МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное учреждение науки
Федеральный исследовательский центр «Коми научный центр Уральского отделения Российской академии наук»
(ФИЦ Коми НЦ УрО РАН)

РОССИЯСА НАУКА ДА ВЫЛЫС ВЕЛӦДЧАН МИНИСТЕРСТВО

«Россияса наукаяс академиялӧн Урал юкӧнса Коми наука шӧрин» туялан удж нуӧдысь федеральнӧй шӧрин
Федеральнӧй канму сьӧмкуд наука учреждение
(ТФШ РНА УрЮ Коми НШ)

ПРИКАЗ

31.10.2024 № 298

г. Сыктывкар

Об утверждении Политики информационной безопасности ФИЦ Коми НЦ УрО РАН

В целях исполнения законодательства Российской Федерации в области обеспечения информационной безопасности

ПРИКАЗЫВАЮ:

1. Утвердить Политику информационной безопасности ФИЦ Коми НЦ УрО РАН согласно приложению к настоящему приказу.
2. Руководителям обособленных и структурных подразделений ФИЦ Коми НЦ УрО РАН:
2.1. Ознакомить с настоящим приказом работников под роспись.
2.2. Листы ознакомления представить в отдел комплексной безопасности ФИЦ Коми НЦ УрО РАН в срок до 28 декабря 2024 г.
3. Начальнику отдела кадров ФИЦ Коми НЦ УрО РАН и руководителям обособленных подразделений ФИЦ Коми НЦ УрО РАН обеспечить ознакомление вновь принимаемых на работу лиц с настоящим приказом под роспись.
4. Контроль исполнения настоящего приказа оставляю за собой.

Директор С.В. Дёгтева

Приложение

УТВЕРЖДЕНО
приказом ФИЦ Коми НЦ УрО РАН
от 31.10.2024 № 298

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное
бюджетное учреждение науки
Федеральный исследовательский центр
«Коми научный центр Уральского отделения
Российской академии наук»
(ФИЦ Коми НЦ УрО РАН)

РОССИЯСА НАУКА ДА ВЫЛЫС ВЕЛӦДЧАН МИНИСТЕРСТВО

«Россияса наукаяс академиялӧн
Урал юкӧнса Коми наука шӧрин»
туялан удж нуӧдысь федеральнӧй шӧрин
Федеральнӧй канму
сьӧмкуд наука учреждение
(ТФШ РНА УрЮ Коми НШ)

Политика информационной безопасности Федерального государственного бюджетного учреждения науки Федерального исследовательского центра «Коми научный центр Уральского отделения Российской академии наук»

Сыктывкар, 2024 год

СОДЕРЖАНИЕ

1. Общие положения

1.1. Настоящая Политика информационной безопасности в Федеральном государственном бюджетном учреждении науки Федеральном исследовательском центре «Коми научный центр Уральского отделения Российской академии наук» (далее – Политика, Центр) разработана в соответствии с Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Указом Президента Российской Федерации от 01.05.2022 № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации», Постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», ГОСТ Р 53114-2008 «Защита информации. Обеспечение информационной безопасности в организации».

1.2. Политика определяет стратегию Центра по защите информации ограниченного доступа, которая не содержит сведений, составляющих государственную тайну (далее – информация), в информационных системах Центра. Эта информация предназначена для внутреннего использования, и её цель – защита от несанкционированного доступа, а также от специальных воздействий на неё и носители информации, направленных на её добывание, уничтожение, искажение или блокирование доступа к ней (далее – защита информации).

1.3. При обработке персональных данных в информационных системах необходимо соблюдать настоящую Политику и требования к защите персональных данных, установленные Постановлением Правительства Российской Федерации от 01.11.2012 № 1119.

2. Термины и определения

В настоящем документе использованы следующие термины и определения:

Безопасность информации (данных) – состояние защищенности информации (данных), при котором обеспечены ее (их) конфиденциальность, доступность и целостность.

Блокирование информации (данных) – временное прекращение сбора, систематизации, накопления, использования, распространения информации, в том числе ее передачи.

Доступ к информации (данным) – возможность получения и использования информации (данных).

Защищаемая информация (защищаемые данные) – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями законодательства Российской Федерации или требованиями, устанавливаемыми собственником информации.

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

Информационная безопасность – защищенность информационных систем (информации и обрабатывающей ее инфраструктуры) от любых случайных или злонамеренных воздействий, результатом которых может явиться нанесение ущерба самой информации, ее владельцам или инфраструктуре.

