КОМИТЕТ ПО ТРУДУ И ЗАНЯТОСТИ НАСЕЛЕНИЯ ЛЕНИНГРАДСКОЙ ОБЛАСТИ

РАСПОРЯЖЕНИЕ

«29» июля 2019 года № 71

Об организации защиты информации в комитете по труду и занятости населения Ленинградской области

В целях исполнения 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 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 по 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 31.08.2010 № 416/489 «Об утверждении Требований по 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, обязательных требований по защите конфиденциальной и иной

информации, предъявляемых в соответствии с законодательством Российской Федерации, Ленинградской области:

1. Утвердить:

- Положение о порядке организации и проведения работ по защите информации согласно приложению 1.

- Перечень защищаемых информационных ресурсов согласно приложению 2.

- Инструкцию лица, ответственного за защиту информации, согласно приложению 3.

- Порядок осуществления доступа в помещения, в которых производится обработка защищаемой информации, и к техническим средствам, предназначенным для её обработки, согласно приложению 4.

- Правила разграничения доступа к защищаемой информации, обрабатываемой с использованием средств вычислительной техники, согласно приложению 5.

- Порядок учета, хранения, передачи и уничтожения машинных носителей, использующихся для работы с защищаемой информацией, согласно приложению 6.

2. Должностному лицу, ответственному за защиту информации в комитете по труду и занятости населения Ленинградской области обеспечить исполнение п.1 настоящего распоряжения.

3. Контроль за исполнением настоящего распоряжения возложить на заместителя председателя комитета по труду и занятости населения Ленинградской области Воронина С.В.

Первый заместитель
председателя комитета А.Ю. Астратова

Утверждено
распоряжением комитета
по труду и занятости населения
Ленинградской области
от «29» июля 2019 года № 71
(приложение 1)

ПОЛОЖЕНИЕ
о порядке организации и проведения работ по защите информации в комитете по труду и занятости населения Ленинградской области

1. Общие положения

1.1. 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 комитета по труду и занятости населения Ленинградской области, при проведении работ, требующих защиты информации на разрабатываемых, реконструируемых и действующих (находящихся в эксплуатации) объектах информатизации.

1.2. К объектам информатизации относиться 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.

1.3. 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.

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

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

1.6. 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 по труду и занятости населения 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 защиты 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. Организацию мероприятий по обеспечению защиты информации осуществляет заместитель председателя комитета по труду и занятости населения Ленинградской области.

3.3. Общую координацию деятельности и методическое руководство по вопросам защиты информации осуществляет уполномоченный по данным вопросам орган исполнительной власти 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 проводится 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 по труду и занятости населения Ленинградской области. По результатам такого контроля составляется справка о состоянии работ по защите информации, которая предоставляется председателю комитета по труду и занятости населения Ленинградской области.

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 мероприятий по обеспечению защиты информации несёт заместитель председателя комитета по труду и занятости населения Ленинградской области.

5.2. Ответственность за разработку и внедрение средств защиты информации несёт уполномоченный ОИВ ЛО и ответственный по защите информации, в пределах своих компетенций.

5.3. Ответственность за выполнение мероприятий по защите информации несут уполномоченный ОИВ ЛО, ответственный за защиту информации и должностные лица, в пределах своих компетенций.

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.

Утверждён
распоряжением комитета
по труду и занятости населения
Ленинградской области
от «29» июля 2019 года № 71
(приложение 2)

ПЕРЕЧЕНЬ
защищаемых информационных ресурсов в комитете по труду и занятости населения Ленинградской области

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 по труду и занятости населения Ленинградской области.

2. При разработке учитывались положения Федеральных законов от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации» и от 27.07.2006 № 152 «О персональных данных», Указа Президента Российской Федерации от 06.03.1997 № 188 «Об утверждении перечня сведений конфиденциального характера», приказа ФСТЭК России от 11.02.2013 № 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 30.08.2002 № 282.

