

Министерство  
социальной политики и труда  
Удмуртской Республики  
(Минсоцполитики УР)



Удмурт Элькуньсь  
мерлыкo политикая  
но ужья министерство  
(УЭ мерполитикмин)

## ПРИКАЗ

«29» июля 2019 г.

№ 194

г. Ижевск

### Об информационной безопасности информационных систем Министерства социальной политики и труда Удмуртской Республики

В соответствии с Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных» п р и к а з ы в а ю:

Утвердить прилагаемые:

Концепцию информационной безопасности информационных систем  
Министерства социальной политики и труда Удмуртской Республики;

Политику информационной безопасности информационных систем  
Министерства социальной политики и труда Удмуртской Республики.

Исполняющий обязанности министра

A handwritten signature in blue ink, appearing to be 'M.E. Belousova'.

М.Е Белоусова

УТВЕРЖДЕНА  
приказом Министерства  
социальной политики и труда  
Удмуртской Республики  
от «29» 07 2019 года № 194

**КОНЦЕПЦИЯ**  
**информационной безопасности информационных систем**  
**Министерства социальной политики и труда Удмуртской Республики**

**I. Общие положения**

1. Настоящая Концепция определяет основные цели и задачи, а также общую стратегию построения системы защиты персональных данных, используемых в информационных системах Министерства социальной политики и труда Удмуртской Республики (далее – Министерство).

2. Настоящая Концепция определяет основные требования и базовые подходы к реализации системы защиты персональных данных для достижения требуемого уровня безопасности информации.

3. Настоящая Концепция разработана в соответствии с системным подходом к обеспечению информационной безопасности. Системный подход предполагает проведение комплекса мероприятий, включающих исследование угроз информационной безопасности и разработку системы защиты персональных данных с позиции комплексного применения технических и организационных мер и средств защиты.

4. Под информационной безопасностью персональных данных понимается защищённость персональных данных и обрабатывающей их инфраструктуры от любых случайных или злонамеренных воздействий, результатом которых может явиться нанесение ущерба самой информации, её владельцам (субъектам персональных данных) или инфраструктуре. Задачи информационной безопасности сводятся к минимизации ущерба от возможной реализации угроз безопасности персональных данных, а также к прогнозированию и предотвращению таких воздействий.

5. Настоящая Концепция является методологической основой для:  
формирования и проведения единой политики в области обеспечения безопасности персональных данных в информационных системах Министерства;

принятия управленческих решений и разработки практических мер для реализации политики безопасности персональных данных и выработки комплекса согласованных мер нормативно-правового, технологического и организационно-технического характера, направленных на выявление, отражение и ликвидацию последствий реализации различных видов угроз персональных данных;

координации деятельности структурных подразделений Министерства при проведении работ по развитию и эксплуатации информационных систем Министерства с соблюдением требований обеспечения безопасности персональных данных;

разработки предложений по совершенствованию правового, нормативного, методического, технического и организационного обеспечения безопасности персональных данных в информационных системах Министерства.

## **II. Построение системы защиты персональных данных в Министерстве**

6. Система защиты персональных данных представляет собой совокупность организационных и технических мероприятий для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также иных неправомерных действий с ними.

7. Безопасность персональных данных достигается путём исключения несанкционированного, в том числе случайного, доступа к ним, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий.

8. Структура, состав и основные функции системы защиты персональных данных определяются исходя из уровня защищённости и класса защищённости информационных систем Министерства.

9. Система защиты персональных данных включает в себя организационные меры и технические средства защиты информации (в том числе шифровальные (криптографические) средства, средства предотвращения несанкционированного доступа, утечки информации по техническим каналам, программно-технических воздействий на технические средства обработки персональных данных), а также используемые в информационной системе информационные технологии.

10. Система защиты персональных данных призвана обеспечить:

конфиденциальность информации (защита от несанкционированного ознакомления);

целостность информации (актуальность и непротиворечивость информации, её защищённость от разрушения и несанкционированного изменения);

доступность информации (возможность за приемлемое время получить требуемую информационную услугу).

11. Организационные меры как составная часть системы защиты персональных данных включают в себя создание и поддержание правовой базы безопасности персональных данных и разработку (введение в действие) организационно-распорядительных документов предусмотренных Политикой информационной безопасности информационных систем Министерства.

12. Технические средства защиты информации реализуются при помощи соответствующих программно-технических средств и методов защиты. Перечень необходимых мер и средств защиты информации определяется по результатам внутренней проверки обеспечения защиты персональных данных в информационных системах Министерства.

### **III. Задачи системы защиты персональных данных в Министерстве**

13. Основной целью системы защиты персональных данных в Министерстве является минимизация ущерба от возможной реализации угроз безопасности персональных данных.

14. Для достижения основной цели система защиты персональных данных информационных систем Министерства должна обеспечивать эффективное решение следующих задач:

1) защита от вмешательства в процесс функционирования информационных систем Министерства посторонних лиц (возможность использования информационных систем Министерства и доступ к её ресурсам должны иметь только зарегистрированные в установленном порядке пользователи);

2) разграничение доступа зарегистрированных пользователей к аппаратным, программным и информационным ресурсам информационных систем Министерства (возможность доступа только к тем ресурсам и выполнения только тех операций с ними, которые необходимы конкретным пользователям информационных систем Министерства для выполнения своих должностных обязанностей), то есть защиту от несанкционированного доступа:

к информации, циркулирующей в информационных системах Министерства;

средствам вычислительной техники информационных систем Министерства;

аппаратным, программным и криптографическим средствам защиты, используемым в информационных системах Министерства;

