Приложение №1 к приказу № 56 от 27 марта 2026 г.

УТВЕРЖДАЮ
Директор ГАПОУ РК «Петрозаводский базовый медицинский колледж»
Е.И. Аксентьева
27 марта 2026 г.

ПОЛИТИКА
защиты информации
в ГАПОУ РК «Петрозаводский базовый медицинский колледж»

1. Общие положения

1.1. Настоящая Политика защиты информации (далее – Политика) определяет систему организационных и технических мер по защите информации, обрабатываемой в информационных системах и информационно-телекоммуникационной инфраструктуре ГАПОУ РК «Петрозаводский базовый медицинский колледж» (далее – Колледж).

1.2. Основной задачей в области защиты информации Колледж признает совершенствование мер и средств обеспечения оптимального уровня информационной безопасности и защиты информации, обрабатываемой информационными системами в информационно-телекоммуникационной инфраструктуре Колледжа в соответствии с требованиями действующего законодательства Российской Федерации, нормативных, методических и организационно-распорядительных документов уполномоченных органов Российской Федерации.

1.3. Политика защиты информации ГАПОУ РК «Петрозаводский базовый медицинский колледж» разработана в соответствии с положениями:

- Федерального закона от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных»;
- Постановления Правительства РФ от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Приказа Федеральной службы по техническому и экспортному контролю от 18.02.2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
- Приказа Федеральной службы по техническому и экспортному контролю от 11.04.2025 г. № 117 «Об утверждении требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений» (далее – Приказ ФСТЭК № 117).

1.4. Политика защиты информации определяет структуру, необходимый уровень и способы защиты информации, собираемой, принимаемой, обрабатываемой, хранимой и передаваемой информационными системами Колледжа.

1.5. Основной целью обеспечения защиты информации Колледжа являются действия, направленные на защиту субъектов информационных отношений от возможного нанесения им материального, физического, морального или иного ущерба посредством случайного или преднамеренного воздействия на информацию. Обеспечение защиты информации направлено на предотвращение следующих негативных последствий:

• угроза жизни и здоровью граждан;

• утечка персональных данных и иной информации ограниченного доступа;

• нарушение функционирования информационных систем, обеспечивающих образовательный процесс;

• материальный ущерб Колледжу и третьим лицам;

• потеря конкурентного преимущества (при наличии коммерческой тайны);

• обеспечения отказоустойчивого функционирования программных и аппаратно-программных средств Колледжа и предоставляемых сервисов;

• соблюдения правового режима использования массивов и средств обработки информации;

• предотвращения реализации угроз безопасности информации при осуществлении деятельности Колледжа.

1.6. Обеспечение защиты информации должно осуществляться в соответствии со следующими основными принципами:

• Принцип законности: при выборе мероприятий по защите информации должно соблюдаться действующее законодательство Российской Федерации в сфере защиты информации. Все работники должны иметь представление об ответственности за правонарушения в сфере защиты информации. Программные и программно-аппаратные средства, применяемые в Колледже, должны иметь соответствующие лицензии, официально приобретаться у представителей разработчиков этих средств.

• Принцип системности: при создании системы защиты должны учитываться актуальные угрозы безопасности информации, возможные объекты и направления атак на неё со стороны нарушителей. Система защиты должна строиться с учетом не только известных каналов утечки информации, но и с учетом возможности появления новых уязвимостей в программном обеспечении.

• Принцип комплексности: комплексное использование средств защиты информации предполагает согласованное применение при построении целостной системы защиты, перекрывающей все существенные угрозы безопасности информации. Защита должна строиться эшелонировано. Физическая защита должна обеспечиваться физическими средствами и организационными мерами. При построении, внедрении и эксплуатации системы защиты информации руководство Колледжа обеспечивает условия для эффективной координации действий всех лиц, обеспечивающих защиту информации.

• Принцип своевременности: разработка системы защиты информации должна вестись параллельно с разработкой информационной системы. Это позволит учесть требования безопасности при проектировании архитектуры и, в конечном счете, создать более эффективные информационные системы, обладающие достаточным уровнем защищенности.

• Принцип преемственности: постоянное совершенствование мер и средств защиты информации на основе преемственности организационных и технических решений, кадрового состава, анализа функционирования информационных систем и системы её защиты с учетом изменений в методах и средствах перехвата информации, нормативных требований по защите информации.

• Принцип достаточности: соответствие уровня затрат на обеспечение информационной безопасности и ценности информационных ресурсов на величину возможного ущерба от их разглашения, уничтожения и искажения. Используемые меры и средства защиты информации не должны ухудшать эргономические показатели компонентов информационных систем.

• Принцип ответственности: возложение ответственности за защиту информации и её обработки на каждого работника в пределах его полномочий. В соответствии с этим принципом распределение прав и обязанностей работников строится таким образом, чтобы в случае любого нарушения был известен нарушитель.

• Принцип обоснованности и технической реализуемости: информационные технологии, программные и программно-аппаратные средства, меры защиты информации должны быть реализованы по современным решениям, обоснованы с точки зрения достижения заданного уровня защищенности информации и экономической целесообразности, а также соответствовать установленным нормам и требованиям по защите информации.

• Принцип профессионализма: реализация мер защиты информации и эксплуатация средств защиты информации должна осуществляться профессиональными специалистами. Привлечение специализированных организаций к разработке средств и реализации мер защиты информации, подготовленных к конкретному виду деятельности по обеспечению защиты информационных ресурсов, имеющих опыт практической работы и лицензии на право оказания услуг в этой области.

• Принцип минимизации привилегий пользователей: обеспечение пользователей привилегиями, минимально достаточными для выполнения ими своих должностных обязанностей.

1.7. В целях обеспечения защиты информации Колледж при взаимодействии с контрагентами должен выполнять следующие мероприятия:

• заключение соглашения о неразглашении информации, содержащей сведения ограниченного распространения, полученной в ходе исполнения договорных обязательств;

• осуществление контроля за действиями представителей контрагентов в пределах контролируемой зоны Колледжа.