Информационная инфраструктура – совокупность объектов информатизации, обеспечивающая доступ потребителей к информационным ресурсам.

Информационные процессы – процессы создания, сбора, обработки, накопления, хранения, поиска, передачи и уничтожения информации.

Информационные ресурсы – данные и (или) документы, организованные для получения информации, представленные в любой знаковой системе, на любом физическом носителе и (или) распространяемые в информационно-телекоммуникационных сетях.

Информационная система – система, представляющая собой совокупность информации, а также информационных технологий и технических средств, позволяющих

осуществлять обработку информации с использованием средств автоматизации или без использования таких средств.

Инцидент информационной безопасности – любое непредвиденное или нежелательное событие, которое может нарушить деятельность или информационную безопасность.

Компьютерный инцидент – факт нарушения и (или) прекращения функционирования объекта критической информационной инфраструктуры, сети электросвязи, используемой для организации взаимодействия таких объектов, и (или) нарушения безопасности обрабатываемой таким объектом информации, в том числе произошедший в результате компьютерной атаки.

Конфиденциальность информации (данных) – обязательное для соблюдения требование о недопущении распространения информации без согласия владельца информации или наличия иного законного основания.

Конфиденциальная информация (данные, сведения) – документированная информация, доступ к которой ограничивается в соответствии с законодательством.

Меры обеспечения информационной безопасности – совокупность действий, направленных на разработку и (или) практическое применение способов и средств обеспечения информационной безопасности.

Мониторинг информационной безопасности – непрерывное наблюдение за состоянием и поведением объектов информационной безопасности с целью их контроля, оценки и прогноза в рамках управления информационной безопасности.

Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами.

Обработка информации (данных) – действия (операции) с информацией, включая ее сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), блокирование, уничтожение.

Оценка риска – процесс, объединяющий идентификацию риска, анализ риска и их количественную оценку.

Политика – общее намерение и направление, официально выраженное руководством.

Технические средства информационных систем – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки информации (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документови 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.

Пользователь информационной системы – лицо, участвующее в функционировании информационной системы либо использующее результаты ее функционирования.

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

Риск – сочетание вероятности события и его последствий. Применительно к информационной безопасности риск – сочетание вероятности нанесения ущерба и тяжести этого ущерба.

Система защиты информации (данных) – совокупность организационных и технических мероприятий для защиты информации от неправомерного или случайного доступа, уничтожения, изменения, блокирования, копирования, распространения, а также иных неправомерных действий с ней.

Третья сторона – лица или организация, которые признаны независимыми от участвующих сторон, по отношению к рассматриваемой проблеме.

Угрозы безопасности информации (данных) – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к информации, результатом которого может стать её уничтожение, изменение, блокирование, копирование, распространение, а также иных несанкционированных действий при её обработке в информационных системах.

Целостность информации (данных) – способность средства вычислительной техники или информационной системы обеспечивать неизменность информации в условиях ее случайного и (или) преднамеренного искажения (разрушения).

В настоящем документе использованы следующие сокращения:

ИБ – информационная безопасность;

ИС – информационная система;

СЗИ – средства защиты информации;

СКЗИ – средства криптографической защиты информации;

ФСБ России – Федеральная служба безопасности Российской Федерации;

ФСТЭК России – Федеральная служба по техническому и экспортному контролю.

3. Область действия Политики

3.1. Требования Политики распространяются на все информационные ресурсы и процессы обработки данных в Центре, для которых установлены требования по защите информации, а также информационно-телекоммуникационную инфраструктуру, на базе которой функционируют информационные системы.

3.2. Соблюдение настоящей Политики является обязательным для всех работников Центра и распространяется на отношения с поставщиками, провайдерами и другими партнерами, чьи услуги связаны с использованием, обработкой или доступом к информации и информационным активам Центра.

3.3. Требования настоящей Политики распространяются на все обособленные и структурные подразделения Центра и покрывают весь жизненный цикл (создание, эксплуатация и вывод из эксплуатации) защищаемых объектов Центра.

4. Цели и показатели эффективности их достижения, задачи защиты информации

4.1. Основной целью Центра является защита информации от внешних и внутренних угроз, связанных с умышленными и непреднамеренными действиями работников Центра и третьих лиц, недопущение возникновения негативных последствий (ущерба) и обеспечение эффективности мероприятий по устранению последствий компьютерных инцидентов.

