КОМИТЕТ СТАВРОПОЛЬСКОГО КРАЯ
ПО ДЕЛАМ АРХИВОВ

ПРИКАЗ

31.12.2013 № **146**

г. Ставрополь

Об утверждении Политики информационной безопасности комитета Ставропольского края по делам архивов

В соответствии Федеральными законами от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации», от 27 июля 2006 года № 152-ФЗ «О персональных данных», от 28 октября 2012 года № 390-ФЗ «О безопасности»

ПРИКАЗЫВАЮ:

1. Утвердить прилагаемую Политику информационной безопасности комитета Ставропольского края по делам архивов.

2. Контроль за исполнением настоящего приказа возложить на заместителя председателя комитета Болотову В.Е.

Председатель комитета Е.И.Долгова

УТВЕРЖДЕНА
приказом комитета
Ставропольского края
по делам архивов
от 31.12.2013 № 146

Политика
информационной безопасности
комитета Ставропольского края по делам архивов

Содержание

1. Вводные положения

1.1. Введение

Политика информационной безопасности комитета Ставропольского края по делам архивов (далее – Комитет) определяет цели и задачи системы обеспечения информационной безопасности (далее – ИБ) и устанавливает совокупность правил, требований и руководящих принципов в области ИБ, которыми руководствуется Комитет в своей деятельности.

1.2. Цели

Основными целями политики ИБ являются защита информации Коми-

тета и обеспечение эффективной работы всего информационно-вычислительного комплекса при осуществлении деятельности, указанной в его Положении.

Общее руководство обеспечением ИБ осуществляет заместитель председателя комитета. Ответственность за организацию мероприятий по обеспечению ИБ и контроль за соблюдением требований ИБ несет сотрудник, отвечающий за функционирование автоматизированной системы и выполняющий функции администратора информационной безопасности (далее - администратор информационной безопасности).

Руководители структурных подразделений комитета ответственны за обеспечение выполнения требований ИБ в своих подразделениях.

Сотрудники комитета обязаны соблюдать порядок обращения с конфиденциальными документами, носителями ключевой информации и другой защищаемой информацией, соблюдать требования настоящей Политики и других документов ИБ.

1.3. Задачи

Политика информационной безопасности направлена на защиту информационных активов от угроз, исходящих от противоправных действий злоумышленников, уменьшение рисков и снижение потенциального вреда от аварий, непреднамеренных ошибочных действий персонала, технических сбоев, неправильных технологических и организационных решений в процессах обработки, передачи и хранения информации и обеспечение нормального функционирования технологических процессов.

Риск аварий и технических сбоев определяется состоянием технического парка, надежностью систем энергоснабжения и телекоммуникаций, квалификацией персонала и его способностью к адекватным действиям в нештатной ситуации.

Разработанная на основе прогноза политика ИБ и в соответствии с ней построенная система управления ИБ является наиболее правильным и эффективным способом добиться минимизации рисков нарушения ИБ для Комитета. Необходимо учитывать, что с течением времени меняется характер угроз, поэтому следует своевременно, используя данные мониторинга и аудита, обновлять модели угроз и нарушителя.

Стратегия обеспечения ИБ заключается в использовании заранее разработанных мер противодействия возможным атакам, а также программно-технических и организационных решений, позволяющих свести к минимуму возможные потери от технических аварий и ошибочных действий персонала.

Задачами настоящей политики являются:

- описание организации системы управления информационной безопасностью в Комитете;
- определение Политик информационной безопасности, а именно:
  - Политика реализации антивирусной защиты;
  - Политика учетных записей;
  - Политика предоставления доступа к информационному ресур-

су;

- Политика защиты АРМ;
- Политика использования паролей;
- Политика конфиденциального делопроизводства;
- определение порядка сопровождения ИС Комитета.

1.4. Область действия

Настоящая Политика распространяется на все структурные подразделения Комитета и обязательна для исполнения всеми его сотрудниками и должностными лицами. Положения настоящей Политики применимы для использования во внутренних нормативных и методических документах, а также в договорах.

1.5. Период действия и порядок внесения изменений

Настоящая политика вводится в действие приказом председателя Комитета.

Политика признается утратившей силу на основании приказа председателя Комитета.

Изменения в политику вносятся приказом председателя Комитета.

Инициаторами внесения изменений в политику информационной безопасности являются:

- заместитель председателя;
- администратор информационной безопасности.

Плановая актуализация настоящей политики производится ежегодно и имеет целью приведение в соответствие определенных политикой защитных мер реальным условиям и текущим требованиям к защите информации.

Внеплановая актуализация политики информационной безопасности производится в обязательном порядке в следующих случаях:

- при изменении политики Российской Федерации в области информационной безопасности, указов и законов Российской Федерации в области защиты информации;
- при изменении внутренних нормативных документов (инструкций, положений, руководств), касающихся информационной безопасности Комитета;
- при происшествии и выявлении инцидента (инцидентов) по нарушению информационной безопасности, влекущего ущерб Комитету.

Ответственными за актуализацию политики информационной безопасности (плановую и внеплановую) несет администратор информационной безопасности.

Контроль за исполнением требований настоящей политики и поддержанием ее в актуальном состоянии возлагается на администратора информационной безопасности.

2. Термины и определения

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

Администратор информационной безопасности – сотрудник Комитета, осуществляющий контроль за обеспечением защиты информации, а также осуществляющий организацию работ по выявлению и предупреждению возможных каналов утечки информации, потенциальных возможностей осуществления НСД к защищаемой информации.

Анализ риска – систематическое использование информации для определения источников и оценки риска.

Аудит информационной безопасности – процесс проверки выполнения установленных требований по обеспечению информационной безопасности. Может проводиться как самим обществом (внутренний аудит), так и с привлечением независимых внешних организаций (внешний аудит). Результаты проверки документально оформляются свидетельством аудита.

