Приложение
к Приказу от 31.08.2026
№ 05-05/100
«Об утверждении политики
информационной безопасности
Государственного казенного
учреждения Ленинградской области
«Оператор «электронного правительства»

ПОЛИТИКА

ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ГОСУДАРСТВЕННОГО КАЗЕННОГО УЧРЕЖДЕНИЯ ЛЕНИНГРАДСКОЙ ОБЛАСТИ «ОПЕРАТОР «ЭЛЕКТРОННОГО ПРАВИТЕЛЬСТВА»

Санкт-Петербург

2026

Содержание

1. Общие положения 3
2. Перечень терминов и определений 4
3. Перечень используемых сокращений 5
4. Описание объекта защиты 5
5.1. Категорирование и обработка информации 6
5.2. Резервное копирование 6
5.3. Защита от вредоносного кода 6
6. Основные принципы построения системы комплексной защиты информации 6
7. Меры, методы и средства обеспечения требуемого уровня защищенности 7
8. Контроль эффективности системы защиты информации 7
10. Модели угроз и нарушителей информационной безопасности 8
10.1. Внутренние нарушители 8
10.2. Внешние нарушители 8
11. Основные требования, правила, принципы, роли и ответственность 8
13. Обеспечение и поддержка СМИБ 9
14. Организационная основа деятельности по обеспечению защиты информации 9
15. Защита персональных данных 10
16. Заключительные положения 10

1. Общие положения

Настоящая Политика информационной безопасности Государственного казенного учреждения Ленинградской области «Оператор «электронного правительства» (далее - Политика) определяет систему взглядов Государственного казенного учреждения Ленинградской области «Оператор «электронного правительства» (далее - Учреждение) на обеспечение информационной безопасности.

Политика является внутренним нормативным документом первого уровня в области информационной безопасности и устанавливает принципы построения, функционирования, поддержки и совершенствования системы менеджмента информационной безопасности Учреждения.

Политика направлена на обеспечение конфиденциальности, целостности и доступности информации, информационных систем, программно-технических средств, каналов связи, помещений, носителей информации и иных информационных активов Учреждения.

Требования Политики обязательны для руководства, работников Учреждения, пользователей информационных ресурсов, а также лиц, привлекаемых для выполнения работ по Государственным контрактам, получивших доступ к информации или информационной инфраструктуре Учреждения.

Положения Политики подлежат учету при разработке частных политик, положений, регламентов, инструкций, методик, планов и иных внутренних документов Учреждения по информационной безопасности.

Политика разработана с учетом:

- Конституции Российской Федерации;
- Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Федеральный закон № 152-ФЗ);
- Федерального закона от 29.07.2004 № 98-ФЗ «О коммерческой тайне»;
- Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи»;
- Федерального закона от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»;
- Указа Президента Российской Федерации от 06.03.1997 № 188 «Об утверждении перечня сведений конфиденциального характера»;
- Указа Президента Российской Федерации от 01.05.2022 № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации»;
- Постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» (далее - постановление Правительства Российской Федерации № 1119);
- Постановления Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- Приказа ФСТЭК России от 11.04.2025 № 117 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных

информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений» (далее - приказ ФСТЭК России № 117);

- Приказа ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» (далее - приказ ФСТЭК России № 21);
- Приказа ФСБ России от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищённости» (далее - приказом ФСБ России № 378) ;
- ГОСТ Р ИСО/МЭК 27000 и иных применимых национальных стандартов;
- иных нормативных правовых актов Российской Федерации и документов уполномоченных органов.

2. Перечень терминов и определений

Информационная безопасность – состояние защищенности информации, обеспечивающее ее конфиденциальность, целостность и доступность.

Информация - это сведения (сообщения, данные) об объектах, процессах и явлениях окружающего мира, их свойствах, параметрах и состоянии, которые воспринимаются живыми существами, техническими устройствами или другими информационными системами.

Конфиденциальность – недоступность информации неавторизованным лицам, процессам или объектам.

Целостность – сохранение точности, полноты и неизменности информации.

Доступность – возможность использования информации авторизованным субъектом по запросу.

Информационная система – совокупность информации, содержащейся в базах данных, и обеспечивающих ее обработку информационных технологий и технических средств.

