|  |
| --- |
|  |
| (Полное наименование оператора) |

## Приказ об утверждении политики информационной безопасности

|  |  |
| --- | --- |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | № \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

В целях исполнения положений Федерального закона от 27.07.2006 N 152-ФЗ «О персональных данных» и Федерального закона от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации",

ПРИКАЗЫВАЮ:

1. Утвердить Политику информационной безопасности \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ с приложениями к ней.
2. Сотрудникам \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ в своей работе руководствоваться положениями настоящей Политики.
3. Сформировать комиссию по уничтожению носителей  информации в составе:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ – председатель комиссии;

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ – член комиссии;

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ – член комиссии.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Руководитель** |  |  |  |  |  |
|  | (должность) |  | (личная подпись) |  | (расшифровка подписи) |

УТВЕРЖДЕНА

приказом \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

от \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ г. № \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Политика информационной безопасности \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. ОБЩИЕ ПОЛОЖЕНИЯ
   1. Настоящая политика информационной безопасности (далее - Политика) утверждена руководителем \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ и описывает мероприятия, процедуры и правила по защите информации в информационных системах \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.
   2. Термины и определения, используемые в Политике, установленны законодательством Российской Федерации об информации, информационных технологиях и о защите информации, а также национальными стандартами в области защиты информации.
   3. Целями настоящей Политики являются:

- предотвращение несанкционированного доступа к защищаемой информации и её распространения;

- обеспечение конфиденциальности, целостности, доступности защищаемой информации;

- выполнение требований действующего законодательства по защите информации.

- нейтрализация актуальных угроз безопасности информации;

- мониторинг событий безопасности;

- реагирование на инциденты безопасности;

- совершенствование подходов к обеспечению информационной безопасности;

- использование "лучших практик" в области информационной безопасности.

* 1. Положения Политики применимы к следующим информационным системам \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_:

|  |
| --- |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

* 1. Реализация положений Политики обязательна для всех пользователей указанных в п. 1.4 информационных систем (далее - Пользователи), а также и для Администратора безопасности (далее – Администратора), системного администратора, Ответственного за организацию обработки персональных данных (далее – Ответственного).
  2. В соответствии с указом Президента Российской Федерации № 188 от 6 марта 1997 года «Об утверждении перечня сведений конфиденциального характера», \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ к сведениям конфиденциального характера отнесены:

- сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях;

- сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией Российской Федерации и федеральными законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и так далее);

- сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (коммерческая тайна).

* 1. Настоящая Политика разработана с учетом положений законодательных и нормативно-правовых актов:

Федеральный закон № 152-ФЗ от 27 июля 2006 года «О персональных данных»;

Федеральный закон № 149-ФЗ от 27 июля 2006 года «Об информации, информатизации и защите информации»;

«Требования к защите персональных данных при их обработке в информационных системах персональных данных», утвержденные Постановлением Правительства РФ № 1119 от 1 ноября 2012 года;

«Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденный приказом ФСТЭК России № 21 от 18 февраля 2013 года;

«Инструкция об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну», утвержденная приказом ФАПСИ от 13 июня 2001 №152.

 «Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации», утвержденное приказом ФСБ от 9 февраля 2005 №66;

 «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности», утверждённые приказом ФСБ России № 378 от 10.07.2014;

1. ПРОЦЕССЫ ОБРАБОТКИ ЗАЩИЩАЕМОЙ ИНФОРМАЦИИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ
   1. Раздел содержит описания технологических процессов обработки защищаемой информации в информационных системах \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. Должностные лица, осуществляющие обработку защищаемой информации, должны руководствоваться описаниями технологических процессов обработки информации при осуществлении такой обработки.
   2. Технологический процесс обработки персональных данных сотрудников \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_:
      1. Порядок осуществления сбора персональных данных:

- сбор персональных данных осуществляется непосредственно от субъекта данных, а также от законного представителя при наличии нотариально заверенной доверенности, либо иных законных оснований;

- источником получения персональных данных субъекта выступают документы сотрудника и заполненная унифицированная форма Т-2 «Личная карточка сотрудника».

* + 1. Внесение персональных данных в базу данных \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ осуществляют сотрудники \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ в рамках своих полномочий.
    2. Систематизация, накопление и хранение персональных данных ведется средствами \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.
    3. Уточнение (обновление, изменение) персональных данных осуществляется при возникновении необходимости, в случае обнаружения неточных, устаревших данных, либо по заявлению субъекта в связи с их изменением.
    4. Извлечение персональных данных производится при формировании бухгалтерской отчетности средствами ПО \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ с использованием средств криптографической защиты информации\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.
    5. Обработка персональных данных включает сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (предоставление, доступ), блокирование, удаление, уничтожение персональных данных.
    6. Передача персональных данных:

- распространение персональных данных сотрудников \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ не допускается;

- предоставление персональных данных возможно в соответствии с законодательством Российской Федерации в следующих целях:

- сдача отчетности в Пенсионный Фонд РФ;

-  налоговая отчетность;

- бухгалтерская отчетность;

- начисление заработной платы;

- воинский учет;

- предоставление субъектам справок;

- предоставление информации в профсоюзные органы по социально-трудовым вопросам.

* + 1. Доступ к персональным данным имеют сотрудники, допущенные к обработке персональных данных в ИСПДн \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ и субъект персональных данных.
  1. Блокирование персональных данных осуществляется в случае поступления мотивированной заявки субъекта при обнаружении нарушения его прав или законных интересов, связанных с неправомерной обработкой его персональных данных в соответствии с законодательством РФ.
  2. Обезличивание персональных данных производится в соответствии с Правилами работы с обезличенными персональными данными, утвержденными Приказом руководителя \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.
  3. Удаление персональных данных, обрабатываемых средствами программного обеспечения, осуществляется при достижении цели обработки. Персональные данные подлежат уничтожению по истечении сроков хранения документов, их содержащих (75 лет).
  4. Технологический процесс обработки персональных данных клиентов в \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_:
     1. Порядок осуществления сбора персональных данных:
        1. сбор персональных данных осуществляется непосредственно от субъекта данных, а также от законного представителя при наличии нотариально заверенной доверенности, либо иных законных оснований;
        2. источником получения персональных данных субъекта являются предоставленные клиентом документы.