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

4. К защищаемым информационным ресурсам в комитете по труду и занятости населения Ленинградской области относятся сведения конфиденциального характера: сведения о фактах, событиях и обстоятельствах частной жизни граждан, позволяющие идентифицировать их личности (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации, в установленных Федеральными законами случаях.

Защищаемые информационные ресурсы в комитете по труду и занятости населения Ленинградской области:

1. Автоматизированная информационная система «ПК Катарсис»;
2. Система электронного документооборота Ленинградской области. Модуль «Обращения граждан».

Утверждена
распоряжением комитета
по труду и занятости населения
Ленинградской области
от «29» июля 2019 года № 71
(приложение 3)

ИНСТРУКЦИЯ
лица, ответственного за защиту информации в комитете по труду и занятости населения Ленинградской области

1. Общие положения

1.1. Настоящая инструкция определяет основные функции и права ответственного за защиту информации в комитете по труду и занятости населения Ленинградской области (далее – Комитет).

1.2. Ответственный за защиту информации назначается председателем Комитета.

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

2.1. Основными функциями ответственного за защиту информации:

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

2) осуществление контроля за соблюдением работниками Комитета и обслуживающими специалистами положений локальных организационно-распорядительных документов по обеспечению безопасности информации;

3) информирование уполномоченного по вопросам защиты информации органа исполнительной власти Ленинградской области (уполномоченный ОИВ ЛО) о выявленных фактах нарушений положений локальных организационно-распорядительных документов по обеспечению безопасности информации, попытках несанкционированного доступа к защищаемым информационным ресурсам или иных неправомерных действиях в отношении к такой информации;

4) учет и хранение машинных носителей информации, содержащих защищаемую информацию;

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

6) присутствие при выполнении технического обслуживания элементов автоматизированных систем в защищенном исполнении (АСЗИ) специалистами сторонних организаций.

3. Права ответственного за защиту информации

3.1. 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. Ответственность

4.1. Ответственный за защиту информации несёт ответственность за выполнение возложенных на него функций.

Утвержден
распоряжением комитета
по труду и занятости населения
Ленинградской области
от «29» июля 2019 года № 71
(приложение 4)

ПОРЯДОК

осуществления доступа в помещения, в которых производится обработка защищаемой информации, и к техническим средствам, предназначенным для её обработки в комитете по труду и занятости населения Ленинградской области

1. Настоящий порядок, устанавливает единые правила осуществления доступа в служебные помещения комитета по труду и занятости населения Ленинградской области, в которых ведётся обработка защищаемой информации (далее – специальные служебные помещения), и к техническим средствам, предназначенным для её обработки.

2. Для специальных служебных помещений действует режим обеспечения безопасности, обеспечивающий сохранность находящихся в них технических средств обработки и защиты информации, и препятствующий возможности неконтролируемого проникновения или пребывания лиц, не имеющих права доступа в такие помещения.

3. Круг лиц, имеющих права доступа в соответствующие специальные служебные помещения определён в приложении 1 к настоящему Порядку.

4. Для специалистов, выполняющих обслуживание и сопровождение технических и программных средств, другие работы (далее - Специалисты) действует режим сеансового санкционированного и контролируемого доступа, который подразумевает следующую организацию и порядок осуществления доступа:

a. доступ Специалистов в специальное служебное помещение осуществляется под контролем ответственного за защиту информации (далее – Ответственный), в согласованное с ним время;

b. непосредственно перед осуществлением доступа в «Журнал учёта сессионного санкционированного контролируемого доступа (ССКД) специалистов в специальные служебные помещения (ССП) комитета по труду и занятости населения Ленинградской области» (приложение 2) Ответственным вносится запись о необходимости осуществить доступ: фиксируется дата осуществления доступа, его цель, номер специального служебного помещения, ФИО и должность (с указанием представляемой организации) Специалиста, ФИО Ответственного, время начала сессии. Специалист удостоверяет факт необходимости осуществления доступа своей подписью. Ответственный удостоверяет факт разрешения доступа и готовность осуществить контроль доступа своей подписью.

c. По окончании сеанса доступа Ответственный проставляет в записи время окончания сеанса доступа и удостоверяет факт его завершения своей подписью.

