Приложение №1
к приказу №73 от 08.05.2024г.

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

Политика информационной безопасности
Федерального государственного бюджетного учреждения науки
Институт сильноточной электроники
Сибирского отделения Российской академии наук

ОПРЕДЕЛЕНИЯ

В настоящей Политике, а также в разработанных в соответствии с ней локальных нормативных документах ИСЭ СО РАН, используются следующие термины и их определения:

Автоматизированная система — система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Автоматизированная обработка информации (в т.ч. персональных данных) — обработка защищаемой информации с помощью средств вычислительной техники.

Аутентификация отправителя данных — подтверждение того, что отправитель полученных данных соответствует заявленному.

Безопасность информации (в т.ч. персональных данных) — состояние защищенности информации (в т.ч. персональных данных), характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность защищаемой информации при ее обработке в соответствующих информационных системах.

Биометрические персональные данные — сведения, которые характеризуют физиологические особенности человека и на основе которых можно установить его личность, включая фотографии, отпечатки пальцев, образ сетчатки глаза, особенности строения тела и другую подобную информацию.

Блокирование информации (в т.ч. персональных данных) — временное прекращение сбора, систематизации, накопления, использования и распространения, защищаемой информации (персональных данных), в том числе ее передачи.

Вирус (компьютерный, программный) — исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению.

Вредоносная программа — программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на защищаемую информацию (в т.ч. персональные данные) или ресурсы информационной системы.

Вспомогательные технические средства и системы — технические средства и системы, не предназначенные для передачи, обработки и хранения защищаемой информации (в т.ч. персональных данных), устанавливаемые совместно с техническими средствами и системами, предназначенными для обработки защищаемой информации или в помещениях, в которых установлены соответствующие информационные системы.

Доступ в операционную среду компьютера (информационной системы персональных данных) — получение возможности запуска на выполнение штатных команд, функций, процедур операционной системы (уничтожения, копирования, перемещения и т.п.), исполняемых файлов прикладных программ.

Доступ к информации — возможность получения и использования информации.

Закладочное устройство — элемент средства съема информации, скрытно внедряемый (закладываемый) в места возможного съема информации (в том числе

в ограждения, конструкции, оборудование, предметы интерьера, транспортные средства, а также в технические средства и системы обработки информации).

Защищаемая информация — информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиям правовых документов или требованиями, устанавливаемыми собственником информации .

Идентификация — присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Информативный сигнал — электрические сигналы, акустические, электромагнитные и другие физические поля, по параметрам которых может быть раскрыта конфиденциальная информация (персональные данные) обрабатываемая в информационной системе.

Информационная система персональных данных (ИСПДн) — информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

Информационные технологии — процессы, метод поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Использование персональных данных — действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц.

Источник угрозы безопасности информации — субъект доступа, материальный объект или физическое явление, являющееся причиной возникновения угрозы безопасности информации.

Контролируемая зона — пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств.

Конфиденциальность персональных данных — обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать распространение без согласия субъекта персональных данных или наличия иного законного основания.

Межсетевой экран — локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в информационную систему и (или) выходящей из информационной системы.

Нарушитель безопасности персональных данных — физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных при обработке информации в информационных системах персональных данных.

Неавтоматизированная обработка персональных данных — обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы, считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из

субъектов персональных данных, осуществляются при непосредственном участии человека.

Недекларированные возможности — функциональные возможности средств вычислительной техники, не оглашенные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

Несанкционированный доступ (несанкционированные действия) — доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых соответствующими информационными системами (в т.ч. системами персональных данных).

Носитель информации — физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

Обезличивание персональных данных — действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных.

Обработка персональных данных — любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Общедоступные персональные данные — персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

Оператор (персональных данных) — государственный орган, муниципальный орган, юридическое или физическое лицо, организующее и (или) осуществляющее обработку персональных данных, а также определяющие состав данных, цели и содержание обработки персональных данных.

Технические средства информационной системы персональных данных — средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки ПДн (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации, применяемые в информационных системах.