Инцидент информационной безопасности – событие или совокупность событий, указывающих на возможную, предпринимаемую либо реализованную угрозу информационной безопасности.

Несанкционированный доступ – доступ к информации или действия с ней с нарушением установленных правил разграничения доступа.

Угроза информационной безопасности – потенциальная причина нежелательного события, способного нанести ущерб Учреждению.

Уязвимость – недостаток или слабое место актива либо меры защиты, которое может быть использовано источником угрозы.

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу.

Средства защиты информации – программные, программно-аппаратные, технические, криптографические и иные средства, предназначенные для предотвращения, выявления и устранения последствий угроз.

Пользователь информационных ресурсов - это субъект (человек, организация, орган власти), который обращается к информационной системе или посреднику за получением необходимой информации и использует её.

Конфиденциальная информация - это сведения, доступ к которым строго ограничен, и их разглашение может нанести вред обладателю, третьим лицам или даже государству.

Материальный носитель ПДн — это любой материальный объект (предмет, среда, вещество, физическое поле или их комбинация), на котором в виде символов, образов или сигналов зафиксированы персональные данные, в т.ч. компьютеры, планшеты, телефоны, магнитные ленты, дискеты, жёсткие диски, CD, DVD, Blu-ray диски, USB-накопитель.

3. Перечень используемых сокращений

Сокращение	Значение
АРМ	Автоматизированное рабочее место
ГКУ ЛО	Государственного казенного учреждения Ленинградской области
«ОЭП»	«Оператор «электронного правительства»
ИБ	Информационная безопасность
ИСПДн	Информационная система персональных данных
КЗ	Контролируемая зона
ЛВС	Локальная вычислительная сеть
НСД	Несанкционированный доступ
ПДн	Персональные данные
ПО	Программное обеспечение
СЗИ	Средства защиты информации
СКЗИ	Средства криптографической защиты информации
СМИБ	Система менеджмента информационной безопасности
СОИБ	Система обеспечения информационной безопасности

4. Описание объекта защиты

К основным объектам защиты Учреждения относятся:

- информационные ресурсы, включая персональные данные и конфиденциальную информацию;
- информационные системы, базы данных, программное обеспечение и сервисы;
- технические средства обработки, хранения и передачи информации;
- каналы связи, ЛВС, сетевое оборудование, серверное оборудование и удаленный доступ;
- средства защиты информации;
- работники Учреждения, пользователи информационных систем, лица, привлекаемые для выполнения работ по Государственным контрактам;
- помещения, в которых размещены информационные системы, серверное и сетевое оборудование;
- материальные носители информации и резервные копии.

5. Цели, задачи и направления

Целью Политики является внедрение, поддержание и постоянное совершенствование СМИБ, обеспечивающей защиту информации и ресурсов Учреждения от внешних и внутренних угроз.

Основными задачами являются:

- обеспечение конфиденциальности, целостности и доступности информации;
- соблюдение требований законодательства Российской Федерации;
- управление рисками ИБ;

- классификация и категорирование информационных активов;
- предотвращение, выявление, расследование и ликвидация последствий инцидентов ИБ;
- обеспечение непрерывности деятельности;
- обеспечение защищенного жизненного цикла информационных систем;
- повышение уровня знаний работников в области ИБ.

5.1. Категорирование и обработка информации

Информация категорируется с учетом ее ценности, критичности, чувствительности к несанкционированному раскрытию, изменению, уничтожению или блокированию, а также требований законодательства и регуляторов.

Результаты категорирования пересматриваются при изменении состава активов, технологий, процессов, законодательства, требований регуляторов и уровня критичности информации.

5.2. Резервное копирование

Резервное копирование значимой информации и программного обеспечения осуществляется ежедневно.

При организации резервного копирования обеспечиваются:

- учет резервных копий и документирование процедур восстановления;
- определение периодичности и объема резервного копирования;
- защита резервных копий от физического повреждения, утраты и НСД;
- шифрование резервных копий, содержащих конфиденциальную информацию;
- регулярное тестирование восстановления данных.

