лицом ЗАПРЕЩЕНО.

9.3. Каждому работнику Университета, допущенному к работе с конкретным информационным ресурсом, должно быть предоставлено персональное уникальное имя (учетная запись пользователя), под которым он

будет регистрироваться и работать в ИС.

В случае необходимости некоторым работникам могут быть представлены несколько уникальных имен (учетных записей). Использование несколькими работниками при работе в Университете одного и того же имени пользователя («группового имени») ЗАПРЕЩЕНО.

За создание, выдачу, изменение и приостановку действия Учетной записи отвечает Управление информационных технологий.

9.4. Предоставление (или изменение) прав доступа пользователя к учетным системам и ресурсам Университета, осуществляется на основании Положения об организации работы сотрудников с информационными ресурсами ФГБОУ ВО СамГМУ Минздрава России.

9.5. При прекращении срока действия полномочий пользователя (окончание договорных отношений, увольнение работника) учетная запись блокируется на следующий день с момента окончания договорных отношений автоматически во всех информационных системах.

9.6. В случае выявления передачи пароля третьим лицам или при обнаружении действий пользователя, которые могут привести к причинению прямого или косвенного ущерба Университету, уполномоченный работник УИТ приостанавливает действие учетной записи пользователя.

9.7. Перечень сервисов Университета, в которых в соответствии со ст. 9 Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи» для обеспечения идентификации и аутентификации пользователей применяется простая электронная подпись:

9.7.1. 1С: Предприятие. Бухгалтерия государственного учреждения;
9.7.2. 1С: Предприятие. Кадры;
9.7.3. ЕМИАС Самарской области;
9.7.4. Контур ФМС;
9.7.5. ЕИОС;
9.7.6. PACS луч-с;
9.7.7. АИС ВМП;
9.7.8. АИС Смертность;
9.7.9. ГИС СО «РМС»;
9.7.10. ФИС ГИА и приема;
9.7.11. Госуслуги. Суперсервис поступления в ВУЗ Онлайн;
9.7.12. Асулон «М-Аптека»;
9.7.13. Тандем;
9.7.14. ГИС СО «Кадры медицинских учреждений»;
9.7.15. ГИС СО «Паспорт медицинского учреждения»;
9.7.16. Федеральный Регистр сахарного диабета;
9.7.17. СУФД;
9.7.18. ГИС ОМС;
9.7.19. ФИС ФРДО;
9.7.20. ФРМР (Федеральный регистр медицинских работников);
9.7.21. ЕГИСЗ;

9.7.22. ИС ЦАМИ СО;
9.7.23. Корпоративная почта;

10. ЧАСТНАЯ ПОЛИТИКА УЧЕТНЫХ ЗАПИСЕЙ

10.1. Политика учетных записей определяет основные правила присвоения
учетных записей пользователям информационных систем Университета.

Виды учетных записей подразделяются на:

а) пользовательские, предназначенные для идентификации и аутентификации пользователей информационных активов Университета;

б) системные, используемые для нужд операционной системы;

в) служебные, предназначенные для обеспечения функционирования отдельных процессов или приложений.

10.2. После активации учетной записи пользователю доступен функционал ИС в рамках должностных обязанностей работника Университета и академических прав и обязанностей, обучающихся Университета.

11. ЧАСТНАЯ ПАРОЛЬНАЯ ПОЛИТИКА

11.1. Настоящая Политика определяет основные правила обращения с паролями, используемыми для доступа к защищаемым информационным системам Университета.