Перехват (информации) — неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов.

Персональные данные (ПДн) — любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных).

Побочные электромагнитные излучения и наводки — электромагнитные излучения технических средств обработки защищаемой информации, возникающие

как побочное явление и вызванные электрическими сигналами, действующими в их электрических и магнитных цепях, а также электромагнитные наводки этих сигналов на токопроводящие линии, конструкции и цепи питания.

Политика «чистого стола» — комплекс организационных мероприятий, контролирующих отсутствие записывания на бумажные носители ключей и атрибутов доступа (паролей) и хранения их вблизи объектов доступа.

Пользователь информационной системы (в т.ч. системы персональных данных) — лицо, участвующее в функционировании информационной системы (в т.ч. системы персональных данных) или использующее результаты ее функционирования.

Правила разграничения доступа — совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

Программная закладка — код программы, преднамеренно внесенный в программу с целью осуществить утечку, изменить, блокировать, уничтожить защищаемую информацию или уничтожить и модифицировать программное обеспечение соответствующей информационной системы и (или) блокировать аппаратные средства.

Программное воздействие — несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ.

Раскрытие персональных данных — умышленное или случайное нарушение конфиденциальности персональных данных.

Распространение информации (в т.ч. персональных данных) — действия, направленные на передачу защищаемой информации (в т.ч. персональных данных) определенному кругу лиц (передача) или на ознакомление с защищаемой информацией неограниченного круга лиц, в том числе обнародование информации в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к информации (персональным данным) каким-либо иным способом.

Ресурс информационной системы — именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы.

Специальные категории персональных данных — персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных, философских убеждений, состояния здоровья, интимной жизни субъекта персональных данных.

Средства вычислительной техники — совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Субъект доступа (субъект) — лицо или процесс, действия которого регламентируются правилами разграничения доступа.

Технический канал утечки информации — совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.

Трансграничная передача информации (в т.ч. персональных данных) — передача информации (в т.ч. персональных данных) оператором через Государственную границу Российской Федерации органу власти иностранного государства, физическому или юридическому лицу иностранного государства.

Угрозы безопасности информации (в т.ч. персональных данных) — совокупность условий и факторов, создающих опасность несанкционированного, в

том числе случайного, доступа к защищаемой информации, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение информации, а также иных несанкционированных действий при ее обработке в соответствующих информационных системах.

Уничтожение информации (в т.ч. персональных данных) — действия, в результате которых невозможно восстановить содержание информации (персональных данных) в соответствующей информационной системе или в результате которых уничтожаются материальные носители информации (персональных данных).

Утечка (защищаемой) информации по техническим каналам — неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

Уязвимость — слабость в средствах защиты, которую можно использовать для нарушения системы ила содержащейся в ней информации.

Целостность информации — способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

АВС — антивирусные средства
АРМ — автоматизированное рабочее место
ВТСС — вспомогательные технические средства и системы
ИС — информационная система
ИСПДн — информационная система персональных данных
ИТ — информационные технологии
КИИ —
критическая информационная инфраструктура
КЗ — контролируемая зона
ЛВС — локальная вычислительная сеть
МН ПДн - машинные носители персональных данных
МЭ — межсетевой экран
НСД — несанкционированный доступ
ОС — операционная система
ПДн — персональные данные
ПМВ — программно-математическое воздействие
ПО — программное обеспечение
ПЭМИН —
побочные электромагнитные излучения и наводки
САЗ — система анализа защищенности
СЗИ — система (средства) защиты информации
СОВ — система обнаружения вторжений
ТКУИ — технические каналы утечки информации
УБИ — угрозы безопасности информации

1. Введение

Настоящая Политика информационной безопасности (далее по тексту — Политика) Федерального государственного бюджетного учреждения науки Институт сильноточной электроники Сибирского отделения Российской академии наук (далее — ИСЭ СО РАН), разработана на основании Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» и Федерального закона от 26.07.2017 г. №187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», определяющих цели, задачи и основные принципы обеспечения безопасности информации в Российской Федерации, и в соответствии с «Концепцией информационной безопасности информационных систем ИСЭ СО РАН».

