РОССИЙСКАЯ ФЕДЕРАЦИЯ
Администрация Ленинградской области
КОМИТЕТ
ОБЩЕГО И ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
ЛЕНИНГРАДСКОЙ ОБЛАСТИ

ПРИКАЗ

25.05.2023 № 20

Об организации деятельности по защите информации в комитете общего и профессионального образования Ленинградской области

На основании Федеральных законов от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» и от 27 июля 2006 г. № 152-ФЗ «О персональных данных», постановления Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Указа Президента Российской Федерации от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена», приказов ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» и 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», приказа Федеральной службы безопасности Российской Федерации и Федеральной службы по техническому и экспортному контролю от 31 августа 2010 г. № 416/489 «Об утверждении Требований о защите информации, содержащейся в информационных системах общего пользования», «Специальных требований и рекомендаций по технической защите конфиденциальной информации (СТР-К)», утверждённых приказом председателя Гостехкомиссии России от 30 августа 2002 г. № 282, других нормативных правовых актов Российской Федерации, нормативных и методических документов в области защиты информации, для выполнения обязательных требований по защите конфиденциальной и иной информации, предъявляемых в соответствии с законодательством Российской Федерации,

Ленинградской области, во исполнение распоряжения Правительства Ленинградской области № 237-р от 19 апреля 2023 г. «О развитии государственной информационной системы «Современное образование Ленинградской области»:

1. Утвердить:

Положение о порядке организации и проведении работ по защите информации согласно приложению № 1 к настоящему приказу;

Перечень защищаемых информационных ресурсов согласно приложению № 2 к настоящему приказу;

Инструкцию должностного лица, ответственного за защиту информации согласно приложению № 3 к настоящему приказу;

Порядок допуска должностных лиц и обслуживающего персонала в помещения, в которых ведётся обработка защищаемых информационных ресурсов и к обрабатывающим их техническим средствам в рабочее и нерабочее время, а также в нештатных ситуациях согласно приложению № 4 к настоящему приказу;

Правила разграничения доступа к защищаемым информационным ресурсам, обрабатываемым с использованием средств вычислительной техники согласно приложению № 5 к настоящему приказу;

Порядок учета, хранения и уничтожения машинных носителей, защищаемых информационных ресурсов согласно приложению № 6 к настоящему приказу.

2. Контроль за исполнением настоящего приказа оставляю за собой.

Исполняющий обязанности
председателя комитета И.А. Голубев

Подлинник электронного документа, подписанного ЭП, хранится в Межведомственной системе электронного документооборота Правительства Ленинградской области

СВЕДЕНИЯ О СЕРТИФИКАТЕ ЭП

Сертификат: 00EE9DC220E212D69E797A9B89CC01B8E0
Владелец: Голубев Илья Александрович
Действителен с 19-08-2022 до 12-11-2023

«УТВЕРЖДЕНО»
приказом комитета общего
и профессионального образования
Ленинградской области
от 25.05.2023 года № 20
(приложение 1)

Положение о порядке организации и проведении работ по защите информации

1. Общие положения

1.1. Положение разработано на основании Федеральных законов от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» и от 27 июля 2006 г. № 152-ФЗ «О персональных данных», Указа Президента Российской Федерации от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена», постановления Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», приказов ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» и 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», «Специальных требований и рекомендаций по технической защите конфиденциальной информации (СТР-К)», утверждённых приказом председателя Гостехкомиссии России от 30 августа 2002 г. № 282, и других нормативных правовых актов Российской Федерации, нормативных и методических документов в области защиты информации.

1.2. Положение определяет порядок организации и проведения работ по защите конфиденциальной информации и (или) информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, содержащейся в государственных информационных системах, и является обязательным для выполнения всеми должностными лицами, имеющими право доступа в служебные помещения комитета общего и профессионального образования Ленинградской области, при проведении работ, требующих защиты информации на разрабатываемых,

реконструируемых и действующих (находящихся в эксплуатации) объектах информатизации.

1.3. К объектам информатизации относится совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, средств обеспечения объекта информатизации, помещений или объектов (зданий, сооружений, технических средств), в которых они установлены, или помещения, предназначенные для ведения конфиденциальных переговоров.

