КОМИТЕТ ПО СОЦИАЛЬНОЙ ЗАЩИТЕ НАСЕЛЕНИЯ
ЛЕНИНГРАДСКОЙ ОБЛАСТИ

ЛЕНИНГРАДСКОЕ ОБЛАСТНОЕ
ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ
«Сланцевский центр социального обслуживания граждан пожилого возраста и инвалидов
«НАДЕЖДА»
188561, г. Сланцы, ул. Ломоносова, д. 10а, тел. 42-942

П Р И К А З

05 ноября 2026 года № 43

Об утверждении политики защиты информации в ЛОГБУ «Сланцевский ЦСО «Надежда»

В целях выполнения требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах, утверждённых приказом ФСТЭК России от 11 апреля 2025г № 117.

ПРИКАЗЫВАЮ:

1.Утвердить прилагаемую Политику защиты информации в ЛОГБУ «Сланцевский ЦСО «Надежда».

2.Документоведу (Родионова О.В.) ознакомить всех работников учреждения с Политикой защиты информации в ЛОГБУ «Сланцевский ЦСО «Надежда» под роспись.

3. Контроль за исполнением приказа оставляю за собой.

Заместитель директора В.М. Бесчастная

Утверждена
приказом ЛОГБУ
"Сланцевский ЦСО "Надежда"
от 05.11.2026 года № 43

ПОЛИТИКА ЗАЩИТЫ ИНФОРМАЦИИ В ЛОГБУ «СЛАНЦЕВСКИЙ ЦСО «НАДЕЖДА»

На _9__ листах
Действует с «_05__» ноября 2026 г.

1. Общие положения

1.1. Назначение и область действия документа

Настоящая Политика защиты информации (далее – Политика) определяет цели, задачи, принципы, организационную структуру и основные направления деятельности по защите информации, обрабатываемой в информационных системах (далее – ИС) Ленинградского областного государственного бюджетного учреждения «Сланцевский центр социального обслуживания граждан пожилого возраста и инвалидов «НАДЕЖДА» (далее – Учреждение).

Политика устанавливает единые подходы к формированию, функционированию и развитию системы защиты информации, а также является обязательной для применения при разработке иных локальных нормативных актов, регламентирующих вопросы информационной безопасности.

Требования Политики также обязательны для подрядных организаций и иных третьих лиц, привлекаемых к выполнению работ или оказанию услуг, связанных с доступом к ИС Учреждения, либо к информации, обрабатываемой в них. Соблюдение указанных требований обеспечивается посредством включения соответствующих обязательств в договорную документацию и контроля их исполнения.

Действие настоящей Политики распространяется на всех работников Учреждения независимо от занимаемой должности и характера выполняемых обязанностей, в части, касающейся их участия в обработке информации и эксплуатации ИС;

Все ИС Учреждения, а также связанные с ними сегменты сети, площадки размещения, программно-аппаратные средства и элементы информационно-телекоммуникационной инфраструктуры утверждается Руководителем учреждения.

1.2. Нормативно-правовые акты, методические документы, национальные стандарты

Политика разработана в соответствии с:

– Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (при обработке ПДн);

– Федеральным законом от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»;

– Указом Президента Российской Федерации от 01.05.2022 № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации»;

– Приказом ФСТЭК России от 11 апреля 2025 г. № 117 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений»;

– Методическим документом ФСТЭК России «Мероприятия и меры по защите информации, содержащейся в информационных системах» (2026 г.);

– Трудовым кодексом Российской Федерации (в части регулирования обязанностей работников по соблюдению требований защиты информации);

– национальными стандартами Российской Федерации в области защиты информации и информационной безопасности;

– иными нормативными и методическими документами ФСТЭК России, ФСБ России, а также внутренними организационно-распорядительными документами.

1.3. Термины и определения

Термины и определения, используемые в настоящей Политике, применяются в значениях, установленных нормативными правовыми актами Российской Федерации и нормативными документами, указанными в пункте 1.2 настоящего документа.

При отсутствии специальных определений в указанных нормативных правовых актах используются термины и определения, закрепленные в национальных стандартах Российской Федерации, в том числе:

– ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»;

– ГОСТ Р 56545-2015 «Защита информации. Информация и информационные технологии. Термины и определения»;

– ГОСТ Р 56546-2015 «Защита информации. Обеспечение информационной безопасности. Термины и определения».

В случае расхождения формулировок приоритет имеют определения, установленные федеральными законами и иными нормативными правовыми актами Российской Федерации.

Использование терминов в настоящей Политике осуществляется в целях обеспечения единообразного понимания требований по защите информации и недопущения неоднозначного толкования положений документа.