5. Двери всех специальных служебных помещений оборудованы замками, закрывающимися на ключ.

6. Ключи от специальных служебных помещений вправе иметь только лица, обладающие соответствующими правами доступа.

7. Запасные ключи от специальных служебных помещений хранятся в специально оборудованном боксе в комнате № 320.

8. Вскрытие и закрытие специальных служебных помещений, производится только лицами, обладающими соответствующими правами доступа.

9. Специальные служебные помещения в отсутствие в них лиц, обладающих соответствующими правами доступа должны запираться на ключ.

10. В случае необходимости принятия в нерабочее время экстренных мер при срабатывании пожарной или охранной сигнализации, авариях в системах энерго-, водо- и теплоснабжения, вскрытие специального служебного помещения и контроль посещения осуществляется работником службы безопасности, который обязан при первой возможности передать информацию об инциденте ответственному за защиту информации или лицам, имеющим право допуска в данное помещение, для сведения и для внесения соответствующей записи в «Журнал учёта ССКД специалистов в ССП комитета по труду и занятости населения Ленинградской области».

11. Ответственность за соблюдение настоящего порядка в рабочее время возлагается на начальников отделов и секторов, в которых ведется обработка защищаемой информации.

Приложения:

1. Перечень должностей государственной гражданской службы комитета по труду и занятости населения Ленинградской области, за которыми закреплено право доступа в помещения, в которых производится обработка защищаемой информации – на 3 л.
2. Журнал учёта сеансового санкционированного контролируемого доступа (ССКД) специалистов в специальные служебные помещения (ССП) комитета по труду и занятости населения Ленинградской области» (Форма) – на 1 л.

Приложение 1
к Порядку осуществления доступа
в помещения, в которых ведётся обработка
защищаемой информации

ПЕРЕЧЕНЬ
должностей государственной гражданской службы комитета по труду и занятости населения Ленинградской области, за которыми закреплено право доступа в помещения, в которых производится обработка защищаемой информации

№	Должность	Ф.И.О.	Кабинет
ФИНАНСОВО-ЭКОНОМИЧЕСКИЙ ОТДЕЛ			
1.	Начальник отдела	Орлова Наталия Александровна	307*
Сектор бюджетного планирования, учета и контроля			
2.	Главный специалист	Пучкова Екатерина Александровна	307*
3.	Ведущий специалист	Соболева Мария Вячеславовна	307*
Сектор социальных выплат			
4.	Главный специалист	Димиржиева Галина Владимировна	307*
ОТДЕЛ ОРГАНИЗАЦИОННО-ПРАВОВОГО ОБЕСПЕЧЕНИЯ И КОНТРОЛЯ			
Сектор правового обеспечения и делопроизводства			
5.	Специалист 1 категории	Маницына Виктория Викторовна	325*
Сектор контроля за соблюдением законодательства о занятости			
6.	Консультант	Абалаков Кирилл Владиславович	325*
7.	Главный специалист	Богданова Виктория Александровна	325*
ОТДЕЛ АНАЛИЗА РЫНКА ТРУДА, ИНФОРМАЦИИ И ПРОГРАММ ЗАНЯТОСТИ			
8.	Начальник отдела	Котов Тимофей Михайлович	312*
9.	Ведущий специалист	Лавренченко Елена Николаевна	320*
10.	Консультант	Романова Елена Владиславовна	312*
11.	Главный специалист	Коробкова Екатерина Александровна	312*