Политика устанавливает структуру и необходимый уровень защищенности информации и объектов информационной инфраструктуры в ИСЭ СО РАН, требования к персоналу, допущенному к работе с защищаемой информацией, степень ответственности персонала, статус и должностные обязанности сотрудников, ответственных за обеспечение безопасности информации в ИСЭ СО РАН.

2. Общие положения

Целью настоящей Политики является обеспечение безопасности информации (в т.ч. ИСПДн) ИСЭ СО РАН от всех видов угроз, внешних и внутренних, умышленных и непреднамеренных, а также минимизация ущерба от возможной реализации угроз безопасности информации (УБИ).

Настоящая Политика 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.

Организационные меры предусматривают создание и поддержание правовой базы безопасности информации и разработку (введение в действие) предусмотренных настоящей Политикой организационно-распорядительных документов.

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

Безопасность информации достигается путем исключения несанкционированного, в том числе случайного, доступа к защищаемой информации, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение данной информации, а также иных несанкционированных действий.

Настоящая Политика предполагает доступность информации и связанных с ней ресурсов для авторизованных пользователей, обеспечивая при этом своевременное обнаружение и реагирование на УБИ, а также предотвращение преднамеренньж или случайных, частичных или полных несанкционированных модификаций или уничтожения информации.

3. Область действия

Требования настоящей Политики распространяются на всех сотрудников ИСЭ СО РАН (штатных, временных, работающих по контракту и т.п.), а также всех прочих лиц (подрядчики, аудиторы и т.п.), вовлеченных в организационные и технологические процессы сбора, записи, систематизации, накопления, хранения, уточнения (обновления, изменения), извлечения, использования, передачи

(предоставления, доступа), обезличивания, блокирования, удаления, уничтожения защищаемой информации.

В ИСЭ СО РАН используется единая информационная система персональных данных (ИСПДн), состоящая из 4-х подсистем, сходных между собой по составу и способу обработки информации.

Объектами защиты в соответствии с настоящей Политикой являются — информация, обрабатываемая в ИС, а также технические средства ее обработки и защиты. Перечень информации, подлежащей защите, определен в Положении об обработке и защите ПДн.

К объектам защиты в рамках Политики относятся:

— обрабатываемая информация;

— технологическая информация;

— программно-технические средства обработки;

— средства защиты информации;

— каналы информационного обмена и телекоммуникации;

— объекты и помещения, в которых размещены компоненты ИС.

4. Система защиты информации (в т.ч. персональных данных)

Система защиты информации (СЗИ) ИСЭ СО РАН предполагает обеспечение четвертого уровня защищенности ПДн, а также обеспечение защиты объектов КИИ третьей категории значимости.

СЗИ выстраивается на основании:

— настоящей Политики и Перечней информации, подлежащей защите;

— Положения об организации работы с персональными данными, определяющего, в т.ч., требуемый уровень защищенности ИСПДн;

— Положения об организации работы с критической информационной инфраструктурой, содержащего, в т.ч., классификацию объектов КИИ;

— Матрицы доступа к защищаемой информации;

— Руководящих документов ФСТЭК России и ФСБ России.

В рамках Политики определяется перечень используемых технических средств защиты, а также программного обеспечения, участвующего в обработке защищаемой информации, для всех информационных систем:

— АРМ пользователей;

— сервера приложений;

— каналов передачи в сети общего пользования и (или) международного обмена, если по ним передаётся защищаемая информация.

В зависимости от требуемого уровня защищенности ИСПДн, классификации объектов КИИ и актуальных угроз, СЗИ может включать следующие технические средства:

— антивирусные средства для рабочих станций пользователей и серверов;

— средства межсетевого экранирования;

— средства анализа защищенности;

— средства криптографической защиты информации, при передаче защищаемой информации по каналам связи.