4.2. Для достижения основной цели необходимо решение следующих задач:

– обеспечение конфиденциальности, целостности, доступности информации и информационных систем Центра путем установления правил использования информации и ИС;

– защита информации от вмешательства посторонних лиц;

– соблюдение норм законодательства Российской Федерации и требований регулирующих органов власти (Регуляторов) в области ИБ;

– обеспечение защиты деловой репутации и имиджа Центра;

– классификация информационных активов Центра;

– оценка рисков ИБ;

– защита информационных активов в соответствии с их классификацией и оценкой рисков;

– мониторинг событий ИБ и управление инцидентами ИБ;

– обеспечение непрерывности деятельности Центра;

– введение согласованной системы контроля и процедур по защите информации в подразделениях Центра;

– распространение информации об общих правилах ИБ среди работников Центра, определяющей обязанности и ответственность каждого работника;

– повышение осведомленности и квалификации работников Центра в области ИБ.

4.3. Для решения этих задач предусмотрены следующие меры:

– учет всех подлежащих защите информационных ресурсов;

– учет действий работников, занимающихся обслуживанием и модификацией программных и программно-аппаратных средств;

– назначение и подготовка работников, ответственных за ИБ;

– регламентация процессов обработки информации и действий работников Центра на основе организационно-распорядительных документов по защите информации;

– реализация организационно-технических мер защиты программного обеспечения и программно-аппаратных средств;

– использование программных и программно-аппаратных средств защиты информации с административной поддержкой;

– обеспечение физической целостности программно-аппаратных средств информационных систем и поддержание необходимого уровня их защищенности;

– предоставление работникам минимально необходимых прав в информационной инфраструктуре согласно их должностным обязанностям;

– соблюдения всеми работниками требований организационно-распорядительных документов по вопросам ИБ;

– контроль соблюдения пользователями информационных систем требований по обеспечению ИБ;

– контроль состояния ИБ Центра;

– реагирование на инциденты ИБ;

– повышение осведомленности в вопросах обеспечения ИБ;

– персональная ответственность работников за свои действия при работе с информационными ресурсами Центра;

– анализ эффективности мер защиты информации и применяемых СЗИ;

– разработка и реализация предложений по совершенствованию систем защиты информации в Центре.

4.4. Оценку состояния защиты информации Центр проводит в соответствии с Методикой оценки показателя состояния защиты информации и обеспечения безопасности объектов критической информационной инфраструктуры Российской Федерации[1].

4.5. Минимально необходимый уровень защиты информации должен соответствовать составу мер, реализация которых предусмотрена нормативно-правовыми актами Российской Федерации[2], и который достаточен для блокирования (нейтрализации) типовых актуальных угроз безопасности информации.

5. Принципы защиты информации

Центр в своей деятельности руководствуется следующими принципами:

Законность. Все действия по обеспечению ИБ должны соответствовать действующему законодательству Российской Федерации в области защиты информации.

---

[1] Методика оценки показателя состояния защиты информации и обеспечения безопасности объектов критической информационной инфраструктуры Российской Федерации, утверждена ФСТЭК России 2 мая 2024 г. (далее – Методика)

[2] Требования к обеспечению защиты информации, содержащейся в информационных системах управления производством, используемых предприятиями оборонно-промышленного комплекса, утвержденные приказом ФСТЭК России от 28 февраля 2017 г. № 31.

Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, утвержденные приказом ФСТЭК России от 25 декабря 2017 г. № 239.

Требования к обеспечению защиты информации в автоматизированных системах управления производственными процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды, утвержденные приказом ФСТЭК России от 14 марта 2013 г. № 31.

Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденные приказом ФСТЭК России от 18 февраля 2013 г. № 21.

Каждый работник Центра должен осознавать свою ответственность за правонарушения в данной сфере.

Комплексность. Необходимо комплексное применение различных средств защиты информации, чтобы охватить все каналы реализации угроз. Защита должна включать физические, организационные, технологические и правовые меры. Это обеспечит инженерно-техническую защиту объектов, предотвратит несанкционированный доступ к компьютерам и серверам, разграничит доступ пользователей к информационным ресурсам.

Системность. Необходимо учитывать актуальные угрозы безопасности информации, возможные объекты и направления атак на нее со стороны нарушителей. Систему защиты информации строят с учетом не только известных каналов утечки информации, но и с учетом возможности появления новых уязвимостей в программном обеспечении.

Непрерывность. Создание системы защиты информации – постоянный процесс, требующий принятия мер на всех этапах жизненного цикла информационных систем, начиная с проектирования.

Идентификация и оценка активов. Все информационные активы должны быть идентифицированы и оценены по их значимости для задач Центра.