1.8. Политика защиты информации размещается на официальном сайте Колледжа и доступна для ознакомления всем заинтересованным лицам.

2. Информационные системы Колледжа и обеспечение защиты информации

2.1. К субъектам правоотношений, связанных с использованием информационных систем Колледжа и обеспечением защиты информации, относятся:

• Колледж, как обладатель информации;

• работники Колледжа, как пользователи информационной системы Колледжа в соответствии с возложенными на них должностными обязанностями;

• студенты Колледжа;

• абитуриенты Колледжа;

• работники организации, обеспечивающей эксплуатацию средств вычислительной техники, сетевой инфраструктуры и информационных систем Колледжа;

• иные пользователи (физические и юридические лица), информация о которых накапливается, обрабатывается и хранится в информационных системах Колледжа.

2.2. Объектами информационных отношений являются:

• информационные технологии и информационные ресурсы Колледжа, включая информационную систему обработки персональных данных и иные информационные системы, обеспечивающие функционирование Колледжа;

• процессы обработки информации в информационных системах Колледжа;

• информационная инфраструктура, в том числе каналы связи и телекоммуникации;

• системы и средства защиты информации;

• объекты и помещения, в которых размещены средства обработки информации.

2.3. Информационная система обработки персональных данных и остальные информационные системы размещаются в разных сегментах локальной вычислительной сети Колледжа, разделенных средствами межсетевого экранирования.

2.4. Конфиденциальная и открытая информация размещается на разных серверах Колледжа.

2.5. Локальная вычислительная сеть защищается от внешнего проникновения и атак сертифицированными средствами защиты информации.

2.6. Использование ресурсов сетей общего доступа и (или) международного обмена – Интернет в Колледже регламентировано соответствующими локальными актами.

2.7. Работники Колледжа имеют доступ к информационным системам Колледжа в соответствии с выполняемыми должностными обязанностями.

2.8. Работники организации, обеспечивающей эксплуатацию средств вычислительной техники, сетевой инфраструктуры и информационных систем Колледжа, имеют доступ к вычислительной и оргтехнике, сетевому и серверному оборудованию Колледжа в соответствии с заключенными договорами и соглашениями о конфиденциальности.

2.9. Уровень доступа к информационной системе Колледжа определяется для каждого работника индивидуально с соблюдением следующих требований:

- каждый работник имеет доступ только к той информации, которая необходима ему для выполнения должностных обязанностей (принцип минимальных привилегий);
- непосредственный руководитель работника имеет право на просмотр информации, используемой работником, в пределах своей компетенции.

2.10. Работники Колледжа, как пользователи информационной системы Колледжа, в соответствии с возложенными на них трудовыми обязанностями, обязаны соблюдать следующие требования:

- знать и соблюдать установленные требования по режиму обработки персональных данных, а также руководящих и организационно-распорядительных документов по работе со сведениями, содержащими персональные данные;
- соблюдать требования локальных нормативных актов Колледжа, регламентирующих вопросы использования съемных машинных носителей информации и парольной защиты;
- соблюдать установленные правила при работе в сетях общего доступа и (или) международного обмена – Интернет и других;
- выполнять на автоматизированном рабочем месте (АРМ) только те процедуры, которые определены для него должностными инструкциями и инструкциями пользователя;
- располагать во время работы экран монитора и принтера так, чтобы исключалась возможность несанкционированного ознакомления посторонними лицами с отображаемой на нём информацией;
- при отсутствии визуального контроля за компьютером доступ к нему должен быть заблокирован (блокировка экрана, завершение сеанса);
- не оставлять открытые помещения, в которых размещены средства вычислительной техники, без присмотра;
- в случае возникновения внештатных либо аварийных ситуаций принимать меры по реагированию с целью ликвидации их последствий в соответствии с инструкциями в рамках и в пределах возложенных на него функций.

2.11. Все работники под роспись ознакомлены с нормативными и организационно-распорядительными документами Колледжа по вопросам защиты информации.

2.12. Все работники, допущенные к работе с информационной системой Колледжа, ознакомлены под подпись с правилами и инструкцией по её использованию и несут персональную ответственность за их нарушение.

2.13. До предоставления доступа к информационной системе Колледжа пользователи под подпись ознакомляются с перечнем информации, содержащей сведения ограниченного распространения, а также организационно-распорядительной, нормативной, технической и эксплуатационной документацией, определяющей требования и порядок обработки такой информации.

2.14. Работники Колледжа несут персональную ответственность за нарушение правил и инструкций по передаче, обработке и хранению информации, содержащей сведения ограниченного распространения.

2.15. Обо всех выявленных нарушениях, связанных с информационной безопасностью и защитой информации, работники обязаны в кратчайший срок сообщить специалисту по защите информации (или лицу, его замещающему).

3. Распределение ответственности за обеспечение защиты информации

3.1. Система управления защитой информации в Колледже строится на принципах персональной ответственности и разграничения прав и обязанностей должностных лиц.

3.2. **Директор Колледжа:**

- несет персональную ответственность за обеспечение защиты информации в Колледже в соответствии с законодательством Российской Федерации;
- утверждает Политику защиты информации, а также иные организационно-распорядительные документы в области защиты информации;
- выделяет необходимые ресурсы (финансовые, материальные, кадровые) для построения и функционирования системы защиты информации на основании обоснованных предложений специалиста по защите информации;
- назначает приказом лицо, ответственное за организацию защиты информации (специалиста по защите информации), и определяет его полномочия;
- принимает решения о применении мер дисциплинарной ответственности к работникам, допустившим нарушения требований по защите информации;
- утверждает составы (перечни) информационных систем, подлежащих защите, и их классы защищенности;
- обеспечивает соответствие квалификации сотрудников, ответственных за обеспечение защиты информации, требованиям, установленным Приказом ФСТЭК № 117.