12.	Главный специалист	Круглов Александр Германович	320**
13.	Ведущий специалист	Щелкунова Наталья Олеговна	312*
СЕКТОР ПРОФЕССИОНАЛЬНОГО ОБУЧЕНИЯ И ПРОФЕССИОНАЛЬНОЙ ОРИЕНТАЦИИ			
14.	Начальник сектора	Турченко Маргарита Михайловна	310*
15.	Главный специалист	Калинина Марина Александровна	310*
16.	Ведущий специалист	Корсак Юлия Александровна	310*
ОТДЕЛ СПЕЦИАЛЬНЫХ ПРОГРАММ И ТРУДОУСТРОЙСТВА			
17.	Начальник отдела	Шквиро Вероника Анатольевна	318*
18.	Главный специалист	Бурулько Оксана Леонидовна	313*
19.	Главный специалист	Зверева Елена Валерьевна	318*
20.	Специалист 1 категории	Лунькова Марина Валериевна	313*
21.	Ведущий специалист	Боровских Татьяна Владимировна	313*
ОТДЕЛ ОХРАНЫ ТРУДА И СОЦИАЛЬНОГО ПАРТНЕРСТВА			
22.	Главный специалист	Котина Марина Сергеевна	326*

* Санкт-Петербург, проспект Трамвайный, д. 12, корп. 2

** Доступ во все помещения, в которых производится обработка защищаемой информации

Утвержден
распоряжением комитета
по труду и занятости населения
Ленинградской области
от «29» июля 2019 года № 71
(приложение 4)

ЖУРНАЛ
учёта сессионного санкционированного контролируемого доступа (ССКД) специалистов в специальные служебные помещения (ССП) комитета по труду и занятости населения Ленинградской области

№ п/п	Запрос ССКД			Запрос ССКД подтверждаю, с Порядком ознакомлен				ССКД разрешаю, контроль обеспечу			ССКД завершен	
	Дата	№ ССП	Цель, основание	ФИО	Должность	Организация	Подпись	ФИО	Начало	Подпись	Конец	Подпись

Утверждены
распоряжением комитета
по труду и занятости населения
Ленинградской области
от «29» июля 2019 года № 71
(приложение 5)

ПРАВИЛА
разграничения доступа к защищаемой информации, обрабатываемой с использованием средств вычислительной техники, в комитете по труду и занятости населения Ленинградской области

1. Общие положения

1.1. Настоящие правила устанавливают порядок регулирования доступа должностных лиц к защищаемой информации, обрабатываемой в электронном виде с использованием средств вычислительной техники в комитете по труду и занятости населения Ленинградской области.

2. Предоставление прав доступа к защищаемой информации

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

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

2.3. Перечень должностных лиц, имеющих право доступа к защищаемой информации (Приложение 1) утверждается председателем комитета по труду и занятости населения Ленинградской области.

2.4. Предоставление или ограничение доступа к информации 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).

2.5. С помощью технических средств осуществляется создание, активация, блокирование или уничтожение соответствующих типов учетных записей (внутреннего пользователя, внешнего пользователя; системная, приложения; гостевая (анонимная), временная и (или) иные типы записей) и управление правами доступа.

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

2.7. 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);
- сетевое имя компьютера;
- инвентарный номер компьютера;
- IP адрес;
- адрес расположения АРМ;
- номер помещения.

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

3. Ответственность

3.1. Начальник структурного подразделения несет ответственность за своевременность подачи заявки о предоставлении, изменении или ограничении прав доступа должностного лица к защищаемой информации 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 защищаемой информации, несут ответственность за нарушение требований безопасности информации, в соответствии с действующим законодательством.

Приложения: 1. Перечень должностных лиц, имеющих право доступа к защищаемой информации в комитете по труду и занятости населения Ленинградской области – на 1 л.

Приложение 1
к Правилам разграничения доступа
к защищаемой информации

ПЕРЕЧЕНЬ
должностных лиц, имеющих право доступа к защищаемой информации в комитете по труду и занятости населения Ленинградской области