Контролируемость. Важна своевременная идентификация и предотвращение попыток нарушений правил ИБ. Постоянный мониторинг, выявление и устранение уязвимостей и контроль событий, влияющих на ИБ, являются неотъемлемой частью эффективной системы ИБ.

Анализ и совершенствование. Регулярную оценку эффективности и улучшение мер защиты информации и СЗИ проводят на основе анализа функционирования ИС, изменений в методах перехвата информации и новых нормативных требований.

Разделение функций. Пользователи должны иметь доступ только к тем информационным ресурсам, которые необходимы для выполнения их обязанностей. Запрещено совмещение функций в рамках одной роли, которое могло бы позволить одному работнику выполнять критически важные операции или иметь неконтролируемый доступ к системе.

Персональная ответственность. Ответственность за обеспечение безопасности информации лежит на каждом работнике в рамках его полномочий.

Взаимодействие и координация. Эффективную защиту информации достигают через взаимодействие и координацию отдела комплексной безопасности Центра, отдела информационных технологий и безопасности Центра с обособленными и структурными подразделениями Центра.

6. Объекты защиты

Основные информационные активы Центра, подлежащие защите:

Информация: служебная и коммерческая тайна, персональные данные, внутренние документы, иная чувствительная информация, представленная в любой форме.

Информационная инфраструктура: системы обработки и анализа информации, технические и программно-аппаратные средства, каналы информационного обмена, системы и средства защиты информации, а также помещения с чувствительными компонентами ИС.

Процессы обработки информации: технологии, регламенты, процедуры сбора, обработки, хранения и передачи информации, жизненный цикл ИС.

Перечень защищаемых информационных активов определяется по результатам инвентаризации и классификации, проводимой в соответствии с внутренними нормативно-правовыми документами Центра.

7. Основные угрозы

7.1. Основными угрозами являются:

- разглашение информации;
- компрометация информации, персональных идентификаторов, паролей;
- несанкционированный доступ к информации;

– нарушение полноты или доступности (блокировка) информации;
– повреждение или уничтожение носителей информации;
– уничтожение (утеря) информации;
– нарушение стабильности функционирования ИС;
– нештатные ситуации в работе программного обеспечения;
– вирусное заражение;
– злонамеренные действия через локальную сеть;
– атаки с использованием уязвимостей «нулевого дня»;
– отказ программно-технических мер защиты;
– нарушение работы технических мер защиты;
– несанкционированные или некорректные изменения в ИС;
– несанкционированное делегирование полномочий или использование привилегий;
– халатность и игнорирование правил ИБ, повышающие вероятность реализации угроз.

7.2. Источники угроз:

– **человеческий фактор**: внешние и внутренние нарушители (хакеры, бывшие работники, пользователи и обслуживающий персонал ИС);

– **природные и техногенные факторы**: стихийные бедствия и неблагоприятные техногенные условия.

7.3. Перечень угроз и нарушителей определяют в ходе моделирования угроз и закрепляют в Модели угроз ИС.

8. Организационная основа деятельности по обеспечению информационной безопасности

8.1. Организацию и контроль выполнения мероприятий в области обеспечения информационной безопасности осуществляет директор Центра или по его решению ответственное лицо[3].

8.2. В целях обеспечения защиты информации, содержащейся в ИС, функции по обеспечению ИБ возложены на отдел комплексной безопасности Центра (далее — Отдел).

8.3. Основные задачи Отдела:

– реализация Политики ИБ;
– определение требований к защите информации;
– координация мероприятий по защите информации во всех структурных и обособленных подразделениях Центра;
– контроль и оценка эффективности мер и средств защиты;
– методическая помощь работникам по вопросам ИБ;
– регулярная оценка и управление рисками ИБ;
– выбор и внедрение СЗИ;
– обеспечение минимально необходимого доступа к информационным ресурсам;
– обучение и повышение квалификации работников в сфере ИБ;
– расследование инцидентов ИБ;
– взаимодействие с Национальным координационным центром по компьютерным инцидентам (далее — НКЦКИ)[4].

8.4. Отдел (специалисты по защите информации) обеспечивает защиту информации, содержащейся в ИС, во взаимодействии с подразделениями (работниками), эксплуатирующими ИС, а также обеспечивающими функционирование ИС. Порядок взаимодействия Отдела с иными подразделениями (работниками) Центра регулируют внутренние регламенты, разрабатываемые в соответствии с настоящими Политикой.

---

[3] Пункт 1 Указа Президента Российской Федерации от 1 мая 2022 г. № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации».
[4] Регламент взаимодействия НКЦКИ и ФИЦ Коми НЦ УрО РАН утвержден 27.06.2024 г.

