Приложение №2
к приказу №43 от 08.05.2024г.

Утверждаю:
Директор ИСЭ СО РАН
_____ /И.В. Романченко.
08.05.2024г

Концепция информационной безопасности информационных систем Федерального государственного бюджетного учреждения науки Институт сильноточной электроники Сибирского отделения Российской академии наук

Введение

Данная Концепция информационной безопасности Федерального государственного бюджетного учреждения науки Институт сильноточной электроники Сибирского отделения Российской академии наук (далее — ИСЭ СО РАН) является официальным документом, в котором определена система взглядов на обеспечение информационной безопасности в ИСЭ СО РАН.

Данная Концепция определяет основные цели и задачи, а также общую стратегию построения системы защиты информации (СЗИ) ИСЭ СО РАН. Концепция определяет основные требования и базовые подходы к их реализации, для достижения требуемого уровня безопасности информации.

Концепция разработана в соответствии с комплексным подходом к обеспечению информационной безопасности. Комплексный подход предполагает проведение ряда 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 в обрабатывающей её инфраструктуре 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.

Настоящая Концепция служит основой для разработки комплекса организационных и технических мер по обеспечению информационной безопасности ИСЭ СО РАН, а также нормативных и методических документов, обеспечивающих ее реализацию, и не предполагает подмены функций государственных органов власти Российской Федерации, отвечающих за обеспечение безопасности информационных технологий и защиту информации.

Концепция является методологической основой для:

— формирования и проведения единой политики в области обеспечения безопасности информации ИСЭ СО РАН;

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

— координации деятельности структурных подразделений ИСЭ ОС РАН при проведении работ по развитию и эксплуатации информационных систем с соблюдением требований обеспечения безопасности информации;

— разработки предложений по совершенствованию правового, нормативного, методического, технического и организационного обеспечения безопасности информации в информационных системах ИСЭ СО РАН.

Область применения Концепции распространяется на всех сотрудников ИСЭ СО РАН, эксплуатирующих технические и программные средства ИС, в которых осуществляется автоматизированная обработка информации, а также на подразделения, осуществляющие сопровождение, обслуживание и обеспечение нормального функционирования ИС.

Правовой базой для разработки настоящей Концепции служат требования действующего законодательства Российской Федерации в области защиты информации.

Общие положения

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

Для достижения основной цели СЗИ должна решать следующие задачи:

— защита от вмешательства в процесс функционирования ИС посторонних лиц (возможность использования ИС и доступ к ее ресурсам должны иметь только зарегистрированные установленным порядком пользователи);

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

а) к информации, обрабатываемой в ИС;

б) средствам вычислительной техники ИС;

в) аппаратным, программным и криптографическим средствам защиты, используемым в ИС;

— регистрацию действий пользователей при использовании защищаемых ресурсов ИС в системных журналах и периодический контроль корректности действий пользователей системы путем анализа содержимого этих журналов;

— контроль целостности (обеспечение неизменности) среды исполнения программ и ее восстановление в случае нарушения;

— защиту от несанкционированной модификации и контроль целостности используемых в ИС программных средств, а также защиту системы от внедрения несанкционированных программ;

— защиту информации от утечки по техническим каналам при ее обработке, хранении и передаче по каналам связи;

— защиту информации, хранимой, обрабатываемой и передаваемой по каналам связи, от несанкционированного разглашения или искажения;

— своевременное выявление источников угроз безопасности информации, причин и условий, способствующих нанесению ущерба владельцам информации, создание механизма оперативного реагирования на угрозы безопасности информации и негативные тенденции;

— создание условий для минимизации и локализации наносимого ущерба неправомерными действиями физических и юридических лиц, ослабление негативного влияния и ликвидация последствий нарушения безопасности информации.

Объекты защиты

В ИСЭ СО РАН производится обработка персональных данных в информационных системах персональных данных (ИСПДн). Кроме того, часть автоматизированных рабочих мест в ИСЭ СО РАН относится к объектам критической информационной инфраструктуры (КИИ), т.к. на них обрабатывается информация, необходимая для исполнения контрактов государственного оборонного заказа.

Объектами защиты являются — информация, обрабатываемая в информационной системе (ИС), технические средства ее обработки и защиты. Перечень информации, подлежащей защите, определяется локальными нормативными документами ИСЭ СО РАН. Объекты защиты включают в себя:

— обрабатываемую информацию;

— технологическую информацию;

— программно-технические средства обработки;

— средства защиты информации;

— каналы информационного обмена и телекоммуникации;

— объекты и помещения, в которых размещены компоненты ИС.

Пользователи ИС

Пользователем ИС является лицо, участвующее в функционировании информационной системы или использующее результаты ее функционирования. Пользователем ИС является любой сотрудник ИСЭ СО РАН, имеющий доступ к ИС и ее ресурсам в соответствии с установленным порядком, в соответствии с выполняемыми функциями и должностными обязанностями.

Категории пользователей определяются для каждой ИС в соответствии с локальными нормативными документами ИСЭ СО РАН.

Основные принципы построения системы комплексной защиты информации

Построение системы обеспечения безопасности информации ИС ИСЭ СО РАН и ее функционирование осуществляются в соответствии с принципами:

— законности;

— системности;

— комплексности;

— непрерывности;

— своевременности;

— преемственности и непрерывности совершенствования;

— персональной ответственности;

— взаимодействия и сотрудничества;

— гибкости системы защиты;

— простоты применения средств защиты;

— технической реализуемости

— обязательности контроля.

Меры, методы и средства обеспечения требуемого уровня защищенности

Обеспечение требуемого уровня защищенности достигается с использованием мер, методов и средств безопасности. Все меры обеспечения безопасности ИС подразделяются на:

— законодательные (правовые);

— морально-этические;

— организационные (административные);

— физические;

— технические (аппаратные и программные).

Реализация концепции

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

— федеральных законов в области обеспечения информационной безопасности и защиты информации;

— постановлений Правительства Российской Федерации;

— руководящих, организационно-распорядительных и методических документов ФСТЭК России;

— потребностей ИС в средствах обеспечения безопасности информации.

Ожидаемый эффект от реализации Концепции

Реализация Концепции безопасности информации в ИС позволит:

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

— разработать распорядительные и нормативно-методические документы применительно к ИС;

— провести классификацию и сертификацию ИС;

— провести организационные и технические мероприятия по обеспечению безопасности Информации в ИС;

— обеспечить необходимый уровень безопасности объектов защиты.

Осуществление этих мероприятий обеспечит создание единой, целостной и скоординированной системы информационной безопасности ИС и создаст условия для ее дальнейшего совершенствования.

Основным локальным нормативным актом ИСЭ СО РАН по реализации настоящей Концепции является «Политика информационной безопасности ИСЭ СО РАН».