АВТОНОМНАЯ НЕКОММЕРЧЕСКАЯ ОРГАНИЗАЦИЯ СРЕДНЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ «МНОГОПРОФИЛЬНЫЙ МЕДИЦИНСКИЙ КОЛЛЕДЖ» (АНО СПО «ММК»)

СОГЛАСОВАНО
Советом АНО СПО «ММК»
(протокол от «11» марта 2026г. № 3)

УТВЕРЖДАЮ
Генеральный директор
АНО СПО «ММК»
_____ П.Г. Харитонова
от «11» марта 2026г.

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
АНО СПО "ММК"
СВЕДЕНИЯ О СЕРТИФИКАТЕ ЭП
029a4a33017db31fb4790936b1f2b223c
Владелец: Харитонова Полина Григорьевна
Должность: Генеральный директор
Структурное подразделение: Руководство
Действителен: с 21.10.2025 до 21.01.2027
2026-03-19 15:48:16

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АВТОНОМНОЙ НЕКОММЕРЧЕСКОЙ ОРГАНИЗАЦИИ СРЕДНЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ «МНОГОПРОФИЛЬНЫЙ МЕДИЦИНСКИЙ КОЛЛЕДЖ»

Санкт-Петербург, 2026

Содержание

1. Общие положения

1.1. Настоящая Политика информационной безопасности (далее - Политика) Автономной некоммерческой организации среднего профессионального образования «Многопрофильный медицинский колледж» (далее - АНО СПО «ММК») разработана в соответствии с целями, задачами и принципами обеспечения безопасности персональных данных.

1.2. Политика разработана в соответствии с требованиями:

- Уголовный кодекс Российской Федерации;
- Федерального закона от 27.07.2006 № 152-ФЗ (последняя редакция) «О персональных данных»;
- Приказа ФСБ России от 10.07.2014 № 378 (последняя редакция) «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»;
- Приказа ФСБ России от 09.02.2005 № 66 (последняя редакция) «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ - 2005)»;
- Постановления Правительства РФ от 06.07.2008 № 512 (последняя редакция) «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных»;
- Указа Президента РФ от 17.03.2008 № 351 (последняя редакция) «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена»;
- Приказа ФСТЭК России от 11.02.2013 № 17 (последняя редакция) «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;
- Постановления Правительства РФ от 15.09.2008 № 687 (последняя редакция) «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- Постановления Правительства РФ от 21.03.2012 № 211 (последняя редакция) «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»;
- Федерального закона от 27.07.2006 № 149-ФЗ (последняя редакция) «Об информации, информационных технологиях и о защите информации»;
- Приказа ФСТЭК России от 18.02.2013 № 21 (последняя редакция) «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
- Постановления Правительства РФ от 01.11.2012 № 1119 (последняя редакция) «Об

утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

- Приказа Роскомнадзора от 19.06.2025 № 140 (последняя редакция) «Об утверждении требований к обезличиванию персональных данных и методов обезличивания персональных данных, за исключением случаев, указанных в пункте 9.1 части 1 статьи 6 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;
- Приказа ФАПСИ от 13.06.2001 № 152 (последняя редакция) «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»;
- «Методические рекомендации по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности» (утв. ФСБ России 31.03.2015 № 149/7/2/6-432);
- «Методический документ. Методика оценки угроз безопасности информации» (утв. ФСТЭК России 05.02.2021).

1.3. В Политике определены требования к персоналу ИСПДн, степень ответственности персонала, структура и необходимый уровень защищенности ИСПДн АНО СПО «ММК».

1.4. Целью настоящей Политики является обеспечение безопасности объектов защиты АНО СПО «ММК» от всех видов угроз, внешних и внутренних, умышленных и непреднамеренных, минимизация ущерба от возможной реализации угроз безопасности ПДн (УБПДн).

1.5. Безопасность персональных данных достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий.

1.6. Информация и связанные с ней ресурсы должны быть доступны для авторизованных пользователей. Должно осуществляться своевременное обнаружение и реагирование на УБПДн.

1.7. Должно осуществляться предотвращение преднамеренных или случайных, частичных или полных несанкционированных модификаций или уничтожения данных.

1.8. Состав объектов защиты представлен в Перечне персональных данных, подлежащих защите.

2. Термины, определения, обозначения и сокращения

Автоматизированная система - система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Безопасность персональных данных - состояние защищенности персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных.

Блокирование персональных данных - временное прекращение сбора, систематизации, накопления, использования, распространения, персональных данных, в том числе их передачи.

Вирус (компьютерный, программный) - исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного

распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению.

Вредоносная программа - программа, предназначенная для осуществления несанкционированного доступа и/или воздействия на персональные данные или ресурсы информационной системы персональных данных.

