УТВЕРЖДАЮ
Генеральный директор
БУ РК «Аэропорт «Петрозаводск»
_____ М.В. Степанов
«30» января 2015г.

КОНЦЕПЦИЯ
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
БУ РК «Аэропорт «Петрозаводск»

д. Бесовец 2015

1. Общие положения

Настоящая Концепция определяет основные цели и задачи, а также общую стратегию построения системы информационной безопасности БУ РК «Аэропорт «Петрозаводск». Концепция определяет основные требования и базовые подходы к их реализации, для достижения требуемого уровня безопасности информации.

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 информации с позиции комплексного применения технических и организационных мер и средств защиты.

Под информационной безопасностью понимается защищенность информации и обрабатывающей её инфраструктуры от любых случайных или злонамеренных воздействий, результатом которых может явиться нанесение ущерба самой информации, ее владельцам или инфраструктуре. Задачи информационной безопасности сводятся к минимизации ущерба от возможной реализации угроз безопасности информации, а также к прогнозированию и предотвращению таких воздействий.

Концепция является методологической основой для:

- формирования и проведения единой политики в области обеспечения информационной безопасности в БУ РК «Аэропорт «Петрозаводск»;
- принятия управленческих решений и разработки практических мер по внедрению политики информационной безопасности и выработки комплекса согласованных мер нормативно-правового, организационного и технического характера, направленных на выявление, отражение и ликвидацию последствий реализации различных видов угроз информационной безопасности;
- координации деятельности работников и структурных подразделений БУ РК «Аэропорт «Петрозаводск» при эксплуатации информационных систем с соблюдением требований обеспечения безопасности информации;
- разработки предложений по совершенствованию правового, нормативного, методического, организационного и технического обеспечения безопасности информации.

Правовой базой для разработки настоящей Концепции служат требования действующего законодательства РФ и других подзаконных и нормативных документов в области обеспечения безопасности конфиденциальной информации.

Система защиты информации представляет собой совокупность организационных и технических мероприятий для защиты информации от неправомерного или случайного доступа, уничтожения, изменения, блокирования, копирования, распространения, а также иных неправомерных действий.

Безопасность информации достигается путем исключения несанкционированного, в том числе случайного, доступа к ней, результатом которого может стать уничтожение, изменение, блокирование, копирование, распростра-

нение конфиденциальной информации, а также иных несанкционированных действий.

Система защиты информации включает организационные меры и технические средства защиты информации, а также используемые в информационной системе информационные технологии.

Эти меры призваны обеспечить:

- конфиденциальность информации (защиту от несанкционированного ознакомления);
- целостность информации (актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения);
- доступность информации (возможность за приемлемое время получить требуемую информацию).

Организационные меры предусматривают разработку, внедрение и поддержание в актуальном состоянии документов, определяющих политику в отношении обработки конфиденциальной информации, локальных актов по вопросам обработки и защиты информации, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений.

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

2. Задачи системы защиты информации

Основной целью системы защиты информации является минимизация ущерба от возможной реализации угроз безопасности информации.

Для достижения основной цели система защиты информации должна обеспечивать эффективное решение следующих задач:

- защиту от вмешательства в процесс функционирования информационной системы посторонних лиц;
- разграничение доступа зарегистрированных пользователей к программным и аппаратным ресурсам информационной системы, защиту от несанкционированного доступа;
- регистрацию действий пользователей при использовании защищаемых ресурсов информационной системы в системных журналах;
- контроль целостности (обеспечение неизменности) среды исполнения программ;
- защиту информации от утечки по техническим каналам при ее обработке;
- своевременное выявление источников угроз безопасности информации;
- создание условий для минимизации и локализации наносимого ущерба неправомерными действиями физических и юридических лиц, ослабление негативного влияния и ликвидация последствий нарушения безопасности информации.

3. Объекты защиты

Объектами защиты является конфиденциальная информация БУ РК «Аэропорт «Петрозаводск», в том числе персональные данные, технические и программные средства обработки, системы и средства защиты информации, каналы информационного обмена и телекоммуникации, а также объекты и помещения, в которых размещены компоненты информационных систем.