3.3. **Специалист по защите информации (лицо, ответственное за организацию защиты информации):**

- организует разработку и актуализацию организационно-распорядительных документов по защите информации (политик, положений, регламентов, инструкций);
- организует проведение классификации информационных систем и формирование моделей угроз;
- координирует работу по внедрению и настройке средств защиты информации;
- осуществляет контроль за соблюдением работниками и пользователями требований по защите информации;
- организует проведение анализа уязвимостей, оценки эффективности принятых мер защиты информации;
- организует расследование инцидентов информационной безопасности и принимает меры по их устранению и предотвращению повторения;
- обеспечивает своевременное информирование директора Колледжа о состоянии защищенности информационных систем и выявленных нарушениях;
- организует обучение и повышение осведомленности персонала в области защиты информации;
- взаимодействует с государственными органами (ФСТЭК России, ФСБ России) по вопросам защиты информации в установленном порядке;
- обеспечивает наличие у сотрудников, привлекаемых к выполнению работ по защите информации, профессионального образования или прохождение ими профессиональной переподготовки в области информационной безопасности.

3.4. **Ведущий инженер-программист (администратор информационных систем, сотрудник, обеспечивающий эксплуатацию):**

- несет ответственность за техническую эксплуатацию информационных систем, средств вычислительной техники, сетевого и серверного оборудования;
- осуществляет установку, настройку и сопровождение системного и прикладного программного обеспечения;

• реализует технические меры защиты информации (настройка межсетевых экранов, антивирусной защиты, систем разграничения доступа) по заданию специалиста по защите информации и в соответствии с утвержденной документацией;

• обеспечивает бесперебойное функционирование информационных систем;

• выполняет резервное копирование данных и контроль целостности программного обеспечения;

• незамедлительно информирует специалиста по защите информации обо всех сбоях, инцидентах и подозрительных событиях в работе информационных систем;

• участвует в проведении анализа уязвимостей и восстановлении работоспособности систем после сбоев;

• ведет эксплуатационную документацию и журналы учета изменений конфигурации.

3.5. **Требования к квалификации сотрудников подразделения по защите информации:**

• В соответствии с требованиями Приказа ФСТЭК № 117 не менее 30 процентов работников структурного подразделения (или работников, на которых возложены функции по обеспечению защиты информации) должны иметь высшее или среднее профессиональное образование в области информационной безопасности либо пройти профессиональную переподготовку в области информационной безопасности.

• При отсутствии у специалиста по защите информации профильного образования он должен быть направлен на профессиональную переподготовку в течение первого года после назначения на должность.

• Квалификация сотрудников, привлекаемых к работам по защите информации, должна подтверждаться соответствующими документами об образовании и (или) о квалификации.

3.6. Все работники Колледжа, являющиеся пользователями информационных систем, несут ответственность за соблюдение требований по защите информации в части, их касающейся (сохранность паролей, блокировка рабочего места при отсутствии визуального контроля, неразглашение информации ограниченного доступа), в соответствии со своими должностными инструкциями.

4. Требования к организации защиты информации, содержащейся в информационных системах Колледжа

4.1. В информационных системах Колледжа объектами защиты являются:

• информация, содержащаяся в информационной системе;

• технические средства (в том числе средства вычислительной техники, машинные носители информации, средства и системы связи и передачи данных, технические средства обработки информации);

• общесистемное, прикладное, специальное программное обеспечение, информационные технологии;

• средства защиты информации.

4.2. Для обеспечения защиты информации, содержащей персональные данные, в Колледже назначается должностное лицо (работник), ответственное за организацию обработки персональных данных. Организацией работ по защите информации в Колледже занимается специалист по защите информации (или лицо, на которое возложены соответствующие функции).

4.3. Для проведения работ по защите информации в ходе создания и ввода в эксплуатацию информационной системы Колледжа в соответствии с законодательством Российской Федерации при необходимости привлекаются организации, имеющие лицензию на деятельность по технической защите конфиденциальной информации в соответствии с Федеральным законом от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности».

4.4. Для обеспечения защиты информации, содержащейся в информационной системе, применяются средства защиты информации, прошедшие оценку соответствия в форме обязательной сертификации на соответствие требованиям по безопасности информации в соответствии со статьей 5 Федерального закона от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании».

4.5. Защита информации, содержащейся в информационной системе, является составной частью работ по созданию и эксплуатации информационной системы и обеспечивается на всех стадиях (этапах) её создания, в ходе эксплуатации и вывода из эксплуатации путем принятия организационных и технических мер защиты информации, направленных на блокирование (нейтрализацию) угроз безопасности информации в информационной системе, в рамках системы (подсистемы) защиты информации информационной системы (далее – система защиты информации информационной системы).

Организационные и технические меры защиты информации, реализуемые в рамках системы защиты информации информационной системы, в зависимости от информации, содержащейся в информационной системе, целей создания информационной системы и задач, решаемых этой информационной системой, должны быть направлены на исключение:

- неправомерных доступа, копирования, предоставления или распространения информации (обеспечение конфиденциальности информации);
- неправомерных уничтожения или модифицирования информации (обеспечение целостности информации);
- неправомерного блокирования информации (обеспечение доступности информации).

4.6. Для обеспечения защиты информации, содержащейся в информационной системе, проводятся следующие мероприятия:

- формирование требований к защите информации, содержащейся в информационной системе;
- разработка системы защиты информации информационной системы;
- внедрение системы защиты информации информационной системы;
- обеспечение защиты информации в ходе эксплуатации аттестованной информационной системы;
- обеспечение защиты информации при выводе из эксплуатации аттестованной информационной системы или после принятия решения об окончании обработки информации.