Аутентификация – проверка принадлежности субъекту доступа предъявленного им идентификатора; подтверждение подлинности. Чаще всего аутентификация выполняется путем набора пользователем своего пароля на клавиатуре компьютера.

Доступ к информации – возможность получения информации и ее использования.

Защищенный канал передачи данных – логические и физические каналы сетевого взаимодействия, защищенные от прослушивания потенциальными злоумышленниками средствами шифрования данных, либо путем их физической изоляции и размещения на охраняемой территории.

Идентификатор доступа – уникальный признак субъекта или объекта доступа.

Идентификация – присвоение субъектам доступа (пользователям, процессам) и объектам доступа (информационным ресурсам, устройствам) идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Информация – это актив, который, подобно другим активам общества, имеет ценность и, следовательно, должен быть защищен надлежащим образом.

Информационная безопасность – механизм защиты, обеспечивающий конфиденциальность, целостность, доступность информации; состояние защищенности информационных активов общества в условиях угроз в информационной сфере. Угрозы могут быть вызваны непреднамеренными ошибками персонала, неправильным функционированием технических средств, стихийными бедствиями или авариями (пожар, наводнение, отключение электроснабжения, нарушение телекоммуникационных каналов и т.п.), либо преднамеренными злоумышленными действиями, приводящими к нарушению информационных активов Комитета.

Информационная система – совокупность программного обеспечения и технических средств, используемых для хранения, обработки и передачи информации, с целью решения задач подразделений Комитета. В Комитете используются различные типы информационных систем для решения управленческих, учетных и других задач.

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

Информационные активы - информационные системы, информационные средства, информационные ресурсы.

Информационные средства – программные, технические, лингвистические, правовые, организационные средства (программы для электронных вычислительных машин; средства вычислительной техники и связи; словари, тезаурусы и классификаторы; инструкции и методики; положения, уставы, должностные инструкции; схемы и их описания, другая эксплуатационная и сопроводительная документация), используемые или создаваемые при проектировании информационных систем и обеспечивающие их эксплуатацию.

Информационные ресурсы – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий.

Инцидент информационной безопасности – действительное, предпринимаемое или вероятное нарушение информационной безопасности, приводящее к нарушению доступности, конфиденциальности и целостности информационных активов Комитета.

Источник угрозы – намерение или метод, нацеленный на умышленное использование уязвимости, либо ситуация или метод, которые могут случайно проявить уязвимость.

Конфиденциальная информация – информация с ограниченным доступом, не содержащая сведений, составляющих государственную тайну, доступ к которой ограничивается в соответствии с законодательством Российской Федерации.

Конфиденциальность – доступ к информации только авторизованных пользователей.

Критичная информация – информация, нарушение доступности, целостности, либо конфиденциальности которой, может оказать негативное влияние на функционирование подразделений Комитета, привести к причинению Организации материального или иного вида ущерба.

Локальная вычислительная сеть (ЛВС) – группа ЭВМ, а также периферийное оборудование, объединенные одним или несколькими автономными высокоскоростными каналами передачи цифровых данных в пределах одного или нескольких близлежащих зданий.

Межсетевой экран (МЭ) – программно-аппаратный комплекс, используемый для контроля доступа между ЛВС, входящими в состав сети, а также между сетью Комитета и внешними сетями (сетью Интернет).

Мониторинг информационной безопасности – постоянное наблюдение

за объектами, влияющими на обеспечение информационной безопасности, сбор, анализ и обобщение результатов наблюдения под заданные цели. Объектом мониторинга в зависимости от целей может быть автоматизированная система или ее часть, информационные технологические процессы учреждения, информационные услуги Комитета и пр.

Несанкционированный доступ к информации (НСД) – доступ к информации, нарушающий правила разграничения уровней полномочий пользователей.

Обработка риска – процесс выбора и осуществления мер по модификации риска.

Остаточный риск – риск, остающийся после обработки риска.

Политика информационной безопасности – комплекс взаимоувязанных руководящих принципов и разработанных на их основе правил, процедур и практических приемов, принятых в учреждении для обеспечения его информационной безопасности.

Пользователь ЛВС – сотрудник Комитета (штатный, временный, работающий по контракту и т.п.), а также прочие лица (подрядчики, аудиторы и т.п.), зарегистрированный в сети в установленном порядке и получивший права на доступ к ресурсам сети в соответствии со своими функциональными обязанностями.

Принятие риска – решение принять риск.

Программное обеспечение – совокупность прикладных программ, установленных на сервере или ЭВМ.

Рабочая станция – персональный компьютер, на котором пользователь сети выполняет свои служебные обязанности.

Регистрационная (учетная) запись пользователя – включает в себя имя пользователя и его уникальный цифровой идентификатор, однозначно идентифицирующий данного пользователя в операционной системе (сети, базе данных, приложении и т.п.). Регистрационная запись создается администратором при регистрации пользователя в операционной системе компьютера, в системе управления базами данных, в сетевых доменах, приложениях и т.п. Она также может содержать такие сведения о пользователе, как Ф.И.О., название подразделения, телефоны, E-mail и т.п.

Роль – совокупность полномочий и привилегий на доступ к информационному ресурсу, необходимых для выполнения пользователем определенных функциональных обязанностей.

Система менеджмента информационной безопасности (СМИБ) – та часть общей системы менеджмента, которая основана на подходе бизнес-рисков при создании, внедрении, функционировании, мониторинге, анализе, поддержке и совершенствовании информационной безопасности.

Системный администратор – сотрудник Комитета, занимающийся сопровождением автоматизированных систем, отвечающий за функционирование локальной сети учреждения и ПК.

Список контроля доступа (ACL) – правила фильтрации сетевых пакетов, настраиваемые на маршрутизаторах и МЭ, определяющие критерии

фильтрации и действия, производимые над пакетами.