Доступ в операционную среду компьютера (информационной системы персональных данных) - получение возможности запуска на выполнение штатных команд, функций, процедур операционной системы (уничтожения, копирования, перемещения и т.п.), исполняемых файлов прикладных программ.

Доступ к информации - возможность получения информации и ее использования.

Закладочное устройство - элемент средства съема информации, скрытно внедряемый (закладываемый или вносимый) в места возможного съема информации (в том числе в ограждение, конструкцию, оборудование, предметы интерьера, транспортные средства, а также в технические средства и системы обработки информации).

Защищаемая информация - информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Идентификация - присвоение субъектам и объектам доступа идентификатора и/или сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Информативный сигнал - электрический сигнал, акустические, электромагнитные и другие физические поля, по параметрам которых может быть раскрыта конфиденциальная информация (персональные данные), обрабатываемая в информационной системе персональных данных.

Информационная система персональных данных (ИСПДн) - информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств[1].

Информационные технологии - процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Использование персональных данных - действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц[2].

Источник угрозы безопасности информации - субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации.

Контролируемая зона - пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств.

Конфиденциальность персональных данных - обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного

[1] ст.3 п.9 Федерального закона от 27.07.2006 № 152-ФЗ
[2] ст.3 п.5 Федерального закона от 27.07.2006 № 152-ФЗ

основания.

Межсетевой экран - локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в информационную систему персональных данных и/или выходящей из информационной системы.

Нарушитель безопасности персональных данных - физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных при их обработке техническими средствами в информационных системах персональных данных.

Неавтоматизированная обработка персональных данных - обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы, считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека[3].

Недекларированные возможности - функциональные возможности средств вычислительной техники, не описанные или не соответствующими описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

Несанкционированный доступ (несанкционированные действия) - доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных.

Носитель информации - физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

Обезличивание персональных данных - действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных[4].

Обработка персональных данных - действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование и уничтожение персональных данных[5].

Общедоступные персональные данные - персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности[6].

Оператор (персональных данных) - государственный орган, муниципальный орган, юридическое или физическое лицо, организующее и/или осуществляющее обработку персональных данных, а также определяющие цели и содержание обработки персональных данных[7].

Перехват (информации) - неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов.

Персональные данные - любая информация, относящаяся к определенному или

---

[3] Постановление Правительства РФ от 15.09.2008 № 687
[4] ст.3 п.8 Федерального закона от 27.07.2006 № 152-ФЗ
[5] ст.3 п.3 Федерального закона от 27.07.2006 № 152-ФЗ
[6] ст.3 п.12 Федерального закона от 27.07.2006 № 152-ФЗ
[7] ст.3 п.2 Федерального закона от 27.07.2006 № 152-ФЗ

определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы и другая информация[8].

Побочные электромагнитные излучения и наводки - электромагнитные излучения технических средств обработки защищаемой информации, возникающие как побочное явление и вызванные электрическими сигналами, действующими в их электрических и магнитных цепях, а также электромагнитные наводки этих сигналов на токопроводящие линии, конструкции и цепи питания.

Пользователь информационной системы персональных данных - лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования.

Правила разграничения доступа - совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

Программная закладка - код программы, преднамеренно внесенный в программу с целью осуществить утечку, изменить, блокировать, уничтожить информацию или уничтожить и модифицировать программное обеспечение информационной системы персональных данных и / или блокировать аппаратные средства.

Программное (программно-математическое) воздействие - несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ.

Распространение персональных данных - действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом[9].

Ресурс информационной системы - именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы.

Специальные категории персональных данных- персональные данные, касающиеся расовой и национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья и интимной жизни субъекта персональных данных.

Средства вычислительной техники - совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Субъект доступа (субъект) - лицо или процесс, действия которого регламентируются правилами разграничения доступа.

Технические средства информационной системы персональных данных- средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки ПДн (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации, применяемые в информационных

[8] ст.3 п.1 Федерального закона от 27.07.2006 № 152-ФЗ
[9] ст.3 п.4 Федерального закона от 27.07.2006 № 152-ФЗ

системах.

Технический канал утечки информации - совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.

Трансграничная передача персональных данных - передача персональных данных оператором через Государственную границу Российской Федерации органу власти иностранного государства, физическому или юридическому лицу иностранного государства[10].

Угрозы безопасности персональных данных - совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.

Уничтожение персональных данных - действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.

Утечка (защищаемой) информации по техническим каналам - неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

Учреждение - государственное образовательное учреждение.

Уязвимость - слабость в средствах защиты, которую можно использовать для нарушения системы или содержащейся в ней информации.