1.4. Защита информации на объекте информатизации достигается выполнением комплекса организационно-технических мероприятий с применением средств защиты информации от утечки по техническим каналам, несанкционированного доступа, по предупреждению преднамеренных программно-технических воздействий с целью нарушения конфиденциальности, целостности и доступности информации в процессе ее производства, сбора, хранения, обработки, передачи, работоспособности технических средств.

1.5. Работы по защите информации являются составной частью служебной деятельности и осуществляются совместно с другими служебными обязанностями.

1.6. Для защиты информации, на объектах информатизации применяются сертифицированные по требованиям безопасности средства защиты информации.

1.7. Объекты информатизации, обрабатывающие защищаемую информацию, должны быть аттестованы по требованиям безопасности информации.

2. Порядок определения защищаемой информации.

2.1. Отнесение информации к защищаемой осуществляется в соответствии с перечнем защищаемых информационных ресурсов, утверждённым председателем комитета общего и профессионального образования Ленинградской области.

2.2. К защищаемой информации может относиться речевая информация, документированная информация, информация обрабатываемая техническими средствами, а также представленная в виде информативных электрических сигналов, физических полей, носителей на оптической, магнитной и иной основе.

2.3. Решение об отнесении информации к защищаемой определяется исполнителем, непосредственно организующим или осуществляющим обработку такой информации, или (и) должностным лицом, подписывающим или утверждающим документ.

3. Организация и проведение работ по защите информации

3.1. Защита информации, обрабатываемой с использованием средств вычислительной техники, является составной частью работ по созданию и эксплуатации объектов информатизации и должна осуществляться в установленном, в соответствии требованиями законодательства Российской Федерации, порядке.

3.2. Организация работ по защите информации возлагается на заместителя председателя комитета – начальника департамента профессионального образования, развития инфраструктуры и организационной деятельности Колыхматова В.И.

3.3. Общую координацию деятельности и методическое руководство по вопросам защиты информации осуществляет Комитет цифрового развития Ленинградской области (далее – уполномоченный ОИВ ЛО).

3.4. Разработка мер и обеспечение защиты информации осуществляется уполномоченным ОИВ ЛО, ответственным за защиту информации и должностными лицами, обрабатывающими защищаемую информацию.

3.5. Деятельность по защите информации осуществляется непрерывно и реализуется в виде системы защиты информации включающей в себя правовые, организационные и технические мероприятия.

3.6. Разработка и внедрение системы защиты информации осуществляется уполномоченным ОИВ ЛО во взаимодействии с ответственным по защите информации, который в рамках свей компетенции участвует в разработке конкретных требований по защите информации, аналитическом обосновании необходимости создания системы защиты информации, согласовании выбора средств вычислительной техники и связи, технических и программных средств защиты информации, организации работ по выявлению возможных каналов утечки информации или воздействий на нее, предупреждению утечки и нарушению целостности защищаемой информации, в аттестации объектов информатизации.

3.7. При решении задач и выполнении обязанностей (функций), связанных с защитой информации, ответственный по защите информации, взаимодействует с уполномоченным ОИВ ЛО.

3.8. Должностные лица, работающие с защищаемой информацией, при обеспечении её защиты руководствуются локальными организационно-распорядительными документами в области информационной безопасности.

3.9. Порядок проведения работ специализированными организациями при разработке, создании и (или) обслуживании объектов информатизации, их задачи и функции на различных стадиях выполнения работ определяются при заключении договоров (контрактов).

4. Контроль организации и состояния работ по защите информации

4.1. С целью своевременного выявления и предотвращения утечки информации по техническим каналам, исключения или существенного

затруднения несанкционированного доступа к ней и предотвращения специальных программно-технических воздействий, вызывающих нарушение конфиденциальности, целостности, доступности информации, проводится периодический контроль организации и состояния работ по защите информации.

4.2. Контроль осуществляется уполномоченным ОИВ ЛО и ответственным за защиту информации, в пределах их компетенции.

4.3. Контроль заключается в проверке выполнения обязательных требований нормативных правовых актов Российской Федерации, нормативных и методических документов федеральных органов исполнительной власти уполномоченных по вопросам информационной безопасности, а также в оценке обоснованности и эффективности принятых мер защиты для обеспечения соблюдения, утвержденных требований и норм по защите информации.

