Утверждено
приказом директора
ГАУ АО АОСРЦ «Русь»
28.05.2026 г. №86

Политика информационной безопасности Государственного автономного учреждения Астраханской области «Астраханский областной социально-реабилитационный центр «Русь»

1. Общие положения

1.1. Настоящая Политика информационной безопасности (далее — Политика) Государственного автономного учреждения Астраханской области «Астраханский областной социально-реабилитационный центр «Русь» (далее — Учреждение) является локальным нормативным актом, определяющим цели, принципы и основные требования к обеспечению информационной безопасности, а также порядок организации защиты информации в Учреждении.

1.2. Учреждение не осуществляет деятельность, связанную с использованием сведений, составляющих государственную тайну. В случае их появления требования к защите такой информации определяются законодательством Российской Федерации.

1.3. Основной задачей в области информационной безопасности Учреждение признает совершенствование мер и средств обеспечения защиты информации объектов информатизации Учреждения.

1.4. При разработке Политики учитывались основные принципы создания систем защиты информации, характеристики и возможности организационно-технических мер и современных программных и аппаратно-программных средств защиты информации.

1.5. В рамках своей деятельности Учреждение обязуется предпринимать все возможные меры для защиты информации от угроз безопасности информации.

1.6. Требования информационной безопасности соответствуют целям деятельности Учреждения и предназначены для снижения вероятности реализации угроз безопасности информации.

1.7. Политика подлежит опубликованию на сайте Учреждения.

2. Цели и задачи обеспечения информационной безопасности

2.1. Субъектами информационных отношений являются:

— работники структурных подразделений (в том числе уволенные);

— физические лица, представители контрагентов в рамках исполнения договорных обязательств;

— граждане, работающие по договорам гражданско-правового характера;

— получатели социальных услуг и их законные представители;

— иные лица, взаимодействующие с Учреждением.

2.2. Объектами информационных отношений являются:

— персональные данные работников и получателей социальных услуг;

— служебная информация Учреждения;

— документы на бумажных и электронных носителях;

— информационные системы;

— технические средства обработки информации (компьютеры, ноутбуки и иные устройства).

2.3. Основной целью обеспечения информационной безопасности является защита информации от несанкционированного доступа, уничтожения, изменения или распространения, в том числе:

— Обеспечение конфиденциальности персональных данных;

— обеспечение целостности информации;

— обеспечение доступности информации для выполнения служебных обязанностей;

— снижение вероятности реализации угроз безопасности информации.

2.4. Достижение целей обеспечения информационной безопасности и свойств информации в Учреждении решается следующими задачами:

— защита от несанкционированного доступа к информации объектов информационных отношений;

— управление доступом субъектов доступа к объектам доступа;

— регистрация и контроль действий пользователей при работе с основными техническими средствами и системами объектов информатизации Учреждения;

— контроль целостности среды исполнения программ и ее восстановление в случае нарушения;

— обеспечение аутентификации и идентификации пользователей при эксплуатации информационных систем;

— своевременное выявление источников угроз безопасности информации, причин и условий, способствующих нанесению ущерба заинтересованным субъектам информационных отношений;

— создание условий для минимизации наносимого ущерба неправомерными действиями и устранение последствий нарушения информационной безопасности.

3. Принципы обеспечения информационной безопасности

3.1. Принцип законности

3.1.1. При выборе мероприятий по защите информации должно соблюдаться действующее законодательство Российской Федерации в сфере защиты информации.

3.1.2. Все работники должны иметь представление об ответственности за правонарушения в сфере защиты информации.

3.1.3. Программные и программно-аппаратные средства, включая средства защиты информации, применяемые в Учреждении, должны иметь соответствующие лицензии и сертификаты соответствия (для средств защиты информации), официально приобретаться у представителей разработчиков таких средств.

3.2. Принцип системности

3.2.1. При создании системы защиты информации должны учитываться актуальные угрозы безопасности информации, возможные объекты и направления атак на нее со стороны нарушителей. Система защиты информации должна строиться с учетом не только известных каналов утечки информации, но и с учетом возможности появления новых уязвимостей в программном обеспечении.

3.3. Принцип комплексности

3.3.1. Комплексное использование средств защиты информации предполагает согласованное применение при построении целостной системы защиты информации, перекрывающей все актуальные угрозы безопасности информации.

3.3.2. При построении, внедрении и эксплуатации системы защиты информации руководство Учреждения обеспечивает условия для эффективной координации действий всех лиц, обеспечивающих информационную безопасность.

3.4. Принцип своевременности

3.4.1. Требования информационной безопасности учитываются при внедрении и использовании информационных систем и программного обеспечения в Учреждении.

3.5. Принцип преемственности

3.5.1. Обеспечение информационной безопасности осуществляется на постоянной основе, изменений в угрозах и требований законодательства.