4.7. Формирование требований к защите информации, содержащейся в информационной системе, осуществляется Колледжем и включает:

- принятие решения о необходимости защиты информации, содержащейся в информационной системе;
- классификацию информационной системы по требованиям защиты информации;
- определение угроз безопасности информации, реализация которых может привести к нарушению безопасности информации в информационной системе, и разработку на их основе модели угроз безопасности информации;
- определение требований к системе защиты информации информационной системы.

4.8. При принятии решения о необходимости защиты информации, содержащейся в информационной системе, осуществляется:

- анализ целей создания информационной системы и задач, решаемых этой информационной системой;
- определение информации, подлежащей обработке в информационной системе;
- анализ нормативных правовых актов, методических документов и национальных стандартов, которым должна соответствовать информационная система;

• принятие решения о необходимости создания системы защиты информации в информационной системе, а также определение целей и задач защиты информации в информационной системе, основных этапов создания системы защиты информации информационной системы и функций по обеспечению защиты информации, содержащейся в информационной системе Колледжа, и уполномоченных лиц.

4.9. Классификация информационной системы проводится в зависимости от значимости обрабатываемой в ней информации в соответствии с действующим законодательством РФ и нормативными документами регуляторов. Результаты классификации информационной системы оформляются актом классификации.

Класс защищенности информационной системы подлежит пересмотру при изменении масштаба информационной системы или значимости обрабатываемой в ней информации.

4.10. Угрозы безопасности информации определяются по результатам оценки возможностей (потенциала) внешних и внутренних нарушителей, анализа возможных уязвимостей информационной системы, возможных способов реализации угроз безопасности информации и последствий от нарушения свойств информации (доступности, целостности и конфиденциальности).

При определении угроз безопасности информации учитываются структурно-функциональные характеристики информационной системы, включающие структуру и состав информационной системы, физические, логические, функциональные и технологические взаимосвязи между сегментами информационной системы, с иными информационными системами и информационно-телекоммуникационными сетями, режимы обработки информации в информационной системе и в её отдельных сегментах, а также иные характеристики информационной системы, применяемые информационные технологии и особенности её функционирования.

Определение угроз безопасности информации проводится при подготовке технического задания на создание и/или изменение информационной системы, при изменении условий эксплуатации, а также периодически, **но не реже одного раза в год** (в соответствии с требованиями Приказа ФСТЭК № 117).

По результатам определения угроз безопасности информации при необходимости разрабатываются рекомендации по корректировке структурно-функциональных характеристик информационной системы, направленные на блокирование (нейтрализацию) отдельных угроз безопасности информации.

5. Внедрение системы защиты информации информационной системы

5.1. Внедрение системы защиты информации информационной системы организуется специалистом по защите информации Колледжа.

5.2. Внедрение системы защиты информации информационной системы осуществляется в соответствии с проектной и эксплуатационной документацией на систему защиты информации информационной системы и в том числе включает:

• установку и настройку средств защиты информации в информационной системе;

• внедрение организационных мер защиты информации;

• анализ уязвимостей информационной системы и принятие мер защиты информации по их устранению;

• приемочные испытания системы защиты информации информационной системы.

5.3. Установка и настройка средств защиты информации в информационной системе должна проводиться в соответствии с эксплуатационной документацией на систему защиты информации информационной системы и документацией на средства защиты информации.

5.4. При внедрении организационных мер защиты информации осуществляются:

• реализация правил разграничения доступа, регламентирующих права доступа субъектов доступа к объектам доступа, и введение ограничений на доступ к информации и

действия пользователей, а также на изменение условий эксплуатации, состава и конфигурации технических средств и программного обеспечения;

- отработка действий должностных лиц и подразделений, ответственных за реализацию мер защиты информации.

5.5. Анализ уязвимостей информационной системы проводится в целях оценки возможности преодоления нарушителем системы защиты информации информационной системы и предотвращения реализации угроз безопасности информации.

Анализ уязвимостей информационной системы включает анализ уязвимостей средств защиты информации, технических средств и программного обеспечения информационной системы.

При анализе уязвимостей информационной системы проверяется отсутствие известных уязвимостей средств защиты информации, технических средств и программного обеспечения, в том числе с учетом информации, имеющейся у разработчиков и полученной из других общедоступных источников, правильность установки и настройки средств защиты информации, технических средств и программного обеспечения, а также корректность работы средств защиты информации при их взаимодействии с техническими средствами и программным обеспечением.

В случае выявления уязвимостей информационной системы, приводящих к возникновению дополнительных угроз безопасности информации, принимаются дополнительные меры защиты информации, направленные на устранение выявленных уязвимостей или исключающие возможность использования нарушителем выявленных уязвимостей.

6. Обеспечение защиты информации в ходе эксплуатации информационной системы

6.1. Обеспечение защиты информации в ходе эксплуатации информационной системы осуществляется Колледжем и включает следующие мероприятия:

- анализ угроз безопасности информации в информационной системе;
- планирование мероприятий по защите информации в информационной системе;
- управление (администрирование) системой защиты информации информационной системы;
- управление конфигурацией информационной системы и её системой защиты информации;
- информирование и обучение персонала информационной системы;
- реагирование на инциденты;
- контроль за обеспечением уровня защищенности информации, содержащейся в информационной системе.

6.2. В ходе анализа угроз безопасности информации в информационной системе осуществляется оценка изменения угроз и возможных последствий их реализации. Периодичность проведения указанных работ определяется Колледжем в организационно-распорядительных документах по защите информации, но **не реже 1 раза в год**.

6.3. В ходе планирования мероприятий по защите информации в информационной системе осуществляются:

- определение лиц, ответственных за реализацию и контроль мероприятий по защите информации в информационной системе;
- определение лиц, ответственных за выявление инцидентов и реагирование на них;
- разработка, утверждение и актуализация плана мероприятий по защите информации в информационной системе;
- определение порядка контроля выполнения мероприятий по обеспечению защиты информации в информационной системе, предусмотренных утвержденным планом.