2. Цели и задачи защиты информации

2.1. Цели защиты информации

Целью обеспечения защиты информации в Учреждении является поддержание установленного уровня конфиденциальности, целостности и доступности информации, обрабатываемой в ИС, а также обеспечение устойчивости и непрерывности их функционирования посредством предупреждения и нейтрализации актуальных угроз безопасности информации и недопущения наступления неприемлемых последствий (ущерба) для деятельности Учреждения.

2.2. Задачи защиты информации

Для достижения поставленной цели защиты информации Учреждения решает следующие задачи:

– определение недопустимых событий, связанных с нарушением безопасности информации;
– систематическое выявление и оценка угроз безопасности информации;
– реализация организационных и технических мер защиты информации, адекватных актуальным угрозам и классу защищённости ИС;
– управление конфигурациями ИС и их уязвимостями;
– непрерывный мониторинг информационной безопасности и реагирование на инциденты;
– обеспечение физической защиты компонентов ИС;
– поддержание необходимого уровня знаний пользователей по вопросам защиты информации.

3. Принципы защиты информации

Деятельность по обеспечению защиты информации в Учреждении осуществляется на основе следующих принципов:

– **Законность** – соблюдение требований законодательства Российской Федерации, нормативных правовых актов уполномоченных органов и локальных нормативных актов Организации при организации и реализации мер защиты информации.
– **Непрерывность** – обеспечение защиты информации на всех этапах жизненного цикла ИС (проектирование, создание, ввод в эксплуатацию, эксплуатация, модернизация и вывод из эксплуатации), а также во всех режимах их функционирования.
– **Адекватность** – соответствие применяемых мер защиты характеру актуальных угроз безопасности информации, категории и уровню защищенности ИС, а также потенциальным возможностям нарушителя.
– **Минимизация прав и привилегий** – предоставление субъектам доступа исключительно тех прав и полномочий, которые необходимы для выполнения возложенных на них функций (принцип минимально необходимых прав, «необходимо знать»).
– **Многоуровневость (эшелонированность)** – построение системы защиты информации по принципу последовательных и взаимодополняющих

уровней защиты с использованием различных по типу и назначению средств и механизмов.

– **Персональная ответственность** – закрепление обязанностей по обеспечению защиты информации за конкретными работниками в соответствии с их должностными обязанностями и локальными нормативными актами Учреждения.

– **Управляемость и контролируемость** – обеспечение возможности планирования, мониторинга и оценки эффективности реализуемых мер защиты информации, а также своевременного выявления и устранения выявленных недостатков.

4. Объекты защиты

Защите подлежат:

– информационные ресурсы (информация ограниченного доступа, включая персональные данные, служебную информацию и т.д.), обрабатываемые в ИС;

– программные, программно-аппаратные и технические средства, входящие в состав ИС (серверы, автоматизированные рабочие места, сетевое оборудование, средства хранения данных, средства защиты);

– информационно-телекоммуникационная инфраструктура, на базе которой функционирует ИС (включая каналы связи, активное оборудование);

– машинные носители информации (съёмные и стационарные);

– помещения (контролируемая зона), где размещены компоненты ИС.

5. Категории лиц, участвующих в защите информации, их обязанности (функции) и полномочия

5.1. Состав действующих лиц

Деятельность по защите информации в Учреждении осуществляется с участием следующих категорий лиц:

– руководитель Учреждения;

– ответственный за организацию защиты информации;

– ответственный за защиту информации в ИС (администратор безопасности);

– ответственный за обеспечение безопасности ПДн;

– ответственный за эксплуатацию СКЗИ;

– ответственный за техническое обслуживание ИС (администратор системы);

– пользователи ИС (работники Учреждения, внешние пользователи).

Распределение обязанностей и полномочий между указанными лицами закрепляется настоящей Политикой, а также приказами руководителя Учреждения, должностными инструкциями и иными внутренними локальными актами Учреждения.

5.2. Обязанности (функции) и полномочия действующих лиц

5.2.1. Руководитель учреждения

Основные обязанности (функции):

утверждает Политику защиты информации и иные локальные нормативные акты; назначает ответственных лиц в области защиты информации; определяет структуру управления; осуществляет ресурсное обеспечение мероприятий по защите информации; осуществляет общий контроль за состоянием защищенности; принимает решения по результатам расследований серьезных инцидентов информационной безопасности; обеспечивает взаимодействие с уполномоченными государственными органами по вопросам защиты информации.

Руководитель вправе:

назначать ответственных лиц и допускать пользователей; утверждать внутренние локальные акты по защите информации; распределять бюджетные средства на мероприятия по защите информации; инициировать служебные проверки и применять дисциплинарные взыскания.