4.4. Контроль проводиться на предмет:

выполнения мероприятий установленных требованиями нормативных и правовых актов, нормативных и методических документов Российской Федерации в области защиты информации;

работоспособности и эффективности применяемых средств защиты информации в соответствии с их эксплуатационной документацией и установленными нормами;

знаний и выполнения должностными лицами своих функциональных обязанностей в части защиты информации.

4.5. Повседневный контроль за состоянием защиты информации проводится уполномоченным ОИВ ЛО, и ответственным за защиту информации, в пределах их компетенции.

4.6. Периодический контроль, проводимый уполномоченным ОИВ ЛО осуществляется по согласованию с председателем комитета общего и профессионального образования Ленинградской области. По результатам такого контроля составляется справка о состоянии работ по защите информации, которая предоставляется председателю комитета общего и профессионального образования Ленинградской области, в отношении которого проводился контроль.

4.7. Защита информации считается эффективной, если принимаемые меры соответствуют установленным требованиям и нормам.

5. Ответственность должностных лиц за своевременность и качество организации и выполнения работ по защите информации

5.1. Ответственность за организацию работ по защите информации возлагается на заместителя председателя комитета общего и профессионального образования Ленинградской области – начальника департамента профессионального образования, развития инфраструктуры и организационной деятельности Колыхматова В.И.

5.2. Ответственность за разработку и внедрение средств защиты информации несет уполномоченный ОИВ ЛО и ответственный по защите информации, в пределах их компетенции.

5.3. Ответственность за выполнение мероприятий по защите информации несут уполномоченный ОИВ ЛО, ответственный по защите информации и должностные лица, имеющих право доступа к защищаемым информационным ресурсам, в пределах их компетенции.

5.4. Должностные лица, организующие работу с защищаемой информацией, несут персональную ответственность за соблюдение требований настоящего положения.

5.5. Должностные лица, принявшие решение об отнесении информации к защищаемой, несут персональную ответственность за обоснованность принятого решения.

5.6. За разглашение конфиденциальной информации, а также нарушение порядка обращения с защищаемой информацией, должностные лица могут быть привлечены к дисциплинарной или иной предусмотренной законодательством Российской Федерации ответственности.

«УТВЕРЖДЕН»
приказом комитета общего
и профессионального образования
Ленинградской области
от 25.05.2023 года № 20
(приложение 2)

Перечень защищаемых информационных ресурсов

1. Настоящий перечень разработан в целях исполнения законодательства Российской Федерации, регулирующего отношения, возникающие при осуществлении права на производство, поиск, получение, хранение, передачу, и распространение информации в комитете общего и профессионального образования Ленинградской области.

2. При разработке учитывались положения федеральных законов от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и защите информации» и от 27 июля 2006 г. № 152 «О персональных данных», Указа Президента Российской Федерации от 06 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера», приказа ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», «Специальных требований и рекомендации по технической защите конфиденциальной информации (СТР-К)», утвержденных приказом Гостехкомиссии России от 30 августа 2002 г. № 282.

3. Данный перечень не включает в себя служебную информацию ограниченного распространения с пометкой «Для служебного пользования».

4. К защищаемым информационным ресурсам в комитете общего и профессионального образования Ленинградской области относятся сведения конфиденциального характера:

сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях.

«УТВЕРЖДЕНА»
приказом комитета общего
и профессионального образования
Ленинградской области
от 25.05.2023 года № 20
(приложение 3)

Инструкция должностного лица, ответственного за защиту информации

1. Общие положения

1.1. Настоящая инструкция определяет основные функции и права ответственного за защиту информации в комитете общего и профессионального образования Ленинградской области.

1.2. Ответственный за защиту информации назначается председателем комитета общего и профессионального образования Ленинградской области.

1.3. Ответственный за защиту информации осуществляет свою деятельность в соответствии с локальными организационно-распорядительными документами по защите информации.

2. Основные функции ответственного за защиту информации

Основными функциями ответственного за защиту информации, в пределах его компетенции, являются:

1) проведение единой политики по обеспечению безопасности информации;

2) осуществление контроля за соблюдением локальных организационно-распорядительных документов в области информационной безопасности, должностными лицами;

3) организация учета и хранения машинных носителей информации, содержащих защищаемую информацию;

4) участие в разработке (доработке) локальных организационно-распорядительных документов по обеспечению безопасности информации;

5) информирование уполномоченного по вопросам защиты информации органа исполнительной власти Ленинградской области (уполномоченный ОИВ ЛО) о выявленных фактах нарушения установленного порядка и попытках несанкционированного доступа к защищаемым информационным ресурсам или иных неправомерных действиях по отношению к такой информации;

6) разработка предложений, участие в проводимых работах по созданию или совершенствованию системы защиты информации;

7) присутствие при выполнении технического обслуживания элементов автоматизированных систем в защищенном исполнении (АСЗИ) сторонними организациями.