11.2 Пароли учетных записей пользователей должны соответствовать следующим требованиям безопасности:

- длина пароля должна быть не менее 8 (восьми) символов;
- пароль должен содержать цифровые символы и буквенные символы латиницы в верхнем и нижнем регистрах;
- при смене пароля новое значение должно отличаться от предыдущего не менее чем в 4 (четырех) позициях;
- пароль не может содержать имя учетной записи пользователя или его часть;
- пароль должен включать в себя:
  - буквы нижнего регистра;
  - буквы верхнего регистра;
  - десятичные цифры (от 0 до 9);
  - специальные символы (!, $, #, % и т.п.);
- запрещается использовать в качестве пароля имя входа в систему, простые пароли типа «123», «111», «qwerty» и им подобные, общепринятые сокращения (ЭВМ, USER, PASSWORD и т.п.), а также имена и даты рождения своей личности и своих родственников, номера автомобилей, телефонов и

другие пароли, которые можно угадать, основываясь на информации о пользователе;

- запрещается использовать в качестве пароля один и тот же повторяющийся символ либо повторяющуюся комбинацию из нескольких символов (например, «аааааааа»);

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

- запрещается использовать пароль домена локальной вычислительной сети (вводится при загрузке ЭВМ) для входа в иные автоматизированные информационные системы;

- запрещается выбирать пароли, которые уже использовались ранее.

- пользователь обязан хранить в тайне свои личные пароли;

- пользователю запрещается передавать любые пароли и доступы третьим лицам, ставшие ему известными в рамках исполнения должностных обязанностей.

11.3. В целях обеспечения информационной безопасности и противодействия попыткам подбора пароля, после пяти неудачных попыток ввода пароля, учётная запись блокируется. Для разблокировки учетной записи необходимо оформить служебную записку на имя начальника центра системного администрирования и развития локально-вычислительных сетей.

11.4. Требования к процессам работы со средствами криптографической защиты информации на съемных (отчуждаемых) носителях устанавливаются в соответствии с утвержденными инструкциями.

12. ЧАСТНАЯ ПОЛИТИКА РЕАЛИЗАЦИИ АНТИВИРУСНОЙ ЗАЩИТЫ

12.1. Настоящая Политика определяет основные правила для реализации антивирусной защиты в Университете.

12.2. Основным способом защиты информации от воздействия компьютерных вирусов на АРМ является применение средств антивирусной защиты (далее — САВЗ). К использованию в ФГБОУ СамГМУ Минздрава России допускаются только лицензионные антивирусные средства, централизованно закупленные Управлением информационных технологий у разработчиков (поставщиков) указанных средств, рекомендованные к применению Центром информационной безопасности.

12.3. Антивирусная защита ИР осуществляется Центром информационной безопасности. Для этой цели используется антивирусное программное обеспечение корпоративного класса, имеющая сервер централизованного администрирования и программы-агенты для установки на сервера и персональные компьютеры, обеспечивающие централизованный мониторинг и управление антивирусом. Антивирусному контролю подлежит

любая информация, поступающая на персональные компьютеры Пользователей, в том числе из Интернета и с внешних носителей.

12.4. Обновление антивирусных баз на рабочих станциях и серверах ФГБОУ ВО СамГМУ Минздрава России производится автоматически, ежечасно, с серверов обновления разработчика антивируса или с сервера антивирусной защиты.

12.5. Контроль исходящей информации должен проводиться Пользователями непосредственно перед архивированием (записью на съемный носитель) в целях подготовки информации к отправке во внешние источники, либо непосредственно перед отправкой по электронной почте.

В случае обнаружения зараженных компьютерными вирусами файлов Пользователь **обязан**:

- приостановить работу;

- поставить в известность о факте обнаружения зараженных вирусом файлов Центр информационной безопасности (телефон: 8 (846) 374-00-66 (вн.: 4729, 4732, 4745), эл. почта: cib@samsmu.ru, либо через систему Lan заявок);

- совместно с Центром информационной безопасности и Центром САиРЛВС провести анализ зараженных вирусом файлов.

13. ЧАСТНАЯ ПОЛИТИКА ЗАЩИТЫ АРМ

13.1. Настоящая Политика определяет основные правила и требования по защите персональных данных и иной конфиденциальной информации Университета от неавторизированного доступа, утраты или модификации.

13.2. Во время работы с конфиденциальной информацией должен предотвращаться ее просмотр не допущенными к ней лицами.

13.3. Несанкционированное использование печатающих, факсимильных, копировально-множительных аппаратов и сканеров должно предотвращаться путем их размещения в помещениях с ограниченным доступом, использования паролей или иных доступных механизмов разграничения доступа.