3) регистрация действий пользователей при использовании защищаемых ресурсов информационных систем Министерства в системных журналах и периодический контроль корректности действий пользователей системы путём анализа содержимого этих журналов;

4) контроль целостности (обеспечение неизменности) среды исполнения программ и её восстановление в случае нарушения;

5) защита от несанкционированной модификации и контроль целостности используемых в информационных системах Министерства программных средств, а также защиту системы от внедрения несанкционированных программ;

6) защита персональных данных от утечки по техническим каналам при их обработке, хранении и передаче по каналам связи;

7) защита персональных данных, хранимых, обрабатываемых и передаваемых по каналам связи, от несанкционированного разглашения или искажения;

8) обеспечение «живучести» криптографических средств защиты информации при компрометации части ключевой системы;

9) своевременное выявление источников угроз безопасности персональных данных, причин и условий, способствующих нанесению ущерба субъектам персональных данных, создание механизма оперативного реагирования на угрозы безопасности персональных данных и негативные тенденции;

10) создание условий для минимизации и локализации наносимого неправомерными действиями физических и юридических лиц ущерба, ослабления негативного влияния и ликвидации последствий нарушения безопасности персональных данных.

#### **IV. Объекты защиты персональных данных в Министерстве**

15. Объектами защиты персональных данных в Министерстве являются информация, обрабатываемая в информационных системах Министерства, и технические средства её обработки и защиты.

16. Перечень персональных данных, подлежащих защите, определяется в Перечне персональных данных и иных объектов, подлежащих защите в информационных системах Министерства, утверждаемый приказом Министерства.

17. Объекты защиты персональных данных в Министерстве включают в себя:

обрабатываемую информацию;

технологическую информацию;

программно-технические средства обработки;

каналы информационного обмена;

помещения, в которых размещены компоненты информационных систем Министерства.

#### **V. Классификация пользователей информационных систем Министерства**

18. Пользователем информационных систем Министерства является лицо, участвующее в функционировании информационной системы Министерства или использующее результаты её функционирования.

19. Пользователи информационных систем Министерства делятся на три основные категории:

1) администратор информационной системы Министерства;

2) пользователь информационной системы Министерства;

3) программист-разработчик информационной системы Министерства.

20. Категории пользователей определяются для каждой информационной системы Министерства.

## **VI. Основные принципы построения системы защиты персональных данных в Министерстве**

21. Построение системы защиты персональных данных в Министерстве и её функционирование должны осуществляться в соответствии со следующими основными принципами:

- законность;
- системность;
- комплексность;
- непрерывность;
- своевременность;
- преемственность и непрерывность совершенствования;
- персональная ответственность;
- минимизация полномочий;
- взаимодействие и сотрудничество;
- гибкость системы защиты;
- открытость алгоритмов и механизмов защиты;
- простота применения средств защиты;
- научная обоснованность и техническая реализуемость;
- специализация и профессионализм;
- обязательность контроля.

22. Принцип законности предполагает осуществление защитных мероприятий и разработку системы защиты персональных данных в Министерстве в соответствии с требованиями законодательства в области защиты персональных данных и других нормативных актов по безопасности информации, утверждённых органами государственной власти в пределах их компетенции.

Пользователи информационных систем Министерства должны быть осведомлены о порядке работы с защищаемой информацией и об ответственности за нарушение режима защиты персональных данных, установленного в Министерстве.

23. Системный подход к построению системы защиты персональных данных в Министерстве предполагает учёт всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, существенно значимых для понимания и решения проблемы обеспечения безопасности персональных данных.

При создании системы защиты персональных данных в Министерстве должны учитываться все слабые и наиболее уязвимые места системы обработки персональных данных, а также характер, возможные объекты и направления атак на систему со стороны нарушителей, пути проникновения в распределённые системы и несанкционированный доступ к информации.

Система защиты персональных данных в Министерстве должна строиться с учётом не только всех известных каналов проникновения и несанкционированного доступа к информации, но и с учётом возможности появления принципиально новых путей реализации угроз безопасности.

24. Комплексное использование методов и средств защиты персональных данных предполагает согласованное применение разнородных средств при построении целостной системы защиты персональных данных, перекрывающей все существенные (значимые) каналы реализации угроз и не содержащей слабых мест на стыках отдельных её компонентов.

Защита персональных данных должна строиться эшелонировано. Для каждого канала утечки информации и для каждой угрозы безопасности должно существовать несколько защитных рубежей. Создание защитных рубежей осуществляется с учётом того, чтобы для их преодоления потенциальному злоумышленнику требовались профессиональные навыки в нескольких невязанных областях.

Внешняя защита должна обеспечиваться физическими средствами, организационными и правовыми мерами. Одним из наиболее укрепленных рубежей призваны быть средства криптографической защиты, реализованные с использованием технологии VPN. Прикладной уровень защиты, учитывающий особенности предметной области, представляет внутренний рубеж защиты.

25. Принцип непрерывности подразумевает непрерывный целенаправленный процесс, предполагающий принятие соответствующих мер на всех этапах жизненного цикла информационных систем Министерства.

Информационные системы должны находиться в защищённом состоянии на протяжении всего времени их функционирования. В соответствии с этим принципом должны приниматься меры по недопущению перехода информационной системы в незащищённое состояние.

Большинству физических и технических средств защиты для эффективного выполнения своих функций необходима постоянная техническая и организационная (административная) поддержка (своевременная смена и обеспечение правильного хранения и применения имён, паролей, ключей шифрования, переопределение полномочий и т.п.). Перерывы в работе средств защиты могут быть использованы злоумышленниками для анализа применяемых методов и средств защиты, для внедрения специальных программных и аппаратных «закладок» и других средств преодоления системы защиты после восстановления её функционирования.