3. Права ответственного за защиту информации

Ответственный за защиту информации имеет право:

1) запрашивать и получать от уполномоченного ОИВ ЛО, в рамках своей компетенции, необходимые материалы для организации и проведения работ по защите информации;

2) разрабатывать проекты локальных организационно-распорядительных документов по обеспечению безопасности информации;

3) контролировать деятельность структурных подразделений в части выполнения ими требований по обеспечению безопасности информации;

4) привлекать необходимых специалистов уполномоченного ОИВ ЛО для установки и настройки средств защиты информаций;

5) запрещать устанавливать на рабочих станциях АСЗИ программное и аппаратное обеспечение, не связанное с выполнением должностными лицами своих обязанностей.

4.Обязанности ответственного за защиту информации

Ответственный за защиту информации обязан:

1) осуществлять планирование работ по защите информации от ее утечки по техническим каналам;

2) организовывать защиту и аттестацию объектов информатизации по выполнению требований защиты информации при проведении работ с информацией ограниченного доступа;

3) организовывать и проводить работы по категорированию информации, по созданию и обновлению перечня конфиденциальной информации и перечня конфиденциальных ресурсов, по классификации автоматизированных систем (АС) обработки информации ограниченного доступа, подлежащих защите от несанкционированного доступа;

4) при необходимости организовывать сертификацию средств защиты информации, систем и средств информатизации и телекоммуникаций, обеспечивающих защищенность информации от утечки по техническим каналам;

5) организовывать и проводить работы по контролю эффективности проводимых мероприятий и принимаемых мер по защите информации;

6) организовывать и проводить в установленном порядке расследование причин и условий появления нарушений в сфере защиты информации;

7) организовывать работу по разработке проектов организационно-распорядительных документов по защите информации;

8) подготавливать, в пределах своей компетенции, для внесения в установленном порядке предложения по финансированию работ, связанных с защитой информации;

9) участвовать в работе по созданию безопасных информационных технологий, отвечающих требованиям комплексной защиты информации.

10) обеспечивать контроль за выполнением требований нормативно-технической документации, за соблюдением установленного порядка выполнения работ, а также действующего законодательства при решении вопросов, касающихся защиты информации;

11) участвовать в рассмотрении проектов договоров, технических заданий на работы по технической защите информации, осуществлять контроль за включением в них требований защиты информации и последующем выполнением этих требований;

12) организовывать взаимодействие с уполномоченным ОИВ ЛО по вопросам технической защиты информации.

5. Ответственность

4.2. Ответственный за защиту информации несет ответственность за выполнение возложенных на него функции в пределах своей компетенции.

«УТВЕРЖДЕН»
приказом комитета общего
и профессионального образования
Ленинградской области
от 25.05.2023 года № 20
(приложение 4)

Порядок допуска должностных лиц и обслуживающего персонала в помещения, в которых ведётся обработка защищаемых информационных ресурсов и обрабатывающим их техническим средствам, в рабочее и нерабочее время, а также в нештатных ситуациях

1. Настоящий порядок, устанавливает единые требования к допуску должностных лиц и обслуживающего персонала в служебные помещения комитета общего и профессионального образования Ленинградской области, в которых ведётся обработка защищаемой информации (далее – служебные помещения) и обрабатывающим их техническим средствам.

2. Для служебных помещений организуется режим обеспечения безопасности, при котором обеспечивается сохранность технических средств обработки и защиты информации, препятствующий возможности неконтролируемого проникновения или пребывания посторонних лиц, не имеющих право доступа в такие помещения.

3. При обработке в служебных помещениях, информации, содержащейся в государственных информационных системах, должны обеспечиваться контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы и помещения и сооружения, в которых они установлены.