Наименование должности	Перечень информационных ресурсов, к которым разрешён доступ
ФИНАНСОВО-ЭКОНОМИЧЕСКИЙ ОТДЕЛ	
1. Начальник отдела	АИС «ПК Катарсис»
Сектор бюджетного планирования, учета и контроля	
2. Главный специалист	АИС «ПК Катарсис»
3. Ведущий специалист	АИС «ПК Катарсис»
Сектор социальных выплат	
4. Главный специалист	АИС «ПК Катарсис»
СЕКТОР ПРОФЕССИОНАЛЬНОГО ОБУЧЕНИЯ И ПРОФЕССИОНАЛЬНОЙ ОРИЕНТАЦИИ	
5. Начальник сектора	АИС «ПК Катарсис»
6. Главный специалист	АИС «ПК Катарсис»
7. Ведущий специалист	АИС «ПК Катарсис»
ОТДЕЛ СПЕЦИАЛЬНЫХ ПРОГРАММ И ТРУДОУСТРОЙСТВА	
8. Начальник отдела	АИС «ПК Катарсис»
9. Главный специалист	АИС «ПК Катарсис»
10. Главный специалист	АИС «ПК Катарсис»
11. Специалист 1 категории	АИС «ПК Катарсис»
12. Ведущий специалист	АИС «ПК Катарсис»
ОТДЕЛ АНАЛИЗА РЫНКА ТРУДА, ИНФОРМАЦИИ И ПРОГРАММ ЗАНЯТОСТИ	
13. Начальник отдела	АИС «ПК Катарсис»
14. Консультант	АИС «ПК Катарсис»
15. Главный специалист	АИС «ПК Катарсис»
16. Главный специалист	АИС «ПК Катарсис»
17. Ведущий специалист	АИС «ПК Катарсис»
18. Ведущий специалист	АИС «ПК Катарсис»
ОТДЕЛ ОРГАНИЗАЦИОННО-ПРАВОВОГО ОБЕСПЕЧЕНИЯ И КОНТРОЛЯ	
Сектор правового обеспечения и делопроизводства	
19. Специалист 1 категории	АИС «ПК Катарсис»
Сектор контроля за соблюдением законодательства о занятости	
20. Консультант	АИС «ПК Катарсис»
21. Главный специалист	АИС «ПК Катарсис»
ОТДЕЛ ОХРАНЫ ТРУДА И СОЦИАЛЬНОГО ПАРТНЕРСТВА	
22. Главный специалист	СЭД Ленинградской области. Модуль «Обращения граждан»

Утверждён
распоряжением комитета
по труду и занятости населения
Ленинградской области
от «29» июля 2019 года № 71
(приложение 6)

ПОРЯДОК
учета, хранения, передачи и уничтожения материальных машинных носителей защищаемой информации в комитете по труду и занятости населения Ленинградской области

1. Общие положения

1.1. Настоящий документ устанавливает порядок учёта, маркировки, хранения, передачи другим лицам, ремонта, технического обслуживания и уничтожения машинных носителей защищаемой информации.

1.2. Действие установленного порядка распространяется на должностных лиц комитета по труду и занятости населения 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:

2.1.1. машинные носители информации (МНИ);
2.1.2. 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 внешние носители информации, предназначенные для хранения и транспортировки записанной на них информации.

2.2.1. Виды МНИ:

a) жесткие магнитные диски;
b) оптические и магнитооптические диски;
c) устройства долговременной электронной памяти «Flash Memory», «Rutoken».

2.2.2. Типы МНИ:

I. съемные носители информации, устанавливаются и/или подключаются к СВТ на время сеанса работы пользователя, а по окончанию его отключаются и хранятся в определенном хранилище;
II. несъемные носители информации в процессе работы пользователя не снимаются и не изымается из состава СВТ автоматизированной системы и находится там постоянно.

III. 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).

3.6. 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.

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

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

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

4. Правила хранения 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.

4.5. 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).

4.6. 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.

4.7. 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

5.1. МНИ подлежат уничтожению в следующих случаях:

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

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

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

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

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

5.7. 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

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

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

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

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

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

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

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

Приложение 1
к Порядку учёта, хранения и уничтожения ММНЗИ

Журнал учета машинных носителей защищаемых информационных ресурсов

Учетный номер	Регистрационный номер	Вид (съемный/несъемный)	Тип(оптический /магнитный /flash) и его емкость	Дата поступления	Расписка в получении (ФИО, подпись, дата)	Расписка в обратном приеме (ФИО, подпись, дата)	Место хранения (№ помещения)	Дата и номер акта об уничтожении	Примечание
1	2	3	4	5	6	7	8	9	10