Целостность информации - способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

АВС - антивирусные средства;
АРМ - автоматизированное рабочее место;
ВТСС - вспомогательные технические средства и системы;
ИСПДн - информационная система персональных данных;
КЗ - контролируемая зона;
ЛВС - локальная вычислительная сеть;
МЭ - межсетевой экран;
НСд - несанкционированный доступ;
ОС - операционная система;
ПДн - персональные данные;
ПМв - программно-математическое воздействие;
ПО - программное обеспечение;
СУБД - система управления базой данных;
ПЭМИН - побочные электромагнитные излучения и наводки;
САЗ - система анализа защищенности;
СЗИ - средства защиты информации;
СЗПДн - система (подсистема) защиты персональных данных;
СОВ - система обнаружения вторжений;
ТКУИ - технические каналы утечки информации;
УБПДн - угрозы безопасности персональных данных;

[10] ст.3 п.11 Федерального закона от 27.07.2006 № 152-ФЗ

ФСТЭК России - Федеральная служба по техническому и экспортному контролю.

3. Область действия

3.1. Требования настоящей Политики распространяются на всех сотрудников АНО СПО «ММК» (штатных, временных, работающих по контракту и т.п.), а также всех прочих лиц (подрядчики, аудиторы и т.п.).

4. Система защиты персональных данных

4.1. Система защиты персональных данных (СЗПДн), строится на основании:
- Перечня персональных данных, подлежащих защите (Приложение 2);
- Модели угроз безопасности персональных данных;
- Положения об обработке персональных данных;
- Руководящих документов ФСТЭК и ФСБ России.

4.2. На основании этих документов определяется необходимый уровень защищенности ПДн каждой ИСПДн Колледжа. На основании анализа актуальных угроз безопасности ПДн описанного в Модели угроз, делается заключение о необходимости использования технических средств и организационных мероприятий для обеспечения безопасности ПДн.

4.3. Для каждой ИСПДн должен быть составлен список используемых технических средств защиты, а также программного обеспечения, участвующего в обработке ПДн, на всех элементах ИСПДн:
- АРМ пользователей;
- сервера приложений;
- СУБД;
- граница ЛВС;
- каналов передачи в сети общего пользования и (или) международного обмена, если по ним передаются ПДн.

4.4. В зависимости от уровня защищенности ИСПДн и актуальных угроз, СЗПДн может включать следующие технические средства:
- антивирусные средства для рабочих станций пользователей и серверов;
- средства межсетевого экранирования;
- средства криптографической защиты информации, при передаче защищаемой информации по каналам связи.

4.5. Так же в список должны быть включены функции защиты, обеспечиваемые штатными средствами обработки ПДн операционными системами (ОС), прикладным ПО и специальными комплексами, реализующими средства защиты. Список функций защиты может включать:
- управление и разграничение доступа пользователей;
- регистрацию и учет действий с информацией;
- обеспечение целостности данных;
- обнаружение вторжений.

4.6. Список используемых средств должен поддерживаться в актуальном состоянии. При изменении состава технических средств защиты или элементов ИСПДн, соответствующие изменения должны быть внесены в Список и утверждены руководителем Колледжа или лицом, ответственным за обеспечение защиты ПДн.

5. Требования к подсистемам СЗПДН

5.1. Подсистемы управления доступом, регистрации и учета СЗПДн включает в себя следующие

подсистемы:

- управления доступом, регистрации и учета;
- обеспечения целостности и доступности;
- антивирусной защиты;
- межсетевого экранирования;
- анализа защищенности;
- обнаружения вторжений;
- криптографической защиты.

5.1.1. Подсистемы СЗПДн имеют различный функционал в зависимости от класса ИСПДн, определенного в Акте классификации информационной системы персональных данных. Список соответствия функций подсистем СЗПДн классу защищенности представлен в Приложении А.

5.1.2. Подсистема управления доступом, регистрации и учета предназначена для реализации следующих функций:

- идентификации и проверка подлинности субъектов доступа при входе в ИСПДн;
- идентификации терминалов, технических средств, узлов сети, каналов связи, внешних устройств по логическим именам;
- идентификации программ, томов, каталогов, файлов, записей, полей записей по именам;
- контроль доступа пользователей к защищаемым ресурсам в соответствии с матрицей доступа;
- регистрации входа (выхода) субъектов доступа в систему (из системы), либо регистрация загрузки и инициализации операционной системы и ее останова;
- регистрация выдачи печатных (графических) материалов на бумажный носитель;
- регистрация запуска (завершения) программ и процессов (заданий, задач), предназначенных для обработки персональных данных;
- регистрации попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам;
- регистрации попыток доступа программных средств к терминалам, каналам связи, программам, томам, каталогам, файлам, записям, полям записей.

5.1.3. Подсистема управления доступом может быть реализована с помощью штатных средств обработки ПДн (операционных систем, приложений и СУБД). Так же может быть внедрено специальное техническое средство или их комплекс осуществляющие дополнительные меры по аутентификации и контролю. Например, применение единых хранилищ учетных записей пользователей и регистрационной информации, использование биометрических и технических (с помощью электронных пропусков) мер аутентификации и других.