Контроль и управление физическим доступом предусматривают:

а) определение лиц, допущенных к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены (Приложение № 1);

б) санкционирование физического доступа к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены;

в) учет физического доступа к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены.

4. В служебных помещениях, в которых размещаются информационные системы персональных данных и где размещены

используемые средства криптографической защиты информации (СКЗИ), хранятся СКЗИ и (или) носители ключевой, аутентифицирующей и парольной информации СКЗИ, необходимо обеспечение режима безопасности, который достигается путем:

а) оснащения таких помещений входными дверьми с замками, обеспечения постоянного закрытия дверей на замок и их открытия только для санкционированного прохода, а также опечатывания их по окончании рабочего дня или оборудование таких помещений соответствующими техническими устройствами, сигнализирующими о несанкционированном вскрытии;

б) утверждения перечня лиц, имеющих право доступа в такие помещения (Приложение № 1).

5. Служебные помещения располагаются в пределах контролируемой зоны, границами которой являются ограждающие конструкции зданий, в которых они размещены, с учётом территорий, контролируемых службами охраны.

6. Вскрытие и закрытие (опечатывание) служебных помещений, производится должностными лицами, имеющими право доступа в данные помещения.

7. Должностные лица, имеющие право доступа в служебные помещения не должны:

оставлять в свое отсутствие незапертым служебное помещение;

оставлять в служебном помещении посторонних лиц, не имеющих право доступа в такое помещение, без присмотра.

8. Обслуживание и сопровождение технических и программных средств, уборка, проведение других работ в служебных помещениях осуществляются в присутствии должностного лица, имеющего право доступа в данное помещение.

9. В случае необходимости принятия в нерабочее время экстренных мер при срабатывании пожарной или охранной сигнализации, авариях в системах энерго-, водо- и теплоснабжения помещение, в котором ведется обработка защищаемой информации, в нерабочее время, вскрытие служебного помещения осуществляется сотрудником службы безопасности, который ставит в известность ответственного за защиту информации и должностных лиц, имеющих право допуска в данное помещение, в начале следующего рабочего дня.

10. Ответственность за соблюдение настоящего порядка возлагается на начальников отделов (структурных подразделений), в которых ведется обработка защищаемых информационных ресурсов.

Приложение № 1
к Порядку допуска...

Перечень лиц, имеющих право доступа в служебные помещения

ФИО	Должность	Каб.
Артамонова Е.Р.	Главный специалист отдела общего образования департамента управления в сфере общего, дополнительного образования и защиты прав детей комитета общего и профессионального образования Ленинградской области	536
Савина Л.Г.	Главный специалист отдела общего образования департамента управления в сфере общего, дополнительного образования и защиты прав детей комитета общего и профессионального образования Ленинградской области	536
Селезнева Г.В.	Начальник отдела защиты прав детей департамента управления в сфере общего, дополнительного образования и защиты прав детей комитета общего и профессионального образования Ленинградской области	519
Атанова А.В.	Начальник сектора дополнительного образования, воспитания и детского отдыха департамента управления в сфере общего, дополнительного образования и защиты прав детей комитета общего и профессионального образования Ленинградской области	532
Дмитриева Н.А.	Главный специалист дополнительного образования, воспитания и детского отдыха департамента управления в сфере общего, дополнительного образования и защиты прав детей комитета общего и профессионального образования Ленинградской области	532
Андрюшин А.В.	Начальник сектора кадровой работы и профессионального развития работников системы образования департамента управления в сфере общего, дополнительного образования и	511

	защиты прав детей комитета общего и профессионального образования Ленинградской области	
Орлова М.И.	Начальник отдела профессионального образования и профессионального обучения департамента профессионального образования, развития инфраструктуры и организационной деятельности комитета общего и профессионального образования Ленинградской области	505
Терентьев И.А.	Ведущий специалист отдела профессионального образования и профессионального обучения департамента профессионального образования, развития инфраструктуры и организационной деятельности комитета общего и профессионального образования Ленинградской области	503
Глевицкая Е.И.	Начальник сектора цифровой трансформации департамента профессионального образования, развития инфраструктуры и организационной деятельности комитета общего и профессионального образования Ленинградской области	525
Николаева М.А.	Ведущий специалист сектора цифровой трансформации департамента профессионального образования, развития инфраструктуры и организационной деятельности комитета общего и профессионального образования Ленинградской области	525

«УТВЕРЖДЕНЫ»
приказом комитета общего
и профессионального образования
Ленинградской области
от 25.05.2023 года № 20
(приложение 5)

Правила разграничения доступа к защищаемым информационным ресурсам, обрабатываемым с использованием средств вычислительной техники

1. Общие положения

1.1. Настоящие правила предназначены для установления правомерного порядка доступа должностных лиц к защищаемым информационным ресурсам, обрабатываемым в электронном виде с использованием средств вычислительной техники в комитете общего и профессионального образования Ленинградской области.