26. Принцип своевременности предполагает упреждающий характер мер обеспечения безопасности персональных данных, то есть постановку задач по комплексной защите информационных систем Министерства и реализацию мер обеспечения безопасности персональных данных на ранних стадиях разработки информационной системы в целом и её системы защиты информации, в частности.

Разработка системы защиты должна вестись параллельно с разработкой и развитием самой защищаемой системы. Это позволит учесть требования

безопасности при проектировании архитектуры и, в конечном счёте, создать более эффективные (как по затратам ресурсов, так и по стойкости) защищённые системы.

27. Принципы преемственности и непрерывности совершенствования мер и средств защиты информации обеспечиваются на основе преемственности организационных и технических решений, кадрового состава, анализа функционирования информационной системы и её системы защиты с учётом изменений в методах и средствах перехвата информации, нормативных требований по защите, достигнутого отечественного и зарубежного опыта в этой области.

28. Принцип персональной ответственности предполагает возложение ответственности за обеспечение безопасности персональных данных и системы их обработки на каждого сотрудника Министерства в пределах его полномочий. В соответствии с этим принципом распределение прав и обязанностей специалистов строится таким образом, чтобы в случае любого нарушения круг виновников был чётко известен или сведён к минимуму.

29. Принцип минимизации полномочий означает предоставление пользователям минимальных прав доступа в соответствии с производственной необходимостью, на основе принципа «всё, что не разрешено, запрещено».

Доступ к персональным данным должен предоставляться только в том случае и объёме, если это необходимо специалисту для выполнения его должностных обязанностей.

30. Принцип взаимодействия и сотрудничества предполагает создание благоприятной атмосферы в коллективах структурных подразделений, обеспечивающих деятельность информационных систем Министерства, для снижения вероятности возникновения негативных действий, связанных с человеческим фактором.

31. Принцип гибкости системы защиты подразумевает возможность расширения, исключения или замены мер защиты информации на работающей информационной системе без нарушения процесса её нормального функционирования.

32. Принцип открытости алгоритмов и механизмов состоит в том, что защита не должна обеспечиваться только за счёт секретности структурной организации и алгоритмов функционирования её подсистем. Знание алгоритмов работы системы защиты не должно давать возможности её преодоления (даже автору). Однако, это вовсе не означает, что информация о конкретной системе защиты должна быть общедоступна.

33. Механизмы защиты должны быть интуитивно понятны и просты в использовании. Применение средств защиты не должно быть связано со знанием специальных языков или с выполнением действий, требующих значительных дополнительных трудовых затрат при обычной работе зарегистрированных в установленном порядке пользователей, а также не должно требовать от пользователя выполнения рутинных малопонятных ему операций (ввод нескольких паролей и имен и т.д.).



34. Информационные технологии, технические и программные средства, средства и меры защиты информации должны быть реализованы на современном уровне развития науки и техники, научно обоснованы с точки зрения достижения заданного уровня безопасности информации и должны соответствовать установленным нормам и требованиям по безопасности персональных данных.

Система защиты персональных данных должна быть ориентирована на решения, возможные риски для которых и меры противодействия этим рискам прошли всестороннюю теоретическую и практическую проверку.

35. Принцип специализации и профессионализма предполагает привлечение к разработке средств и реализации мер защиты информации специализированных организаций, наиболее подготовленных к конкретному виду деятельности по обеспечению безопасности персональных данных, имеющих опыт практической работы и лицензию на право оказания услуг в этой области. Реализация административных мер и эксплуатация средств защиты должна осуществляться профессионально подготовленными специалистами Министерства.

36. Принцип обязательности контроля предполагает обязательность и своевременность выявления и пресечения попыток нарушения установленных правил обеспечения безопасности персональных данных на основе используемых систем и средств защиты информации при совершенствовании критериев и методов оценки эффективности этих систем и средств.

Контроль за деятельностью любого пользователя, каждого средства защиты и в отношении любого объекта защиты персональных данных в Министерстве должен осуществляться на основе применения средств оперативного контроля и регистрации и должен охватывать как несанкционированные, так и санкционированные действия пользователей.

## **VII. Меры и средства обеспечения требуемого уровня защищённости информационных систем Министерства**

37. Обеспечение требуемого уровня защищённости должно достигаться с использованием мер, методов и средств безопасности.

38. Все меры обеспечения безопасности информационных систем подразделяются на:

- законодательные (правовые);
- морально-этические;
- организационные (административные);
- физические;
- технические (аппаратно-программные).

39. К законодательным (правовым) мерам обеспечения безопасности информационных систем относятся действующие в Российской Федерации нормативные акты, регламентирующие правила обращения с персональными данными, закрепляющие права и обязанности участников информационных

отношений в процессе её обработки и использования, а также устанавливающие ответственность за нарушения этих правил, препятствуя тем самым неправомерному использованию персональных данных и являющиеся сдерживающим фактором для потенциальных нарушителей. Законодательные (правовые) меры защиты носят в основном упреждающий, профилактический характер и требуют постоянной разъяснительной работы с пользователями информационных систем.

40. К морально-этическим мерам обеспечения безопасности информационных систем относятся нормы поведения, которые традиционно сложились или складываются по мере распространения информационных технологий. Морально-этические меры защиты являются профилактическими и требуют постоянной работы по созданию здорового морального климата в Министерстве и снижают вероятность возникновения негативных действий, связанных с человеческим фактором.

41. Организационные (административные) меры обеспечения безопасности информационных систем – это меры организационного характера, регламентирующие процессы функционирования информационных систем, использование ресурсов информационных систем, деятельность обслуживающего персонала, а также порядок взаимодействия пользователей таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности или снизить размер потерь в случае их реализации.