6.4. В ходе управления конфигурацией информационной системы и её системы защиты информации осуществляются:

• определение лиц, которым разрешены действия по внесению изменений в конфигурацию информационной системы и её системы защиты информации, и их полномочий, контроль за их действиями;

• определение компонентов информационной системы и её системы защиты информации, подлежащих изменению в рамках управления конфигурацией (идентификация объектов управления конфигурацией);

• управление изменениями информационной системы и её системы защиты информации;

• разработка параметров настройки, обеспечивающих защиту информации, анализ потенциального воздействия планируемых изменений на обеспечение защиты информации, санкционирование внесения изменений в информационную систему и её систему защиты информации, документирование действий по внесению изменений в информационную систему и сохранение данных об изменениях конфигурации;

• контроль действий по внесению изменений в информационную систему и её систему защиты информации.

6.5. Реализованные процессы управления изменениями информационной системы и её системы защиты информации должны включать процессы гарантийного и (или) технического обслуживания, в том числе дистанционного (удаленного), программных и программно-аппаратных средств, включая средства защиты информации, информационной системы.

6.6. В ходе реагирования на инциденты осуществляются:

• обнаружение и идентификация инцидентов, в том числе отказов в обслуживании, сбоев (перезагрузок) в работе технических средств, программного обеспечения и средств защиты информации, нарушений правил разграничения доступа, неправомерных действий по сбору информации, внедрений вредоносных компьютерных программ (вирусов) и иных событий, приводящих к возникновению инцидентов;

• своевременное информирование пользователями и администраторами лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в информационной системе;

• анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий;

• планирование и принятие мер по устранению инцидентов, в том числе по восстановлению информационной системы и её сегментов после сбоев, устранению последствий нарушения правил разграничения доступа, неправомерных действий по сбору информации, внедрения вредоносных компьютерных программ (вирусов) и иных событий, приводящих к возникновению инцидентов;

• планирование и принятие мер по предотвращению повторного возникновения инцидентов.

6.7. В ходе информирования персонала информационной системы осуществляются:

• информирование персонала информационной системы о появлении актуальных угроз безопасности информации, о правилах безопасной эксплуатации информационной системы;

• доведение до персонала информационной системы требований по защите информации, а также положений организационно-распорядительных документов по защите информации с учетом внесенных в них изменений;

• контроль осведомленности персонала информационной системы об угрозах безопасности информации и уровня знаний персонала по вопросам обеспечения защиты информации.

Периодичность проведения практических занятий и тренировок с персоналом, мероприятий по обучению персонала и контролю осведомленности персонала устанавливается Колледжем в организационно-распорядительных документах по защите

информации с учетом особенностей функционирования информационной системы, но **не реже 1 раза в два года** (в соответствии с требованиями Приказа ФСТЭК № 117).

7. Обеспечение защиты информации при выводе из эксплуатации информационной системы или после принятия решения об окончании обработки информации

7.1. Обеспечение защиты информации при выводе из эксплуатации информационной системы или после принятия решения об окончании обработки информации осуществляется Колледжем в соответствии с эксплуатационной документацией на систему защиты информации информационной системы, нормативными и организационно-распорядительными документами по защите информации и в том числе включает:

- архивирование информации, содержащейся в информационной системе;
- гарантированное уничтожение (стирание) данных и остаточной информации с машинных носителей информации и (или) уничтожение машинных носителей информации.

7.2. Архивирование информации, содержащейся в информационной системе, осуществляется при необходимости дальнейшего использования информации в деятельности Колледжа.

7.3. Уничтожение (стирание) данных и остаточной информации с машинных носителей информации производится при необходимости передачи машинного носителя информации другому пользователю информационной системы или в сторонние организации для технического обслуживания, ремонта или утилизации.

7.4. При выводе из эксплуатации машинных носителей информации, на которых осуществлялись хранение и обработка информации, содержащей сведения ограниченного распространения, и невозможности гарантированного уничтожения информации в соответствии с требованиями нормативных документов осуществляется физическое уничтожение этих машинных носителей информации.

8. Требования к защите информации, содержащейся в информационной системе

8.1. Организационные и технические меры защиты информации, реализуемые в информационной системе в рамках её системы защиты информации, в зависимости от угроз безопасности информации, используемых информационных технологий и структурно-функциональных характеристик информационной системы должны обеспечивать:

- идентификацию и аутентификацию субъектов доступа и объектов доступа;
- управление доступом субъектов доступа к объектам доступа;
- ограничение программной среды;
- защиту машинных носителей информации;
- регистрацию событий безопасности;
- антивирусную защиту;
- обнаружение (предотвращение) вторжений;
- контроль (анализ) защищенности информации;
- целостность информационной системы и информации;
- доступность информации;
- защиту среды виртуализации (при ее использовании);
- защиту технических средств;
- защиту информационной системы, её средств, систем связи и передачи данных.

8.2. При идентификации и аутентификации субъектов доступа и объектов доступа должно обеспечиваться присвоение субъектам и объектам доступа уникального признака (идентификатора), сравнение предъявляемого субъектом (объектом) доступа идентификатора с перечнем присвоенных идентификаторов, а также проверка принадлежности субъекту (объекту) доступа предъявленного им идентификатора

(подтверждение подлинности). Для привилегированных пользователей (администраторов информационных систем, специалиста по защите информации, ведущего инженера-программиста) при осуществлении привилегированного доступа применяется строгая аутентификация (двухфакторная аутентификация). В случае технической невозможности применения строгой аутентификации используется усиленная многофакторная аутентификация. Все попытки привилегированного доступа подлежат обязательной регистрации.

8.3. При управлении доступом субъектов доступа к объектам доступа должно обеспечиваться управление правами и привилегиями субъектов доступа, разграничение доступа субъектов доступа к объектам доступа на основе совокупности установленных в информационной системе правил разграничения доступа, а также обеспечивать контроль соблюдения этих правил.