2. Предоставление прав доступа к защищаемым информационным ресурсам

2.1. Предоставление прав доступа к информационным ресурсам реализуется в форме разрешительной системы доступа и основывается на функциональных обязанностях, выполняемых должностными лицами, связанных с обработкой защищаемых информационных ресурсах, с учетом требований, предъявляемых к безопасности информации.

2.2. Реализация разрешительной системы доступа обеспечивается определением перечня должностных лиц, имеющих право доступа к защищаемым информационным ресурсам и предоставлением или ограничением такого доступа с помощью технических и программных средств защиты информации.

2.3. Перечень должностных лиц, имеющих право доступа к защищаемым информационным ресурсам (Приложение № 1) утверждается председателем комитета общего и профессионального образования Ленинградской области. Предоставление или ограничение доступа к информационным ресурсам реализуется с помощью технических и программных средств защиты информации, прошедших установленным порядком процедуру оценки соответствия в форме обязательной сертификации по требованиям безопасности информации (далее – технические средства).

2.4. С помощью технических средств осуществляется заведение, активация, блокирование или уничтожение соответствующих типов учетных

записей (внутреннего пользователя, внешнего пользователя; системная, приложения; гостевая (анонимная), временная и (или) иные типы записей) и управление предоставления прав доступа.

2.5. Управление правами доступа реализуются администратором безопасности информации на основании заявки должностного лица, в отношении которого принимаются меры по разграничению доступа к информационным ресурсам.

2.6. Заявка формируется службой технической поддержки и должна содержать следующую информацию, предоставленную заявителем:

полное наименование должности и ФИО лица, которому необходимо предоставить/изменить/ограничить права доступа;

наименование информационной системы и информационного ресурса к которым необходимо разграничение прав доступа;

цель разграничения прав доступа для (выполнения функциональных обязанностей/решения иных задач);

имя компьютера;

наименование учётной записи:

IP адрес;

адрес расположения АРМ;

номер помещения.

2.7. Администратор безопасности обеспечивает настройку параметров доступа технических средств в соответствии полученной заявкой и предоставляет указанному должностному лицу права чтения, записи, изменения или удаления информации в информационной системе в зависимости от его должностных функций (обязанностей).

3. Ответственность

3.1. Начальник структурного подразделения несет ответственность за своевременность подачи заявки о предоставлении, изменении или ограничении прав доступа должностному лицу к защищаемым информационным ресурсам и контроль выполнения должностным лицом установленных требований безопасности информации.

3.2. Администратор безопасности информации несёт ответственность за своевременность и правильность настроек параметров технических средств разграничения доступа.

3.3. Должностные лица, допущенные к защищаемым информационным ресурсам, несут ответственность за нарушение требований безопасности информации, в соответствии с действующим законодательством.

Приложение № 1
к Правилам разграничения доступа….

Перечень должностных лиц, имеющих право доступа к защищаемым информационным ресурсам в комитете общего и профессионального образования Ленинградской области

Наименование должности	Перечень информационных ресурсов, к которым необходим доступ
Департамент управления в сфере общего, дополнительного образования и защиты прав детей	
Отдел общего образования	
Главный специалист – Артамонова Е.Р.	Персональные данные воспитанников дошкольных образовательных организаций Ленинградской области, содержащиеся в ГИС «Современное образование Ленинградской области»
Главный специалист – Савина Л.Г.	Персональные данные обучающихся образовательных организаций Ленинградской области, содержащиеся в ГИС «Современное образование Ленинградской области»
Отдел защиты прав детей	
Начальник отдела защиты прав детей– Селезнева Г.В.	Персональные данные обучающихся и сотрудников образовательных организаций Ленинградской области, содержащиеся в ГИС «Современное образование Ленинградской области»
Сектор дополнительного образования, воспитания и детского отдыха	
Начальник сектора – Атанова А.В.	Персональные данные обучающихся и сотрудников образовательных организаций Ленинградской области, содержащиеся в ГИС «Современное образование Ленинградской области»
Главный специалист – Дмитриева Н.А.	Персональные данные обучающихся и сотрудников образовательных организаций Ленинградской области, содержащиеся в ГИС «Современное образование Ленинградской области»
Сектор кадровой работы и профессионального развития работников системы образования	
Начальник сектора –	Персональные данные сотрудников