Собственник – лицо или организация, которые имеют утвержденные обязательства по менеджменту для контроля разработки, поддержки, использования и безопасности активов. Термин «собственник» не означает, что лицо действительно имеет какие-либо права собственности на актив.

Средства криптографической защиты информации – средства шифрования, средства имитозащиты, средства электронной подписи, средства кодирования, средства изготовления ключевых документов (независимо от вида носителя ключевой информации), ключевые документы (независимо от вида носителя ключевой информации).

Угрозы информационным данным – потенциально существующая опасность случайного или преднамеренного разрушения, несанкционированного получения или модификации данных, обусловленная структурой системы обработки, а также условиями обработки и хранения данных, т.е. это потенциальная возможность источника угроз успешно выявить определенную уязвимость системы.

Управление информационной безопасностью – совокупность целенаправленных действий, осуществляемых в рамках политики информационной безопасности в условиях угроз в информационной сфере, включающая в себя оценку состояния объекта управления (например, оценку и управление рисками), выбор управляющих воздействий и их реализацию (планирование, внедрение и обслуживание защитных мер).

Уязвимость – недостатки или слабые места информационных активов, которые могут привести к нарушению информационной безопасности учреждения при реализации угроз в информационной сфере.

Целостность информации – состояние защищенности информации, характеризуемое способностью АС обеспечивать сохранность и неизменность конфиденциальной информации при попытках несанкционированных или случайных воздействий на нее в процессе обработки или хранения.

ЭВМ – электронная - вычислительная машина, персональный компьютер.

Электронная подпись - информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.

3. Обозначения и сокращения

АРМ - Автоматизированное рабочее место.
АС - Автоматизированная система.
БД - База данных.
ЗИ - Защита информации.
ИБ - Информационная безопасность.
ИС - Информационная система.
ИТС - Информационно-телекоммуникационная система.

КЗ - Контролируемая зона.
МЭ - Межсетевой экран.
НСД - Несанкционированный доступ.
ОС - Операционная система.
ПБ - Политики безопасности.
ПО - Программное обеспечение.
СВТ - Средства вычислительной техники.
СЗИ - Средство защиты информации.
СКЗИ - Средство криптографической защиты информации.
СПД - Система передачи данных.
СУБД - Система управления базами данных.
СУИБ - Система управления информационной безопасностью.
СЭД - Система электронного документооборота.
ЭВМ - Электронная - вычислительная машина, персональный компьютер.
ЭП - Электронная подпись.

4. Политика информационной безопасности Комитета

4.1.Назначение политики информационной безопасности

Политика информационной безопасности Комитета - это совокупность норм, правил и практических рекомендаций, на которых строится управление, защита и распределение информации в Комитете.

Под политикой безопасности понимается совокупность документированных управленческих решений, направленных на защиту информации и ассоциированных с ней ресурсов.

Политики информационной безопасности относятся к административным мерам обеспечения информационной безопасности и определяют стратегию Организации в области ИБ.

Политика информационной безопасности (далее, ПБ) регламентирует эффективную работу средств защиты информации. Она охватывает все особенности процесса обработки информации, определяя поведение ИС и ее пользователей в различных ситуациях. Политика информационной безопасности реализуется посредством административно-организационных мер, физических и программно-технических средств и определяет архитектуру системы защиты.

4.2.Основные принципы обеспечения ИБ

Основными принципами обеспечения ИБ являются следующие:

- Постоянный и всесторонний анализ информационного пространства общества с целью выявления уязвимостей информационных активов.
- Своевременное обнаружение проблем, потенциально способных повлиять на ИБ общества, корректировка моделей угроз и нарушителя.

- Разработка и внедрение защитных мер, адекватных характеру выявленных угроз, с учетом затрат на их реализацию. При этом меры, принимаемые для обеспечения ИБ, не должны усложнять достижение уставных целей Комитета, а также повышать трудоемкость технологических процессов обработки информации.
- Контроль эффективности принимаемых защитных мер.
- Персонификация и адекватное разделение ролей и ответственности между сотрудниками учреждения, исходя из принципа персональной и единоличной ответственности за совершаемые операции.

4.3.Соответствие ПБ действующему законодательству

Правовую основу политики составляют законы Российской Федерации и другие нормативные правовые акты, определяющие права и ответственность граждан, сотрудников и государства в сфере безопасности, а также нормативные, отраслевые и ведомственные документы, по вопросам безопасности информации, утвержденные органами государственного управления различного уровня в пределах их компетенции.

4.4.Ответственность за реализацию политики информационной безопасности

Ответственность за разработку мер и контроль обеспечения защиты информации несёт администратор информационной безопасности.

Ответственность за реализацию политики возлагается:

- в части, касающейся разработки и актуализации правил внешнего доступа и управления доступом, антивирусной защиты, а также доведения правил политики до сотрудников Комитета - на администратора информационной безопасности;
- в части, касающейся исполнения правил политики, - на каждого сотрудника Комитета, согласно должностным и функциональным обязанностям, и иных лиц, попадающих под область действия настоящей политики.

4.5.Порядок подготовки персонала по вопросам информационной безопасности и допуска его к работе

Организация просвещения сотрудников Комитета в области информационной безопасности возлагается на администратора информационной безопасности. Обучение сотрудников Комитета правилам обращения с конфиденциальной информацией, проводится путем самостоятельного изучения сотрудниками внутренних нормативных документов Комитета.

Допуск сотрудников к работе с защищаемыми информационными ресурсами Комитета осуществляется только после его ознакомления с настоящей политикой, а также после ознакомления пользователей другими внутренними документами, затрагивающими работу с информационными системами.

Правила допуска к работе с информационными ресурсами лиц, не являющихся сотрудниками Комитета, определяются на договорной основе с этими лицами или с организациями, представителями которых являются эти лица.