5.2. Подсистемы управления доступом, регистрации и учета.

5.2.1. Подсистема обеспечения целостности и доступности предназначена для обеспечения целостности и доступности ПДн, программных и аппаратных средств ИСПДн Колледжа, а также средств защиты, при случайной или намеренной модификации.

5.2.2. Подсистема обеспечения целостности и доступности предназначена для реализации следующих функций:

- резервное копирование обрабатываемых данных;
- обеспечение целостности программных средств защиты персональных данных, обрабатываемой информации, а также неизменность программной среды;

- периодическое тестирование функций системы защиты персональных данных с помощью тест-программ, имитирующих попытки несанкционированного доступа;
- наличие средств восстановления системы защиты персональных данных.

5.2.3. Подсистема реализуется с помощью организации резервного копирования обрабатываемых данных, проверкой при загрузке системы контрольных сумм компонентов средств защиты информации, ведением двух копий программных компонент средств защиты информации и их периодическим обновлением и контролем работоспособности, а так же резервированием ключевых элементов ИСПДн.

5.3. Подсистема антивирусной защиты.

5.3.1. Подсистема антивирусной защиты предназначена для обеспечения антивирусной защиты серверов и АРМ пользователей ИСПДн АНО СПО «ММК».

5.3.2. Средства антивирусной защиты предназначены для реализации следующих функций:

- резидентный антивирусный мониторинг;
- антивирусное сканирование;
- скрипт-блокирование;
- централизованную/удаленную установку/деинсталляцию антивирусного продукта, настройку, администрирование, просмотр отчетов и статистической информации по работе продукта;
- автоматизированное обновление антивирусных баз;
- ограничение прав пользователя на остановку исполняемых задач и изменения настроек антивирусного программного обеспечения;
- автоматический запуск сразу после загрузки операционной системы.

5.3.3. Подсистема реализуется путем внедрения специального антивирусного программного обеспечения на все элементы ИСПДн.

5.4. Подсистема межсетевого экранирования.

5.4.1. Подсистема межсетевого экранирования предназначена для реализации следующих функций:

- фильтрацию на сетевом уровне для каждого сетевого пакета независимо (решение о фильтрации принимается на основе сетевых адресов отправителя и получателя или на основе других эквивалентных атрибутов);
- фильтрацию пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств;
- фильтрацию с учетом входного и выходного сетевого интерфейса как средства проверки подлинности сетевых адресов;
- фильтрацию с учетом любых значимых полей сетевых пакетов;
- фильтрацию на транспортном уровне запросов на установление виртуальных соединений с учетом транспортных адресов отправителя и получателя;
- фильтрацию на прикладном уровне запросов к прикладным сервисам с учетом прикладных адресов отправителя и получателя;
- фильтрацию с учетом даты и времени;
- аутентификацию входящих и исходящих запросов методами, устойчивыми к пассивному и (или) активному прослушиванию сети;
- регистрацию и учет фильтруемых пакетов (в параметры регистрации включаются адрес, время и результат фильтрации);

- регистрацию и учет запросов на установление виртуальных соединений;
- локальную сигнализацию попыток нарушения правил фильтрации;
- идентификацию и аутентификацию администратора межсетевого экрана при его локальных запросах на доступ по идентификатору (коду) и паролю условно-постоянного действия;
- предотвращение доступа неидентифицированного пользователя или пользователя, подлинность идентификации которого при аутентификации не подтвердилась;
- идентификацию и аутентификацию администратора межсетевого экрана при его удаленных запросах методами, устойчивыми к пассивному и активному перехвату информации;
- регистрацию входа (выхода) администратора межсетевого экрана в систему (из системы) либо загрузки и инициализации системы и ее программного останова (регистрация выхода из системы не проводится в моменты аппаратурного отключения межсетевого экрана);
- регистрацию запуска программ и процессов (заданий, задач);
- регистрацию действия администратора межсетевого экрана по изменению правил фильтрации;
- возможность дистанционного управления своими компонентами, в том числе возможность конфигурирования фильтров, проверки взаимной согласованности всех фильтров, анализа регистрационной информации;
- контроль целостности своей программной и информационной части;
- контроль целостности программной и информационной части межсетевого экрана по контрольным суммам;
- восстановление свойств межсетевого экрана после сбоев и отказов оборудования;
- регламентное тестирование реализации правил фильтрации, процесса регистрации, процесса идентификации и аутентификации запросов, процесса идентификации и аутентификации администратора межсетевого экрана, процесса регистрации действий администратора межсетевого экрана, процесса контроля за целостностью программной и информационной части, процедуры восстановления.

5.4.2. Подсистема реализуется внедрением программно-аппаратных комплексов межсетевого экранирования на границе J1СВ, классом не ниже 4.

5.5. Подсистема анализа защищенности.