Андрюшин А.В.	образовательных организаций Ленинградской области, содержащиеся в ГИС «Современное образование Ленинградской области»
Департамент профессионального образования, развития инфраструктуры и организационной деятельности	
Отдел профессионального образования и профессионального обучения	
Начальник отдела – Орлова М.И.	Персональные данные обучающихся и сотрудников образовательных организаций Ленинградской области, содержащиеся в ГИС «Современное образование Ленинградской области»
Ведущий специалист – Терентьев И.А.	Персональные данные обучающихся и сотрудников образовательных организаций Ленинградской области, содержащиеся в ГИС «Современное образование Ленинградской области»
Сектор цифровой трансформации	
Начальник сектора – Глевицкая Е.И.	Персональные данные обучающихся и сотрудников образовательных организаций Ленинградской области, содержащиеся в ГИС «Современное образование Ленинградской области»
Ведущий специалист – Николаева М.А.	Персональные данные обучающихся и сотрудников образовательных организаций Ленинградской области, содержащиеся в ГИС «Современное образование Ленинградской области»

«УТВЕРЖДЕН»
приказом комитета общего
и профессионального образования
Ленинградской области
от 25.05.2023 года № 20
(приложение 6)

Порядок учета, хранения и уничтожения материальных машинных носителей защищаемых информационных ресурсов

1. Общие положения

1.1. Настоящий порядок, определяет порядок учёта, маркировки, хранения, передачи другим лицам, ремонта, технического обслуживания и уничтожения машинных носителей защищаемых информационных ресурсов.

1.2. Действие установленного порядка распространяется на должностных лиц комитета общего и профессионального образования Ленинградской области, осуществляющих обработку защищаемой информации и ответственного за защиту информации.

2. Материальные носители информации

2.1. В настоящем документе рассматриваются следующие виды материальных носителей информации:

- машинные носители информации (МНИ);
- носители информации на бумажной основе.

2.2. Машинные носители информации – изделия и устройства, предназначенные для записи и обработки информации входящие в состав средств вычислительной техники (СВТ), а также для хранения и перемещения записанной информации на внешние носители информации.

Виды МНИ:

- жесткие магнитные диски;
- оптические и магнитооптические диски;
- устройства долговременной электронной памяти «Flash Memory»;

Типы МНИ:

а) съемные носители информации, устанавливаются и/или подключаются к СВТ на время сеанса работы пользователя, а по окончанию его отключаются и хранятся в определенном хранилище;

– несъемные носители информации в процессе работы пользователя не снимаются и не изымается из состава СВТ автоматизированной системы и находится там постоянно.

2.3. Носители информации на бумажной основе – материальные носители графической и буквенно-цифровой информации, отраженной (зафиксированной) на бумаге.

3. Порядок обращения с материальными носителями защищаемых информационных ресурсов

3.1. Все МНИ подлежат обязательному учету в «Журнале учета машинных носителей защищаемых информационных ресурсов» (Приложение № 1).

3.2. Ответственность за ведение журнала возлагается на ответственного за защиту информации.

3.3. Учет бумажных носителей информации осуществляется в соответствии с установленными правилами делопроизводства.

3.4. Выдача МНИ фиксируется в документе «Журнал учета машинных носителей защищаемых информационных ресурсов» и подтверждается подписью пользователя.

3.5. Все МНИ должны маркироваться и содержать учетный номер, дату ввода в эксплуатацию, наименование органа исполнительной власти Ленинградской области (владельца МНИ).

МНИ содержащие биометрические персональные данные должны позволять идентифицировать информационную систему персональных данных, в которую была осуществлена запись биометрических персональных данных, а также оператора, осуществившего такую запись.

3.6. Съемные носители информации маркируются этикеткой, закрепленной на лицевой стороне носителя.