4.6.Защищаемые информационные ресурсы Комитета

Различаются следующие категории информационных ресурсов, подлежащих защите в Комитете:

Конфиденциальная – информация, определенная в соответствии с Федеральным Законом от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», от 27.07.2006 г. № 152-ФЗ «О персональных данных», указом президента Российской Федерации от 06.03.1997 г. №188 «Об утверждении перечня сведений конфиденциального характера», постановлением правительства Российской Федерации от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», предусмотренная Перечнем сведений конфиденциального характера.

Публичная - информация, получаемая из публичных источников (публикации в СМИ, теле и радиовещание и т.д.). Информация, предназначенная для размещения на внешних публичных ресурсах;

Открытая - информация, полученная от физических или юридических лиц, запрет на распространение и обработку которой был ими официально снят. Информация, сформированная в результате деятельности Комитета, которую запрещено относить конфиденциальной на основании законодательства РФ. Информация, представляемая в публичный доступ, используемая в хозяйственной деятельности Комитета;

Ограниченного доступа - информация, не попадающая под остальные категории, доступ к которой должен быть ограничен определенной категории лиц.

Конфиденциальная информация представляет собой сведения ограниченного доступа, включая персональные данные, для которых в качестве основной угрозы безопасности рассматривается нарушение конфиденциальности путем раскрытия ее содержимого третьим лицам, не допущенным в установленном порядке к работе с этой информацией.

Правила отнесения информации к конфиденциальной и порядок работы с конфиденциальными документами, определяются нормативно-правовыми актами Российской Федерации, а также внутренними документами Комитет.

Подходы к решению проблемы защиты информации в Комитете, в общем виде, сводятся к исключению неправомерных или неосторожных действий со сведениями, относящимися к информации ограниченного распространения, а также с информационными ресурсами, являющимися критичными для обеспечения функционирования процессов Комитета.

Для этого в Комитете выполняются следующие мероприятия:

- определяется порядок работы с документами, образцами изделиями

и др., содержащими конфиденциальные сведения;
- устанавливается круг лиц и порядок доступа к подобной информации;
- вырабатываются меры по контролю обращения с документами, содержащими конфиденциальные сведения.

Защита конфиденциальной информации, принадлежащей третьей стороне, осуществляется на основании договоров, заключаемых Комитетом с другими организациями. Персональные данные сотрудника Комитета - информация, необходимая Комитету в связи с трудовыми отношениями и касающаяся конкретного сотрудника.

Согласно п. 7 ст. 86 Трудового кодекса РФ защита персональных данных сотрудника от неправомерного их использования или утраты должна быть обеспечена работодателем за счет его средств в порядке, установленном федеральным законом.

Согласно ст. 88 Трудового кодекса РФ при передаче персональных данных сотрудника работодатель должен соблюдать следующие требования:
- осуществлять передачу персональных данных сотрудника в пределах одной организации в соответствии с локальным нормативным актом Комитета, с которым сотрудник должен быть ознакомлен под расписку;
- разрешать доступ к персональным данным сотрудников только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные сотрудника, которые необходимы для выполнения конкретных функций.

Согласно ст. 90 Трудового кодекса РФ лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных сотрудника, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с федеральными законами.

4.7.Организация системы управления информационной безопасностью Комитета

4.7.1. Организация системы управления ИБ

Система управления информационной безопасностью Комитета (СУИБ) предназначенная для создания, реализации, эксплуатации, мониторинга, анализа, поддержки и повышения информационной безопасности Комитета.

Для успешного функционирования СУИБ Комитета должны быть реализованы следующие процессы:
- определение и уточнение области действия СУИБ и выбор подхода к оценке рисков ИБ.
- определение и уточнение области действия СУИБ должно осуществляться на основе результатов оценки рисков, связанных с основной деятельностью Комитета, а также оценки правовых

рисков деятельности Комитета;

- анализ и оценка рисков ИБ, варианты обработки рисков ИБ для наиболее критичных информационных активов.
- выбор и уточнение целей ИБ и защитных мер и их обоснование для минимизации рисков ИБ.
- принятие руководством остаточных рисков и решения о реализации и эксплуатации/совершенствовании СУИБ. Остаточные риски ИБ должны быть соотнесены с рисками деятельности Комитета, и оценено их влияние на достижение целей деятельности.

4.7.2. Реализация системы управления ИБ

В системе управления ИБ должны быть реализованы следующие процессы:

- разработка плана обработки рисков ИБ;
- реализация плана обработки рисков ИБ и реализация защитных мер, управление работами и ресурсами, связанными с реализацией СУИБ;
- реализация программ по обучению и осведомленности ИБ;
- обнаружение и реагирование на инциденты безопасности;
- обеспечение непрерывности деятельности и восстановления после прерываний.

На этапе планирования определяется политика и методология управления рисками, а также выполняется оценка рисков, включающая в себя инвентаризацию активов, составление профилей угроз и уязвимостей, оценку эффективности контрмер и потенциального ущерба, определение допустимого уровня остаточных рисков.

На этапе реализации производится обработка рисков и внедрение механизмов контроля, предназначенных для их минимизации. Компетентным лицом принимается одно из четырех решений по каждому идентифицированному риску: проигнорировать, избежать, передать внешней стороне, либо минимизировать. После этого разрабатывается и внедряется план обработки рисков.

На этапе проверки отслеживается функционирование механизмов контроля, контролируются изменения факторов риска (активов, угроз, уязвимостей), проводятся аудиты и выполняются различные контролирующие процедуры.

На этапе действия по результатам непрерывного мониторинга и проводимых проверок, выполняются необходимые корректирующие действия, которые могут включать в себя, в частности, переоценку величины рисков, корректировку политики и методологии управления рисками, а также плана обработки рисков.