5.5.1. Подсистема анализа защищенности, должна обеспечивать выявления уязвимостей, связанных с ошибками в конфигурации ПО ИСПДн, которые могут быть использованы нарушителем для реализации атаки на систему.

5.5.2. Функционал подсистемы может быть реализован программными и программно-аппаратными средствами анализа защищенности.

5.6. Подсистема обнаружения вторжений.

5.6.1. Подсистема обнаружения вторжений, должна обеспечивать выявление сетевых атак на элементы ИСПДн подключенные к сетям общего пользования и (или) международного обмена.

5.6.2. Функционал подсистемы может быть реализован программными и программно-аппаратными средствами обнаружения вторжений.

5.7. Подсистема криптографической защиты.

5.7.1. Подсистема криптографической защиты предназначена для исключения НСД к защищаемой информации в ИСПДн Колледжа, при ее передаче по каналам связи сетей общего пользования и (или) международного обмена.

5.7.2. Подсистема реализуется внедрения криптографических программно-аппаратных комплексов.

6. Пользователи ИСПДн

6.1. В Концепции информационной безопасности определены основные категории пользователей. На основании этих категорий должна быть произведена типизация пользователей ИСПДн, определен их уровень доступа и возможности.

6.2. В ИСПДн АНО СПО «ММК» можно выделить следующие группы пользователей, участвующих в обработке и хранении ПДн:

- Специалист, который настраивает, поддерживает и защищает ИТ-инфраструктуру (далее – Системный администратор);
- Оператор АРМ.

6.3. Данные о группах пользователях, уровне их доступа и информированности должен быть отражен в Положении об обработке персональных данных.

6.4. Системный администратор.

6.4.1. Системный администратор, сотрудник АНО СПО «ММК», ответственный за настройку, внедрение и сопровождение ИСПДн. Обеспечивает функционирование подсистемы управления доступом ИСПДн и уполномочен осуществлять предоставление и разграничение доступа конечного пользователя (Оператора АРМ) к элементам, хранящим персональные данные, ответственный за функционирование СЗПДн, включая обслуживание и настройку административной, серверной и клиентской компонентов. Является ответственным за функционирование телекоммуникационной подсистемы ИСПДн. Осуществляет обслуживание и настройку периферийного оборудования ИСПДн.

6.4.2. Системный администратор обладает следующим уровнем доступа и знаний:

- обладает полной информацией о системном и прикладном программном обеспечении ИСПДн;
- обладает полной информацией о технических средствах и конфигурации ИСПДн;
- имеет доступ ко всем техническим средствам обработки информации и данным ИСПДн;
- обладает правами конфигурирования и административной настройки технических средств ИСПДн;
- имеет физический доступ к техническим средствам обработки информации и средствам защиты;
- обладает правами Администратора ИСПДн;
- обладает полной информацией об ИСПДн;
- имеет доступ к средствам защиты информации и протоколирования и к части ключевых элементов ИСПДн.

6.4.3. Системный администратор уполномочен:

- реализовывать политики безопасности в части настройки СКЗИ, межсетевых экранов и систем обнаружения атак, в соответствии с которыми пользователь (Оператор АРМ) получает возможность работать с элементами ИСПДн;
- осуществлять аудит средств защиты;

- устанавливать доверительные отношения своей защищенной сети с другими сетями АНО СПО «ММК».

6.5. Оператор АРМ.

6.5.1. Оператор АРМ, сотрудник АНО СПО «ММК», осуществляющий обработку ПДн. Обработка ПДн включает:

- возможность просмотра ПДн;
- ручной ввод ПДн в систему ИСПДн;
- формирование справок и отчетов по информации, полученной из ИСПД.

6.5.2. Оператор не имеет полномочий для управления подсистемами обработки данных и СЗПДн.

6.5.3. Оператор ИСПДн обладает следующим уровнем доступа и знаний:

- обладает всеми необходимыми атрибутами (например, паролем), обеспечивающими доступ к некоторому подмножеству ПДн;
- располагает конфиденциальными данными, к которым имеет доступ.

7. Требования к персоналу по обеспечению защиты ПДн

7.1. Все сотрудники АНО СПО «ММК», являющиеся пользователями ИСПДн, должны четко знать и строго выполнять установленные правила и обязанности по доступу к защищаемым объектам и соблюдению принятого режима безопасности ПДн.

7.2. При вступлении в должность нового сотрудника непосредственный начальник подразделения, в которое он поступает, обязан организовать его ознакомление с должностной инструкцией и необходимыми документами, регламентирующими требования по защите ПДн, а также обучение навыкам выполнения процедур, необходимых для санкционированного использования ИСПДн.

7.3. Сотрудник должен быть ознакомлен со сведениями настоящей Политики, принятых процедур работы с элементами ИСПДн и СЗПДн.