3.6. Принцип достаточности

3.6.1. Меры по обеспечению информационной безопасности должны быть достаточными для защиты информации и соразмерными возможным рискам, при этом не должны существенно затруднять выполнение служебных обязанностей.

3.7. Принцип ответственности

3.7.1. Каждый работник Учреждения несет персональную ответственность за соблюдение требований информационной безопасности в пределах своих должностных обязанностей.

3.8. Принцип обоснованности и технической реализуемости

3.8.1. Применяемые меры защиты информации должны быть обоснованы, соответствовать законодательству Российской Федерации и возможностям Учреждения.

3.9. Принцип профессионализма

3.9.1. Обеспечение информационной безопасности осуществляется работниками, обладающими необходимыми знаниями и навыками.

3.9.2. При необходимости могут привлекаться специализированные организации в установленном порядке.

3.10. Принцип минимизации привилегий пользователей

3.10.1. Пользователям предоставляются права доступа, необходимые только для выполнения их должностных обязанностей.

4. Основные требования по защите информации ограниченного доступа

4.1. Организация защиты информации

4.1.1. Учреждение при осуществлении своей деятельности обязано:

— соблюдать права и законные интересы субъектов персональных данных;

— принимать необходимые меры по защите информации;

— ограничивать доступ к информации в соответствии с законодательством Российской Федерации.

4.1.2. Защита информации ограниченного доступа включает реализацию организационных и технических мер, направленных на:

— обеспечение конфиденциальности информации;

— обеспечение целостности информации;

— обеспечение доступности информации для уполномоченных лиц.

4.1.3. При организации защиты информации в Учреждении учитываются требования законодательства Российской Федерации в области информации, информационных технологий и защиты информации, в том числе:

— 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»;

— иных нормативных правовых актов Российской Федерации, регулирующих вопросы защиты информации и обработки персональных данных.

4.1.4. В Учреждении реализуются следующие основные меры защиты информации:

— разграничение доступа к информации;

— использование антивирусной защиты;

— своевременное обновление программного обеспечения;

— контроль доступа к информации;

— резервное копирование данных;

— защита носителей информации;

— информирование работников о требованиях информационной безопасности.

4.1.5. Работники Учреждения, имеющие доступ к информации ограниченного доступа, подлежат обязательному ознакомлению с требованиями по ее защите и несут ответственность за соблюдение установленных правил.

4.1.6. Учреждение принимает меры по повышению уровня защищенности информации, в том числе путем:

— проведения инструктажей работников;

— анализа возникающих угроз и инцидентов;

— совершенствования применяемых мер защиты.

4.2. Особенности защиты персональных данных

4.2.1. Учреждение, являясь оператором персональных данных, обеспечивает выполнение требований законодательства Российской Федерации в области защиты персональных данных.

В Учреждении реализуются следующие меры:

— назначение ответственного за организацию обработки персональных данных;

— разработка и утверждение локальных нормативных актов по обработке и защите персональных данных;

— ограничение доступа к персональным данным;

— ознакомление работников с требованиями законодательства о персональных данных;

— проведение инструктажей и обучение работников;
— опубликование политики обработки персональных данных.

4.2.2. Обеспечение безопасности персональных данных достигается путем:

— определения угроз безопасности персональных данных;
— установления правил доступа к персональным данным;
— применения средств защиты информации (антивирус, пароли и иные меры);
— предотвращения несанкционированного доступа к персональным данным;
— восстановления персональных данных при их утрате;
— контроля за соблюдением требований по защите персональных данных.

5. Основные требования к процессам обеспечения информационной безопасности

Обеспечение информационной безопасности в Учреждении осуществляется путем реализации организационных и технических мер защиты информации.

5.1. Физическая безопасность

5.1.1. В Учреждении обеспечивается защита помещений и рабочих мест, в которых осуществляется обработка информации, путем:

— ограничения доступа работников в помещения в соответствии с их должностными обязанностями;
— контроля присутствия посторонних лиц;
— соблюдения порядка использования технических средств;
— предотвращения несанкционированного выноса оборудования и носителей информации.

5.1.2. Помещения Учреждения оборудуются средствами охранно-пожарной сигнализации.

5.1.3. Работники обязаны обеспечивать сохранность используемых технических средств и не оставлять их без присмотра вне территории Учреждения.

5.2. Безопасность на рабочем месте

5.2.1. Запрещается записывать пароли в открытом виде на бумажных и иных носителях, а также передавать их третьим лицам.

5.2.2. Документы и носители с информацией ограниченного доступа должны храниться в закрываемых шкафах или иных местах, исключающих несанкционированный доступ.

При уходе с рабочего места пользователь обязан заблокировать компьютер или завершить рабочую сессию. Автоматический вход в систему не допускается.