2.7.2. Внесение персональных данных в базу данных \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ осуществляют сотрудники \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ в рамках своих полномочий.

2.7.3. Обработка персональных данных включает сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (предоставление, доступ), блокирование, удаление, уничтожение персональных данных.

2.7.4. Распространение персональных данных клиентов не осуществляется. Предоставление персональных данных возможно в предусмотренных законодательством Российской Федерации случаях.

2.7.5. Доступ к персональным осуществляют сотрудники, допущенные к обработке персональных данных в ИСПДн \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ исключительно в пределах своих должностных полномочий и субъект персональных данных в отношении собственных данных.

2.7.6.Блокирование персональных данных осуществляется в случае поступления мотивированной заявки субъекта при обнаружении нарушения его прав или законных интересов, связанных с неправомерной обработкой его персональных данных в соответствии с законодательством РФ.

2.7.7.Уточнение (обновление, изменение) персональных данных осуществляется при возникновении необходимости: в случае обнаружения неточных, устаревших данных, либо по заявлению субъекта в связи с их изменением.

2.7.9. Уничтожение персональных данных, обрабатываемых средствами программного обеспечения, осуществляется при достижении цели обработки.

1. ПОРЯДОК ИДЕНТИФИКАЦИИ И АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ, ПОЛИТИКА РАЗГРАНИЧЕНИЯ ДОСТУПА К РЕСУРСАМ ИНФОРМАЦИОННЫХ СИСТЕМ
   1. Каждому сотруднику \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, допущенному к обработке персональных данных, предоставляется уникальная учетная запись. Работа в информационных системах с использованием учетной записи, закрепленной за другим лицом, не допускается. В качестве учетной записи Пользователя рассматривается учетная запись для доступа к информационной системе в домене Active Directory.
   2. Для Администратора безопасности информационных систем, для системного администратора информационных систем, для удаленных пользователей (работающих с ресурсами информационных систем посредством внешних телекоммуникационных сетей) предусмотрена двухфакторная аутентификация в информационных системах. Двухфакторная аутентификация подразумевает под собой обязательное выполнение двух факторов для успешной аутентификации в системе: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_; \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.
   3. Регистрация (создание учетной записи с правами доступа) пользователя информационной системы осуществляется по заявке руководителя подразделения, к которому относится приступающий к работе с информационной системой сотрудник. Заявка составляется по форме Приложении № \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  к Политике. В заявке указывается:

- суть необходимых изменений (регистрация пользователя информационной системы, удаление учетной записи пользователя, настройка прав доступа к ресурсам информационной системы существующей, либо новой учетной записи пользователя);

- ФИО сотрудника, должность и структурное подразделение;

- указание прав, которые следует предоставить учетной записи пользователя, либо которые следует изъять;

- изменение в правах доступах согласовывается с Администратором путем проставления им визы на заявке.

* 1. При поступлении к Администратору заявки по форме Приложения №\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ он анализирует должностные обязанности лица, в отношении которого запрашиваются права доступа, перед визированием заявки осуществляет верификацию пользователя (подтверждает его личность), а также уточняет его должностные и функциональные обязанности. После проставления визы Администратор актуализирует документы:

- положения о разграничении прав доступа в информационных системах (по форме Приложения №\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  к настоящей Политике);

- перечень лиц, должностей, служб и процессов, допущенных к работе с ресурсами информационных систем (Приложение № \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ к настоящей Политике).

* 1. После визирования заявки Администратор определяет тип учетной записи (внутренний пользователь, внешний пользователь, системная, учетная запись приложения, временная, гостевая), настраивает СЗИ от НСД, создает учетную запись и первичный пароль. Затем производится ознакомление с инструкцией Пользователя информационной системы под роспись, предоставление идентификационных данных для первичного доступа в информационную систему. Далее Пользователь самостоятельно формирует пароль доступа к своей учетной записи в соответствии с требованиями Инструкции Пользователя информационной системы.
  2. По окончании обработки заявки в ней проставляется соответствующая отметка. Заявка подлежит хранению у Администратора и может быть использована для восстановления настроек доступа после сбоев в работе информационной системы, для проверки правомерности наличия у пользователя прав доступа к тем или иным ресурсам информационной системы при разборе инцидентов безопасности.
  3. Лицам, не являющимися сотрудниками \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, которым необходим временный доступ в информационную систему для осуществления технических или иных работ, предоставляется гостевая временная учетная запись «Guest». Активация гостевой временной учетной записи осуществляется только в случае возникновения необходимости, в остальное время она остается дезактивированной. Все работы от имени такой учетной записи проводятся только под контролем Администратора.
  4. Разграничение доступа к ресурсам информационных систем осуществляется по ролевой модели. Роль в разграничительной системе информационной системы определяется выполняемыми должностными обязанностями, стоящими задачами и необходимостью доступа к ресурсам информационных систем. Возможные роли в информационной системе указаны в Приложении №  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ к Политике. Наряду с Пользователями доступ к информационной системе имеют системные службы и процессы.
  5. Перечень должностных лиц, служб и процессов, допущенных к работе с ресурсами информационных систем и присвоенные им роли указываются в Приложении № \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ к Политике. Актуальность перечня обеспечивается Администратором.
  6. Помещения, в которых ведется работа с ресурсами информационных систем, и в которых установлены технические средства информационных систем, перечень лиц, обладающих допуском в эти помещения, указан в Приложении № \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ к настоящей Политике. Администратор обеспечивает оперативное обновление и актуальность данного перечня.
  7. Идентификация и аутентификация на сетевом оборудовании (коммутаторы, маршрутизаторы, точки доступа и т. д.) производится исключительно администраторами безопасности, системными администраторами и сотрудниками сторонних организаций, допущенных к осуществлению работ в сети \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ на договорной основе и под контролем Администратора .
  8. На вводимом в эксплуатацию сетевом оборудовании обязательно меняются идентификационные и аутентификационные данные, установленные производителем. Производимые изменения должны соответствовать действующей парольной политике.
  9. До прохождения идентификации и аутентификации Пользователи не могут совершать какие-либо действия в информационных системах, за исключением Администратора, , в соответствии с должностными инструкциями.