8.4. При ограничении программной среды должна обеспечиваться установка и (или) запуск только разрешенного к использованию в информационной системе программного обеспечения или исключаться возможность установки и (или) запуска запрещенного к использованию в информационной системе программного обеспечения.

8.5. При защите машинных носителей информации (средства обработки (хранения) информации, съемные машинные носители информации) должна быть исключена возможность несанкционированного доступа к машинным носителям и хранящейся на них информации, а также несанкционированное использование съёмных машинных носителей информации.

8.6. При регистрации событий безопасности должны обеспечиваться сбор, запись, хранение и защита информации о событиях безопасности в информационной системе, а также возможность просмотра и анализа информации о таких событиях и реагирование на них.

8.7. При антивирусной защите должно обеспечиваться обнаружение в информационной системе компьютерных программ либо иной компьютерной информации, предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирование на обнаружение этих программ и информации.

8.8. При обнаружении (предотвращении) вторжений должно обеспечиваться обнаружение действий в информационной системе, направленных на преднамеренный несанкционированный доступ к информации, специальные воздействия на информационную систему и (или) информацию в целях её добывания, уничтожения, искажения и блокирования доступа к информации, а также реагирование на эти действия.

8.9. При анализе защищенности информации должен обеспечиваться контроль уровня защищенности информации, содержащейся в информационной системе, путем проведения мероприятий по оценке защищенности информационной системы.

8.10. При обеспечении целостности информационной системы и информации должно обеспечиваться обнаружение фактов несанкционированного нарушения целостности информационной системы и содержащейся в ней информации, а также возможность восстановления информационной системы и содержащейся в ней информации.

8.11. При обеспечении доступности информации должен обеспечиваться авторизованный доступ пользователей, имеющих права по такому доступу, к информации, содержащейся в информационной системе, в штатном режиме функционирования информационной системы.

8.12. При защите среды виртуализации (в случае ее использования) должен быть исключен несанкционированный доступ к информации, обрабатываемой в виртуальной инфраструктуре, и к компонентам виртуальной инфраструктуры, а также воздействие на информацию и компоненты.

8.13. При защите технических средств должен быть исключен несанкционированный доступ к стационарным техническим средствам, обрабатывающим информацию, средствам, обеспечивающим функционирование информационной системы, и в помещения, в которых они постоянно расположены, обеспечена защита технических средств от внешних воздействий, а также защита информации, представленной в виде информативных электрических сигналов и физических полей.

8.14. При защите информационной системы, её средств, систем связи и передачи данных должны обеспечиваться защита информации при взаимодействии информационной системы или её отдельных сегментов с иными информационными системами и информационно-телекоммуникационными сетями посредством применения архитектуры информационной системы, проектных решений по её системе защиты информации, направленных на обеспечение защиты информации.

8.15. Технические меры защиты информации реализуются посредством применения средств защиты информации, в том числе программных (программно-аппаратных) средств, в которых они реализованы, имеющих необходимые функции безопасности. В информационных системах применяются средства защиты информации, сертифицированные на соответствие обязательным требованиям по безопасности информации, установленным ФСТЭК России, или на соответствие требованиям, указанным в технических условиях (заданиях по безопасности).

9. Требования к программно-техническим средствам информационной системы Колледжа

Программно-технические средства информационной системы Колледжа должны:

- располагаться на территории Российской Федерации;
- в соответствии с действующим законодательством и нормативными документами быть сертифицированными Федеральной службой по техническому и экспортному контролю Российской Федерации и Федеральной службой безопасности Российской Федерации (в соответствующей части) в отношении входящих в их состав средств защиты информации, включающих программно-аппаратные и программные средства защиты информации от несанкционированного доступа, антивирусное программное обеспечение, средства криптографической защиты информации и средства защиты информации от нелегитимного уничтожения, модификации и блокирования доступа к ней;
- обеспечивать хранение документации в форме электронных документов, предусматривая резервное копирование документов и метаданных, восстановление документов и метаданных из резервных копий;
- обеспечивать протоколирование и сохранение сведений о предоставлении доступа и о других операциях с документами и метаданными в автоматизированном режиме, а также автоматизированное ведение электронных журналов учета точного времени и фактов размещения, изменения и удаления информации, содержания вносимых изменений;
- функционировать в бесперебойном режиме, за исключением установленных периодов проведения работ по обслуживанию информационных систем и устранению неисправностей в работе, суммарная длительность которых не должна превышать 4 часов в месяц (за исключением перерывов, связанных с обстоятельствами непреодолимой силы).

10. Порядок взаимодействия информационной системы Колледжа с иными информационными системами

10.1. Взаимодействие информационной системы Колледжа с иными информационными системами (государственными информационными системами, ведомственными системами Министерства образования, порталами государственных услуг и другими) осуществляется с соблюдением требований законодательства Российской Федерации в области защиты информации.

10.2. Подключение иных информационных систем к информационной системе Колледжа допускается при условии соответствия таких систем требованиям по защите информации, установленным законодательством Российской Федерации.

10.3. Передача информации ограниченного доступа (в том числе персональных данных) из информационной системы Колледжа в иные информационные системы осуществляется с использованием защищенных каналов связи и с применением сертифицированных средств криптографической защиты информации (при необходимости).

10.4. При взаимодействии с иными информационными системами должны обеспечиваться:

- идентификация и аутентификация взаимодействующих систем;
- подтверждение целостности и подлинности передаваемой информации (с использованием электронной подписи при необходимости);
- регистрация событий информационного взаимодействия;
- защита информации от несанкционированного доступа в процессе передачи.

10.5. Колледж осуществляет контроль за соблюдением требований по защите информации при взаимодействии с иными информационными системами, в том числе путем анализа защищенности каналов связи и применяемых средств защиты.