13.4. Пользователи получают доступ к ресурсам вычислительной сети после ознакомления с настоящей Политикой, иными документами по обеспечению ИБ и перечнями конфиденциальной информации.

13.5. Конечным пользователям предоставляется доступ только к тому функционалу, который необходим для выполнения их должностных обязанностей.

13.6. Доступ к информации предоставляется только лицам, имеющим обоснованную необходимость в работе с этими данными для выполнения своих должностных обязанностей.

13.7. Локальное техническое обслуживание должно осуществляться при личном присутствии пользователя.

13.8. Все компьютерное оборудование: серверы, стационарные и

портативные компьютеры; периферийное оборудование: принтеры, сканеры, МФУ; аксессуары: манипуляторы типа «мышь», дисководы для оптических дисков; коммуникационное оборудование: сетевые адаптеры, коммутаторы, концентраторы, шлюзы (далее – Компьютерное оборудование), предоставленное пользователю для выполнения его служебных обязанностей, является собственностью ФГБОУ ВО СамГМУ Минздрава России и предназначено для использования исключительно в производственных целях. Каждый сотрудник, получивший в пользование портативный компьютер, обязан принять надлежащие меры по обеспечению его сохранности. Каждый стационарный компьютер, ноутбук или неттоп, принадлежащий организации, должен находиться в домене ФГБОУ ВО СамГМУ Минздрава России. Каждый пользователь должен обладать собственной и уникальной учетной записью в домене.

13.9 Программное обеспечение должно устанавливаться со специальных ресурсов или съемных носителей и в соответствии с лицензионным соглашением с его правообладателем.

14. ЧАСТНАЯ ПОЛИТИКА СОПРОВОЖДЕНИЯ ИС

14.1. ИБ должна обеспечиваться на всех стадиях жизненного цикла ИС:
а) разработка;
б) пилотная эксплуатация;
в) промышленная эксплуатация;
г) архивная копия.

14.2. Разработка технических заданий, проектирование, создание, тестирование, приемка средств и систем защиты ИС проводятся при участии уполномоченных работников Центра информационной безопасности. Порядок разработки и внедрения ИС должен быть регламентирован и контролироваться.

14.3. Ввод в действие, эксплуатация, снятие с эксплуатации ИС в части вопросов ИБ должны осуществляться при участии уполномоченных работников Центра информационной безопасности.

14.4. На стадиях, связанных с разработкой ИС (определение требований заинтересованных сторон, анализ требований, архитектурное проектирование, реализация, интеграция и верификация, поставка, ввод в действие), разработчиком должна быть обеспечена защита от угроз:

а) неверной формулировки требований к ИС;

б) выбора некорректной модели жизненного цикла ИС, в том числе

в) некорректного выбора процессов и вовлеченных в них участников;

г) принятия неверных проектных решений;

д) внесения разработчиком дефектов на уровне архитектурных решений;

е) неполной, противоречивой и некорректной реализации требований к ИС;

ж) разработки некачественной документации;

3) установки ИС разработчиком/производителем с нарушением

требований, что приводит к появлению недокументированных возможностей в ИС либо к неадекватной реализации требований;

и) неверного конфигурирования ИС;

к) приемки ИС, не отвечающей требованиям заказчика.

Привлекаемые для разработки средств и систем защиты ИС на договорной основе физические и юридические лица должны иметь все необходимые разрешения на данный вид деятельности в соответствии с законодательством Российской Федерации.

14.5. При приобретении готовых ИС и их компонентов разработчиком должна быть предоставлена документация, в том числе содержащая описание защитных мер, предпринятых разработчиком в отношении угроз ИБ.

Также разработчиком должна быть представлена документация, содержащая описание защитных мер, предпринятых разработчиком ИС и их компонентов относительно безопасности разработки, безопасности поставки, эксплуатации, поддержки жизненного цикла, включая описание модели жизненного цикла, оценки уязвимости.

В договор (контракт) о приобретении ИС и их компонентов рекомендуется включать положения по сопровождению поставляемых изделий на весь срок их службы.