1. ПРАВИЛА И ПРОЦЕДУРЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННЫМИ ПОТОКАМИ
   1. В информационных системах осуществляется управление информационными потоками при передаче информации между устройствами, сегментами в рамках информационной системы, включающее:

а) фильтрацию информационных потоков в соответствии с установленными правилами управления потоками;

б) разрешение передачи информации в ИСПДн только по установленному маршруту;

в) изменение (перенаправление) маршрута передачи информации в случаях необходимости, по согласованию с Администратором.

* 1. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
  2. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. ПОРЯДОК ПРОВЕДЕНИЯ УСТАНОВОК (ИНСТАЛЛЯЦИЙ) КОМПОНЕНТОВ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ
   1. В информационных системах \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ допустимо использование только необходимого для функционирования информационной системы программного обеспечения (утилит, драйверов), а также программного обеспечения для выполнения служебных (должностных) обязанностей Пользователями.
   2. Перечень разрешенного программного обеспечения в информационных системах указан в Приложении № \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  к Политике.
   3. Процедуры инсталляции программного обеспечения, его компонентов, утилит и драйверов, осуществление их настроек производится исключительно системным администратором. Любые манипуляции с установкой программного обеспечения (его компонентов) Пользователями без предварительного согласования с Администратором не допускаются.
   4. При возникновении необходимости согласования Пользователь подает служебную записку о включении в список разрешенного в информационной системе программного обеспечения нового программного обеспечения с обоснованием необходимости его использования. Рассмотрение служебной записки производится в срок не более 5 рабочих дней.
   5. Администратор\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ с помощью инструмента \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ проводит проверку соответствия установленного программного обеспечения списку разрешенного ПО. Обнаружение несанкционированного ПО является основанием созыва группы реагирования на инциденты информационной безопасности в соответствии с инструкцией по реагированию на инциденты информационной безопасности.
2. ЗАЩИТА МАШИННЫХ НОСИТЕЛЕЙ ИНФОРМАЦИИ,КОНТРОЛЬ ИНТЕРФЕЙСОВ ВВОДА-ВЫВОДА, ГАРАНТИРОВАННОЕ УНИЧТОЖЕНИЕ ИНФОРМАЦИИ

* 1. Защита машинных носителей подразумевает ведение их учета. Учет машинных носителей осуществляется Администратором в соответствующих журналах. Администратор несет ответственность за достоверность и своевременность сведений, отраженных в журнале учета машинных носителей информации.
  2. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ ведет учет в отношении:

• съемных машинных носителей информации (флэш-накопители, внешние накопители на жестких дисках и иные подобные устройства);

• машинных носителей информации, встроенных в корпус средств вычислительной техники (накопители на жестких дисках).

* 1. Учет машинных носителей информации включает присвоение регистрационных (учетных) номеров носителям. В качестве регистрационных номеров могут использоваться идентификационные (серийные) номера машинных носителей, присвоенных производителями этих машинных носителей информации, номера инвентарного учета, в том числе инвентарные номера технических средств, имеющих встроенные носители информации, и иные номера.
  2. При использовании в составе одного технического средства информационной системы нескольких встроенных машинных носителей информации, конструктивно объединенных в единый ресурс для хранения информации, допускается присвоение регистрационного номера техническому средству в целом.
  3. Администратор маркирует съемные машинные носители, использование которых разрешено за пределами контролируемой зоны и информационной системы и делает соответствующую отметку в журнале. Использование немаркированного соответствующим образом носителя информации за пределами контролируемой зоны и/или информационной системы является инцидентом информационной безопасности и расследуется в установленном порядке.
  4. Использование неучтенных съемных носителей (в том числе личных) запрещено.
  5. Невозможность использования неучтенных съемных носителей информации обеспечивается путем программных настроек СЗИ от НСД. Настройками СЗИ от НСД неучтенные носители информации блокируются на всех стационарных устройствах использования неучтенных съемных носителей информации фиксируются средствами СЗИ от НСД. Такие попытки являются инцидентами безопасности и расследуются в установленном порядке.
  6. К устройствам ввода относятся: клавиатуры, мыши, сканеры, кард-ридеры, сенсорные экраны (панели), сканеры штрих-кодов, лабораторное и диагностическое оборудование и другие устройства. К интерфейсам ввода допущены все легальные пользователи информационной системы. Допуск к тем или иным интерфейсам ввода организовывается Администратором, в зависимости от выполняемых пользователем должностных обязанностей. Дополнительный контроль устройств ввода не осуществляется.
  7. Вывод информации на печать дополнительно не контролируется.
  8. Гарантированное уничтожение (стирание) информации на машинных носителях организовывается Администратором в случаях:

•возвращения учтенного съемного носителя информации Администратору;

•при вводе в эксплуатацию нового машинного носителя или технического средства со встроенными носителями информации;

•при передаче носителя информации в сторонние организации (в том числе и для проведения ремонта технического средства);

•при утилизации технических средств.