4.7.3. Методы оценивания информационных рисков

Оценка информационных рисков Комитета выполняется по следующим основным этапам:

- идентификация и количественная оценка информационных ресурсов, значимых для работы Комитета;
- оценивание возможных угроз;
- оценивание существующих уязвимостей;
- оценивание эффективности средствобеспечения информационной безопасности.

Предполагается, что значимые уязвимые информационные ресурсы Комитета подвергаются риску, если по отношению к ним существуют какие-либо угрозы.

При этом информационные риски зависят от:

- показателей ценности информационных ресурсов;
- вероятности реализации угроз для ресурсов;
- эффективности существующих или планируемых средств обеспечения информационной безопасности .

Цель оценивания рисков состоит в определении характеристик рисков информационной системы и ее ресурсов. В результате оценки рисков становится возможным выбрать средства, обеспечивающие желаемый уровень информационной безопасности организации.

При оценивании рисков учитываются:ценность ресурсов, значимость угроз и уязвимостей, эффективность существующих и планируемых средств защиты. Сами показатели ресурсов, значимости угроз и уязвимостей, эффективность средств защиты могут быть определены как количественными методами, например, при определении стоимостных характеристик, так и качественными, например учитывающими штатные или чрезвычайно опасные нештатные воздействия внешней среды.

Возможность реализации угрозы оценивается вероятностью ее реализации в течение заданного отрезка времени для некоторого ресурса Комитета.

При этом вероятность того, что угроза реализуется, определяется следующими основными показателями:

- привлекательностью ресурса, используется при рассмотрении угрозы от умышленного воздействия со стороны человека;

- возможностью использования ресурса для получения дохода, также используется при рассмотрении угрозы от умышленного воздействия со стороны человека;

- техническими возможностями реализации угрозы, используется при умышленном воздействии со стороны человека;

- степенью легкости, с которой уязвимость может быть использована.

4.8.Политика информационной безопасности

4.8.1. Политика предоставления доступа к информационному ресурсу

4.8.2. Назначение

Настоящая Политика определяет основные правила предоставления сотрудникам доступа к защищаемым информационным ресурсам Комитета.

4.8.2.1. Положение политики

К работе с информационным ресурсом допускаются пользователи, ознакомленные с правилами работы с информационным ресурсом и ответственностью за их нарушение, а также настоящей политикой.

Каждому сотруднику Комитета, допущенному к работе с конкретным информационным ресурсом, должно быть сопоставлено персональное уникальное имя (учетная запись пользователя), под которым он будет регистрироваться и работать в ИС.

В случае необходимости некоторым сотрудникам могут быть сопоставлены несколько уникальных имен (учетных записей). Использование несколькими сотрудниками при работе в Комитете одного и того же имени пользователя («группового имени») ЗАПРЕЩЕНО.

4.8.2.2.Порядок создания (продления) учетной записи пользователя

Процедура регистрации (создания учетной записи), так же продления срока действия временной учетной записи пользователя для сотрудника Комитета инициируется заявкой, в которой указывается:

- должность (с полным наименованием подразделения), фамилия, имя и отчество сотрудника;
- основание для регистрации учетной записи (номер приказа о принятии на работу в Комитет или иного договорного документа, определяющего необходимость предоставления сотруднику доступа к информационным ресурсам Комитета).

Заявку подписывает руководитель структурного подразделения.

Заявка согласуется с администратором информационной безопасности и передается системному администратору.

Системный администратор рассматривает представленную заявку и совершает необходимые операции по созданию (удалению) учетной записи пользователя, присвоению ему начального значения пароля и минимальных прав доступа к ресурсам Комитета.

По окончании регистрации учетной записи пользователя в заявке делается отметка о выполнении задания за подписями исполнителей.

4.8.2.3.Порядок предоставления (изменения) полномочий пользователя

Процедура предоставления (или изменения) прав доступа пользователя к ресурсам Комитета инициируется заявкой сотрудника.

В заявке указывается:

- должность, фамилия, имя и отчество сотрудника;
- имя пользователя (учетной записи) данного сотрудника;
- наименование информационного актива (системы, ресурса),к которому необходим допуск (или изменение полномочий пользователя);
- полномочия, которых необходимо лишить пользователя или которые необходимо добавить пользователю (путем указания решаемых пользовате-

лем задач на конкретных информационных ресурсах ИС) с указанием разрешенных видов доступа к ресурсу (ролей).

Заявка согласовывается с руководителем структурного подразделения или заместителем председателя и передается администратору информационной безопасности на исполнение.

По окончании внесения изменений в заявке делается отметка о выполнении задания за подписями исполнителей.

4.8.2.4. Порядок удаления учетной записи пользователя

При наступлении момента прекращения срока действия полномочий пользователя (окончание договорных отношений, увольнение сотрудника) учетная запись должна немедленно блокироваться.

Предпочтительно использовать механизмы автоматического блокирования учетных записей уволенных сотрудников, используя соответствующие ИС. При невозможности автоматического блокирования учетных записей, сотрудникам сопоставляются временные учетные записи (с фиксированным сроком действия), о чем делается отметка в заявке при ее исполнении и в обязательном порядке доводится до инициатора заявки.

Допускается регистрация постоянных учетных записей при отсутствии механизмов автоматической блокировки. В этом случае руководитель соответствующего структурного подразделения обязан своевременно подавать заявки на блокирование учетной записи сотрудника не позднее, чем за сутки до момента прекращения срока действия полномочий пользователя.

В заявке указывается:

- должность сотрудника, фамилия, имя и отчество сотрудника;
- имя пользователя (учетной записи) данного сотрудника;
- дата прекращения полномочий пользователя.

Заявку подписывает руководитель структурного подразделения, утверждая тем самым факт прекращения срока действия полномочий пользователя.