7.4. Сотрудники АНО СПО «ММК», использующие технические средства аутентификации, должны обеспечивать сохранность идентификаторов (электронных ключей) и не допускать НСД к ним, а также возможность их утери или использования третьими лицами. Пользователи несут персональную ответственность за сохранность идентификаторов.

7.5. Сотрудники АНО СПО «ММК» должны следовать установленным процедурам поддержания режима безопасности ПДн при выборе и использовании паролей (если не используются технические средства аутентификации).

7.6. Сотрудники АНО СПО «ММК» должны обеспечивать надлежащую защиту оборудования, оставляемого без присмотра, особенно в тех случаях, когда в помещение имеют доступ посторонние лица. Все пользователи должны знать требования по безопасности ПДн и процедуры защиты оборудования, оставленного без присмотра, а также свои обязанности по обеспечению такой защиты.

7.7. Сотрудникам запрещается устанавливать постороннее программное обеспечение, подключать личные мобильные устройства и носители информации, а также записывать на них защищаемую информацию.

7.8. Сотрудникам запрещается разглашать защищаемую информацию, которая стала им известна при работе с информационными системами АНО СПО «ММК» третьим лицам.

7.9. При работе с ПДн в ИСПДн сотрудники АНО СПО «ММК» обязаны обеспечить отсутствие возможности просмотра ПДн третьими лицами с мониторов АРМ или терминалов.

7.10. При завершении работы с ИСПДн сотрудники обязаны защитить АРМ или терминалы с

помощью блокировки ключом или эквивалентного средства контроля, например, доступом по паролю, если не используются более сильные средства защиты.

7.11. Сотрудники АНО СПО «ММК» должны быть проинформированы об угрозах нарушения режима безопасности ПДн и ответственности за его нарушение. Они должны быть ознакомлены с утвержденной формальной процедурой наложения дисциплинарных взысканий на сотрудников, которые нарушили принятые политику и процедуры безопасности ПДн.

7.12. Сотрудники обязаны без промедления сообщать обо всех наблюдаемых или подозрительных случаях работы ИСПДн, могущих повлечь за собой угрозы безопасности ПДн, а также о выявленных ими событиях, затрагивающих безопасность ПДн, руководству подразделения и лицу, отвечающему за немедленное реагирование на угрозы безопасности ПДн.

8. Ответственность сотрудников ИСПДн

8.1. В соответствии со ст. 24 Федерального закона РФ от 27.07.2006 № 152-ФЗ «О персональных данных» лица, виновные в нарушении требований настоящего Федерального закона, несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

8.2. Действующее законодательство РФ позволяет предъявлять требования по обеспечению безопасной работы с защищаемой информацией и предусматривает ответственность за нарушение установленных правил эксплуатации ЭВМ и систем, неправомерный доступ к информации, если эти действия привели к уничтожению, блокированию, модификации информации или нарушению работы ЭВМ или сетей[11].

8.3. Системный администратор и Администратор сети несут ответственность за все действия, совершенные от имени их учетных записей или системных учетных записей, если не доказан факт несанкционированного использования учетных записей.

8.4. При нарушениях сотрудниками АНО СПО «ММК» - пользователей ИСПДн правил, связанных с безопасностью ПДн, они несут ответственность, установленную действующим законодательством Российской Федерации.

8.5. Приведенные выше требования нормативных документов по защите информации должны быть отражены в Положениях о подразделениях АНО СПО «ММК», осуществляющих обработку ПДн в ИСПДн и должностных инструкциях сотрудников АНО СПО «ММК».

8.6. Необходимо внести в Положения о подразделениях АНО СПО «ММК», осуществляющих обработку ПДн в ИСПДн сведения об ответственности их руководителей и сотрудников за разглашение и несанкционированную модификацию (искажение, фальсификацию) ПДн, а также за неправомерное вмешательство в процессы их автоматизированной обработки.

9. Заключительные положения

9.1. Настоящая Политика является локальным нормативным актом и утверждается приказом генерального директора колледжа.

9.2. Все изменения и дополнения, вносимые в настоящую Политику, оформляются в письменной форме в соответствии с действующим законодательством Российской Федерации.

9.3. Настоящая Политика вступает в силу с момента ее утверждения.

9.4. После принятия Политики (или изменений и дополнений отдельных пунктов и разделов) в новой редакции предыдущая редакция автоматически утрачивает силу.

---

[11] ст. 272, 273, 274 Уголовного кодекса Российской Федерации от 13.06.1996 № 63-ФЗ

Приложение 1

Под актуальными угрозами безопасности персональных данных понимается совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к персональным данным при их обработке в информационной системе, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия.

Угрозы 1-го типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в системном программном обеспечении, используемом в информационной системе.

Угрозы 2-го типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в прикладном программном обеспечении, используемом в информационной системе.

Угрозы 3-го типа актуальны для информационной системы, если для нее актуальны угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе.