* 1. Уничтожение (стирание) информации на машинных носителях должно исключать возможность восстановления защищаемой информации. Контроль невозможности восстановления уничтоженной информации производится Администратором с помощью специализированных утилит по восстановлению информации.
  2. При возвращении учтенного съемного носителя информации Пользователем, а также при вводе в эксплуатацию нового машинного носителя, информация уничтожается путем использования механизма СЗИ от НСД затирания файлов случайной битовой последовательностью.
  3. При передаче носителя информации в сторонние организации (не с целью передачи на нем информации), в том числе и для ремонта носителя или технического средства, информация уничтожается путем полной многократной перезаписи машинного носителя информации специальными битовыми последовательностями, зависящими от типа накопителя и используемого метода кодирования информации. Затем производится очистка всего физического пространства накопителя, включая сбойные и резервные элементы памяти специализированными программами или утилитами производителя.
  4. При утилизации технических средств, а также при возникновении необходимости уничтожения информации на не перезаписываемых машинных носителях (например, CD-R), физически уничтожается сам машинный носитель.
  5. В случае физического уничтожения машинного носителя информации, составляется Комиссией по уничтожению машинных носителей акт уничтожения по Форме приложения №\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

1. РЕГЛАМЕНТАЦИЯ И КОНТРОЛЬ ИСПОЛЬЗОВАНИЯ ТЕХНОЛОГИЙ БЕСПРОВОДНОГО ДОСТУПА И ЗАЩИТА БЕСПРОВОДНЫХ СОЕДИНЕНИЙ
   1. Беспроводной доступ к информационным системам и ресурсам для работников разрешается при соблюдении требований безопасности.
   2. Настройка и поддержка эксплуатации точек беспроводного доступа и устройств, с которых осуществляются беспроводные соединения, производится системными администраторам.
   3. Запрещается использование Пользователями беспроводных точек доступа для подключения принадлежащего им личного оборудования (смартфонов, планшетов, ноутбуков, итд).
   4. Запрещается раздача с принадлежащих Пользователю устройств Интернета на оборудование \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.
   5. Беспроводной доступ осуществляется Пользователями по предоставляемым им Администратором учетным данным. Использование чужих учётных записей для доступа к беспроводной сети запрещено.
   6. В отношении к паролям доступа к беспроводным точкам доступа установлены следующие требования:

- минимальная длина пароля составляет 10 символов, пароль должен содержать буквы английского алфавита верхнего и нижнего регистров, как минимум одну цифру и один спецсимвол;

- при смене пароля, новый пароль должен отличаться минимум на два символа от предыдущего;

- запрещается использование пользователями пяти последних использованных паролей при создании новых паролей;

Смена пароля осуществляется в случае его компрометации (подозрения компрометации), или раз в месяц.

1. ОБЕСПЕЧЕНИЕ ДОВЕРЕННОЙ ЗАГРУЗКИ СРЕДСТВ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ
   1. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ использует модули доверенной загрузки \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (далее - МДЗ) в качестве средства доверенной загрузки технических средств.
   2. Работа с ресурсами информационных систем осуществляется на технических средствах, в которых возможно заблокировать выбор источника загрузки в обход базовой системы ввода-вывода (BIOS/UEFI).
   3. Администратор контролирует работоспособность \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ в рамках плана мероприятий по обеспечению безопасности. Результаты проверки подлежат фиксации в журнале периодического тестирования средств защиты информации.
   4. При обнаружении сбоев в работе МДЗ на автоматизированном рабочем месте (далее - АРМ), работа с информационными системами не производится до окончания ремонта/замены МДЗ. В случае, если сохраняется необходимость работы на данном АРМ, применяются следующие компенсирующие меры:

- заглушиваются и опечатываются USB-порты, входы для карт памяти SD/Micro-SD и других карт памяти, CD/DVD/Blu-Ray-приводы и сами технические средства;

- настраивается вход в BIOS/UEFI только по паролю администратора и отключается возможность вызова окна выбора источника загрузки нажатием функциональной клавиши (F1-F12) при загрузке;

- проводится обязательный визуальный контроль за техническим средством и состояния установленных заглушек/печатей/пломб.

* 1. В случае, если использование МДЗ на АРМ не предусмотренно, используются компенсирующие меры, нейтрализующие угрозы, связанные с использованием средств недоверенной загрузки: опечатывание USB-портов, входов для SD/Micro-SD и других карт памяти, CD/DVD/Blu-Ray-приводов и самих технических средств, установка пароля доступа на вход в BIOS/UEFI.