5.2.2. Ответственный за организацию защиты информации

Основные обязанности (функции):

организует выполнение организационных и технических мер защиты; контролирует соблюдение нормативно-правовых актов; координирует деятельность работников по защите информации; организует проведение оценки состояния защиты; организует обучение работников; планирует мероприятия по повышению уровня защищенности; взаимодействует с подрядными организациями по вопросам защиты информации; докладывает руководителю о состоянии защищенности, а также о необходимости дополнительных ресурсов.

Ответственный вправе:

запрашивать у подразделений информацию, необходимую для выполнения задач; давать обязательные для исполнения указания в пределах своей компетенции; инициировать служебные расследования инцидентов; приостанавливать работу ИС при выявлении критических угроз (с незамедлительным уведомлением руководителя); представлять Организацию в вопросах защиты информации перед третьими лицами; вносить предложения о совершенствовании системы защиты информации.

5.2.3. Ответственный за защиту информации в ИС (администратор безопасности)

Основные обязанности (функции):

реализует организационные и технические меры защиты информации в закрепленных за ним ИС; разрабатывает и актуализирует локальные акты по защите информации в ИС; управляет учетными записями в соответствии с установленными правилами; настраивает и эксплуатирует средства защиты информации; осуществляет управление уязвимостями (выявление, устранение (нейтрализация)); контролирует конфигурации ИС, выявляет и устраняет уязвимости, управляет обновлениями программного обеспечения; осуществляет мониторинг событий

безопасности, выявляет инциденты и принимает меры по реагированию; контролирует процедуры резервного копирования; выполняет оценку показателей защищенности; уведомляет о выявленных инцидентах ответственного за организацию защиты информации.

Ответственный вправе:

проводить настройку средств защиты информации; блокировать доступ пользователей при нарушении требований безопасности; требовать от пользователей соблюдения правил работы в ИС; инициировать внеочередные проверки защищенности; запрашивать у подразделений, обеспечивающих техническое обслуживание, информацию, необходимую для выполнения обязанностей; вносить предложения о совершенствовании системы защиты информации.

5.2.4. Ответственный за обеспечение безопасности ПДн

Основные обязанности (функции):

разрабатывает и актуализирует локальные акты по защите ПДн; контролирует законность обработки ПДн, в том числе наличия согласий; работает с обращениями субъектов ПДн; обеспечивает конфиденциальность бумажных и электронных носителей, содержащих ПДн; информирует о нарушениях ответственного за организацию защиты информации и руководителя Учреждения.

Ответственный вправе:

получать доступ к ИС, базам данных и документам, содержащим персональные данные, в объеме, необходимом для выполнения контрольных функций; требовать от подразделений соблюдения правил обработки ПДн; инициировать служебные проверки по фактам нарушений; представлять Организацию во взаимодействии с Роскомнадзором (при необходимости); вносить предложения о совершенствовании системы защиты ПДн.

5.2.5. Ответственный за эксплуатацию СКЗИ

Основные обязанности (функции):

разрабатывает и актуализирует локальные акты по защите информации с применением СКЗИ; настраивает СКЗИ в соответствии с требованиями по эксплуатации; осуществляет ведение журналов учета СКЗИ; проводит инструктаж пользователей СКЗИ; контролирует условия эксплуатации СКЗИ; подготавливает заключения о возможности допуска пользователей к самостоятельной работе с СКЗИ, а также о возможности эксплуатации СКЗИ; информирует о нарушениях ответственного за организацию защиты информации, ответственного за защиту информации в ИС, а также в случае серьезных нарушений руководителя Учреждения.

Ответственный вправе:

осуществлять учет и контроль использования криптографических средств; отказывать в допуске к работе с СКЗИ при несоответствии требованиям (с незамедлительным уведомлением ответственного за защиту информации в ИС и ответственного за организацию защиты информации); инициировать замену или обновление криптографических средств; требовать соблюдения правил хранения

ключевой информации; приостанавливать эксплуатацию СКЗИ при нарушении условий их применения.

5.2.6. Ответственный за техническое обслуживание ИС (администратор системы)

Основные обязанности (функции):

проводит инвентаризацию активов; выполняет установку и настройку оборудования и программных средств; осуществляет обслуживание сетевого оборудования, серверов и рабочих станций; контролирует целостность программно-аппаратной среды; устраняет технические неисправности и ошибки в работе ПО; информирует о нарушениях ответственного за организацию защиты информации и ответственного за защиту информации в ИС.

Ответственный вправе:

получать доступ к оборудованию и системному программному обеспечению; изменять конфигурации технических средств в рамках утвержденных процедур; приостанавливать эксплуатацию оборудования при выявлении угроз безопасности (с незамедлительным уведомлением ответственного за защиту информации в ИС и ответственного за организацию защиты информации); запрашивать у подразделений и пользователей информацию, необходимую для технического обслуживания и устранения неисправностей.

