Приложение №1
к приказу директора МБУ
Мошковского района
Новосибирской области КЦСОН
от 25.03.2019 г. № 58 - о

КОНЦЕПЦИЯ
информационной безопасности информационных систем Муниципального бюджетного учреждения Мошковского района Новосибирской области «Комплексный центр социального обслуживания населения»

1. Общие положения

1.1. Настоящая Концепция определяет основные цели и задачи, а также общую стратегию построения системы защиты персональных данных, используемых в информационных системах Муниципального бюджетного учреждения Мошковского района Новосибирской области «Комплексный центр социального обслуживания населения» (далее - Учреждение).

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

1.3. 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.

1.4. 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.

2. Построение системы защиты персональных данных в Учреждении

2.1. 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.

2.2. 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.

2.3. 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).

2.4. Технические средства защиты информации реализуются при помощи соответствующих программно-технических средств и методов защиты.

3. Задачи системы защиты персональных данных в Учреждении

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

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

1) защиту от вмешательства в процесс функционирования информационных систем Учреждения посторонних лиц (возможность использования информационных систем Управления 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 Учреждения (возможность доступа только к тем ресурсам и выполнения только тех операций с ними, которые необходимы конкретным пользователям информационных систем Учреждения для выполнения своих должностных обязанностей), то есть защиту от несанкционированного доступа:

к информации, циркулирующей в информационных системах Учреждения;

средствам вычислительной техники информационных систем Учреждения;

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

3) регистрацию действий пользователей при использовании защищаемых ресурсов информационных систем Учреждения 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) защиту от несанкционированной модификации и контроль целостности используемых в информационных системах Учреждения программных средств, а также защиту системы от внедрения несанкционированных программ;

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

7) защиту 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 ликвидация последствий нарушения безопасности персональных данных.

4. Объекты защиты персональных данных в Учреждении

4.1. Объектами защиты персональных данных в Учреждении являются информация, обрабатываемая в информационных системах Учреждения, и технические средства еѐ обработки и защиты.

4.2. Объекты защиты персональных данных в Учреждении включают в себя:

обрабатываемую информацию;

технологическую информацию;

программно-технические средства обработки;

каналы информационного обмена;

помещения, в которых размещены компоненты информационных систем Учреждения.

5. Классификация пользователей информационных систем Учреждения

5.1. Пользователем информационных систем Учреждения является лицо, участвующее в функционировании информационной системы Учреждения или использующее результаты еѐ функционирования.

5.2. Пользователем информационных систем Учреждения является любой сотрудник Учреждения, имеющий доступ к информационной системе персональных данных и ее ресурсам в соответствии с установленным порядком, в соответствии с его функциональными обязанностями.

6. Основные принципы построения системы защиты персональных данных в Учреждении

6.1. Построение системы защиты персональных данных в Учреждении 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.

6.2. Принцип законности предполагает осуществление защитных мероприятий и разработку системы защиты персональных данных в Учреждении в соответствии с требованиями законодательства в области защиты персональных данных.

6.3. Системный подход к построению системы защиты персональных данных в Учреждении 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 Учреждении 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 распределѐнные системы и несанкционированный доступ к информации.

6.4. 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 еѐ компонентов.

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

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

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

6.7. 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 учѐтом изменений в методах и средствах перехвата информации, нормативных требований по защите, достигнутого отечественного и зарубежного опыта в этой области.

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

6.9. Принцип минимизации полномочий означает предоставление пользователям минимальных прав доступа в соответствии с производственной необходимостью.

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

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

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

6.12. Принцип открытости алгоритмов и механизмов состоит в том, что защита не должна обеспечиваться только за счёт секретности структурной организации и алгоритмов функционирования её подсистем.

6.13. 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 трудозатрат 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.).

6.14. 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.

6.15. 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 наиболее подготовленными и опытными сотрудниками Учреждения.

6.16. 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.

7. Меры и средства обеспечения требуемого уровня защищённости информационных систем Учреждения

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

7.2. Все меры обеспечения безопасности информационных систем подразделяются на:

законодательные (правовые);

морально-этические;

организационные (административные);

физические;

технические (аппаратно-программные).

7.3. 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.

7.4. 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 Учреждении и снижают вероятность возникновения негативных действий, связанных с человеческим фактором.

7.5. 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.

7.6. 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.

7.7. 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.).

В состав системы защиты персональных данных в Учреждении должны быть включены следующие средства:

средства защиты от несанкционированного доступа;

средства идентификации (опознавания) и аутентификации (подтверждения подлинности) пользователей информационных систем;

средства разграничения доступа зарегистрированных пользователей системы к ресурсам информационных систем Учреждения;

средства обеспечения и контроля целостности программных и информационных ресурсов;

средства оперативного контроля и регистрации событий безопасности;

средства защиты 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.

8. Модель угроз безопасности персональных данных при их обработке в информационных системах Учреждения

8.1. Для информационных систем Учреждения выделяются следующие основные категории угроз безопасности персональных данных:

угрозы от утечки по техническим каналам;

угрозы несанкционированного доступа к информации:

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

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

угрозы 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 ненадѐжности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера;

угрозы преднамеренных действий внутренних нарушителей;

угрозы несанкционированного доступа по каналам связи.

8.2. Модель нарушителя безопасности персональных данных при их обработке в информационных системах Учреждения определяется общими положениями моделей угроз безопасности персональных данных при их обработке в информационных системах, утверждѐнными приказом Учреждения.

9. Ответственность

9.1. Ответственным за разработку мер защиты персональных данных и контроль за обеспечением безопасности персональных данных является директор Учреждения.

9.2. Директор Учреждения может делегировать часть полномочий по обеспечению безопасности персональных данных одному из своих заместителей.

9.3. При взаимодействии со сторонними организациями в случаях, когда сотрудникам этих организаций предоставляется доступ к персональным данным, обрабатываемым в Учреждении, с этими организациями заключается соглашение о конфиденциальности либо соглашение о соблюдении режима безопасности персональных данных.

10. Ожидаемый эффект от реализации настоящей Концепции

10.1 Реализация настоящей Концепции позволит:

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

разработать организационно-распорядительные документы применительно к информационных системам Учреждения;

провести классификацию информационных систем Учреждения;

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

обеспечить необходимый уровень безопасности объектов защиты персональных данных в Учреждении.

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