Уровень защищенности ИСПДн			
Категория ПДн + кол-во	**АУ 1 типа**	**АУ 2 типа**	**АУ 3 типа**
Спец. категории ПДн более чем 100 ООО субъектов ПДн, не являющихся сотрудниками оператора	1	1	2
Спец. категории ПДн сотрудников оператора или специальные категории персональных данных менее чем 100 ООО субъектов ПДн, не являющихся сотрудниками оператора	1	2	3
Биометрические ПДн	1	2	3
Иные категории ПДн более чем 100 ООО субъектов ПДн, не являющихся сотрудниками оператора	1	2	3
Иные категории ПДн данных сотрудников оператора или иные категории ПДн менее чем 100000 субъектов ПДн, не являющихся сотрудниками оператора	1	3	4
Общедоступные ПДн более чем 100 000 субъектов ПДн, не являющихся сотрудниками оператора	2	2	4
Общедоступные ПДн сотрудников оператора или общедоступные ПДн менее чем 100 000 субъектов ПДн, не являющихся сотрудниками оператора	2	3	4

Перечень требований к уровням защищенности				
Требования	**1**	**2**	**3**	**4**
Регулярный контроль за выполнением требований Контроль за выполнением настоящих требований организуется и проводится оператором (уполномоченным лицом) самостоятельно и (или) с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации. Указанный контроль проводится не реже 1 раза в 3 года в сроки, определяемые оператором (уполномоченным лицом)	*	*	*	*
Физ. безопасность и контроль доступа Организация режима обеспечения безопасности помещений, в которых размещена ИСПДн, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения	*	*	*	*
Безопасность носителей Обеспечение сохранности носителей персональных данных	*	*	*	*
Перечень допущенных лиц Утверждение руководителем оператора документа, определяющего перечень лиц, доступ	*	*	*	*

которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей				
Сертифицированные СЗИ Использование СЗИ, прошедших процедуру оценки соответствия требованиям законодательства РФ в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз	*	*	*	*
Назначение ответственного за безопасность ПДн Назначение должностного лица (работника), ответственного за обеспечение безопасности ПДн в ИСПДн	*	*	*	
Контроль доступа к эл. журналу доступа Обеспечение доступа к содержанию электронного журнала сообщений исключительно для должностных лиц (работников) оператора или уполномоченного лица, которым сведения, содержащиеся в указанном журнале, необходимы для выполнения служебных (трудовых) обязанностей	*	*		
Автоматическая регистрация в эл. журнале доступа Автоматическая регистрация в электронном журнале безопасности изменения полномочий сотрудника оператора по доступу к ПДн, содержащимся в ИСПДн	*			
Создание структурного подразделения Создание структурного подразделения, ответственного за обеспечение безопасности ПДн в ИСПДн, либо возложение на одно из структурных подразделений функций по обеспечению такой безопасности	*			

Приложение 2

Перечень персональных данных, подлежащих защите

1. Работники АНО СПО «ММК», бывшие работники, кандидаты на замещение вакантных должностей, а также родственники работников.

В данной категории субъектов оператором обрабатываются персональные данные в связи с реализацией трудовых отношений:

- фамилия, имя, отчество;
- пол;
- гражданство;
- дата (число, месяц, год) и место рождения (страна, республика, край, область, район, город, поселок, деревня, иной населенный пункт);
- адрес места проживания (почтовый индекс, страна, республика, край, область, район, город, поселок, деревня, иной населенный пункт, улица, дом, корпус, квартира);
- сведения о регистрации по месту жительства или пребывания (почтовый индекс, страна, республика, край, область, район, город, поселок, деревня, иной населенный пункт, улица, дом, корпус, квартира);
- номера телефонов (домашний, мобильный, рабочий), адрес электронной почты;
- замещаемая должность;
- сведения о трудовой деятельности (наименования организаций (органов) и занимаемых должностей, продолжительность работы (службы) в этих организациях (органах));
- идентификационный номер налогоплательщика (дата (число, месяц, год) и место постановки на учет, дата (число, месяц, год) выдачи свидетельства);
- данные страхового свидетельства обязательного пенсионного страхования;
- данные полиса обязательного медицинского страхования;
- данные паспорта или иного удостоверяющего личность документа;
- данные паспорта, удостоверяющего личность гражданина Российской Федерации за пределами территории Российской Федерации;
- данные трудовой книжки, вкладыша в трудовую книжку;
- сведения о воинском учете (серия, номер, дата (число, месяц, год) выдачи, наименование органа, выдавшего военный билет, военно-учетная специальность, воинское звание, данные о принятии/снятии на (с) учет(а), о прохождении военной службы, о пребывании в запасе, о медицинском освидетельствовании и прививках);
- сведения об образовании (наименование образовательной организации, дата (число, месяц, год) окончания, специальность и квалификация, ученая степень, звание, реквизиты документа об образовании и о квалификации);
- сведения о получении дополнительного профессионального образования (дата (число, месяц, год), место, программа, реквизиты документов, выданных по результатам);
- сведения о владении иностранными языками (иностранный язык, уровень владения);
- сведения о судимости (наличие (отсутствие) судимости, дата (число, месяц, год) привлечения к уголовной ответственности (снятия или погашения судимости), статья);
- сведения о дееспособности (реквизиты документа, устанавливающие опеку (попечительство), основания ограничения в дееспособности, реквизиты решения суда);
- сведения об участии в управлении хозяйствующим субъектом (за исключением жилищного, жилищно-строительного, гаражного кооперативов, садоводческого,