1. ПРАВИЛА И ПРОЦЕДУРЫ ПРИМЕНЕНИЯ УДАЛЕННОГО ДОСТУПА
   1. Удаленный доступ к информационной системе осуществляется на основании направляемых Ответственному заявок, подписанных непосредственным руководителем Пользователя, которому необходим удаленный доступ. В заявке надлежит указывать ФИО, должность Пользователя, цель предоставления доступа, необходимый срок предоставления удаленного доступа.
   2. Удаленный доступ пользователей к информационной системе прекращается на основании заявок, а также по истечении срока, указанного в заявке на предоставление удаленного доступа.
   3. Удаленный доступ пользователей к информационным системам обеспечивается на основе зарегистрированных персональных учетных записей, с использованием технологии VPN.
   4. В случае возникновения опасности причинения ущерба безопасности информации удаленный доступ может быть заблокирован системными администраторами, с последующим уведомлением Администратора в форме докладной записки с описанием ситуации и указанием причины ограничения доступа.
   5. При использовании удаленного доступа Пользователи обязаны использовать только свою персональную учетную запись.
2. ВЫЯВЛЕНИЕ, АНАЛИЗ И УСТРАНЕНИЕ УЯЗВИМОСТЕЙ
   1. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ в качестве средства выявления уязвимостей использует сертифицированный сканер уязвимостей \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.
   2. Администратором проводится полное сканирование системы на выявление уязвимостей не реже двух раз в месяц. При появлении информации из новостных источников об уязвимостях и/или обнаружении таких уязвимостей в операционных системах и/или прикладном программном обеспечении, применяемых в информационных системах, он незамедлительно обновляет базу данных сканера уязвимостей и проводит внеочередное полное сканирование информационной системы.
   3. Отчеты по результатам сканирования подлежат анализу Администратором. В случае обнаружения уязвимостей принимается решение об их немедленном устранении, либо о корректировке плана мероприятий по обеспечению безопасности информации в части включения в план необходимых мероприятий для реагирования на уязвимости, если обнаруженные уязвимости не критичны и существует возможность исключить их эксплуатацию.
   4. В случае обнаружения уязвимостей Администратор анализирует содержание системных журналов и журналов средств защиты информации, с целью обнаружить возможные случаи эксплуатации выявленной уязвимости в информационной системе и последствия эксплуатации
   5. Вывод о степени критичности уязвимостей может быть установлен на основании рейтинга уязвимости по шкале CVSS, а также в соответствии с результатами оценки по ГОСТ Р ИСО/МЭК 27005-2010 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности».
   6. Если оперативное устранение критичной уязвимости невозможно, Администратор незамедлительно уведомляет об этом руководителя \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ для принятия решения о корректировке бизнес-процессов.
3. КОНТРОЛЬ УСТАНОВКИ ОБНОВЛЕНИЙ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ
   1. С целью противодействия попыткам эксплуатации известных уязвимостей, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ осуществляет контроль установки обновлений системного и прикладного ПО.
   2. Обновление прикладного, системного программного обеспечения и средств защиты информации осуществляется Администратором.
   3. Обновление микропрошивок и программного обеспечения BIOS/UEFI производится только при поступлении информации о критичных уязвимостях в таком ПО, применяемом \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.
   4. Обновления программного обеспечения должны устанавливаться только из доверенных источников.
   5. Частота проверки обновлений программного обеспечения устанавливается в рамках плана мероприятий по обеспечению безопасности информации.
4. КОНТРОЛЬ СОСТАВА ТЕХНИЧЕСКИХ СРЕДСТВ, ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ
   1. Технические средства, программное обеспечение и средства защиты информации, используемые в информационных системах, фиксируются в технических паспортах на информационные системы. Мероприятия по периодическому контролю проводятся по техническому паспорту информационной системы, который рассматривается в качестве эталона состава технических средств, программного обеспечения, средств защиты информации.
   2. Администратор осуществляет контроль состава технических средств, программного обеспечения, средств защиты информации с периодичностью, установленной планом мероприятий по обеспечению безопасности информации.
   3. Добавление новых технических средств, программного обеспечения и средств защиты информации в состав информационной системы, удаление и/или замена существующих компонентов, отражается в Техническом паспорте информационной системы на основании акта ввода в эксплуатацию (или акта вывода из эксплуатации).
   4. Обнаружение расхождений состава технических средств, программного обеспечения и средств защиты информации c техническим паспортом информационной системы расценивается как инцидент  информационной безопасности. При выявлении фактов расхождения Администратором устанавливаются причины их возникновения, либо созывается ГРИИБ.
   5. При обнаружении несоответствий техническому паспорту фактического состава технических средств, программного обеспечения и средств защиты информации, используемых в информационной системе, Администратор оперативно принимает меры по приведению к соответствию фактического состава информационной системы техническому паспорту.
   6. Администратором контролируется соблюдение условий и сроков действия сертификатов соответствия на средства защиты информации и принимаются меры по устранению обнаруженных недостатков. По истечению срока действия сертификата соответствия, и его продления производителем средства защиты информации, Администратор обязан направить запрос к производителю о предоставлении актуальной заверенной копии сертификата. Если такой сертификат не был продлен производителем средства защиты информации, то Администратор сообщает об этом руководителю\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, который принимает решение об организации самостоятельной сертификации использующегося средства защиты информации, либо обновлении до актуальной версии, либо о замене на аналогичное сертифицированное средство.

1. РЕЗЕРВИРОВАНИЕ ТЕХНИЧЕСКИХ СРЕДСТВ, ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, БАЗ ДАННЫХ, СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ И ИХ ВОССТАНОВЛЕНИЯ ПРИ ВОЗНИКНОВЕНИИ НЕШТАТНЫХ СИТУАЦИЙ
   1. Администратор производит резервирование информационных ресурсов (программного обеспечения, баз данных, средств защиты информации) в информационных системах в соответствии с должностной инструкцией и в соответствии с Приложением № \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ к настоящей Политике.
   2. Резервирование технических средств, програмного обеспечения, баз данных, средств защиты информации и их восстановления должно производиться в соответствии с положениями проектной документации системы защиты информации информационной системы.
   3. Администратор в соответствии с планом мероприятий по обеспечению безопасности информации производит проверку средств резервного копирования, средств хранения резервных копий и средств восстановления информации из резервных копий на предмет их исправного функционирования. Результат проведенной проверки подлежит фиксации в журнале учета мероприятий по контролю за соблюдением режима защиты информации. При обнаружении недостатков в функционировании системы резервирования, должны осуществляться меры по восстановлению ее исправной работы. Вне плана резервное копирование должно быть проведено после восстановления работоспособности системы резервирования.
   4. Восстановление из резервных копий - основной метод восстановления работоспособности информационной системы после ликвидации нештатных ситуаций.
   5. Нештатными ситуациями являются:

• несанкционированный доступ к защищаемой информации:

- несанкционированное подключение технических средств к информационным системам;

- использование закладочных устройств;

- использование злоумышленником легальных учетных записей пользователей для доступа к ресурсам информационных систем;

- эксплуатация злоумышленником уязвимостей программного обеспечения информационных систем;

- эксплуатация злоумышленником программных закладок;

- заражение информационных систем программными вирусами;

- хищение носителей информации;

- нарушение функционирования технических средств обработки информации;

- блокирование доступа к защищаемой информации через перегрузку ложными запросами технических средств;

• разглашение информации ограниченного доступа сотрудниками \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, имеющими к ней право доступа, в том числе:

- передача информации по незащищенным каналам связи;

- обработка информации на незащищенных технических средствах обработки информации;

- разглашение информации лицам, не наделенными правами доступа к защищаемой информации;

- размещение информации в открытом доступе (открытой печати) и других средствах массовой информации;

- передача носителя c защищаемой информацией лицу, не имеющему права доступа к ней;

- утрата носителя с защищаемой информацией.