42. Организационные меры обеспечения безопасности должны предусматривать регламент информационных отношений, исключающих возможность несанкционированных действий в отношении объектов защиты; определять коалиционные и иерархические принципы и методы разграничения доступа к персональным данным; определять порядок работы с программно-математическими и техническими (аппаратными) средствами защиты и криптозащиты и других защитных механизмов; организовать меры противодействия несанкционированного доступа на этапах аутентификации, авторизации, идентификации, обеспечивающих гарантии реализации прав и ответственности субъектов информационных отношений.

43. Организационные меры должны состоять из регламента доступа в контролируемую зону; порядка допуска сотрудников Министерства к использованию ресурсов информационных систем Министерства; инструкций (пользователя информационной системы, администратора информационной системы, администратора безопасности) и других документов, регламентирующих порядок функционирования информационных систем в Министерстве.

44. Физические меры обеспечения безопасности информационных систем основаны на применении разного рода механических, электро- или электронно-механических устройств и сооружений, специально предназначенных для создания физических препятствий на возможных путях проникновения и доступа потенциальных нарушителей к компонентам системы и защищаемой

информации, а также технических средств визуального наблюдения, связи и охранной сигнализации.

45. Физическая защита зданий, помещений, объектов и средств информатизации должна осуществляться путём установления соответствующих постов охраны, с помощью технических средств охраны или любыми другими способами, предотвращающими или существенно затрудняющими проникновение в здание, помещения посторонних лиц, хищение информационных носителей, самих средств информатизации, исключая нахождение внутри контролируемой (охраняемой) зоны технических средств разведки.

46. Технические (аппаратно-программные) меры обеспечения безопасности информационных систем основаны на использовании различных электронных устройств и специальных программ, входящих в состав информационных систем и выполняющих (самостоятельно или в комплексе с другими средствами) функции защиты (идентификацию и аутентификацию пользователей, разграничение доступа к ресурсам, регистрацию событий, криптографическое закрытие информации и т.д.).

47. В состав системы защиты персональных данных в Министерстве должны быть включены следующие средства:

защита от несанкционированного доступа;

идентификация (опознавания) и аутентификация (подтверждения подлинности) пользователей информационных систем;

разграничение доступа зарегистрированных пользователей системы к ресурсам информационных систем Министерства;

обеспечение и контроль целостности программных и информационных ресурсов;

оперативный контроль и регистрация событий безопасности;

защита от утечки информации по техническим каналам связи и по каналам побочных электромагнитных излучений и наводок;

криптографические и антивирусные средства защиты персональных данных;

программно-аппаратные средства защиты информации.

48. Успешное применение технических мер обеспечения безопасности информационных систем на основании основных принципов построения системы комплексной защиты информации предполагает, что выполнение перечисленных ниже требований обеспечено организационными (административными) мерами и используемыми физическими средствами защиты:

обеспечена физическая целостность всех компонентов информационных систем;

обеспечен учёт и хранение съёмных носителей информации и их обращение, исключая хищение, подмену и уничтожение;

обеспечено резервирование технических средств, дублирование носителей информации;

обеспечена электромагнитная развязка между линиями связи и другими цепями вспомогательных технических средств и систем, выходящими за пределы контролируемой зоны, и информационными цепями;

обеспечено использование антивирусных средств защиты от вредоносного программного обеспечения и криптографических средств защиты информации;

обеспечено использование средств защиты информации, позволяющих вести собственные журналы регистрации событий параллельно со встроенными в информационными системами;

обеспечено использование межсетевого экранирования как при использовании программных, так и при использовании аппаратных межсетевых экранов;

каждый пользователь информационных систем имеет уникальное системное имя и минимально необходимые для выполнения ими своих функциональных обязанностей полномочия по доступу к ресурсам информационной системы;

разработка и отладка программ осуществляется за пределами информационных систем на выделенных персональных компьютерах;

все изменения конфигурации технических и программных средств информационных систем производятся в строго установленном порядке (регистрируются и контролируются) только на основании распоряжений руководства Министерства;

сетевое оборудование (концентраторы, коммутаторы, маршрутизаторы и т.п.) располагается в местах, недоступных для посторонних (специальных помещениях, шкафах, и т.п.);

пользователями информационных систем осуществляется непрерывное управление и административная поддержка функционирования средств защиты.

### **VIII. Модель угроз безопасности персональных данных при их обработке в информационных системах Министерства**

49. Для информационных систем Министерства выделяются следующие основные категории угроз безопасности персональных данных:

угроза от утечки по техническим каналам;

угроза несанкционированного доступа к информации:

угроза уничтожения, хищения аппаратных средств информационных систем, носителей информации путём физического доступа к элементам информационных систем;

угроза хищения, несанкционированной модификации или блокирования информации путём несанкционированного доступа с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий);

угроза непреднамеренных действий пользователей и нарушений безопасности функционирования информационных систем и средств защиты персональных данных в её составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадёжности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера;

угроза преднамеренных действий внутренних нарушителей;

угроза несанкционированного доступа по каналам связи.

50. Модель нарушителя безопасности персональных данных при их обработке в информационных системах Министерства определяется общими положениями моделей угроз безопасности персональных данных при их обработке в информационных системах Министерства, утверждёнными приказом Министерства.

## **IX. Контроль эффективности системы защиты персональных данных в Министерстве**

51. Контроль эффективности системы защиты персональных данных должен осуществляться на периодической основе. В Министерстве целью контроля эффективности является своевременное выявление ненадлежащих режимов работы системы защиты персональных данных (отключение средств защиты, нарушение режимов защиты, несанкционированное изменение режима защиты и т.п.), а так же прогнозирование и превентивное реагирование на новые угрозы безопасности персональных данных.