огороднического, дачного потребительских кооперативов, товарищества собственников недвижимости и профсоюза, зарегистрированного в установленном порядке), занятии предпринимательской деятельностью;

- сведения, содержащиеся в медицинском заключении установленной формы об отсутствии у гражданина заболевания, препятствующего поступлению на гражданскую службу или ее прохождению (наличие (отсутствие) заболевания, форма заболевания);
- сведения о наградах, иных поощрениях и знаках отличия (название награды, поощрения, знака отличия, дата (число, месяц, год) присвоения, реквизиты документа о награждении или поощрении);
- сведения о дисциплинарных взысканиях;
- сведения, содержащиеся в материалах служебных проверок;
- сведения о семейном положении (состояние в браке (холост (не замужем), женат (замужем), повторно женат (замужем), разведен(а), вдовец (вдова), с какого времени в браке, с какого времени в разводе, количество браков, состав семьи, реквизиты свидетельства о заключении брака);
- сведения о близких родственниках, свойственниках (степень родства, фамилия, имя, отчество, дата (число, месяц, год) и место рождения, место и адрес работы (службы), адрес места жительства, сведения о регистрации по месту жительства или пребывания);
- сведения, содержащиеся в справках о доходах, расходах, об имуществе и обязательствах имущественного характера;
- номер расчетного счета;
- информация об оформленных допусках к государственной тайне;
- фотографии;
- и другие сведения, предусмотренные действующим законодательством.

2. Клиенты и контрагенты оператора (физические лица).

В данной категории субъектов оператором обрабатываются персональные данные, полученные оператором в связи с заключением договора, стороной которого является субъект персональных данных, и используемые оператором исключительно для исполнения указанного договора и заключения договоров с субъектом персональных данных:

- фамилия, имя, отчество;
- пол;
- гражданство;
- дата (число, месяц, год) и место рождения (страна, республика, край, область, район, город, поселок, деревня, иной населенный пункт);
- адрес места проживания (почтовый индекс, страна, республика, край, область, район, город, поселок, деревня, иной населенный пункт, улица, дом, корпус, квартира);
- сведения о регистрации по месту жительства или пребывания (почтовый индекс, страна, республика, край, область, район, город, поселок, деревня, иной населенный пункт, улица, дом, корпус, квартира);
- номера телефонов (домашний, мобильный, рабочий), адрес электронной почты;
- замещаемая должность;
- идентификационный номер налогоплательщика (дата (число, месяц, год) и место постановки на учет, дата (число, месяц, год) выдачи свидетельства);
- данные паспорта или иного удостоверяющего личность документа;
- сведения об участии в управлении хозяйствующим субъектом (за исключением

жилищного, жилищно-строительного, гаражного кооперативов, садоводческого, огороднического, дачного потребительских кооперативов, товарищества собственников недвижимости и профсоюза, зарегистрированного в установленном порядке), занятии предпринимательской деятельностью;

- номер расчетного счета;
- и другие сведения, предусмотренные действующим законодательством.

3. Представители/работники клиентов и контрагентов АНО СПО «ММК» (юридических лиц).

В данной категории субъектов оператором обрабатываются персональные данные, полученные оператором в связи с заключением договора, стороной которого является клиент/контрагент (юридическое лицо), и используемые оператором исключительно для исполнения указа иного договора:

- фамилия, имя, отчество;
- пол;
- номера телефонов (домашний, мобильный, рабочий), адрес электронной почты;
- замещаемая должность;
- данные паспорта или иного удостоверяющего личность документа;
- сведения об участии в управлении хозяйствующим субъектом (за исключением жилищного, жилищно-строительного, гаражного кооперативов, садоводческого, огороднического, дачного потребительских кооперативов, товарищества собственников недвижимости и профсоюза, зарегистрированного в установленном порядке), занятии предпринимательской деятельностью;
- и иные сведения, предусмотренные действующим законодательством.

4. Обработка специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, допускается:

- в случае, если субъект персональных данных дал согласие в письменной форме на обработку своих персональных данных;
- в соответствии с законодательством о государственной социальной помощи, трудовым законодательством, пенсионным законодательством Российской Федерации.

5. Обработка биометрических персональных данных может осуществляться только при наличии согласия в письменной форме субъекта персональных данных.