Кроме того, в рамках Политики определяются функции защиты, обеспечиваемые штатными средствами обработки информации, операционными

системами (ОС), прикладным ПО и специальными комплексами, реализующими средства защиты. Список функций защиты может включать:

— управление и разграничение доступа пользователей;

— регистрацию и учет действий с информацией;

— обеспечивать целостность данных;

— производить обнаружение вторжений.

5. Требования к составу СЗПДн

СЗИ должна соответствовать требованиям Приказа ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» и приказа ФСТЭК России № 239 от 25.12.2017 г. «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации». Данные приказы определяют требования к составу и содержанию мер по защите информации и не рассматривают вопросы обеспечения безопасности, связанные с применением криптографической защиты информации.

Приказ ФСБ России от 10 июля 2014 г. № 378 г. «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности» устанавливает требования к применяемым средствам криптографической защиты для каждого из уровней защищенности.

6. Принципы построения системы комплексной защиты информации

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

— законности, предполагающим разработку локальных нормативных актов в области защиты информации и непосредственное осуществление защитных мероприятий в полном соответствии с действующим законодательством РФ;

— системности, предполагающим учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, существенно значимых для понимания и решения вопросов обеспечения безопасности информации и ИС (в т.ч. учет не только всех известньж каналов проникновения и НСД к информации, но и возможности появления принципиально новых путей реализации угроз безопасности);

— комплексности, предполагающим согласованное применение разнородных средств при построении целостной системы защиты, перекрывающей все существенные (значимые) каналы реализации угроз и не содержащей слабых мест на стыках отдельных ее компонентов;

— непрерывности, предполагающим защиту ИС на протяжении всего времени их функционирования (в т.ч. с помощью своевременной смены и

обеспечения правильного хранения и применения имен, паролей, ключей шифрования, переопределение полномочий и т.п.);

— своевременности, предполагающим упреждающий характер мер обеспечения безопасности информации, т.е. постановку задач по комплексной защите ИС и реализацию мер обеспечения безопасности информации на ранних стадиях разработки ИС в целом, и ее системы защиты информации, в частности;

— преемственности и непрерывности совершенствования, предполагающим постоянное совершенствование мер и средств защиты информации на основе преемственности организационных и технических решений, кадрового состава, анализа функционирования ИС и ее системы защиты с учетом изменений в методах и средствах перехвата информации, нормативных требований по защите, достигнутого отечественного и зарубежного опыта в этой области;

— персональной ответственности, предполагающим возложение ответственности за обеспечение безопасности информации и системы их обработки на каждого сотрудника в пределах его полномочий (с тем, чтобы в случае любого нарушения круг виновников был четко известен или сведен к минимуму);

— минимизации полномочий, предполагающим предоставление пользователям минимальных прав доступа в соответствии с производственной необходимостью, на основе принципа «все, что не разрешено, то запрещено»;

— взаимодействия и сотрудничества, предполагающим создание благоприятной атмосферы в коллективах подразделений для снижения вероятности возникновения негативных действий, связанных с человеческим фактором;

— гибкости системы защиты, предполагающим обеспечение возможности варьировать уровень защищенности ИС путем сочетания различных механизмов и средств защиты;

— открытости алгоритмов и механизмов защиты, предполагающим возможность знания алгоритмов работы системы защиты с одновременным обеспечением секретности структурной организации и алгоритмов функционирования ее подсистем и ограничением возможности ее преодоления (даже авторам);

— простоты применения средств защиты, предполагающим отсутствие необходимости знания специальных языков или выполнения действий, требующих значительных дополнительных трудозатрат при обычной работе обычного пользователя, а также не требующим от пользователя выполнения рутинных малопонятных ему операций (ввод нескольких паролей и имен и т.д.);

— научной обоснованности и технической реализуемости, предполагающим соответствие используемых средств защиты современному уровню развития науки и техники, а также установленным нормам и требованиям по безопасности информации;

— специализации и профессионализма, предполагающим 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 государственную лицензию на право оказания услуг в этой области;

— обязательности контроля, предполагающим 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.

7. Пользователи ИС

Настоящей Политикой определены основные возможные категории пользователей информацией, подлежащей защите:

— Администратор ИС;

— Администратор безопасности ИС;

— Пользователь ИС;

— Администратор сети;

— Технический специалист по обслуживанию периферийного оборудования.