4. Принципы построения системы защиты информации

4.1. Законность

Предполагает осуществление защитных мероприятий и разработку системы защиты информации в соответствии с действующим законодательством РФ и других нормативных актов по безопасности информации, утвержденных органами государственной власти и управления в пределах их компетенции.

Пользователи и обслуживающий персонал должны быть осведомлены о порядке работы с защищаемой информацией и об ответственности за защиту информации.

4.2. Системность

Системный подход к построению системы защиты информации предполагает учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, значимых для решения проблемы обеспечения информационной безопасности.

При создании системы защиты должны учитываться все слабые и уязвимые места системы обработки конфиденциальной информации, а также характер, возможные объекты и направления атак на систему со стороны потенциальных нарушителей (особенно высококвалифицированных злоумышленников), пути проникновения в распределенные системы и несанкционированного доступа к информации. Система защиты должна строиться с учетом не только всех известных каналов утечки информации, но и с учетом возможности появления принципиально новых путей реализации угроз безопасности информации.

4.3. Совместимость

Комплексное использование методов и средств защиты предполагает согласованное применение разнородных средств при построении целостной системы защиты, перекрывающей все значимые каналы реализации угроз и не содержащей слабых мест на стыках отдельных ее компонентов.

4.4. Непрерывность защиты информации

Защита информации является непрерывным целенаправленным процессом, предполагающим принятие соответствующих мер на всех этапах жизненного цикла информационной системы.

Информационные системы должны находиться в защищенном состоянии на протяжении всего времени их функционирования. В соответствии с

этим принципом должны приниматься меры по недопущению перехода информационных систем в незащищенное состояние.

4.5. Своевременность

Своевременность предполагает превентивный (упреждающий) характер мер защиты информации, то есть постановку задач по комплексной защите информационных систем и реализацию мер обеспечения безопасности информации на ранних стадиях разработки системы защиты информации.

4.6. Преемственность и совершенствование

Постоянное совершенствование мер и средств защиты информации должно осуществляться на основе преемственности организационных и технических решений, кадрового состава, анализа функционирования информационной системы и системы защиты информации с учетом изменений в возможных методах и средствах реализации угроз безопасности информации, требований законодательства и нормативных документов, достигнутого отечественного и зарубежного опыта в области защиты информации.

4.7. Персональная ответственность

Ответственность за обеспечение безопасности конфиденциальной информации должна быть возложена на каждого ответственного сотрудника в пределах его полномочий. В соответствии с этим принципом распределение прав и обязанностей сотрудников строится таким образом, чтобы в случае любого нарушения круг виновных лиц был четко известен или сведен к минимуму.

4.8. Принцип минимизации полномочий

Предоставление сотрудникам минимально необходимых для исполнения служебных обязанностей прав доступа к ресурсам защищенных информационных систем.

4.9. Взаимодействие и сотрудничество

Создание благоприятной атмосферы в коллективах подразделений для снижения вероятности возникновения негативных воздействий связанных с человеческим фактором. Сотрудники должны осознанно соблюдать установленные правила и оказывать содействие в работе подразделений и сотрудников, ответственных за защиту информации.

4.10.Гибкость системы защиты

Принятые меры и установленные средства защиты, особенно в начальный период их эксплуатации, могут обеспечивать как чрезмерный, так и недостаточный уровень защиты. Для обеспечения возможности варьирования уровня защищенности, средства защиты должны обладать определенной гибкостью. Особенно важным это свойство является в тех случаях, когда установку средств защиты необходимо осуществлять на работающую систему, не нарушая процесса ее нормального функционирования.

4.11.Простота применения средств защиты

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 пользователей.

Должна быть предусмотрена максимальная автоматизация действий пользователей и администраторов информационной системы.

4.12.Научная обоснованность и техническая реализуемость

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 информации.

4.13.Специализация и профессионализм

Привлечение к разработке средств и реализации мер защиты информации специализированных организаций, наиболее подготовленных к конкретному виду деятельности по обеспечению безопасности информации, имеющих опыт практической работы и разрешение (лицензию) на право оказания услуг в области технической защиты конфиденциальной информации. Реализация организационных и технических мер, эксплуатация средств защиты должна осуществляться профессионально подготовленными специалистами.