В случае невозможности включения в договор (контракт) указанных требований к разработчику должна быть рассмотрена возможность приобретения полного комплекта рабочей конструкторской документации на изделие, обеспечивающее возможность сопровождения ИС и их компонентов без участия разработчика.

14.6. На стадии эксплуатации должна быть обеспечена защита от следующих угроз:

а) умышленное несанкционированное раскрытие, модификация или уничтожение информации;

б) неумышленная модификация или уничтожение информации:

в) недоставка или ошибочная доставка информации;

г) отказ в обслуживании или ухудшение обслуживания.

14.7 На стадии сопровождения должна быть обеспечена защита от угроз:

а) внесения изменений в ИС, приводящих к нарушению ее функциональности

либо к появлению недокументированных возможностей:

б) невнесения разработчиком/поставщиком изменений, необходимых для поддержки правильного функционирования и правильного состояния ИС.

14.8 На стадии снятия с эксплуатации должно быть обеспечено удаление информации, несанкционированное использование которой может нанести ущерб Университету, и информации, используемой средствами обеспечения ИБ, из постоянной памяти ИС или с внешних носителей.

14.9 Требования ИБ должны включаться во все договоры (контракты) на проведение работ или оказание услуг, связанных с обслуживанием ИС, на всех стадиях жизненного цикла ИС.

15. ПРОФИЛАКТИКА НАРУШЕНИЙ ПОЛИТИКИ

15.1. 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 с точностью до периода тестирования.

Контрольное тестирование функций СЗИ может быть частичным или полным и должно проводиться с установленной в ИС Университета степенью периодичности.

15.2. 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.

Администратор ИБ (возможно, при помощи сторонней организации, специализирующейся в области информационной безопасности) собирает и анализирует информацию о выявленных уязвимых местах в составе операционных
систем и/или программного обеспечения относительно ИС Университета.

Источниками подобного рода сведений могут служить официальные издания и публикации различных компаний, объединений и других организаций, специализирующихся в области защиты информации.

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

Плановая и внеплановая разъяснительная работа по правилам настоящей политики, а также инструктаж работников/обучающихся Университета по соблюдению требований нормативных и регламентных документов по информационной безопасности, принятых в Университете, проводится при пересмотре настоящей Политики и/или при возникновении инцидента нарушения правил Политики.

16. ЛИКВИДАЦИЯ ПОСЛЕДСТВИЙ НАРУШЕНИЯ ПОЛИТИКИ

16.1. 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.

16.2. 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 Центра информационной безопасности (телефон: 8 (846) 374-00-66 (вн.: 4729, 4732, 4745), эл. почта: cib@samsmu.ru, либо через систему Lan заявок).

После устранения инцидента УЦТ составляет акт о факте нарушения и принятых мерах по восстановлению работоспособности ИС, а также регистрирует факт нарушения в журнале учета нарушений, ликвидации их причин и последствий.

17. ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ ПОЛИТИКИ

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

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

17.3 Ответственность за реализацию Политики в части, касающейся разработки и актуализации правил внешнего доступа и управления доступом, антивирусной защиты - возлагается на Центр информационной безопасности и Центр САиРЛВС.

Приложение А
Перечень сведений конфиденциального характера в ФГБОУ ВО СамГМУ Минздрава России