На основании этих категорий производится типизация пользователей ИС, определяется их уровень доступа и возможности.

Данные о группах пользователей ИСЭ СО РАН, участвующих в обработке и хранении защищаемой информации, уровне их доступа и информированности закрепляются локальными нормативными документами, в частности «»Матрицей досиупа».

7.1. Администратор ИС

Администратор ИС — сотрудник ИСЭ СО РАН, ответственный за настройку, внедрение и сопровождение ИС. Обеспечивает функционирование подсистемы управления доступом ИС и уполномочен осуществлять предоставление и разграничение доступа конечного пользователя (Оператора АРМ) к элементам, хранящим персональные данные. Администратор ИС обладает следующим уровнем доступа и знаний:

— обладает полной информацией о системном и прикладном программном обеспечении ИС;

— обладает полной информацией о технических средствах и конфигурации ИС;

— имеет доступ ко всем техническим средствам обработки информации и данным ИС;

— обладает правами конфигурирования и административной настройки технических средств ИС.

7.2. Администратор безопасности ИС

Администратор безопасности ИС — сотрудник ИСЭ СО РАН, ответственный за функционирование СЗИ, включая обслуживание и настройку административной, серверной и клиентской компонент.

Администратор безопасности обладает следующим уровнем доступа и знаний:

— обладает правами Администратора ИС;

— обладает полной информацией об ИС;

— имеет доступ к средствам защиты информации и протоколирования и к части ключевых элементов ИС;

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

Администратор безопасности уполномочен:

— реализовывать политики безопасности в части настройки СЗИ, межсетевых экранов и систем обнаружения атак, в соответствии с которыми пользователь (Оператор АРМ) получает возможность работать с элементами ИС;

— осуществлять аудит средств защиты;

— устанавливать доверительные отношения своей защищенной сети с сетями других организаций.

7.3. Пользователь ИС

Пользователь ИС — сотрудник ИСЭ СО РАН, осуществляющий обработку информации. Обработка информации включает: возможность просмотра, ручной ввод в ИС, формирование справок и отчетов по информации, полученной из ИС. Пользователь не имеет полномочий для управления подсистемами обработки данных и СЗИ.

Пользователь ИС обладает следующим уровнем доступа и знаний:

— обладает всеми необходимыми атрибутами (например, паролем), обеспечивающими доступ к некоторому подмножеству информации;

— располагает конфиденциальными данными, к которым имеет доступ.

7.4. Администратор сети

Администратор сети — сотрудник ИСЭ СО РАН, ответственный за функционирование телекоммуникационной подсистемы. Администратор сети не имеет полномочий для управления подсистемами обработки данных и безопасности.

Администратор сети обладает следующим уровнем доступа и знаний:

— обладает частью информации о системном и прикладном программном обеспечении ИС;

— обладает частью информации о технических средствах и конфигурации ИС;

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

— знает, по меньшей мере, одно легальное имя доступа.

7.5. Технический специалист по обслуживанию периферийного оборудования

Технический специалист по обслуживанию — сотрудник ИСЭ СО РАН, осуществляет обслуживание и настройку периферийного оборудования ИС. Технический специалист по обслуживанию не имеет доступа к информации, не имеет полномочий для управления подсистемами обработки данных и безопасности.

Технический специалист по обслуживанию обладает следующим уровнем доступа и знаний:

— обладает частью информации о системном и прикладном программном обеспечении ИС;

— обладает частью информации о технических средствах и конфигурации ИС; — знает, по меньшей мере, одно легальное имя доступа.

8. Требования к персоналу по обеспечению защиты информации

Все сотрудники ИСЭ СО РАН, являющиеся пользователями ИС, должны четко знать и строго выполнять установленные правила и обязанности по доступу к защищаемым объектам и соблюдению принятого режима безопасности информации.

При вступлении в должность нового сотрудника непосредственный начальник подразделения, в которое он поступает, обязан организовать его ознакомление в установленном порядке с должностной инструкцией и необходимыми документами, регламентирующими требования по защите информации, а также организовать обучение навыкам выполнения процедур, необходимых для санкционированного использования ИС.