• неправомерные действия со стороны лиц, имеющих право доступа к защищаемой информации:

- несанкционированное копирование информации;

- несанкционированное изменение информации;

• сбои, отказы и аварии систем обеспечения информационной системы;

• дефекты, сбои, отказы программного обеспечения информационных систем;

• дефекты, сбои, отказы, аварии технических средств в информационных системах;

• природные явления, стихийные бедствия:

- термические, климатические факторы (аномально низкие или аномально высокие температуры воздуха, пожары, наводнения, снегопады и т. д.);

- механические факторы (повреждения зданий, землетрясения и т. д.);

- электромагнитные факторы (отключение электропитания, скачки напряжения, удары молний и т. д.).

* 1. Действия по оповещению должностных лиц и сроки проведения мероприятий при нештатных ситуациях определены в Приложении № \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ настоящей Политики.
  2. При возникновении нештатной ситуации, для которой в Политике не содержится предусмотренного порядка действий, Администратором, Ответственным и ГРИИБ разрабатывается план действий с учетом сложившейся ситуации.
  3. При нештатных ситуациях, сопровождающихся нарушением целостности, доступности или конфиденциальности защищаемой информации по вине внутреннего или внешнего нарушителя, привлекается ГРИИБ, которая реагирует на такой инцидент в соответствии с инструкцией по реагированию на инциденты информационной безопасности.
  4. Для повышения уровня взаимодействия должностных лиц и оперативности устранения последствий нештатных ситуаций периодически проводятся тренировки по устранению различных видов нештатных ситуаций.
  5. При обнаружении недостатков в Политике по результатам тренировок и/или опыта устранения инцидентов информационной безопасности (нештатных ситуаций), в нее могут вноситься изменения.
  6. При возникновении сбоев, отказов и аварий в системах электроснабжения, вентиляции, иных обеспечивающих инженерных систем проводятся следующие мероприятия:

• Пользователи корректно отключают и обесточивают свои АРМ;

• системный администратор корректно отключает и обесточивает серверы и сетевое оборудование;

• Администратор предпринимает меры к эвакуации носителей информации и носителей резервных копий;

• при нарушении штатного функционирования технических средств информационных систем в результате стихийных бедствий или природных явлений вышедшее из строя оборудование подлежит ремонту, либо замене на новое;

• при возникновении ситуации утраты защищаемых данных, нарушения целостности программного обеспечения и/или баз данных, средств защиты информации после стихийных бедствий или природных явлений, Администратор восстанавливает их из резервных копий;

• при возникновении стихийных действий/природных явлений, представляющих угрозу жизни и/или здоровью человека в первую очередь, проводится эвакуация персонала и только при наличии возможности организуется эвакуация технических средств, носителей информации и носителей с резервными копиями.

* 1. При возникновении нештатных ситуаций, проистекающих из стихийных бедствий и опасных природных явлений, предпринимаются следующие меры реагирования:

- корректное отключение технических средств информационных систем до разряда аккумуляторов источников бесперебойного питания, перегрева технических средств и/ или иных негативных последствий;

- устранение причин, повлекших сбои, отказы и аварии средств информационных систем, замена/ремонт средств и систем, пришедших в негодность;

- восстановление поврежденных/утраченных/несанкционированно модифицированных данных из резервных копий.

1. КОНТРОЛЬ ЦЕЛОСТНОСТИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ
   1. Администратор в средстве защиты информации от несанкционированного доступа производит настройку контроля целостности через расчет эталонных контрольных сумм файлов и директорий прикладного программного обеспечения, операционных систем и средств защиты информации.
   2. На АРМ – персональных компьютерах контроль целостности осушествляется в отношении системных файлов операционной системы и файлов установленных средств защиты.
   3. Каждый факт нарушения целостности программного обеспечения рассматривается в качестве инцидента информационной безопасности. При выявлении таких инцидентов, Администратором принимаются меры реагирования для их устранения самостоятельно или в составе ГРИИБ.
   4. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ не допускается использование средств разработки и отладки программ, за исключением Пользователей, которым данное ПО необходимо для исполнения их трудовых обязанностей.
2. ПРАВИЛА ИСПОЛЬЗОВАНИЯ ЭЛЕКТРОННОЙ ПОЧТЫ И ЗАЩИТЫ ОТ СПАМА
   1. Сервис электронной почты \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ предназначен для ведения служебной или деловой переписки, использования в бизнес- и технологических процессах.
   2. За каждым сотрудником, использующим сервис электронной почты, закреплен свой персональный адрес, или список адресов. Использование почтовых адресов, не закрепленных за лицом, не допускается.
   3. Все электронные почтовые сообщения, проходящие через сервера электронной почты, в обязательном порядке проверяются антивирусным программным обеспечением.
   4. При пользовании сервисом электронной почты Пользователям запрещается организовывать несанкционированные массовые рассылки, распространять спам, а также запрещается использование электронной почты в целях и в формах, противоречащих действующему законодательству Российской Федерации.
   5. Автоматическая пересылка и хранение почтовых сообщений на внешних серверах почтовых систем, облачных сервисов, не допускается.
   6. Пользователям следует рационально подходить к числу и размеру отправляемых и хранимых сообщений. Надлежит периодически очищать почтовый ящик, удалять старые сообщения, которые больше не нужны и перемещать необходимые сообщения в соответствующие почтовые папки.
3. КОНТРОЛЬ ИСПОЛЬЗОВАНИЯ ТЕХНОЛОГИЙ МОБИЛЬНОГО КОДА

18.1 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ не разрешено использование технологий мобильного кода .