5.2.3. Документы, содержащие информацию ограниченного доступа, должны своевременно изыматься из печатающих устройств. Уничтожение документов осуществляется способом, исключающим возможность восстановления информации.

5.2.4. При использовании мобильных технических средств (ноутбуков, носителей информации) работники обязаны обеспечивать их сохранность и не допускать несанкционированного доступа к информации.

5.2.5. Нахождение посторонних лиц в помещениях, где обрабатывается информация ограниченного доступа, допускается только в присутствии работника Учреждения.

5.2.6. Размещение экранов и иных средств отображения информации должно исключать возможность просмотра информации посторонними лицами.

5.2.7. Технические средства должны использоваться и храниться с соблюдением мер, предотвращающих их повреждение и несанкционированный доступ.

5.3. Техническое обслуживание оборудования

5.3.1. Технические средства Учреждения должны проходить обслуживание и проверку работоспособности по мере необходимости, а также в соответствии с рекомендациями производителей оборудования.

5.3.2. Ремонт и техническое обслуживание оборудования выполняются работниками Учреждения либо привлекаемыми специалистами, обладающими необходимой квалификацией.

5.3.3. При проведении технического обслуживания оборудования должны приниматься меры по предотвращению несанкционированного доступа к информации, в том числе при привлечении сторонних организаций.

5.4. Взаимодействие с третьими лицами

5.4.1. При взаимодействии с третьими лицами в Учреждении должны соблюдаться следующие требования:

— при необходимости заключаются соглашения о неразглашении информации ограниченного доступа;

— доступ представителей сторонних организаций к информации и помещениям Учреждения осуществляется под контролем работников Учреждения;

— третьим лицам предоставляется доступ только к информации, необходимой для выполнения договорных обязательств.

5.5. Управление жизненным циклом информационных систем

5.5.1. При использовании информационных систем Учреждения должны обеспечиваться меры по защите информации на всех этапах их эксплуатации.

5.5.2. Установка программного обеспечения и внесение изменений в настройки информационных систем должны осуществляться с учетом требований информационной безопасности.

5.5.3. Обновление программного обеспечения должно выполняться своевременно с целью устранения уязвимостей и повышения безопасности.

5.5.4. При выводе из эксплуатации технических средств и носителей информации должны приниматься меры по удалению или уничтожению содержащейся на них информации способом, исключающим возможность ее восстановления.

5.5.5. Контроль выполнения требований информационной безопасности при эксплуатации информационных систем осуществляется ответственными лицами Учреждения.

5.6. Контроль доступа к информационным системам

5.6.1. Права доступа пользователей к информационным системам определяются в соответствии с их должностными обязанностями.

5.6.2. Предоставление и изменение прав доступа осуществляется ответственными лицами Учреждения.

5.6.3. В Учреждении осуществляется контроль соблюдения требований локальных нормативных актов в области информационной безопасности.

5.7. Идентификация и аутентификация

5.7.1. Доступ пользователей к информационным системам предоставляется при использовании индивидуальных учетных записей и средств аутентификации (логин и пароль).

5.8. Управление доступом

5.8.1. В Учреждении реализуется разграничение доступа к информации в зависимости от должностных обязанностей работников.

5.9. Безопасность при работе с носителями

5.9.1. Работники Учреждения используют только разрешенные съемные носители информации.

5.9.2. Съемные носители информации должны храниться в местах, исключающих несанкционированный доступ.

5.9.3. В случае утраты или компрометации носителей информации работники обязаны незамедлительно сообщить ответственному лицу. Учреждением принимаются меры по минимизации последствий инцидента.

5.10. Антивирусная защита информации

5.10.1. В Учреждении используются средства антивирусной защиты информации.

5.10.2. Проверке антивирусными средствами подлежит информация, получаемая из внешних источников, а также данные, записываемые на съемные носители.

5.10.3. Обновление антивирусных баз должно осуществляться регулярно.

5.10.4. Пользователям запрещается отключать антивирусную защиту или изменять ее настройки без разрешения ответственных лиц.

5.11. Контроль защищенности информации

5.11.1 В Учреждении принимаются меры по своевременному выявлению и устранению уязвимостей программного обеспечения, в том числе путем установки обновлений.

5.12. Использование программного обеспечения

5.12.1. В Учреждении используется программное обеспечение, необходимое для выполнения служебных задач и соответствующее требованиям законодательства Российской Федерации.

5.12.2. При возможности предпочтение отдается программному обеспечению, включенному в реестр российского программного обеспечения.

5.12.3. Установка и использование нелицензионного программного обеспечения запрещается.

5.13. Использование средств криптографической защиты информации

5.13.1. При передаче информации по открытым каналам связи могут применяться средства криптографической защиты информации в соответствии с требованиями законодательства Российской Федерации.