8.5. Отдел информационных технологий и безопасности (специалисты), а также работники обособленных подразделений Центра, обеспечивающие функционирование ИС, обеспечивают защиту информации в ходе сервисного обслуживания, настройки и технической поддержки, ремонта ИС и иных видов регламентных работ в объеме, установленном для них во внутренних регламентах и стандартах, разрабатываемых в соответствии с настоящей Политикой.

8.6. Структурные и обособленные подразделения (работники) Центра, эксплуатирующие ИС, принимают меры, направленные на защиту информации, в ходе их эксплуатации в объеме, установленном для них во внутренних регламентах и стандартах, разрабатываемых в соответствии с настоящими Политикой.

8.7. С учетом структуры и состава Отдела для выполнения отдельных функций по защите информации, содержащихся в ИС, Центр может привлекать организации, имеющие лицензию на деятельность по технической защите конфиденциальной информации.

8.8. Внутренние регламенты, разрабатываемые и утвержденные в Центре, должны содержать порядок проведения мероприятий по защите информации, содержащейся в ИС, перечень лиц, участвующих в реализации этих мероприятий, и порядок их взаимодействия.

8.9. Внутренние регламенты содержат следующие меры:

– порядок обеспечения защиты информации на стадиях жизненного цикла ИС;

– порядок предоставления удаленного доступа к ИС работникам Центра, а также лицам, не являющимся работниками Центра;

– порядок предоставления доступа к ИС подрядных организаций и (или) передачи им информации, содержащейся в ИС;

– порядок обращения с информаций, для которой в соответствии с Федеральными законами установлены требования к обеспечению ее конфиденциальности, и ее носителями;

– порядок доступа работников Центра к сети «Интернет» и ее использования, взаимодействия с иными внешними информационно-телекоммуникационными сетями и ИС;

– порядок обучения и повышения уровня осведомленности работников Центра в области защиты информации;

– порядок выявления, оценки и устранения уязвимостей ИС;

– порядок обновления программного обеспечения;

– порядок предоставления внутренним и внешним пользователям сервисов, доступ к которым осуществляется с использованием сети «Интернет»;

– порядок мониторинга информационной безопасности ИС;

– порядок проведения инвентаризации ИС и управления их конфигурацией;

– порядок заведения, контроля и блокирования учетных записей пользователей, средств аутентификации в ИС;

– порядок администрирования ИС;

– порядок контроля за обеспечением уровня защищенности информации.

8.10. Внутренние стандарты в Центре устанавливают следующие требования:

– к первичной идентификации пользователей;

– к конфигурации и настройкам программных, программно-аппаратных средств;

– к защите средств вычислительной техники внутренних пользователей, имеющих постоянный доступ к сети «Интернет»;

– к сбору, регистрации и анализу событий, связанных с нарушением безопасности информации или нарушением функционирования ИС;

– к применяемым моделям доступа пользователей.

8.11. Внутренние регламенты и стандарты утверждаются приказом Центра. Эти документы доводятся до сведения всех работников Центра, а также подрядных организаций, если они затрагивают их интересы.

8.12. Отдел (специалисты по защите информации) своевременно разрабатывает и представляет руководству Центра (ответственному лицу) обоснованные предложения о ресурсах, необходимых для проведения мероприятий и реализации мер по защите

информации. В обоснование этих предложений включаются сведения о целях защиты информации, показателях её эффективности, для достижения которых нужны ресурсы, а также о прогнозируемых негативных последствиях (ущербе), которые могут наступить в случае отказа в выделении ресурсов.

8.13. Деятельность по защите информации предусматривает реализацию Отделом следующих мероприятий:

– разработка и планирование мероприятий по защите информации;

– проведение мероприятий по защите информации;

– оценка состояния защиты информации;

– совершенствование защиты информации.

8.14. При разработке и планировании мероприятий по защите информации Отдел:

– определяет события в ИС, наступление которых может привести к нарушению целей защиты информации, установленных в настоящей Политике;

– определяет ИС, их программные, программно-аппаратные средства, несанкционированный доступ к которым и (или) воздействие на которые может привести к нарушению целей защиты информации;

– выявляет и оценивает угрозы безопасности информации, реализация (возникновение) которых может привести к нарушению целей защиты информации;

– планирует к реализации меры по защите информации, направленные на защиту от актуальных угроз безопасности информации, и оцениваются необходимые для этого ресурсы.