10.6. В случае если иная информационная система обрабатывает персональные данные, полученные из информационной системы Колледжа, такая система должна соответствовать требованиям к защите персональных данных, установленным законодательством Российской Федерации.

10.7. Для подключения иной информационной системы к информационной системе Колледжа оператор иной информационной системы предоставляет в Колледж заявку на подключение. Колледж проводит тестирование информационного взаимодействия и принимает решение о подключении или об отказе в подключении в случае несоответствия иной информационной системы требованиям по защите информации.

10.8. В случае самостоятельной разработки Колледжем программного обеспечения, предназначенного для использования в информационных системах, должны быть учтены меры, предусмотренные разделами 4 и 5 ГОСТ Р 56939-2024 «Защита информации. Безопасная разработка программного обеспечения».

10.9. При привлечении подрядных организаций для разработки программного обеспечения:

- требования к безопасной разработке включаются в техническое задание;
- работники подрядных организаций не допускаются к разработке и тестированию непосредственно в эксплуатируемых информационных системах;
- обязанности по соблюдению требований настоящей Политики закрепляются в договорах с подрядчиками.

11. Обеспечение защиты персональных данных

11.1. Защита, хранение, обработка и передача персональных данных работников, студентов и иных лиц осуществляются с соблюдением требований Конституции Российской Федерации, Трудового кодекса Российской Федерации, Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных», постановления Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

11.2. Персональные данные работника – информация, необходимая Колледжу в связи с трудовыми отношениями и касающаяся конкретного работника.

Персональные данные студента – информация, полученная Колледжем при заключении договора об образовании, а также информация, полученная в процессе обучения.

11.3. Состав обрабатываемых персональных данных определен в Политике в отношении обработки персональных данных в ГАПОУ РК «Петрозаводский базовый медицинский колледж» и Положении об организации и проведении работ по обеспечению безопасности персональных данных обрабатываемых в информационных системах персональных данных и/или без использования средств автоматизации.

11.4. Все персональные сведения о работниках и студентах Колледж получает преимущественно от них самих. В случаях, когда Колледж получает необходимые персональные данные у третьего лица, Колледж уведомляет об этом субъекта персональных данных и получает от него письменное согласие.

11.5. Колледж сообщает субъектам персональных данных о целях, способах и источниках получения персональных данных, а также о характере подлежащих получению персональных данных и возможных последствиях отказа дать письменное согласие на их получение.

11.6. Персональные данные являются конфиденциальной информацией и не могут быть использованы Колледжем или любым иным лицом в личных целях.

11.7. При определении объема и содержания персональных данных Колледж руководствуется Конституцией Российской Федерации, Трудовым кодексом Российской Федерации, иными федеральными законами.

11.8. Колледж обрабатывает в информационных системах с использованием средств автоматизации категории персональных данных, необходимые для осуществления образовательной и трудовой деятельности, обеспечивает их защиту с учетом определенного типа угроз безопасности и уровня защищенности персональных данных.

11.9. Колледж принимает организационные и технические меры по обеспечению безопасности персональных данных при их обработке в информационных системах, предусмотренные Приказом Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» и Приказом ФСТЭК № 117.

При защите персональных данных Колледж:

- обеспечивает режим безопасности помещений, в которых размещена информационная система, препятствующий возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;
- обеспечивает сохранность носителей персональных данных;
- утверждает перечень работников, доступ которых к персональным данным необходим для выполнения ими служебных (трудовых) обязанностей;
- использует средства защиты информации, прошедшие процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации.

11.10. В случае выявления неправомерной обработки персональных данных при обращении субъекта персональных данных Колледж осуществляет блокирование неправомерно обрабатываемых персональных данных с момента такого обращения на период проверки.

11.11. В случае выявления неточных персональных данных при обращении субъекта персональных данных Колледж осуществляет блокирование персональных данных с момента такого обращения на период проверки, если блокирование персональных данных не нарушает права и законные интересы субъекта персональных данных или третьих лиц. В случае подтверждения факта неточности персональных данных Колледж на основании

сведений, представленных субъектом персональных данных, уточняет персональные данные в течение семи рабочих дней со дня представления таких сведений и снимает блокирование персональных данных.

11.12. В случае если обеспечить правомерность обработки персональных данных невозможно, Колледж в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки персональных данных, уничтожает такие персональные данные.

11.13. В случае достижения цели обработки персональных данных Колледж прекращает обработку персональных данных и уничтожает их в срок, не превышающий тридцати дней с даты достижения цели обработки.

11.14. В случае отзыва субъектом персональных данных согласия на обработку его персональных данных Колледж прекращает их обработку и, если сохранение персональных данных более не требуется для целей обработки, уничтожает их в срок, не превышающий тридцати дней с даты поступления указанного отзыва.

11.15. Об уничтожении персональных данных Колледж уведомляет субъекта персональных данных.

11.16. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных, привлекаются к дисциплинарной и материальной ответственности в порядке, установленном федеральными законами, а также к гражданско-правовой, административной и уголовной ответственности в порядке, установленном федеральными законами.

11.17. Моральный вред, причиненный субъекту персональных данных вследствие нарушения его прав, правил обработки персональных данных, установленных Федеральным законом, а также требований к защите персональных данных, подлежит возмещению в соответствии с законодательством Российской Федерации.

12. Обеспечение защиты информации ограниченного доступа (врачебной тайны в части, касающейся деятельности медицинского колледжа)

12.1. Учитывая профиль деятельности Колледжа (медицинский колледж), при организации практической подготовки студентов в медицинских организациях, а также при функционировании собственной медицинской деятельности (при наличии) в Колледже может обрабатываться информация, составляющая врачебную тайну.

12.2. Информация, содержащая врачебную тайну, – это информация о факте обращения гражданина за оказанием медицинской помощи, состоянии его здоровья и диагнозе, иных сведений, полученных при его медицинском обследовании и лечении.