Администратор информационной безопасности удаляет соответствующую учетную запись.

По окончании внесения изменений в заявке делается отметка о выполнении задания за подписями исполнителей.

В случае необходимости сохранения персональных документов (профайла пользователя) на АРМ сотрудника, после прекращения срока действия его полномочий, сотрудник (или его непосредственный руководитель) должен своевременно (не позднее, чем за 3 суток до момента прекращения срока действия своих полномочий) подать заявку на блокирование учетной записи пользователя с указанием срока хранения указанной информации. Заявка должна подаваться даже в случае применения механизмов автоматической блокировки учетных записей уволенных сотрудников.

4.8.2.5. Порядок хранения исполненных заявок

Исполненные заявки хранятся в финансово-хозяйственном отделе комитета в течение 5 лет с момента окончания предоставления доступа к ин-

формационному ресурсу Комитета.

Они могут впоследствии использоваться:

- для восстановления полномочий пользователей после аварий в ИС Комитета;
- для контроля правомерности наличия у конкретного пользователя прав доступа к информационному ресурсу;
- тем или иным ресурсам системы при разборе конфликтных ситуации;
- для проверки системным администратором правильности настройки средств разграничения доступа к ресурсам системы.

В случае невозможности исполнения инициатору заявки направляется мотивированный отказ с приложением заявки.

4.8.3. Политика учетных записей

4.8.3.1. Назначение

Настоящая политика определяет основные правила присвоения учетных записей пользователям информационных активов Комитета.

4.8.3.2. Положение политики

Регистрационные учетные записи подразделяются на:

- пользовательские – предназначенные для идентификации/ аутентификации пользователей информационных активов Комитета;
- системные - используемые для нужд операционной системы;
- служебные - предназначенные для обеспечения функционирования отдельных процессов или приложений.

Каждому пользователю информационных активов Комитета назначается уникальная пользовательская регистрационная учетная запись. Допускается привязка более одной пользовательской учетной записи к одному и тому же пользователю (например, имеющих различный уровень полномочий).

Запрещено создавать и использовать общую пользовательскую учетную запись для группы пользователей. Системные регистрационные учетные записи формируются операционной системой и должны использоваться только в случаях, предписанных документацией на операционную систему.

Служебные регистрационные учетные записи используются только для запуска сервисов или приложений.

Использование системных или служебных учетных записей для регистрации пользователей в системе категорически запрещено.

4.8.4. Политика использования паролей

4.8.4.1. Назначение

Настоящая политика определяет основные правила обращения с паролями, используемыми для доступа к защищаемым информационным активам Комитета.

4.8.5. Политика реализации антивирусной защиты

4.8.5.1. Назначение

Настоящая Политика определяет основные правила для реализации антивирусной защиты в Комитете.

4.8.5.2. Положения политики

Положения политики закрепляются в Инструкции по организации антивирусной защиты в ИСПДн».

4.8.6. Политика защиты АРМ

4.8.6.1. Назначение

Настоящая Политика определяет основные правила и требования по защите персональных данных и иной конфиденциальной информации Комитета от неавторизованного доступа, утраты или модификации.

4.8.6.2. Положения политики

Во время работы с конфиденциальной информацией должен предотвращаться ее просмотр не допущенными к ней лицами.

При любом оставлении рабочего места, рабочая станция должна быть заблокирована, съемные машинные носители, содержащие конфиденциальную информацию, заперты в помещении, шкафу или ящике стола или в сейфе.

Несанкционированное использование печатающих, факсимильных, копировально-множительных аппаратов и сканеров должно предотвращаться путем их размещения в помещениях с ограниченным доступом, использования паролей или иных доступных механизмов разграничения доступа.

Сотрудники получают доступ к ресурсам вычислительной сети после ознакомления с документами, утвержденными стандартами Комитета, (согласно занимаемой должности), а именно с инструкциями по обращению с носителями конфиденциальной информации.

Доступ к компонентам операционной системы и командам системного администрирования на рабочих станциях пользователей ограничен. Право на доступ к подобным компонентам предоставлено только администратор информационной безопасности. Конечным пользователям предоставляется доступ только к тем командам, которые необходимы для выполнения их должностных обязанностей.

Доступ к информации предоставляется только лицам, имеющим обоснованную необходимость в работе с этими данными для выполнения своих должностных обязанностей.

Пользователям запрещается устанавливать неавторизованные программы на компьютеры.

Конфигурация программ на компьютерах должна проверяться ежемесячно на предмет выявления установки неавторизованных программ.

Техническое обслуживание должно осуществляться только на основании обращения пользователя к системному администратору.

Локальное техническое обслуживание должно осуществляться только в личном присутствии пользователя.

Дистанционное техническое обслуживание должно осуществляться только со специально выделенных автоматизированных рабочих мест, конфигурация и состав которых должны быть стандартизованы, а процесс эксплуатации регламентирован и контролироваться.

При проведении технического обслуживания должен выполняться минимальный набор действий, необходимых для устранения проблемы, явившейся причиной обращения, и использоваться любые возможности, позволяющие впоследствии установить авторство внесенных изменений.

Копирование конфиденциальной информации и временное изъятие носителей конфиденциальной информации (в том числе в составе АРМ) допускаются только с санкции пользователя. В случае изъятия носителей, содержащих конфиденциальную информацию, пользователь имеет право присутствовать при дальнейшем проведении работ.

Программное обеспечение должно устанавливаться со специальных ресурсов или съемных носителей и в соответствии с лицензионным соглашением с его правообладателем.

Конфигурации устанавливаемых рабочих станций должны быть стандартизованы, а процессы установки, настройки и ввода в эксплуатацию - регламентированы.

АРМ, на которых предполагается обрабатывать конфиденциальную информацию, должны быть закреплены за соответствующими сотрудниками Организации. Запрещается использование указанных АРМ другими пользователями без согласования с администратором информационной безопасности Организации. При передаче указанного АРМ другому пользователю, должна производиться гарантированная очистка диска (форматирование).