Сотрудник должен быть ознакомлен со сведениями настоящей Политики, принятых процедур работы с элементами ИС и СЗИ.

Сотрудники, использующие технические средства аутентификации, должны обеспечивать сохранность идентификаторов (электронных ключей) и не допускать НСД к ним, а также возможность их утери или использования третьими лицами. Пользователи несут персональную ответственность за сохранность идентификаторов.

Сотрудники должны следовать установленным процедурам поддержания режима безопасности информации при выборе и использовании паролей (если не используются технические средства для прохождения процедуры аутентификации).

Сотрудники ИСЭ СО РАН обязаны обеспечивать надлежащую защиту оборудования, оставляемого без присмотра, особенно в тех случаях, когда в помещение имеют доступ посторонние лица. Все пользователи обязаны знать требования по безопасности информации и процедуры защиты оборудования, оставленного без присмотра, а также свои обязанности по обеспечению такой защиты.

Сотрудникам запрещается устанавливать постороннее программное обеспечение, подключать личные мобильные устройства и носители информации, а так же записывать на них защищаемую информацию.

Сотрудникам запрещается разглашать защищаемую информацию, которая стала им известна при работе с информационными системами ИСЭ СО РАН, третьим лицам.

При работе с информацией, сотрудники обязаны обеспечить отсутствие возможности просмотра информации третьими лицами с мониторов АРМ или терминалов.

При завершении работы с ИС сотрудники обязаны защитить АРМ или терминалы с помощью блокировки ключом или эквивалентного средства контроля, например, доступом по паролю, если не используются более сильные средства защиты.

Сотрудники должны быть проинформированы об угрозах нарушения режима безопасности информации и ответственности за его нарушение. Они должны быть ознакомлены с утвержденной формальной процедурой наложения дисциплинарных взысканий на сотрудников, которые нарушили принятые Политику и процедуры безопасности информации в ИСЭ СО РАН.

Сотрудники обязаны без промедления сообщать обо всех наблюдаемых или подозрительных случаях работы ИС, могущих повлечь за собой угрозы безопасности информации, а также о выявленных ими событиях, затрагивающих безопасность

информации, руководству подразделения и лицу, отвечающему за немедленное реагирование на угрозы безопасности информации.

9. Должностные обязанности пользователей ИС

Должностные обязанности пользователей ИС ИСЭ СО РАН описаны в следующих локальных нормативных документах:

— Инструкции Администратора ИС;

— Инструкции Администратора безопасности ИС;

— Инструкции Пользователь ИС;

— Инструкции Администратора сети;

— Инструкции Технического специалиста по обслуживанию периферийного оборудования.

10. Меры, методы и средства обеспечения требуемого уровня защищенности

Обеспечение требуемого уровня защищенности в соответствии с настоящей Политикой должно достигаться с использованием мер, методов и средств безопасности. Все меры обеспечения безопасности ИС подразделяются на:

— законодательные (правовые), к которым относятся действующие в стране законы, указы и нормативные акты, регламентирующие правила обращения с информацией, закрепляющие права и обязанности участников информационных отношений в процессе ее обработки и использования, а также устанавливающие ответственность за нарушения этих правил, препятствуя тем самым неправомерному использованию информации и являющиеся сдерживающим фактором для потенциальных нарушителей; данные меры защиты носят в основном упреждающий, профилактический характер и требуют постоянной разъяснительной работы с пользователями и обслуживающим персоналом системы;

— морально-этические, к которым относятся нормы поведения, традиционно сложившиеся в обществе в области использования ЭВМ; эти нормы носят, в основном, профилактический характер и требуют постоянной работы по созданию здорового морального климата в коллективах подразделений, т.к. снижают вероятность возникновения негативных действий, связанных с человеческим фактором;