5.3. Защита от вредоносного кода

В Учреждении применяются меры по предотвращению, обнаружению и устранению последствий воздействия вредоносного программного обеспечения, включая:

- использование антивирусных средств;
- своевременное обновление антивирусных баз и ПО;
- запрет неавторизованного программного обеспечения;
- контроль файлов, электронной почты и веб-ресурсов;
- мониторинг уязвимостей;
- проведение регулярных проверок критических систем;

6. Основные принципы построения системы комплексной защиты информации

Система защиты информации Учреждения строится на принципах:

1. законности;
2. системности;
3. комплексности;
4. непрерывности защиты;
5. своевременности;
6. преемственности и постоянного совершенствования;
7. персональной ответственности;
8. минимизации полномочий;

9. взаимодействия и сотрудничества;
10. гибкости системы защиты;
11. открытости алгоритмов и механизмов защиты;
12. простоты применения средств защиты;
13. научной обоснованности и технической реализуемости;
14. специализации и профессионализма;
15. обязательности контроля.

Права доступа предоставляются исключительно в объеме, необходимом для исполнения должностных обязанностей, по принципу: **«все, что не разрешено, запрещено».**

7. Меры, методы и средства обеспечения требуемого уровня защищенности

Для обеспечения требуемого уровня защищенности применяются:

- правовые меры;
- организационные меры;
- физические меры;
- технические меры;
- программные и программно-аппаратные средства защиты;
- криптографические средства защиты информации;
- меры повышения осведомленности работников.

К техническим мерам относятся идентификация и аутентификация пользователей, разграничение доступа, регистрация событий безопасности, антивирусная защита, межсетевое экранирование, защита удаленного доступа, контроль целостности, резервное копирование и криптографическая защита информации.

8. Контроль эффективности системы защиты информации

Контроль эффективности мер защиты осуществляется каждые 14 дней, а также при изменении информационной инфраструктуры, обработке инцидентов ИБ и выявлении новых угроз.

Контроль проводится ответственными работниками Учреждения, назначенными директором Учреждения, а при необходимости – привлекаемыми организациями, имеющими необходимые лицензии и компетенции.

Целями контроля являются:

- выявление нарушений режимов работы СЗИ;
- проверка выполнения требований Политики;
- оценка достаточности и эффективности реализованных мер;
- своевременное выявление уязвимостей и новых угроз;
- подготовка предложений по улучшению СОИБ.

9. Угрозы информационной безопасности

Угрозы ИБ подразделяются на:

- **природные** – стихийные бедствия, неблагоприятные климатические и геофизические явления и т.п.;

- **техногенные** – отказы оборудования, сбои электроснабжения, повреждение линий связи, аварии и т.п.;
- **антропогенные** – ошибки работников, нарушения правил обработки информации, умышленные действия нарушителей, социальная инженерия, вредоносное ПО и т.п..

Источники угроз могут быть внутренними, внешними либо комбинированными.

10. Модели угроз и нарушителей информационной безопасности

Модели угроз и нарушителей являются инструментами оценки рисков, выбора мер защиты, развития и совершенствования СОИБ.

Модели угроз и нарушителей подлежат пересмотру при изменении состава информационных систем, архитектуры инфраструктуры, состава обрабатываемой информации, законодательства, требований регуляторов в сфере ИБ, выявлении новых угроз или по результатам инцидентов ИБ.

10.1. Внутренние нарушители

К внутренним нарушителям могут относиться:

- авторизованные пользователи;
- разработчики программных, программно-аппаратных средств;
- работники учреждения
- лица, обеспечивающие функционирование объекта кии, лица, обеспечивающие системы оператора, а также лица, привлекаемые для выполнения работ по государственным контрактам;
- обслуживающий персонал;
- лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ;
- системные администраторы и администраторы безопасности.

10.2. Внешние нарушители

К внешним нарушителям могут относиться:

- бывшие работники (пользователи);
- лица, обеспечивающие поставку программных, программно-аппаратных средств;
- операторы;
- отдельные физические лица (хакеры);
- подрядные организации;
- преступные группы (криминальные структуры);
- специальные службы иностранных государств;
- террористические, экстремистские группировки.