8.15. Проведение мероприятий по защите информации, содержащейся в ИС, должно обеспечивать достижение целей защиты информации и показателей эффективности их достижения, установленных в настоящей Политике, препятствовать наступлению негативных последствий (ущербу) для Центра. В зависимости от целей защиты информации мероприятия по защите информации должны быть направлены на:

– исключение утечки конфиденциальной информации;

– предотвращение несанкционированного доступа к ИС и содержащейся в них информации, своевременное обнаружение фактов такого несанкционированного доступа и реагирование на них;

– недопущение воздействий на ИС и содержащуюся в них информацию;

– недопущение нецелевого использования ИС и содержащейся в них информации;

– обеспечение возможности восстановления в установленные сроки доступа авторизованных пользователей к ИС и содержащейся в них информации, заблокированной вследствие реализации (возникновения) угроз безопасности информации;

– обеспечение возможности восстановления в установленные сроки информации, модифицированной или уничтоженной вследствие реализации (возникновения) угроз безопасности информации;

– контроль уровня защищенности ИС и содержащейся в них информации.

8.16. Оценку состояния защиты информации в Центре проводят на основе показателя, характеризующего текущее состояние защиты информации от актуальных угроз безопасности информации.

8.17. Показатели состояния защиты информации являются ключевыми показателями эффективности деятельности по защите информации в Центре[5].

Периодичность и порядок проведения оценки состояния защищенности устанавливают во внутренних регламентах (организационно-распорядительной документации) и составляет не реже одного раза в шесть месяцев. Кроме того, предусмотрена внеочередная оценка состояния защищенности в случаях:

– возникновения инцидента ИБ, повлекшего наступление негативных последствий (возникновение значимого инцидента);

---

[5] Для расчета значений показателей состояния защиты информации применяется методические документы, утвержденные ФСТЭК России.

– развития (изменения) архитектуры ИС;
– запроса директора Центра о текущем значении показателя защищенности;
– запроса ФСТЭК России или Минобрнауки России.

8.18. Отдел информирует директора Центра о результатах оценки показателей состояния защиты информации. Если эти показатели не соответствуют установленным нормам, то Отдел представляет информацию директору Центра с целью принятия решения о необходимости совершенствования системы защиты информации, содержащейся в ИС.

8.19. Процесс совершенствования системы защиты информации осуществляется на основе анализа результатов оценки показателей состояния защиты информации Центра. По указанию директора Центра Отдел разрабатывает план мероприятий по улучшению защиты информации совместно с подразделениями (работниками), которые эксплуатируют ИС и обеспечивают ее функционирование.

9. Основные требования по защите информации

Система защиты информации в Центре предусматривает принятие комплекса организационных и технических мер. Выполнение требований достигается за счет внедрения на объектах информатизации следующих мер:

– управление доступом;
– категорирование и обработка информации;
– физическая безопасность;
– области, ориентированные на конечного пользователя (информационные активы, передача информации, дистанционная работа, ограничения в работе);
– резервное копирование;
– защита от вредоносного кода (антивирусная защита);
– криптография;
– безопасность коммуникаций;
– конфиденциальность и защита персональных данных;
– регистрация и мониторинг событий;
– управление инцидентами информационной безопасности и информирование о компьютерном инциденте;
– взаимодействие с третьими лицами.

9.1. Управление доступом

В целях обеспечения безопасности и устойчивого функционирования информационной инфраструктуры осуществляют управление доступом пользователей к ее информационным ресурсам, прикладным системам и соответствующим техническим средствам объектов защиты.

Пользователей наделяют минимальными правами доступа и привилегиями, необходимыми им для выполнения служебных задач.

Порядок управления доступом пользователей, включая удаленный доступ, регулируют нормативные и организационно-распорядительные документы Центра в области ИБ.

9.2. Категорирование и обработка информации

Информацию классифицируют в соответствии с нормативными требованиями, ценностью, критичностью и чувствительностью к несанкционированному раскрытию или изменению.

Каждому уровню защищенности присваивают соответствующий индекс. Категорирование информации и связанные меры защиты пересматривают в соответствии с изменениями в законодательстве Российской Федерации и требованиями регуляторов.

9.3. Физическая безопасность

Физическая защита объектов информационной инфраструктуры.

В целях предотвращения несанкционированного доступа к объектам защиты информационной инфраструктуры Центра обеспечивают физическую защиту мест их эксплуатации (размещения).

Технические средства обработки, хранения и передачи информации размещают в запираемых шкафах, располагаемых в специализированных помещениях, доступ посторонних лиц к которым ограничивают.