3.7. Несъёмные носители информации учитываются отдельно и (или) в составе СВТ. При этом маркируется сам носитель или корпус СВТ, в состав которого входит носитель.

3.8. СВТ в состав которого входит МНИ, вскрывается в присутствии ответственного за защиту информации и должностного лица эксплуатирующего данное СВТ.

4. Правила хранение носителей защищаемых информационных ресурсов

4.1.При хранении МНИ должны соблюдаться условия, обеспечивающие сохранность информации, и исключающие к ним несанкционированный доступ, хищение, подмену и уничтожение.

4.2. Хранение и использование МНИ должно осуществляться в условиях, соответствующих техническим условиям изготовителя и не более установленного срока эксплуатации.

4.3. Необходимо обеспечивать раздельное хранение материальных носителей персональных данных, обработка которых осуществляется в различных целях, а также носителей персональных данных от носителей, содержащих иную защищаемую информацию.

4.4. Для хранения носителей информации используются хранилища (сейфы, металлические шкафы, и т.п.), оборудованные внутренними замками с двумя или более дубликатами ключей и приспособлениями для опечатывания замочных скважин или кодовыми замками.

В случае если на съемном МНИ хранятся только данные в зашифрованном с использованием средств криптографической защиты информации (СКЗИ) виде, допускается хранение таких носителей в служебных помещениях вне сейфов (металлических шкафов).

4.5. МНИ с резервными копиями защищаемой информации не выдаются для работы обычным пользователям и служат только для восстановления в случае аварии или поломки основного МНИ. МНИ с резервными копиями рекомендуется хранить в отдельном хранилище.

4.6. В случае если на основании договора, хранение носителей поручено другому лицу, существенным условием такого договора является обязанность обеспечения таким лицом безопасности переданной ему защищаемой информации

5. Порядок уничтожения носителей защищаемых информационных ресурсов

5.2. МНИ подлежат уничтожению в следующих случаях:

– достижения целей обработки информации или в случае утраты необходимости в их достижении, для носителей, уничтожение информации на которых невозможно без уничтожения самого носителя;

– выхода из строя, повреждение МНИ, в результате которого невозможно осуществлять корректную обработку информации с использованием данного носителя;

– возникновения иных обстоятельств, в результате которых необходимо уничтожить носители, содержащие защищаемую информацию.

5.3. Уничтожение осуществляется ответственным за защиту информации, с составлением акта об уничтожении МНИ, которые хранятся не менее трех лет.

5.4. Вышедшие из строя МНИ ремонту не подлежат. Такие носители уничтожаются методом разборки и физического разрушения.

5.5. Уничтожение МНИ должно обеспечивать полное физическое и невосстановимое уничтожение информации, содержащейся на таких носителях.

6. Права и обязанности работников при обращении с носителями защищаемых информационных ресурсов

6.2. Запрещается выносить носители из служебных помещений (за пределы контролируемой зоны) для работы с ними на дому, в гостиницах, общественном транспорте и т.д.

6.3. Права на перемещение МНИ за пределы контролируемой зоны предоставлено только тем лицам, которым оно необходимо для выполнения своих должностных обязанностей (функции).

6.4. Запрещается принимать и передавать МНИ без соответствующего разрешения и оформления в установленном порядке.

6.5. Должностное лицо, осуществляющее работу с МНИ, обязано работать только с вверенными ему МНИ. Самовольная передача МНИ другим лицам запрещается.

6.6. Запрещается хранить МНИ на рабочих столах, либо оставлять их без присмотра.

6.7. Руководители подразделений, в которых осуществляется работа с МНИ, должны пресекать действия, которые могут привести к хищению или разрушению носителей.

6.8. О фактах утраты носителей немедленно должен быть поставлен в известность ответственный за защиту информации.

Приложение № 1
к Порядку учёта, хранения и уничтожения...

Журнал учета машинных носителей защищаемых информационных ресурсов

Регистрационный (заводской) номер	Вид (съемный/ несъемный)	Тип (оптический /магнитный/ flash), его емкость	Дата поступления	Расписка в получении (ФИО, подпись, дата)	Расписка в обратном приеме (ФИО, подпись, дата)	Место хранения (адрес, помещение)	Дата и номер акта об уничтожении	Примечание
1	3	4	5	6	7	8	9	10