— организационные (административные), к которым относятся меры, регламентирующие процессы функционирования ИС, использование ресурсов ИС, деятельность обслуживающего персонала, а также порядок взаимодействия пользователей с ИС таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности или снизить размер потерь в случае их реализации; служат, прежде всего, основой для формирования политики информационной безопасности и инструментом для ее выполнения, выделяя необходимые ресурсы и контролируя текущее состояние дел;

— физические, к которым относятся меры защиты, основанные 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; физическая защита зданий,

помещений, объектов и средств информатизации осуществляется 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, самих средств информатизации, исключающими нахождение внутри контролируемой (охраняемой) зоны технических средств разведки;

— технические (аппаратные и программные), к которым относятся меры, основанные на использовании различных электронных устройств и специальных программ, входящих в состав ИС 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 их состав включаются:

-средства идентификации (опознавания) и аутентификации (подтверждения подлинности) пользователей ИС;

- средства разграничения доступа зарегистрированных пользователей системы к ресурсам ИС;

-средства обеспечения и контроля целостности программных и информационных ресурсов;

-средства оперативного контроля и регистрации событий безопасности;

-криптографические средства защиты информации.

Специалистами ИСЭ СО РАН осуществляется непрерывное управление и административная поддержка функционирования всех комплексно используемых средств защиты, таких как:

— идентификация и аутентификация субъектов доступа и объектов доступа;

— управление доступом субъектов доступа к объектам доступа;

— защита машинных носителей ПДн;

— регистрация событий безопасности;

— контроль (анализа) защищенности ПДн;

— антивирусная защита;

— обеспечение целостности;

— обеспечение доступности;

— защита технических средств и систем;

— защита ИС, ее средств связи и передачи данных.

11. Контроль эффективности СЗИ

Настоящая Политика предполагает 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.

Контроль эффективности СЗИ надлежит осуществлять на периодической основе. Целью контроля эффективности является своевременное выявление ненадлежащих режимов работы СЗИ (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 как Администраторами безопасности ИС (оперативный контроль в процессе информационного взаимодействия в ИС), так и привлекаемыми для этой цели компетентными организациями, имеющими лицензию на данный вид деятельности, а также ФСТЭК России и ФСБ России в пределах их компетенции.

Контроль может осуществляться Администратором безопасности ИС как с помощью штатных средств системы защиты информации, так и с помощью специальных программных средств контроля.

Оценка эффективности мер защиты информации проводится с использованием технических и программных средств контроля на предмет соответствия установленным требованиям.

12. Основные модели угроз для ИС

Основными источниками угроз безопасности информации для ИСЭ СО РАПН могут выступать:

— нарушитель;

— аппаратная закладка;

— носитель вредоносной программы.

В связи с чем, основными моделями угроз для ИСЭ СО РАН являются Модель нарушителя безопасности информации и Модель угроз безопасности информации.

В рамках настоящей Политики обеспечивается защита информации от следующих видов угроз:

— несанкционированного копирования информации, обрабатываемой в ИС;

— разглашения (публикации) защищаемой информации, обрабатываемой в ИС, а также состава и конфигурации средств защиты ИС;

— несанкционированной модификации защищаемой информации, обрабатываемой в ИС;

— нарушения функционирования и отказа средств хранения информации;

— внедрения (классического) программного вируса;

— анализа сетевого трафика, передаваемого во внешнюю сеть из внешней сети4 — сканирования сети;

— скрытого отказа в обслуживании, вызванного привлечением части ресурсов ИСПДн;

— явного отказа в обслуживании, вызванного исчерпанием ресурсов ИСПДн;

— явного отказа в обслуживании, вызванного передачей злоумышленником пакетов с нетрадиционными атрибутами;

— удаленного запуска приложений путем распространения файлов, содержащих несанкционированный исполняемый код;

— удаленного запуска приложений путем использования возможностей удаленного управления системой;

— внедрения кода или данных;

— деструктивного изменения конфигурации/среды окружения программ;

— доступа к защищаемым файлам с использованием обходного пути;

— использования альтернативных путей доступа к ресурсам;

— использования механизмов авторизации для повышения привилегий;

— несанкционированного доступа к аутентификационной информации;

— обнаружения открытых портов и идентификации привязанных к ним сетевых служб;

— обнаружения «хвостов»;

— определения типов объектов защиты;

— определения топологии вычислительной сети;

— перехвата информации, вводимой и выводимой на периферийные устройства;

— перехвата данных, передаваемых по вычислительной сети;

— подмены содержимого сетевых ресурсов;

— приведения системы в состояние «отказ в обслуживании»;

— утраты носителей информации;

— неправомерного шифрования информации;

— «фишинга»;

— несанкционированной модификации защищаемой информации.