  Приложение № \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ к Политике информационной безопасности

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,  утвержденной приказом

от \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ г. №\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

ЗАЯВКА

о внесении изменений в списки пользователей и наделение пользователей полномочиями доступа к ресурсам

информационной системы \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Прошу зарегистрировать пользователя информационной системы:  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

предоставив ему полномочия, необходимые для решения задач:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

|  |  |  |
| --- | --- | --- |
| Начальник | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(подпись) |  |

|  |  |  |
| --- | --- | --- |
| Согласовано | Администратор безопасности | |
| «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_ г. | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(подпись) | (фамилия) |

ЗАДАНИЕ

 на изменения в списки пользователей информационной системы \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

|  |  |
| --- | --- |
|  | Администратору безопасности информации \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
|  | Произвести изменения в списках пользователей |
|  | \_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
|  |  |

Обратная сторона заявки

Присвоен идентификатор \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (имя учетной записи) и предоставлены полномочия, необходимые для решения следующих задач:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Администратор безопасности \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Имя учетной записи, персональный идентификатор (имя учетной записи) и начальное значение пароля получил, о необходимости смены пароля при первом входе в систему проинструктирован, с инструкцией Пользователя \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ ознакомлен.

Пользователь \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(подпись, фамилия)

«\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_ года

Приложение № \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ к Политике информационной безопасности \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, утвержденной приказом

от \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ г. № \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Положение о разграничении прав доступа в информационной системе \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Учитывая особенности обработки защищаемой информации в \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ устанавливается перечень, состоящий из групп Пользователей, служб и процессов, задействованных в обработке защищаемой информации. Перечень ролей и описание параметров доступа к ресурсам информационной системы указан в таблице.

|  |  |
| --- | --- |
| Роль | Параметры доступа к ресурсам информационной системы для данной роли |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

Приложение № \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ к Политике информационной безопасности \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, утвержденной приказом

от \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ г. № \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Перечень лиц, должностей, служб и процессов, допущенных к работе с ресурсами информационной системы \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Перечень представляет собой таблицу со списком должностных лиц и процессов, допущенные к работе с ресурсами информационной системы \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. Сведения, связанные с использованием средств криптографической защиты информации в данном перечне не отражаются, они подлежат отражению в иных документах в случае использования этих средств. Для должностного лица в таблице указывается должность, присвоенная учетная запись и роль в соответствии с Положением о разграничении прав доступа в информационной системе, а также тип и серийный номер выданного идентификатора при выдаче электронного ключа. Сотрудник, получивший электронный ключ, должен расписаться в его получении.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| № п/п | ФИО сотрудника / Наименование службы или процесса | Должность | Присвоенная учетная запись | Роль | Сведение о выдаче электронного ключа | Роспись о получении электронного ключа |
|  | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |  |

Приложение № \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ к Политике информационной безопасности

 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,  утвержденной приказом

от \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ г. № \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Список помещений, в которых ведется работа с использованием информационной системы \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, где находятся технические средства информационной системы, а также перечень лиц, допущенных в эти помещения

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| № п/п | Название/номер помещения | Техническое средство информационной системы | | | | | | Сотрудники, допущенные в помещение | |
| Тип | Модель | Учетный №(серийный, инвентарный) | Сетевое имя | IP-адрес | MAC-адрес | ФИО | Должность |
|  | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

Приложение №  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  к Политике информационной безопасности \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

утвержденной приказом

от \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ г. № \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Перечень разрешенного программного обеспечения в информационной системе \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| № п/п | Наименование ПО | Тип ПО | Цель применения ПО в информационной системе | Место установки компонентов ПО |
|  | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

Приложение № \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ к Политике информационной безопасности \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

утвержденной приказом

от \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ г. № \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Список прикладного программного обеспечения информационной системы, доступного пользователям внешней информационной системы \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| № п/п | Наименование ПО | Тип ПО | Обоснование необходимости допуска внешних пользователей | Список допущенных внешних пользователей |
|  | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

Приложение № \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ к Политике информационной безопасности

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, утвержденной приказом

от \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ г. № \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Список пользователей информационной системы \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ и внешних пользователей, которым предоставляется удаленный доступ к системе в соответствии с должностными обязанностями

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| № п/п | ФИО | Сотрудник \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | Указание ресурсов, к которым открыт удаленный доступ | Основание для предоставления удаленного доступа (должностные обязанности) | Учетная запись для удаленного доступа | Лимит продолжительности сеанса удаленного доступа |
|  | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

Приложение  № \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ к Политике информационной безопасности

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, утвержденной приказом

 от \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ г. № \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

### АКТ №\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ от \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ г.

 Комиссией в составе:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ – председатель комиссии;

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ – член комиссии;

 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ – член комиссии;

уничтожены машинные носители информации:

|  |  |  |  |
| --- | --- | --- | --- |
| № п/п | Учетный номер машинного носителя | Вид носителя | Примечания |
|  | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
|  | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

 Выполнено уничтожение \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ носителей. Произведена сверка записей Акта с записями Журналов учета машинных носителей информации, эксплуатационной и технической документации к ним.