52. Контроль эффективности системы защиты персональных данных может проводиться как администратором безопасности информационных систем Министерства, так и привлекаемыми для этой цели компетентными организациями, имеющими лицензию на этот вид деятельности, а также Федеральной службой по техническому и экспортному контролю Российской Федерации и Федеральной службой безопасности Российской Федерации в пределах их компетенции.

53. Контроль может осуществляться администратором безопасности информационных систем Министерства как с помощью штатных средств системы защиты персональных данных, так и с помощью специальных программных средств контроля.

54. Оценка эффективности системы защиты персональных данных проводится с использованием технических и программных средств контроля на предмет соответствия установленным требованиям.

## **X. Ответственность**

55. Ответственным за разработку мер защиты персональных данных и контроль за обеспечением безопасности персональных данных является министр социальной политики и труда Удмуртской Республики (далее – министр).

56. Министр может делегировать часть полномочий по обеспечению безопасности персональных данных одному из своих заместителей.

57. При взаимодействии со сторонними организациями в случаях, когда сотрудникам этих организаций предоставляется доступ к персональным данным, обрабатываемым в Министерстве, с этими организациями заключается соглашение о конфиденциальности либо соглашение о соблюдении режима безопасности персональных данных. Подготовка типовых вариантов указанных соглашений осуществляется управлением информационных ресурсов Министерства.

## **XI. Ожидаемый эффект от реализации настоящей Концепции**

58. Реализация настоящей Концепции позволит:

оценить состояние безопасности информации информационных систем Министерства, выявить источники внутренних и внешних угроз информационной безопасности, определить приоритетные направления предотвращения, отражения и нейтрализации этих угроз;

разработать организационно-распорядительные документы применительно к информационным системам Министерства;

провести классификацию информационных систем Министерства;

провести организационно-режимные и технические мероприятия по обеспечению безопасности персональных данных в Министерстве;

обеспечить необходимый уровень безопасности объектов защиты персональных данных в Министерстве.

59. Осуществление этих мероприятий обеспечит создание единой и целостной системы информационной безопасности информационных систем персональных данных и создаст условия для её дальнейшего совершенствования.

---

УТВЕРЖДЕНА  
приказом Министерства  
социальной политики и труда  
Удмуртской Республики  
от «29» 07 2019 года № 194

**ПОЛИТИКА**  
**информационной безопасности информационных систем**  
**Министерства социальной политики и труда Удмуртской Республики**

**I. Общие положения**

1. Настоящая Политика разработана в соответствии с целями, задачами и принципами обеспечения безопасности персональных данных, изложенными в Концепции информационной безопасности информационных систем Министерства социальной политики и труда Удмуртской Республики (далее -- Министерство).

2. Целью настоящей Политики является обеспечение безопасности объектов защиты персональных данных Министерства от всех видов угроз, внешних и внутренних, умышленных и непреднамеренных, минимизация ущерба от возможной реализации угроз безопасности персональных данных.

3. Безопасность персональных данных достигается путём исключения несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий.

4. В Министерстве обеспечивается осуществление своевременного обнаружения и реагирования на угрозы безопасности персональных данных, предотвращение преднамеренных или случайных, частичных или полных несанкционированных модификаций или уничтожения персональных данных.

5. Требования настоящей Политики распространяются на всех сотрудников Министерства (постоянных, временных), а также иных лиц (подрядчиков, исполнителей, аудиторов и т.п.).

**II. Система защиты персональных данных**

6. Система защиты персональных данных строится в Министерстве на основании:

законодательства Российской Федерации в области защиты персональных данных, руководящих документов Федеральной службы по техническому и экспортному контролю России и Федеральной службы безопасности России;

организационно-распорядительных документов Министерства в сфере защиты персональных данных (приложение к настоящей политике).

На основании указанных документов определяется необходимый уровень защищённости персональных данных каждой информационной системы Министерства.

7. На основании анализа актуальных угроз безопасности персональных данных, описанного в моделях угроз безопасности при их обработке в информационных системах Министерства и отчёте о результатах проведения внутренней проверки обеспечения защиты персональных данных в информационных системах Министерства, делается вывод о необходимости использования технических средств и организационных мероприятий для обеспечения безопасности персональных данных.

8. Для каждой информационной системы должен быть составлен список используемых технических средств защиты, а также программного обеспечения, участвующего в обработке персональных данных, на всех элементах информационных систем:

- персональные компьютеры пользователей;
- серверы приложений;
- система управления базами данных – СУБД;
- граница локальной вычислительной сети;
- каналы передачи в сети общего пользования и (или) международного обмена, если по ним передаются персональные данные.

9. В зависимости от уровня защищённости информационных систем и актуальных угроз система защиты персональных данных может включать в себя следующие технические средства:

- антивирусные средства для персональных компьютеров пользователей и серверов;
- средства межсетевого экранирования;
- средства криптографической защиты информации при передаче защищаемой информации по каналам связи.

Также в список должны быть включены функции защиты, обеспечиваемые штатными средствами обработки персональных данных операционной системы, прикладным программным обеспечением и специальными комплексами, реализующими средства защиты. Список функций защиты может включать в себя:

- управление и разграничение доступа пользователей;
- регистрацию и учёт действий с информацией;
- обеспечение целостности данных;
- осуществление обнаружения вторжений.

### **III. Требования к подсистемам системы защиты персональных данных**

10. Система защиты персональных данных включает в себя следующие подсистемы:

- управления доступом;
- регистрации и учёта;



обеспечения целостности и доступности;  
антивирусной защиты;  
межсетевого экранирования;  
анализа защищённости;  
обнаружения вторжений;  
криптографической защиты.