Защита территорий, зданий и помещений.

В целях обеспечения защиты информации и технических средств обработки, хранения и передачи информации обеспечивают защиту территорий, зданий и помещений Центра:

– устанавливают пропускной режим, препятствующий бесконтрольному посещению его охраняемых помещений;

– порядок посещения и поведения в зданиях и помещениях Центра регламентируют нормативными и организационно-распорядительными документами Центра в области ИБ;

– здания и помещения Центра обеспечивают техническими средствами охраны, системами контроля доступа и пожарной безопасности.

При проведении работ на охраняемых территориях Центра, в его зданиях и защищаемых помещениях третьими лицами обеспечивают контроль их деятельности.

Порядок защиты помещений, в которых располагаются технические средства (серверы, сетевое оборудование и средства защиты информации), определяют внутренними регламентами Центра.

9.4. Области, ориентированные на конечного пользователя

Работников Центра и внешних пользователей, использующих или имеющих доступ к информационным активам Центра, осведомляют о требованиях ИБ. Они несут ответственность за неправомерное использование ими любых ресурсов обработки информации и любое подобное использование, осуществляемое в зоне их ответственности.

В целях предотвращения несанкционированного доступа, а также компрометации или утраты информации и средств обработки информации определяют ответственность пользователей за соблюдение правил доступа при использовании автоматизированного рабочего места.

Пользователи несут ответственность за соблюдение установленных правил при выборе и использовании паролей. Запрещено записывать пароли в открытом виде, документы и носители с конфиденциальной информацией необходимо убирать в сейфы (шкафы) при уходе с рабочего места.

Пользователям запрещено работать под чужими учетными записями, а также сообщать свои пароли и передавать средства аутентификации другим пользователям.

Парольная политика и правила использования паролей определены нормативными и организационно-распорядительными документами Центра.

9.5. Резервное копирование

В целях обеспечения возможности восстановления информационных ресурсов в случае их утраты или нарушения целостности в Центре осуществляют их резервное копирование. Должна быть обеспечена целостность создаваемых резервных копий.

Способ и периодичность резервного копирования, сроки хранения резервных копий определяют в зависимости от назначения и особенностей системы, в которой информация обрабатывается, а также от ценности информации.

Порядок резервного копирования информационных ресурсов регламентируют отдельным внутренним документом.

9.6. Защита от вредоносного кода

Для защиты от вредоносных программ в Центре реализуют меры обеспечения ИБ, связанные с обнаружением, предотвращением и восстановлением инфраструктуры, в сочетании с соответствующим информированием пользователей.

Защита от вредоносных программ основана на применении программного обеспечения для обнаружения вредоносных программ, осведомленности работников в части

требований ИБ, соответствующих мерах контроля доступа к системе и управлению изменениями.

9.7. Криптография

В целях обеспечения конфиденциальности, целостности и аутентичности обрабатываемой, хранимой и передаваемой информации в информационной инфраструктуре Центра применяют сертифицированные установленным порядком криптографические средства защиты.

Электронные документы, для которых необходимо обеспечить целостность и аутентичность, защищают с помощью электронной цифровой подписи.

Порядок применения средств криптографической защиты определяют нормативными и организационно-распорядительными документами Центра.

9.8. Безопасность коммуникаций

В Центре реализуют меры для обеспечения безопасности информации в сетях и защиты подключенных сервисов от несанкционированного доступа. В частности, учитывают следующие ключевые меры:

– определяют обязанности и процедуры управления сетевым оборудованием;

– устанавливают специальные меры обеспечения ИБ для защиты конфиденциальности, целостности и доступности данных, передаваемых по сетям общего пользования или беспроводным сетям, в том числе для защиты подключенных систем и приложений;

– пользователи, с целью доступа к системам и сетям Центра проходят процедуру аутентификации и авторизации;

– вводят необходимые ограничение на подключение систем к корпоративным сетям.

9.9. Конфиденциальность и защита персональных данных

Центр уделяет особое внимание защите персональных данных и считает подобную информацию одним из важнейших активов. В Центре устанавливают порядок защиты персональных данных работников, предусматривающий правовые, организационные и технические меры.

Перечень мер по защите персональных данных регламентируется Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных».

Работников, ответственных за обработку и обеспечение безопасности персональных данных, назначают приказом Центра.

Порядок работы с персональными данными и их защиты в Центре регулируют Политика в отношении обработки персональных данных, а также нормативные и организационно-распорядительные документы Центра.