4.14.Обязательность контроля

Обязательность и своевременность выявления и пресечения попыток нарушения установленных правил обеспечения безопасности информации 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 должен осуществляться на основе применения средств оперативного контроля и регистрации и должен охватывать как несанкционированные, так и санкционированные действия пользователей.

5. Меры, методы и средства обеспечения требуемого уровня защиты

Обеспечение требуемого уровня защиты информации должно достигаться применением необходимого и достаточного комплекса мер. Меры обеспечения безопасности информации подразделяются на:

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

5.1. Правовые меры защиты

К правовым мерам защиты относятся действующие законы, подзаконные акты, нормативные и руководящие документы, регламентирующие правила обработки и защиты конфиденциальной информации, 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 информации и являющиеся сдерживающим фактором для потенциальных нарушителей.

Правовые меры защиты носят в основном упреждающий, профилактический характер и требуют постоянной разъяснительной работы с пользователями и обслуживающим персоналом системы.

5.2. Морально-этические меры защиты

К морально-этическим мерам относятся нормы поведения, которые традиционно сложились или складываются в обществе. Эти нормы большей частью не являются обязательными, как законодательно утвержденные нормативные акты, тем не менее, их несоблюдение ведет обычно к падению авторитета, престижа человека, группы лиц или организации. Морально-этические нормы бывают как неписаные (например, общепризнанные нормы честности, патриотизма и т.п.), так и писаные, то есть оформленные в некий свод (устав) правил или предписаний.

Морально-этические меры защиты являются профилактическими и требуют постоянной работы по созданию здорового морального климата в коллективе. Морально-этические меры защиты снижают вероятность возникновения негативных действий, связанных с человеческим фактором.

5.3. Организационные меры защиты

Организационные (административные) меры защиты – это меры организационного характера, регламентирующие процессы функционирования информационной системы и использование её ресурсов, деятельность обслуживающего персонала, а также порядок взаимодействия пользователей с информационной системой таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности информации или снизить размер ущерба в случае их реализации.

Основной целью административных мер, предпринимаемых на высшем управленческом уровне, является формирование политики информационной безопасности и обеспечение её выполнения путем выделения необходимых ресурсов и контроля.

Политика верхнего уровня должна четко сформировать область влияния и ограничения при определении целей обеспечения безопасности информации, определить какими ресурсами (техническими, организационными) они будут достигнуты и найти разумный компромисс между приемлемым уровнем безопасности и функциональностью системы.

На организационном уровне определяются процедуры и правила достижения целей и решения задач информационной безопасности, в частности:

- область применения политики информационной безопасности;
- роли и обязанности должностных лиц, отвечающих за реализацию политики информационной безопасности;
- права доступа к конфиденциальной информации;
- меры и средства обеспечения безопасности информации;
- меры и средства контроля соблюдения введенного режима безопасности.

Организационные меры:

- регламентируют информационные отношения, исключающие возможность несанкционированных действий в отношении объектов защиты;
- определяют принципы и методы разграничения доступа к информации;
- определяют порядок работы с программными, программно-аппаратными и техническими средствами защиты;
- определяют меры противодействия реализации несанкционированного доступа, обеспечивающие права и обязанности субъектов информационных отношений.

Организационные меры регламентируют следующие процедуры:

- режим безопасности и доступ в помещения информационных систем;
- допуск сотрудников к использованию ресурсов защищенных информационных систем;
- ведение баз данных, обработка конфиденциальной информации, осуществление ее модификации, уничтожения и иных действий;
- обслуживание и усовершенствование аппаратных и программных ресурсов информационной системы, а также системы защиты информации;
- действия при возникновении внештатных ситуаций;
- контроль исполнения законодательства, нормативных актов и локальных документов.

5.4. Физические меры защиты

Физические меры защиты основаны на применении различных механических или электронно-механических устройств и сооружений, специально предназначенных для создания физических препятствий на пути проникновения потенциального нарушителя к компонентам системы и защищаемой информации, а также средств видеонаблюдения, связи и охранной сигнализации.