5.13.2. Использование криптографических средств осуществляется при необходимости и в установленном порядке.

5.14. Использование электронной почты

5.14.1. Электронная почта используется работниками в служебных целях.

5.14.2. При использовании электронной почты запрещается:

— передавать персональные данные и иную информацию ограниченного доступа без соблюдения мер защиты;

— передавать третьим лицам данные своей учетной записи;

— использовать электронную почту в целях, не связанных с исполнением должностных обязанностей;

— открывать вложения из неизвестных источников без проверки антивирусным программным обеспечением.

5.15. Работа в сетях общего пользования

5.15.1. Доступ к сети Интернет предоставляется работникам для выполнения служебных задач.

5.15.2. Учреждение вправе ограничивать доступ к интернет-ресурсам, не связанным с выполнением должностных обязанностей, а также к ресурсам, запрещенным законодательством Российской Федерации.

5.15.3. При использовании сети Интернет запрещается:

— посещение сайтов, содержание которых противоречит законодательству Российской Федерации;

— использование несанкционированных программ и сервисов;

— распространение недостоверной информации об Учреждении.

5.16. Резервное копирование и восстановление данных

5.16.1. В Учреждении осуществляется резервное копирование информации, имеющей значение для деятельности Учреждения, включая данные информационных систем и рабочие документы.

5.16.2. Периодичность резервного копирования определяется с учетом важности информации и необходимости ее восстановления.

5.16.3. Резервное копирование и восстановление данных выполняются уполномоченными работниками Учреждения.

5.16.4. Хранение резервных копий должно обеспечивать их сохранность и возможность восстановления информации в случае ее утраты.

6. Основные требования к процессам управления информационной безопасностью

6.1. Мониторинг информационной безопасности

6.1.1. В Учреждении осуществляется контроль состояния информационной безопасности и соблюдения установленных требований.

6.1.2. Контроль включает:

— проверку соблюдения работниками требований информационной безопасности;

— анализ возникающих инцидентов и нарушений;

— оценку эффективности применяемых мер защиты информации.

6.1.3. Работники, ответственные за обеспечение информационной безопасности:

— фиксируют выявленные нарушения;

— принимают меры по их устранению;

— при необходимости информируют руководство Учреждения.

6.1.4. Информация о выявленных нарушениях и инцидентах хранится с соблюдением требований конфиденциальности.

6.2. Управление рисками

6.2.1. В Учреждении проводится оценка угроз информационной безопасности и возможных рисков утечки, утраты или искажения информации.

6.2.2. По результатам оценки принимаются меры, направленные на снижение рисков и обеспечение защиты информации.

6.3. Управление инцидентами информационной безопасности

6.3.1. В Учреждении осуществляется учет и рассмотрение инцидентов информационной безопасности с целью минимизации их последствий и предотвращения повторного возникновения.

6.3.2. Работники обязаны незамедлительно сообщать ответственному лицу о выявленных инцидентах информационной безопасности, в том числе:

— утрате или компрометации носителей информации;

— несанкционированном доступе к информации;

— выявлении вредоносного программного обеспечения.

6.3.3. По факту инцидента принимаются меры по его устранению и снижению возможного ущерба.

6.4. Аудит системы обеспечения информационной безопасности

6.4.1. В Учреждении проводится периодическая оценка состояния информационной безопасности.

6.4.2. В ходе оценки:

— проверяется соблюдение требований локальных нормативных актов;

— анализируются выявленные инциденты;

— при необходимости разрабатываются предложения по улучшению мер защиты информации.

6.5. Повышение осведомленности работников

6.5.1. В Учреждении осуществляется повышение осведомленности работников в области информационной безопасности.

6.5.2 Повышение осведомленности работников включает:

— ознакомление с локальными нормативными актами по информационной безопасности;

— информирование о применяемых мерах защиты информации;

— обучение правилам безопасной работы с информационными системами и средствами защиты информации.

7. Заключение

7.1. В случае изменения законодательства Российской Федерации в области защиты информации положения настоящей Политики применяются в части, не противоречащей действующему законодательству.

7.2. Учреждение обеспечивает соблюдение требований законодательства Российской Федерации в области информационной безопасности и поддерживает локальные нормативные акты в актуальном состоянии.

7.3. В Учреждении в приоритетном направлении должен рассматриваться переход на программное обеспечение отечественного производителя, включенное в единый реестр российских программ для электронных вычислительных машин и баз данных или единый реестр программ для электронных вычислительных машин и баз данных государств - членов Евразийского экономического союза.

7.4. Пересмотр и актуализация настоящей Политики осуществляются по мере необходимости, а также при изменении законодательства или условий деятельности Учреждения.