12.1. Модель нарушителя безопасности

Под нарушителем в ИСЭ СО РАН понимается лицо, которое в результате умышленных или неумышленных действий может нанести ущерб защищаемым информационным ресурсам.

Нарушители подразделяются по признаку принадлежности к ИС и подразделяются на две группы:

— внешние нарушители — физические лица, не имеющие права пребывания на территории контролируемой зоны, в пределах которой размещается оборудование ИС;

— внутренние нарушители — физические лица, имеющие право пребывания на территории контролируемой зоны, в пределах которой размещается оборудование ИС.

Классификация нарушителей, их потенциалы и возможности более подробно отражаются в «Модели угроз и нарушителя безопасности информации при ее обработке в ИС ИСЭ СО РАН».

12.2. Модель угроз безопасности

Для ИС ИСЭ СО РАН выделяются следующие основные категории угроз безопасности данных (в т.ч. персональных данных):

— угрозы от утечки по техническим каналам;

— угрозы несанкционированного доступа к информации:
— угрозы уничтожения, хищения аппаратных средств ИС носителей информации путем физического доступа к элементам ИС;
— угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий);
— угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИС и СЗИ в ее составе из-за сбоев в программном обеспечении, а также от угроз не антропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера;
—угрозы преднамеренных действий внутренних нарушителей; угрозы несанкционированного доступа по каналам связи.

Более детальное описание категорий угроз безопасности информации, оценка их опасности, а также вероятности и возможностей реализации отражается в «Модели угроз и нарушителя безопасности информации при ее обработке в ИС ИСЭ СО РАН».

13. Ответственность сотрудников ИСЭ СО РАН

В соответствии со ст. 24 Федерального закона Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных» и ст. 14 Федерального закона Российской Федерации от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», лица, виновные в нарушении требований данных Федеральных законов и локальных нормативных документов ИСЭ СО РАН в сфере информационной безопасности, несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

Действующее законодательство РФ позволяет предъявлять требования по обеспечению безопасной работы с защищаемой информацией и предусматривает ответственность за нарушение установленных правил эксплуатации ЭВМ и систем, неправомерный доступ к информации, если эти действия привели к уничтожению, блокированию, модификации информации или нарушению работы ЭВМ или сетей (статьи 272, 273 и 274 УК РФ).

Ответственными за разработку мер и контроль над обеспечением безопасности персональных данных является ответственное лицо, назначенное приказом директора ИСЭ СО РАН.

Сфера ответственности ответственного лица включает следующие направления обеспечения безопасности информации:

— планирование и реализация мер по обеспечению безопасности информации;

— анализ угроз безопасности информации;

— разработку, внедрение, контроль исполнения и поддержание в актуальном состоянии политик, руководств, концепций, процедур, регламентов, инструкций и других организационных документов по обеспечению безопасности;

— контроль защищенности ИТ-инфраструктуры ИСЭ СО РАН;

— обучение и информирование пользователей ИС, о порядке работы с информации и средствами защиты;

— предотвращение, выявление, реагирование и расследование нарушений безопасности информации.

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», либо «Соглашение о соблюдении режима безопасности Информации при выполнении работ в ИС».

Администратор ИС и Администратор безопасности несут ответственность за все действия, совершенные от имени их учетных записей или системных учетных записей, если не доказан факт несанкционированного использования учетных записей.

При нарушениях сотрудниками ИСЭ СИ РАН — пользователями ИС правил, связанных с безопасностью информации, они несут ответственность, установленную действующим законодательством Российской Федерации.