Физическая защита зданий, помещений, объектов и средств информатизации должна осуществляться путем 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, средств информатизации.

5.5. Технические меры защиты

Технические (аппаратно-программные) меры защиты 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 и т.д.).

С учетом требований и принципов обеспечения безопасности информации по всем направлениям защиты в состав системы защиты включаются следующие средства:

- средства идентификации (опознавания) и аутентификации (подтверждения подлинности) пользователей информационной системы;
- средства разграничения доступа зарегистрированных пользователей к ресурсам информационной системы;
- средства обеспечения и контроля целостности программных и информационных ресурсов;
- средства оперативного контроля и регистрации событий безопасности.

Успешное применение технических средств защиты предполагает, что выполнение перечисленных ниже требований обеспечено организационными (административными) мерами и используемыми физическими средствами защиты:

- обеспечена физическая целостность всех компонент информационной системы;
- каждый пользователь (группа пользователей) имеет уникальное системное имя и минимально необходимые для выполнения им своих функциональных обязанностей полномочия по доступу к ресурсам системы;
- разработка и отладка программ, используемых в информационной системе, осуществляется за пределами информационной системы с целью избегания временного открытия каналов утечки информации;
- все изменения конфигурации технических и программных средств информационной системы производятся в строго установленном порядке (регистрируются и контролируются) на основании распоряжений руководства;
- сетевое оборудование располагается в местах, недоступных для посторонних (специальных помещениях, шкафах, и т.п.).
- осуществляется непрерывное управление и администрирование средств защиты информации.

6. Контроль эффективности

Контроль эффективности системы защиты информации должен осуществляется на периодической основе. Целью контроля эффективности является своевременное выявление ненадлежащих режимов работы системы защиты информации (отключение средств защиты, нарушение режимов защиты, несанкционированное изменение режима защиты и т.п.), а также прогнозирование и превентивное реагирование на новые угрозы безопасности информации.

Контроль может проводиться администраторами безопасности (оперативный контроль в процессе информационного взаимодействия) или привлекаемыми для этой цели компетентными организациями. Контроль может осуществляться при помощи штатных средств системы защиты информации или при помощи специальных программных средств контроля.

Оценка соответствия требованиям по безопасности информации проводится организациями, имеющими лицензию на техническую защиту конфиденциальной информации, с использованием технических и программных средств контроля не реже чем 1 раз в 3 года.

7. Сферы ответственности

Ответственным за разработку мер и контроль обеспечения информационной безопасности является руководитель БУ РК «Аэропорт «Петрозаводск». Руководитель может делегировать часть полномочий по обеспечению информационной безопасности ответственным сотрудникам БУ РК «Аэропорт «Петрозаводск».

Сфера ответственности руководителя включает следующие направления обеспечения безопасности информации:

- планирование и реализация мер по обеспечению безопасности информации;
- анализ угроз безопасности информации;
- разработка, внедрение, контроль исполнения и поддержание в актуальном состоянии политик, руководств, концепций, процедур, регламентов, инструкций и других локальных документов по обеспечению информационной безопасности;
- контроль защищенности ИТ-инфраструктуры БУ РК «Аэропорт «Петрозаводск» от угроз информационной безопасности;
- обучение и информирование пользователей информационной системы о порядке работы с конфиденциальной информацией и средствами защиты;
- предотвращение, выявление, реагирование и расследование нарушений информационной безопасности.

При взаимодействии со сторонними организациями в случаях, когда сотрудникам этих организаций предоставляется доступ к объектам защиты, с этими организациями должно быть заключено «Соглашение о конфиденциальности». Подготовка типовых вариантов этих соглашений осуществляется совместно с Юридическим отделом.

8. Механизм реализации Концепции

Реализация Концепции осуществляется на основе перспективных программ и планов, которые составляются на основании и во исполнение:

- законов РФ в области обеспечения информационной безопасности;
- постановлений Правительства и других подзаконных актов РФ;
- руководящих и методических документов Федеральной службы по техническому и экспортному контролю, Федеральной службы безопасности, Минкомсвязи России и других государственных органов;
- потребностей информационной системы в средствах обеспечения безопасности конфиденциальной информации.