11. Подсистемы системы защиты персональных данных имеют различный функционал в зависимости от класса информационной системы, установленного в акте классификации информационной системы.

12. Подсистема управления доступом предназначена для реализации следующих функций:

идентификация и проверка подлинности субъектов доступа при входе в информационную систему;

идентификация терминалов, узлов сети, каналов связи, внешних устройств по логическим именам;

идентификация программ, томов, каталогов, файлов, записей, полей записей по именам.

Подсистема управления доступом может быть реализована с помощью штатных средств обработки персональных данных (операционных систем, приложений и СУБД). Также может быть внедрено специальное техническое средство или их комплекс, осуществляющие дополнительные меры по аутентификации и контролю.

13. Подсистема регистрации и учёта предназначена для реализации следующих функций:

регистрация входа (выхода) субъектов доступа в систему (из системы) либо регистрация загрузки и инициализации операционной системы и её остановка;

регистрация попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам;

регистрация попыток доступа программных средств к терминалам, каналам связи, программам, томам, каталогам, файлам, записям, полям записей.

Подсистема регистрации и учёта может быть реализована с помощью организационных мер защиты информации. Также может быть внедрено специальное техническое средство или их комплекс, осуществляющие дополнительные меры по регистрации действий, осуществляемых в информационной системе.

14. Подсистема обеспечения целостности и доступности предназначена для обеспечения целостности и доступности персональных данных, программных и аппаратных средств информационных систем, а также средств защиты при случайной или намеренной модификации.

Подсистема реализуется с помощью организации резервного копирования обрабатываемых данных, а так же резервированием ключевых элементов информационных систем.

15. Подсистема антивирусной защиты предназначена для обеспечения антивирусной защиты персональных компьютеров пользователей и серверов.

Средства антивирусной защиты предназначены для реализации следующих функций:

резидентный антивирусный мониторинг;

антивирусное сканирование;

скрипт-блокирование;

централизованная /удалённая установка/ деинсталляция антивирусного продукта, настройка, администрирование, просмотр отчётов и статистической информации по работе продукта;

автоматизированное обновление антивирусных баз;

ограничение прав пользователя на остановку исполняемых задач и изменения настроек антивирусного программного обеспечения;

автоматический запуск сразу после загрузки операционной системы.

Подсистема реализуется путём внедрения специального антивирусного программного обеспечения на все элементы информационных систем.

16. Подсистема межсетевого экранирования предназначена для реализации следующих функций:

1) фильтрация открытого и зашифрованного (закрытого) IP-трафика по следующим параметрам:

фиксация во внутренних журналах информации о проходящем открытом и закрытом IP-трафике;

идентификация и аутентификации администратора межсетевого экрана при его локальных запросах на доступ;

регистрация входа (выхода) администратора межсетевого экрана в систему (из системы) либо загрузки и инициализации системы и её программного останова;

контроль целостности своей программной и информационной части;

2) фильтрация пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств;

3) фильтрация с учётом входного и выходного сетевого интерфейса как средство проверки подлинности сетевых адресов;

4) регистрация и учёт запрашиваемых сервисов прикладного уровня;

5) блокирование доступа неидентифицированного объекта или субъекта, подлинность которого при аутентификации не подтвердилась, методами, устойчивыми к перехвату;

6) контроль за сетевой активностью приложений и обнаружения сетевых атак.

Подсистема реализуется внедрением программно-аппаратных комплексов межсетевого экранирования на границе локальной вычислительной сети классом не ниже 4.

17. Подсистема анализа защищённости должна обеспечивать выявления уязвимостей, связанных с ошибками в конфигурации программного обеспечения информационных систем, которые могут быть использованы нарушителем для реализации атаки на систему.

Функционал подсистемы может быть реализован программными и программно-аппаратными средствами.

18. Подсистема обнаружения вторжений должна обеспечивать выявление сетевых атак на элементы информационных систем, подключённые к сетям общего пользования и (или) международного обмена.

Функционал подсистемы может быть реализован программными и программно-аппаратными средствами.

19. Подсистема криптографической защиты предназначена для исключения несанкционированного доступа к защищаемой информации при её передаче по каналам связи сетей общего пользования и (или) международного обмена.

Подсистема реализуется путём внедрения криптографических программно-аппаратных комплексов.

#### **IV. Категории пользователей информационных систем Министерства**

20. В Концепции информационной безопасности информационных систем Министерства социальной политики и труда Удмуртской Республики определены основные категории пользователей информационных систем Министерства.

21. Для определения требований к пользователям информационных систем, степени ответственности, уровня защищённости, должностным обязанностям сотрудников, ответственных за обеспечение безопасности персональных данных выделяются следующие группы пользователей информационных систем Министерства, участвующих в обработке и хранении персональных данных:

1) администратор информационной системы Министерства:

администратор информационной системы;

администратор безопасности информационной системы;

администратор сети;

2) пользователь информационной системы Министерства:

пользователь информационной системы;

технический специалист по обслуживанию периферийного оборудования;

3) программист-разработчик информационной системы Министерства:

программист-разработчик информационной системы.

22. Данные о группах пользователей, уровне их доступа и информированности отражаются в Положении о разграничении прав доступа к обрабатываемым персональным данным в информационных системах Министерства.

#### **V. Администратор информационных систем Министерства**

23. Администратором информационной системы Министерства является специалист Министерства, который выполняет функции настройки, внедрения и сопровождения информационной системы Министерства.

24. Администратор информационной системы Министерства обеспечивает функционирование подсистемы управления доступом информационных систем Министерства и уполномочен осуществлять предоставление и разграничение доступа пользователей к элементам информационных систем, хранящим персональные данные.