Системный администратор вправе отказать в устранении проблемы, вызванной наличием на рабочем месте программного обеспечения или оборудования, установленного или настроенного пользователем в обход действующей процедуры.

4.9.Порядок сопровождения ИС Комитета

Обеспечение информационной безопасности информационных систем на стадиях жизненного цикла ИБ ИС должна обеспечиваться на всех стадиях жизненного цикла (ЖЦ) ИС, автоматизирующих технологические процессы, с учетом всех сторон, вовлеченных в процессы ЖЦ (разработчиков, заказчиков, поставщиков продуктов и услуг, эксплуатирующих и надзорных подразделений организации). Разработка технических заданий, проектирование, создание, тестирование, приемка средств и систем защиты ИС проводится при участии администратора информационной безопасности и системного администратора. Порядок разработки и внедрения ИС должен быть регламентирован и контролироваться.

При разработке ИС необходимо придерживаться требований и методических указаний, определенных стандартами.

Ввод в действие, эксплуатация, снятие с эксплуатации ИС в части вопросов ИБ должны осуществляться при участии администратора информационной безопасности.

На стадиях, связанных с разработкой ИС (определение требований заинтересованных сторон, анализ требований, архитектурное проектирование, реализация, интеграция и верификация, поставка, ввод в действие), разработчиком должна быть обеспечена защита от угроз:

- неверной формулировки требований к ИС;
- выбора неадекватной модели ЖЦ ИС, в том числе неадекватного выбора процессов ЖЦ и вовлеченных в них участников;
- принятия неверных проектных решений;
- внесения разработчиком дефектов на уровне архитектурных решений;
- внесения разработчиком недокументированных возможностей в ИС;
- неадекватной (неполной, противоречивой, некорректной и пр.) реализации требований к ИС;
- разработки некачественной документации;
- сборки ИС разработчиком/производителем с нарушением требований, что приводит к появлению недокументированных возможностей в ИС либо к неадекватной реализации требований;
- неверного конфигурирования ИС;
- приемки ИС, не отвечающей требованиям заказчика;
- внесения недокументированных возможностей в ИС в процессе проведения приемочных испытаний посредством недокументированных возможностей функциональных тестов и тестов ИБ.

Привлекаемые для разработки средств и систем защиты ИС на договорной основе специализированные организации должны иметь лицензии на данный вид деятельности в соответствии с законодательством Российской Федерации.

При приобретении готовых ИС и их компонентов разработчиком должна быть предоставлена документация, содержащая, в том числе, описание защитных мер, предпринятых разработчиком в отношении угроз информационной безопасности.

Также разработчиком должна быть представлена документация, содержащая описание защитных мер, предпринятых разработчиком ИС и их компонентов относительно безопасности разработки, безопасности поставки, эксплуатации, поддержки жизненного цикла, включая описание модели жизненного цикла, оценки уязвимости. Данная документация может быть представлена в рамках декларации о соответствии или быть результатом оценки соответствия изделия, проведенной в рамках соответствующей системы оценки.

В договор (контракт) о поставке ИС и их компонентов рекомендуется включать положения по сопровождению поставляемых изделий на весь срок их службы. В случае невозможности включения в договор (контракт) указанных требований к разработчику должна быть рассмотрена возможность при-

обретения полного комплекта рабочей конструкторской документации на изделие, обеспечивающее возможность сопровождения ИС и их компонентов без участия разработчика. Если оба указанных варианта неприемлемы, например, вследствие высокой стоимости, руководство Комитета, должно обеспечить анализ влияния угрозы невозможности сопровождения ИС и их компонентов на обеспечение непрерывности работы.

На стадии эксплуатации должна быть обеспечена защита от следующих угроз:

- умышленное несанкционированное раскрытие, модификация или уничтожение информации;
- неумышленная модификация или уничтожение информации;
- недоставка или ошибочная доставка информации;
- отказ в обслуживании или ухудшение обслуживания.

Кроме этого, актуальной является угроза отказа от авторства сообщения. На стадии сопровождения должна быть обеспечена защита от угроз:

- внесения изменений в ИС, приводящих к нарушению ее функциональности либо к появлению недокументированных возможностей;
- невнесения разработчиком/поставщиком изменений, необходимых для поддержки правильного функционирования и правильного состояния ИС.

На стадии снятия с эксплуатации должно быть обеспечено удаление информации, несанкционированное использование которой может нанести ущерб Комитету, и информации, используемой средствами обеспечения ИБ, из постоянной памяти ИС или с внешних носителей.

Требования ИБ должны включаться во все договора и контракты на проведение работ или оказание услуг на всех стадиях ЖЦ ИС.

4.9.1. Профилактика нарушений политик информационной безопасности

Под профилактикой нарушений политик информационной безопасности понимается проведение регламентных работ по защите информации, предупреждение возможных нарушений информационной безопасности в Комитете и проведение разъяснительной работы по информационной безопасности среди пользователей.

Проведение в ИС Комитета регламентных работ по защите информации предполагает выполнение процедур контрольного тестирования (проверки) функций СЗИ, что гарантирует ее работоспособность с точностью до периода тестирования. Контрольное тестирование функций СЗИ может быть частичным или полным и должно проводиться с установленной в ИС Комитета степенью периодичности.

Задача предупреждения в ИС Комитета возможных нарушений информационной безопасности решается по мере наступления следующих событий:

- включение в состав ИС Комитета новых программных и технических средств (новых рабочих станций, серверного или комму-

никационного оборудования и др.) при условии появления уязвимых мест в СЗИ ИС Комитета;

- изменение конфигурации программных и технических средств ИС (изменение конфигурации программного обеспечения рабочих станций, серверного или коммуникационного оборудования и др.) при условии появления уязвимых мест в СЗИ ИС Комитета;
- при появлении сведений о выявленных уязвимых местах в составе операционных систем и/или программного обеспечения технических средств, используемых в ИС Комитета.