12.3. Не допускается разглашение информации, составляющей врачебную тайну, лицами, которым она стала известна при исполнении трудовых, должностных, служебных и иных обязанностей, за исключением случаев, установленных Федеральным законом от 21 ноября 2011 г. № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации».

12.4. Работники Колледжа, участвующие в организации практической подготовки студентов или имеющие доступ к медицинской информации, обязаны сохранять врачебную тайну.

12.5. В целях сохранения врачебной тайны Колледж:

- обеспечивает наличие письменного обязательства работников о неразглашении врачебной тайны;
- устанавливает различные уровни доступа должностных лиц к информации, содержащей врачебную тайну;
- обеспечивает защиту информационных систем, содержащих врачебную тайну, в соответствии с настоящей Политикой.

12.6. Передача сведений, составляющих врачебную тайну, допускается с письменного согласия гражданина или его законного представителя.

12.7. Предоставление сведений, составляющих врачебную тайну, без согласия гражданина допускается исключительно в установленных действующим законодательством РФ случаях.

12.8. Неправомерное разглашение врачебной тайны влечет за собой дисциплинарную, административную, гражданскую и уголовную ответственность в соответствии с законодательством Российской Федерации.

13. Обеспечение организационно-распорядительной документацией

Для реализации требований настоящей Политики в Колледже разрабатываются и утверждаются следующие внутренние документы:

13.1. **Стандарты защиты информации**, определяющие:

- требования к первичной идентификации пользователей и применяемым моделям доступа;
- перечень разрешенного и запрещенного программного обеспечения;
- требования к типовым конфигурациям и настройкам программных и программно-аппаратных средств;
- требования к обеспечению безопасной дистанционной работы;
- требования к защите мобильных устройств;
- требования к непрерывности функционирования информационных систем и резервному копированию.

13.2. **Регламенты защиты информации**, устанавливающие порядок:

- создания, учета, изменения и блокирования учетных записей (включая привилегированные);
- предоставления удаленного доступа;
- допуска работников подрядных организаций к информационным системам;
- выявления, оценки и устранения уязвимостей;
- получения, тестирования и применения обновлений программного обеспечения;
- обработки и хранения информации ограниченного доступа;
- мониторинга информационной безопасности;
- восстановления штатного функционирования после сбоев;
- контроля уровня защищенности информации.

14. Мониторинг информационной безопасности и отчетность

14.1. В Колледже организуется непрерывный мониторинг информационной безопасности информационных систем, взаимодействующих с сетью «Интернет», в соответствии с требованиями ГОСТ Р 59547-2021 (раздел 5).

14.2. Проводится регулярная оценка состояния защиты информации на основе:

- **показателя защищенности** — не реже одного раза в шесть месяцев;
- **показателя уровня зрелости** — не реже одного раза в два года.

14.3. Результаты оценки состояния защиты информации направляются в территориальный орган ФСТЭК России не позднее 5 рабочих дней после их расчета.

14.4. В случае недостижения нормированных значений показателей разрабатывается план мероприятий по совершенствованию защиты информации.

14.5. О выявленных новых уязвимостях, которые могут привести к нарушению безопасности информации, специалист по защите информации информирует ФСТЭК России в течение 5 рабочих дней с момента обнаружения.

15. Управление уязвимостями

15.1. Установлены следующие сроки устранения выявленных уязвимостей:

- **критические уязвимости** — не более 24 часов с момента выявления;
- **уязвимости высокой степени опасности** — не более 7 календарных дней;

• **уязвимости средней и низкой степени опасности** — в сроки, установленные планом мероприятий, но не более 30 календарных дней.

15.2. Контроль установки обновлений программного обеспечения, направленных на устранение уязвимостей, является обязательным.

16. Требования к удаленному доступу и использованию мобильных устройств

16.1. Удаленный доступ пользователей к информационным системам Колледжа для выполнения служебных обязанностей осуществляется:

• с использованием сетей связи, расположенных на территории Российской Федерации;

• с применением средств защиты каналов передачи данных (VPN и др.);

• со строгой аутентификацией пользователей (аппаратные токены, одноразовые пароли или сертифицированные средства криптографической защиты информации).

16.2. Допускается использование личных мобильных устройств работников для доступа к информационным системам при соблюдении следующих условий:

• соответствие мобильных устройств требованиям безопасности, установленным в Колледже;

• наличие у Колледжа возможности контроля использования мобильных устройств;

• применение на устройствах антивирусных средств и строгой аутентификации.

16.3. Беспроводные сети связи, используемые для доступа к информационным системам Колледжа, должны быть отделены от сетей, предназначенных для доступа в Интернет и общедоступной информации.

17. Аттестация и контроль защищенности информационных систем

17.1. Аттестация информационных систем (подтверждение соответствия требованиям защиты информации) проводится:

• для государственных информационных систем — в обязательном порядке в соответствии с приказом ФСТЭК России № 77;

• для иных информационных систем — по решению директора Колледжа.

17.2. Контроль уровня защищенности информации проводится не реже одного раза в три года или после компьютерного инцидента. Методы контроля определяются во внутреннем регламенте.

17.3. Результаты контроля оформляются отчетом, который представляется директору Колледжа в течение 3 рабочих дней. В случае выявления нарушений, информация направляется в ФСТЭК России в порядке, установленном законодательством.

18. Заключительные положения

18.1. Настоящая Политика вступает в силу с даты ее утверждения директором Колледжа.

18.2. Изменения и дополнения в настоящую Политику вносятся путем утверждения новой редакции Политики либо путем утверждения изменений и дополнений к ней.

18.3. Контроль за соблюдением требований настоящей Политики возлагается на специалиста по защите информации (или иное назначенное приказом лицо).

18.4. Вопросы, не урегулированные настоящей Политикой, регулируются действующим законодательством Российской Федерации и локальными нормативными актами Колледжа.