5.2.7. Пользователи ИС

Основные обязанности (функции):

соблюдать требования настоящей Политики, регламентов и инструкций при работе в ИС; использовать ИС исключительно для выполнения служебных задач; сохранять конфиденциальность учетных данных (паролей, токенов) и не передавать их третьим лицам; незамедлительно уведомлять ответственного за организацию защиты информации или администратора безопасности о подозрительных событиях, попытках несанкционированного доступа, утрате носителей информации или компрометации учетных записей; проходить инструктажи и обучение по вопросам информационной безопасности; не устанавливать несанкционированное программное обеспечение, не изменять настройки средств защиты информации.

Пользователи вправе:

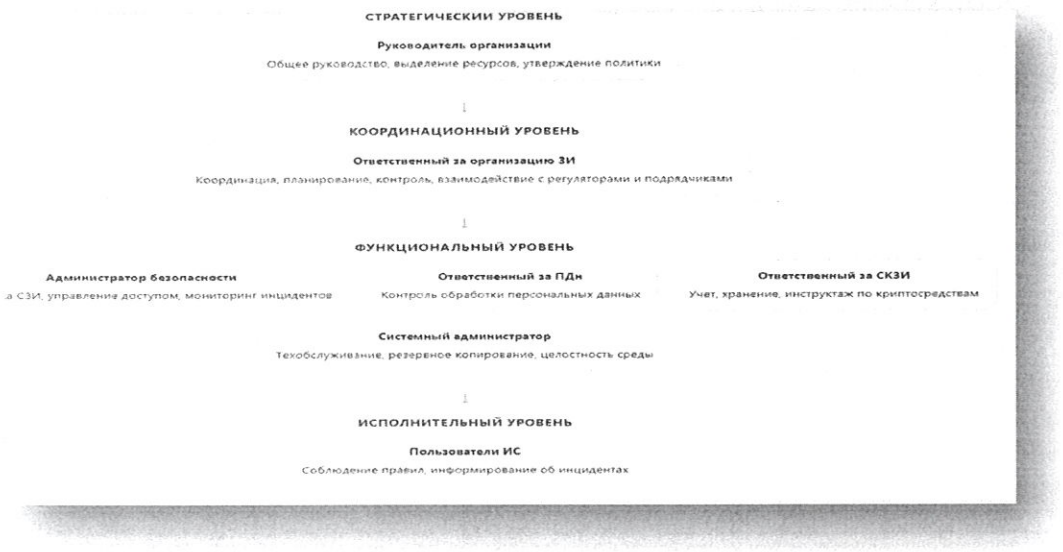
получать доступ к ИС, ресурсам и данным в объеме, необходимом для выполнения должностных обязанностей; использовать предоставленные программные и технические средства в соответствии с их назначением; запрашивать и получать информацию о действующих правилах обработки информации и политиках безопасности (в части, их касающейся); подавать заявки на предоставление, изменение или продление прав доступа к информационным ресурсам в установленном порядке; сообщать руководству и ответственным лицам о выявленных нарушениях, уязвимостях, инцидентах и подозрительной активности.

6. Организационная система управления деятельностью по защите информации

6.1. Организационная структура

В Учреждении применяется Организациализованная модель управления деятельностью по защите информации, при которой стратегическое руководство осуществляется руководителем Учреждения, а оперативная реализация мероприятий распределяется между назначенными ответственными лицами.

Система управления деятельностью по защите информации функционирует на основе процессного подхода и принципов, изложенных в настоящей Политике, и охватывает все этапы жизненного цикла ИС.



6.2. Механизмы взаимодействия и контроля

6.2.1. Вертикальные связи — в порядке подчиненности и отчетности: ответственный за организацию защиты информации отчитывается перед руководителем Учреждения; функциональные специалисты отчитываются перед ответственным за организацию защиты информации; пользователи информируют ответственных лиц о подозрительных событиях.

6.2.2. Горизонтальные связи — между функциональными специалистами: администратор безопасности взаимодействует с системным администратором; ответственный за ПДн взаимодействует с администратором безопасности; ответственный за СКЗИ взаимодействует с администратором безопасности и системным администратором.

6.2.3. Условия совмещения ролей — в целях обеспечения рационального распределения кадровых ресурсов в Учреждении допускается возложение на одного работника обязанностей по нескольким направлениям деятельности в области защиты информации. Совмещение ролей допускается исключительно при невозможности их разделения и при условии реализации компенсирующих мер, включая: участие руководителя Учреждения в оценке эффективности защиты; оценка состояния защиты должна проводиться с привлечением постоянно действующей комиссии; работник должен иметь необходимую квалификацию; при необходимости привлечение лицензиата ФСТЭК России.