11. Основные требования, правила, принципы, роли и ответственность

Учреждение обеспечивает:

- определение критических процессов и информационных активов;
- правила физического и логического доступа;
- антивирусную защиту;

- защиту сети и удаленного доступа;
- криптографическую защиту информации при необходимости;
- регистрацию и анализ событий ИБ;
- реагирование на инциденты;
- контроль за выполнение требований к третьим лицам в договорах, государственных контрактах и соглашениях;
- повышение уровня знаний работников в сфере иб;
- разработку планов обеспечения непрерывности деятельности.

Каждый работник и лица, привлекаемые для выполнения работ по государственным контрактам, имеющие доступ к информации или инфраструктуре Учреждения, обязаны соблюдать требования Политики и несут ответственность за их нарушение в соответствии с законодательством Российской Федерации, трудовыми договорами, соглашениями и внутренними документами Учреждения.

12. Планирование системы менеджмента информационной безопасности

Учреждение организует процесс оценки и обработки рисков ИБ, предусматривающий:

- установление критериев оценки и принятия рисков;
- идентификацию информационных активов и владельцев рисков;
- определение угроз и уязвимостей;
- оценку вероятности реализации угроз и возможного ущерба;
- определение уровня рисков;
- выбор способа обработки рисков;
- подготовку и реализацию плана обработки рисков;
- принятие остаточных рисков уполномоченными лицами;
- формирование и ведение ведомости применимости мер защиты.

13. Обеспечение и поддержка СМИБ

Учреждение определяет и выделяет ресурсы, необходимые для создания, функционирования и постоянного улучшения СМИБ.

Обеспечиваются:

- наличие работников с необходимой квалификацией;
- повышение квалификации работников, ответственных за обеспечение ИБ;
- повышение уровня знаний работников в сфере ИБ
- информирование работников о требованиях Политики;
- документирование процессов СМИБ;
- защита внутренней документации от НСД, утраты и несанкционированного изменения;
- управление обработкой, хранением, распространением, актуализацией, архивированием и уничтожением документов.

14. Организационная основа деятельности по обеспечению защиты информации

В Учреждении определяются следующие роли:

Ответственный за обеспечение ИБ – организует обеспечение защиты информации, координирует деятельность в области ИБ;

Структурное подразделение – осуществляет оперативное планирование, внедрение, сопровождение, мониторинг и совершенствование СОИБ;

Работники Учреждения – соблюдают требования ИБ, выявляют и сообщают об угрозах и инцидентах;

Руководители подразделений – обеспечивают выполнение требований ИБ в подчиненных подразделениях.

Структурное подразделение обеспечивает разработку и актуализацию внутренних документов ИБ, контроль соблюдения требований, мониторинг событий, участие в расследовании, устранении и ликвидации последствий инцидентов, развитие средств защиты и повышение уровня знаний работников в сфере ИБ.

15. Защита персональных данных

Обработка и защита персональных данных в Учреждении осуществляются в соответствии с Федеральным законом № 152-ФЗ, постановлением Правительства Российской Федерации № 1119, приказом ФСТЭК России № 117, приказом ФСТЭК России № 21, приказом ФСБ России № 378 и иными применимыми требованиями.

Для защиты ПДн применяются правовые, организационные и технические меры, направленные на предотвращение неправомерного или случайного доступа, уничтожения, изменения, блокирования, копирования, предоставления и распространения ПДн.

Работники, осуществляющие обработку ПДн, должны быть ознакомлены с требованиями к обработке и защите ПДн в пределах своих должностных обязанностей.

Руководители подразделений, эксплуатирующих ИСПДн, обеспечивают соблюдение требований безопасности ПДн и сохранность материальных носителей ПДн.

16. Заключительные положения

Требования настоящей Политики развиваются и уточняются иными внутренними нормативными документами Учреждения.

При изменении законодательства Российской Федерации, требований регуляторов, организационной структуры, информационной инфраструктуры либо состава обрабатываемой информации Политика подлежит пересмотру.

Плановый пересмотр Политики осуществляется не реже одного раза в 24 месяца.

Внеплановый пересмотр осуществляется по результатам инцидентов ИБ, аудитов, проверок, оценки рисков, изменения угроз, выявления недостаточности или неэффективности мер защиты.

Ответственность за инициирование внесения изменений в Политику несет ответственный за обеспечение ИБ.