9.10. Регистрация и мониторинг событий

Центр осуществляет регулярный мониторинг и регистрацию системных событий, действий пользователей и администраторов, ошибок и событий ИБ.

Все зарегистрированные события анализируют на предмет наличия признаков инцидента ИБ, создают механизмы, позволяющие оценивать и отслеживать типы инцидентов, их масштаб и связанные с ними затраты.

Вопросы регистрации и мониторинга событий регламентированы отдельным внутренним документом Центра.

9.11. Управление инцидентами информационной безопасности и информирование о компьютерных инцидентах

Центр осуществляет уведомление о происшествиях в области ИБ, а также реагирует на такие происшествия, включающие в себя действия, которые следует выполнять при поступлении сообщений о происшествии.

Всех работников Центра Отдел ознакамливает с процедурой уведомления, а в их обязанностях закрепляют максимально быструю передачу информации о происшествиях.

Центр, являясь субъектом критической информационной инфраструктуры, информирует ФСБ России обо всех компьютерных инцидентах, связанных

с функционированием принадлежащих ему объектов критической информационной инфраструктуры.

Информирование осуществляют путем направления информации в НКЦКИ в соответствии с Регламентом взаимодействия НКЦКИ и Центром.

9.12. Взаимодействие с третьими лицами

При организации доступа сторонних организаций к защищаемым информационным ресурсам в Центре осуществляют мероприятия по обеспечению ИБ:

– определение рисков, связанных с предоставлением доступа сторонней организации к конфиденциальной информации;

– формирование на основе оценки рисков перечня мероприятий по обеспечению ИБ при предоставлении доступа сторонней организации к конфиденциальной информации Центра и их реализация;

– заключение соглашения о конфиденциальности со сторонними организациями, которым предоставляют доступ к конфиденциальной информации Центра.

Допуск на объекты защиты Центра представителей сторонней организации регламентируют нормативными, организационно-распорядительными и информационными документами Центра в области ИБ.

10. Порядок утверждения, внесение изменений и дополнений

10.1. Политика может быть пересмотрена в случае изменении целей и задач Центра в области обеспечения ИБ, функций подразделения, ответственного за ИБ, или изменении требований законодательства Российской Федерации и требований Регулятора в области ИБ.

10.2. Внесение изменений в настоящую Политику, а также ее актуализация и утверждение, осуществляют с периодичностью не реже одного раза в пять лет. При актуализации Политики учитывают результаты контроля эффективности обеспечения ИБ за предыдущий период.

Процедура актуализации Политики включает:

– анализ и выявление несоответствий действующей Политики текущим условиям;

– разработка предложений по совершенствованию Политики;

– утверждение новой редакции Политики.

При осуществлении процедуры актуализации учитывают:

– результаты контроля состояния ИБ и предложения структурных и обособленных подразделений Центра о совершенствовании процедур обеспечения ИБ;

– изменения в организационной структуре и информационной инфраструктуре Центра;

– изменения в законодательной и нормативной базе в части ИБ, произошедшие с момента утверждения предыдущей Политики;

– результаты анализа произошедших инцидентов ИБ, а также уязвимости и угрозы, выявленные в Центре за время, прошедшее с момента утверждения предыдущей Политики;

– изменения в управлении ИБ, включая изменения в распределении ресурсов и обязанностей при обеспечении ИБ.

11. Ответственность за соблюдение положений Политики

11.1. Руководство Центра отвечает за состояние ИБ в Центре и обеспечивает реализацию Политики, включая регулярный контроль ее исполнения, выделение необходимых для обеспечения ИБ ресурсов.

11.2. Ответственность за поддержание положений настоящей Политики в актуальном состоянии, создание, внедрение, координацию и внесение изменений в процесс системы информационной безопасности, а также организацию осведомленности и обучения работников в области обеспечения ИБ лежит на руководстве Отдела.

11.3. Ответственность за обеспечение ИБ объектов защиты Центра возложена на работников, ответственных за их эксплуатацию.

Работники Центра обязаны:

– соблюдать требования настоящей политики ИБ и других нормативных и организационно-распорядительных документов Центра в области ИБ;

– использовать технические средства обработки информации только в служебных целях;

– осуществлять информирование Отдела о выявленных инцидентах ИБ.

11.4. Работникам Центра запрещено нарушать установленные правила обеспечения ИБ и скрывать факты возникновения инцидентов ИБ.

11.5. Работники Центра, не выполняющие требования настоящей политики ИБ или требования нормативных и организационно-распорядительных документов Центра в области ИБ, могут быть привлечены к ответственности в установленном порядке.