25. Администратор информационной системы Министерства обладает следующим уровнем доступа:

обладает полной информацией о системном и прикладном программном обеспечении информационной системы Министерства;

обладает полной информацией о технических средствах и конфигурации информационной системы Министерства;

имеет доступ ко всем техническим средствам обработки информации и данным информационной системы Министерства;

обладает правами конфигурирования и административной настройки технических средств информационной системы Министерства.

26. Администратором безопасности является специалист Министерства, уполномоченный на проведение работ по реализации технических мер защиты персональных данных и поддержания достигнутого уровня защиты информационных систем персональных данных, ответственный за функционирование системы защиты персональных данных, включая обслуживание и настройку административного, серверного и клиентского компонентов на этапах промышленной эксплуатации и модернизации.

27. Администратор безопасности обладает следующим уровнем доступа и знаний:

обладает правами администратора информационной системы Министерства;

обладает полной информацией об информационной системе Министерства;

имеет доступ к средствам защиты информации и протоколирования и к части ключевых элементов информационной системы Министерства;

не имеет прав доступа к конфигурированию технических средств сети, за исключением контрольных (инспекционных).

28. Администратор безопасности уполномочен:

реализовывать политику безопасности в части настройки средств криптографической защиты информации, межсетевых экранов и систем обнаружения атак, в соответствии с которыми пользователь информационной системы получает возможность работать с элементами информационной системы;

осуществлять аудит средств защиты;

устанавливать доверительные отношения своей защищённой сети с сетями других учреждений.

29. Администратором сети является специалист Министерства, ответственный за функционирование телекоммуникационной подсистемы информационной системы. Администратор сети не имеет полномочий для управления подсистемами обработки данных и безопасности.

30. Администратор сети обладает следующим уровнем доступа и знаний:  
обладает частью информации о системном и прикладном программном обеспечении информационной системы Министерства;

обладает частью информации о технических средствах и конфигурации информационной системы Министерства;

имеет физический доступ к техническим средствам обработки информации и средствам защиты;

знает, по меньшей мере, одно легальное имя доступа.

## **VI. Пользователь информационных систем Министерства**

31. Пользователем информационной системы Министерства является специалист Министерства, участвующий в процессе эксплуатации информационной системы Министерства и осуществляющий обработку персональных данных.

32. Пользователь информационной системы Министерства обладает следующим уровнем доступа:

обладает всеми необходимыми атрибутами (например, паролем), обеспечивающими доступ к некоторому подмножеству персональных данных;  
располагает конфиденциальными данными, к которым имеет доступ.

33. Техническим специалистом по обслуживанию периферийного оборудования является специалист Министерства, осуществляющий обслуживание и настройку периферийного оборудования информационных систем Министерства.

34. Технический специалист по обслуживанию периферийного оборудования не имеет полномочий для управления подсистемами обработки данных и безопасности.

35. Технический специалист по обслуживанию периферийного оборудования обладает следующим уровнем доступа и знаний:

обладает частью информации о системном и прикладном программном обеспечении информационных систем Министерства;

обладает частью информации о технических средствах и конфигурации информационных систем Министерства;

знает, по меньшей мере, одно легальное имя доступа.

## **VII. Программист-разработчик информационной системы Министерства**

36. Программист-разработчик информационной системы Министерства – специалист, осуществляющий разработку прикладного программного обеспечения, обеспечивающий его сопровождение на защищаемом объекте. К

данной группе могут относиться как специалисты Министерства, так и сотрудники сторонних организаций.

37. Программист-разработчик информационной системы Министерства обладает следующим уровнем доступа:

обладает информацией об алгоритмах и программах обработки информации на информационной системе Министерства;

обладает возможностями внесения ошибок, недеklarированных возможностей, программных закладок, вредоносных программ в программное обеспечение информационной системы на стадии её разработки, внедрения и сопровождения;

может располагать любыми фрагментами информации о топологии информационной системы Министерства и технических средствах обработки и защиты персональных данных.

### **VIII. Требования к пользователям информационных систем Министерства по обеспечению защиты персональных данных**

38. Все пользователи информационных систем Министерства должны чётко знать и строго выполнять установленные правила и обязанности по доступу к защищаемым объектам и соблюдению принятого режима безопасности персональных данных.

39. Сотрудник Министерства при назначении на должность должен быть ознакомлен с настоящей Политикой и документами, регламентирующими требования по защите персональных данных в Министерстве, а также обучен навыкам выполнения процедур, необходимых для санкционированного использования информационных систем Министерства.

40. Пользователи информационных систем Министерства, использующие технические средства аутентификации, должны:

обеспечивать сохранность идентификаторов (электронных ключей);

не допускать несанкционированный доступ к ним;

исключить возможность их утери или использования третьими лицами.

Пользователи информационных систем Министерства несут персональную ответственность за сохранность идентификаторов.

41. Пользователи информационных систем Министерства не использующие технические средства аутентификации должны:

следовать установленным процедурам поддержания режима безопасности персональных данных при выборе и использовании паролей;

не допускать несанкционированный доступ сторонних лиц к паролям.

42. Все пользователи информационных систем Министерства должны: обеспечивать надлежащую защиту оборудования, оставляемого без присмотра, особенно в тех случаях, когда в помещение имеют доступ посторонние лица;

знать требования по безопасности персональных данных и процедуры защиты оборудования, оставленного без присмотра, а также свои обязанности по обеспечению такой защиты.

43. Пользователям информационных систем Министерства запрещается: устанавливать постороннее программное обеспечение; подключать личные мобильные устройства и носители информации, а также записывать на них защищаемую информацию; разглашать защищаемую информацию третьим лицам.