Администратор информационной безопасности (возможно, при помощи сторонней организации, специализирующейся в области информационной безопасности) собирает и анализирует информацию о выявленных уязвимых местах в составе операционных систем и/или программного обеспечения относительно ИС Комитета. Источниками подобного рода сведений могут служить официальные издания и публикации различных компаний, общественных объединений и других организаций, специализирующихся в области защиты информации.

Администратор информационной безопасности (возможно, при помощи сторонней организации, специализирующейся в области информационной безопасности) организовывает периодическую проверку СЗИ ИС Комитета путем моделирования возможных попыток осуществления НСД к защищаемым информационным ресурсам.

Для решения задач контроля защищенности ИС используются инструментальные средства для тестирования реализованных в составе СЗИ ИС Комитета средств и функций защиты.

Плановая разъяснительная работа по правилам настоящих политик, а также инструктаж сотрудников Комитета по соблюдению требований нормативных и регламентных документов по информационной безопасности, принятых в Комитете, проводится администратором информационной безопасности ежегодно.

Внеплановая разъяснительная работа по правилам настоящих политик, а также инструктаж сотрудников Комитета по соблюдению требований нормативных и регламентных документов по информационной безопасности, принятых в Комитет, проводится при пересмотре настоящей политики, при возникновении инцидента нарушения правил настоящих политик.

Прием на работу новых сотрудников должен сопровождаться ознакомлением их с правилами и требованиями настоящих политик.

4.9.2. Ликвидация последствий нарушения политики информационной безопасности

Администратор информационной безопасности, используя данные, полученные в результате применения инструментальных средств контроля (мониторинга) безопасности информации ИС, должен своевременно обнаруживать нарушения информационной безопасности, факты осуществления

НСД к защищаемым информационным ресурсам и предпринимать меры по их локализации и устранению.

В случае обнаружения подсистемой защиты информации факта нарушения информационной безопасности или осуществления НСД к защищаемым информационным ресурсам ИС рекомендуется уведомить администратора информационной безопасности и/или начальника информационного отдела, и далее следовать их указаниям.

Действия администратора информационной безопасности и системного администратора при признаках нарушения политик информационной безопасности регламентируются следующими внутренними документами:

- Инструкцией пользователя автоматизированной системы;
- Политикой информационной безопасности;
- Должностными обязанностями администратора информационной безопасности;
- Должностными обязанностями системного администратора.

После устранения инцидента необходимо составить акт о факте нарушения и принятых мерах по восстановлению работоспособности ИС, а также зарегистрировать факт нарушения в журнале учета нарушений, ликвидации их причин и последствий.

4.9.3. Ответственность нарушителей ПБ

Ответственность за выполнение правил Политики безопасности несет каждый сотрудник Комитета в рамках своих служебных обязанностей и полномочий.

Все сотрудники несут персональную (в том числе материальную) ответственность за прямой действительный ущерб, причиненный Комитету в результате нарушения ими правил политики.

За неправомерный доступ к компьютерной информации, создание, использование или распространение вредоносных программ, а также нарушение правил эксплуатации ЭВМ, следствием которых явилось нарушение работы ЭВМ (автоматизированной системы обработки информации), уничтожение, блокирование или модификация защищаемой информации, сотрудники Комитета несут ответственность в соответствии со статьями 272, 273 и 274 Уголовного кодекса Российской Федерации.

5. Регулирующие законодательные нормативные документы

При организации и обеспечении работ по информационной безопасности сотрудники Комитета должны руководствоваться следующими законодательными нормативными документами:

5.1. Основополагающие нормативные документы

К основополагающим нормативным документам относятся:

- Доктрина информационной безопасности Российской Федерации (утверждена Президентом РФ от 9 сентября 2000 г. № Пр-1895).

5.2. Законы Российской Федерации

- Федеральный закон от 28.10.2012 г. № 390-ФЗ «О безопасности»;
- Гражданский кодекс Российской Федерации;
- Федеральный закон от 06.04.2011 г. № 63-ФЗ «Об электронной подписи»;
- Федеральный закон от 27.07.2006 г. № 152-ФЗ «О персональных данных»;
- Федеральный закон от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Уголовный кодекс РФ;
- Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании»;
- Федеральный закон от 04.05.2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности».

5.3. Указы и распоряжения президента Российской Федерации

- Указ Президента Российской Федерации от 20.01.1994г. № 170 «Об основах государственной политики в сфере информатизации»;
- Указ Президента Российской Федерации от 03.04.1995 г. № 334 «О мерах по соблюдению законности в области разработки, производства, реализации и эксплуатации шифровальных средств, а также предоставления услуг в области шифрования информации»;
- Указ Президента Российской Федерации от 06.03.1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера».

5.4. Постановления и распоряжения Правительства Российской Федерации

- Постановление Правительства Российской Федерации от 03.11.1994г. № 1233;
- Постановление Правительства Российской Федерации от 26.06.1995г. № 608 «О сертификации средств защиты информации».

6. Заключительные положения

Требования настоящей Политики могут развиваться другим внутренними нормативными документами Комитета, которые дополняют и уточняют ее.

В случае изменения действующего законодательства и иных нормативных актов, а также Положения о Комитете настоящая Политика и изменения к ней применяются в части, не противоречащей вновь принятым законодательным и иным нормативным актам, а также Положению о Комитете. В этом случае ответственное подразделение обязано незамедлительно инициировать внесение соответствующих изменений.

Ответственным за внесение изменений в настоящую Политику является руководитель структурного подразделения, по инициативе которого были внесены изменения.