1. Сведения об обучающемся и/или поступающем, позволяющие идентифицировать его личность (персональные данные):
1.1 фамилия, имя, отчество;
1.2 пол:
1.3 дата рождения:
1.4 место рождения;
1.5 гражданство, подданство:
1.6 серия и номер основного документа, удостоверяющего личность: сведения о дате выдачи указанного документа и выдавшем его органе;
1.7 состав семьи:
1.8 адрес регистрации по месту жительства, домашний и мобильный телефон, а также адрес личной электронной почты;
1.9 результаты Единого государственного экзамена / вступительных испытаний, проводимых в ФГБОУ ВО СамГМУ самостоятельно;
1.10 материалы вступительных испытаний:
1.11 номер учебной группы;
1.12 основа обучения (источник финансирования);
1.13 форма обучения;
1.14 факультет/институт, направление подготовки/специальность, направленность (профиль/специализация);
1.15 текущая и итоговая успеваемость;
1.16 сведения о воинском учете (для военнообязанных и лиц, подлежащих призыву на военную службу);
1.17 сведения о законных представителях;
1.18 сведения в медицинской справке о прохождении медицинского осмотра (медицинской книжке), если это требуется в связи с прохождением обучения;
1.19 сведения о документе о предыдущем уровне образования;
1.20 номер страхового индивидуального лицевого счета;
1.21 сведения о дисциплинарных взысканиях;
1.22 сведения о социальных льготах, которые предоставляются в соответствии с законодательством Российской Федерации, а также коллективными договорами и локальными нормативными актами Университета;
1.23 иные сведения, являющиеся персональными данными.
2. Сведения о работнике образовательной организации, позволяющие идентифицировать его личность (персональные данные):
2.1 фамилия, имя, отчество;
2.2 пол
2.3 дата рождения;
2.4 место рождения;
2.5 гражданство, подданство:

2.6 серия и номер основного документа, удостоверяющего личность: сведения о дате выдачи указанного документа и выдавшем его органе;
2.7 идентификационный номер налогоплательщика:
2.8 номер страхового свидетельства государственного пенсионного страхования;
2.9 сведения о номере, дате выдачи страхового медицинского полиса и страховой компании, выдавшей его:
2.10 образование, специальность, квалификация, сведения о документе об образовании;
2.11 ученая степень, ученое звание:
2.12 стаж работы;
2.13 предыдущее место работы;
2.14 семейное положение:
2.15 состав семьи:
2.16 адрес регистрации по месту жительства, домашний телефон и мобильный телефон, а также адрес личной электронной почты;
2.17 сведения о воинском учете (для военнообязанных и лиц, подлежащих призыву на военную службу):
2.18 сведения о заработной плате;
2.19 сведения, содержащиеся в документах, подтверждающие право на дополнительные гарантии и компенсации по определенным основаниям (об инвалидности, о беременности и т.д.):
2.20 сведения о дисциплинарных взысканиях:
2.21 сведения о социальных льготах, которые предоставляются в соответствии с законодательством Российской Федерации, а также коллективными договорами и локальными нормативными актами Университета:
2.22 любые иные сведения, с которыми работник считает нужным ознакомить работодателя или в предоставлении которых работодателю возникла необходимость.
3. Тестовые задания и контрольные измерительные материалы для оценки уровня учебных достижений обучающихся, содержащиеся в банке тестовых заданий, за исключением переведенных в установленном порядке в открытый доступ, текущего календарного года на бумажных и электронных носителях.
4. Сведения о сущности изобретения, полезной модели или промышленного образца до момента официального опубликования информации о них образовательной организацией.
5. Сведения, содержащие информацию о прохождении и решениях, принимаемых на промежуточных этапах рассмотрения аттестационных дел работников.
6. Сведения, содержащие данные по результатам внутреннего и внешнего контроля объемов и качества образовательных услуг и служебным проверкам.
7. Сведения о финансовых операциях до момента их официального опубликования.
8. Сведения о состоянии банковских счетов до момента их официального

опубликования.
9. Сведения о планах закупок и инвестициях до момента их официального опубликования.
10. Сведения относительно оборудования помещений охранной и пожарной сигнализацией и места ее установления.
11. Сведения об объемах поступающих средств (из бюджета, из внебюджетных фондов, от предпринимательской деятельности, от спонсоров и жертвователей) до момента их официального опубликования.
12. Сведения о деятельности комиссий по осуществлению конкурентных закупок.
13. Сведения, раскрывающие содержание плана гражданской обороны образовательной организации.
14. Сведения, раскрывающие вопросы защиты образовательной организации от чрезвычайных ситуаций техногенного характера \ террористической деятельности.
15. Другие сведения, связанные с деятельностью образовательной организации, которые не составляют государственную тайну, и разглашение которых может привести к причинению вреда образовательной организации, повлечь материальный, нематериальный и репетиционный ущерб.