44. При работе с персональными данными пользователи информационных систем Министерства обязаны обеспечить отсутствие возможности просмотра персональных данных третьими лицами с мониторов персональных компьютеров или терминалов.

При завершении работы в информационной системе пользователи информационных систем Министерства обязаны защитить персональный компьютер или терминал с помощью блокировки ключом или эквивалентного средства контроля, например, доступом по паролю, если не используются более сильные средства защиты.

45. Пользователи информационных систем Министерства должны быть проинформированы об угрозах нарушения режима безопасности персональных данных и ответственности за его нарушение.

46. Пользователи информационных систем Министерства обязаны без промедления сообщать обо всех наблюдаемых или подозрительных случаях работы информационных систем, которые могут повлечь за собой угрозы безопасности персональных данных, а также о выявленных ими событиях, затрагивающих безопасность персональных данных, руководителю подразделения и лицу, отвечающему за немедленное реагирование на угрозы безопасности персональных данных.

## **IX. Ответственность**

47. Пользователи информационных систем Министерства, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных, несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

---

Приложение  
к Политике информационной  
безопасности информационных  
систем Министерства социальной  
политики и труда Удмуртской  
Республики

**ПЕРЕЧЕНЬ**  
**организационно-распорядительных документов Министерства**  
**социальной политики и труда Удмуртской Республики в сфере защиты**  
**персональных данных**

В Министерстве социальной политики и труда Удмуртской Республики (далее – Министерство) принимаются следующие виды организационно-распорядительных документов в сфере защиты персональных данных, обрабатываемых в информационных системах Министерства:

- 1) Акт классификации информационных систем Министерства;
- 2) Должностная инструкция ответственного за обеспечение безопасности персональных данных в информационных системах Министерства;
- 3) Должностная инструкция ответственного за организацию обработки персональных данных в Министерстве;
- 4) Инструкция администратора безопасности информационных систем Министерства;
- 5) Инструкция администратора информационных систем Министерства;
- 6) Инструкция о порядке допуска сотрудников Министерства к самостоятельной работе со средствами криптографической защиты информации;
- 7) Инструкция о порядке учёта, хранения и уничтожения электронных носителей персональных данных в Министерстве;
- 8) Инструкция по обеспечению безопасности эксплуатации шифровальных (криптографических) средств в информационных системах Министерства;
- 9) Инструкция по организации антивирусной защиты информационных систем Министерства;
- 10) Инструкция по организации парольной защиты в информационных системах Министерства;
- 11) Инструкция пользователя информационных систем Министерства;
- 12) Инструкция пользователя информационных систем по обеспечению безопасности обработки персональных данных при возникновении внештатных ситуаций в Министерстве;



- 13) Концепция информационной безопасности информационных систем Министерства;
- 14) Модель нарушителя в информационных системах Министерства;
- 15) Модель угроз безопасности персональных данных при их обработке в информационных системах Министерства;
- 16) Описание технологического процесса обработки информации в Государственной информационной системе Удмуртской Республики;
- 17) Отчёт о результатах проведения внутренней проверки обеспечения защиты персональных данных в информационных системах Удмуртской Республики;
- 18) Перечень абонентских пунктов защищённой сети передачи данных Министерства;
- 19) Перечень должностных лиц и должностей государственной гражданской службы Удмуртской Республики в Министерстве, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным;
- 20) Перечень должностей государственной гражданской службы Удмуртской Республики в Министерстве, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных;
- 21) Перечень информационных систем Министерства;
- 22) Перечень мер защиты информации информационных систем персональных данных Министерства;
- 23) Перечень персональных данных, обрабатываемых в Министерстве;
- 24) Перечень персональных данных и иных объектов, подлежащих защите в информационных системах Министерства;
- 25) Перечень регистрируемых событий безопасности в Государственной информационной системе Удмуртской Республики;
- 26) Перечень средств защиты информации информационных систем Министерства;
- 27) План мероприятий по обеспечению защиты персональных данных в информационных системах Министерства;
- 28) Политика информационной безопасности информационных систем Министерства;
- 29) Положение об обработке персональных данных в Министерстве;
- 30) Порядок доступа сотрудников Министерства в помещения, в которых ведётся обработка персональных данных;
- 31) Порядок резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации в информационных системах Министерства;
- 32) Правила обработки персональных данных в Министерстве;
- 33) Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным Федеральным законом «О персональных данных», в Министерстве;

- 34) Правила работы с обезличенными персональными данными в Министерстве;
  - 35) Правила рассмотрения запросов субъектов персональных данных или их представителей в Министерстве;
  - 36) Приказ о вводе в эксплуатацию информационных систем Министерства;
  - 37) Приказ о Технической комиссии по защите информации;
  - 38) Приказ о назначении ответственного за обеспечение безопасности персональных данных в информационных системах в Министерстве;
  - 39) Приказ о назначении ответственного за организацию обработки персональных данных в Министерстве;
  - 40) Приказ об установлении границ контролируемой зоны в Министерстве и определения лиц, имеющих доступ в контролируемую зону Министерства;
  - 41) Разграничение прав доступа к обрабатываемым персональным данным в информационных системах Министерства;
  - 42) Регламент защищённой сети передачи данных Министерства;
  - 43) Список лиц, наделённых правом использования электронной подписи;
  - 44) Список лиц, являющихся уполномоченными пользователями защищённой сети передачи данных Министерства;
  - 45) Список ответственных лиц, допущенных к работе со средствами криптографической защиты информации в Министерстве;
  - 46) Технический паспорт государственной информационной системы Министерства.
-