Списаны с учета машинные носители в Журналах учета машинных носителей информации.

|  |  |  |
| --- | --- | --- |
| Председатель комиссии: |  | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| Члены комиссии: |  | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
|  |  | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

Приложение № \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ к Политике информационной безопасности\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, утвержденной приказом

от \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ г. № \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Порядок резервирования информационных ресурсов в информационной системе \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| № п/п | Наименование информационного ресурса | Место размещения ресурса в системе | Вид резервного копирования | Ответственный за резервное копирование | Место хранения резервной копии | Периодичность проведения копирования |
|  | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

Приложение №  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ к Политике информационной безопасности \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, утвержденной приказом

от \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ г. № \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

План обеспечения непрерывности функционирования информационной системы \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| № п/п | Разновидность нештатной ситуации | Критерии нештатной ситуации | Кому и в какие сроки докладывается в рабочее время | Кому и в какие сроки докладывается в нерабочее время | Срок реализации первоочередных действий | Максимальное время для всех необходимых мероприятий |
|  | Разглашение защищаемой информации сотрудниками, имеющими легальные права доступа к ней |  | Администратору сразу после обнаружения инцидента | Администратору не позднее 8 часов после инцидента | 1 час | 1 день |
|  | Обнаружение несанкционированно скопированной или измененной конфиденциальной информации |  | Администратору сразу после обнаружения инцидента | Администратору не позднее 8 часов после инцидента | 1 час | 1 день |
|  | Несанкционированное копирование или изменение конфиденциальной информации в текущий момент времени со стороны лиц имеющих право доступа к ней |  | Администратору сразу после обнаружения инцидента | Администратору сразу после обнаружения инцидента | Сразу после получения информации об инциденте | 1 день |
|  | Обнаружение подключения технических средств к средствам и системам объекта информатизации |  | Администратору сразу после обнаружения инцидента | Администратору не позднее 8 часов после инцидента | 1 час | 3 часа |
|  | Подключение технических средств к средствам информационной системы в текущий момент времени |  | Администратору сразу после обнаружения инцидента | Администратору сразу после обнаружения инцидента | Сразу после получения информации об инциденте | 3 часа |
|  | Обнаружение закладочных устройств |  | Администратору сразу после обнаружения инцидента | Администратору не позднее 8 часов после инцидента | Сразу после получения информации об инциденте | 1 день |
|  | Установка закладочных устройств злоумышленником в текущий момент времени |  | Администратору сразу после обнаружения инцидента | Администратору сразу после обнаружения инцидента | 10 минут в рабочее время (1 час в нерабочее) | 12 часов |
|  | Маскировка под зарегистрированного пользователя внешним злоумышленником в текущий момент времени |  | Администратору сразу после обнаружения инцидента | Администратору сразу после обнаружения инцидента | 10 минут в рабочее время (1 час в нерабочее) | 12 часов |
|  | Маскировка под зарегистрированного пользователя внутренним злоумышленником или обнаружением факта маскировки |  | Администратору сразу после обнаружения инцидента | Администратору не позднее 8 часов после инцидента | 10 минут в рабочее время (1 час в нерабочее) | 12 часов |
|  | Использование дефектов программного обеспечения ОИ внешним нарушителем в текущий момент времени |  | Администратору сразу после обнаружения инцидента | Администратору сразу после обнаружения инцидента | 10 минут в рабочее время (1 час в нерабочее) | 12 часов |
|  | Использование программных закладок внешним нарушителем в текущий момент времени |  | Администратору сразу после обнаружения инцидента | Администратору сразу после обнаружения инцидента | 10 минут в рабочее время (1 час в нерабочее) | 12 часов |
|  | Использование программных закладок внутренним злоумышленником или обнаружение факта использования |  | Администратору сразу после обнаружения инцидента | Администратору не позднее 8 часов после инцидента | 10 минут в рабочее время (1 час в нерабочее) | 12 часов |
|  | Обнаружение программных вирусов |  | Администратору сразу после обнаружения инцидента | Администратору не позднее 8 часов после инцидента | 10 минут в рабочее время (1 час в нерабочее) | 12 часов |
|  | Хищение носителя защищаемой информации |  | Администратору сразу после обнаружения инцидента | Администратору не позднее 8 часов после инцидента | 1 сутки | 3 дня |
|  | Нарушение функционирования ТС обработки информации в текущий момент времени злоумышленником | Нарушена работа одного пользователя | Администратору сразу после обнаружения инцидента | Администратору сразу после обнаружения инцидента | 10 минут в рабочее время (1 час в нерабочее) | 2 дня |
| Нарушена работа группы пользователей | Администратору сразу после обнаружения инцидента | Администратору сразу после обнаружения инцидента | 10 минут в рабочее время (1 час в нерабочее) | 1 день |
|  | Обнаружение нарушения функционирования ТС обработки информации произведенного злоумышленником | Нарушена работа одного пользователя | Администратору сразу после обнаружения инцидента | Администратору сразу после обнаружения инцидента | 10 минут в рабочее время (1 час в нерабочее) | 2 дня |
| Нарушена работа группы пользователей | Администратору сразу после обнаружения инцидента | Администратору сразу после обнаружения инцидента | 10 минут в рабочее время (1 час в нерабочее) | 1 день |
|  | Блокирование доступа к защищаемой информации путем перегрузки технических средств обработки информации ложными заявками на ее обработку внешним злоумышленником в текущий момент времени |  | Администратору сразу после обнаружения инцидента | Администратору не позднее 8 часов после инцидента | 20 минут в рабочее время (1 час в нерабочее) | 7 дней |
|  | Блокирование доступа к защищаемой информации путем перегрузки технических средств обработки информации ложными заявками на ее обработку внутренним злоумышленником в текущий момент времени |  | Администратору сразу после обнаружения инцидента | Администратору не позднее 8 часов после инцидента | 20 минут в рабочее время (1 час в нерабочее) | 1 день |
|  | Обнаружение произошедшего факта блокировки доступа к защищаемой информации |  | Администратору сразу после обнаружения инцидента | Администратору не позднее 8 часов после инцидента | 20 минут в рабочее время (1 час в нерабочее) | 1 день |
|  | Ошибки пользователей системы при эксплуатации ТС, программных средств, средств и систем защиты информации, повлекшие утерю или повреждение защищаемой информации |  | Администратору сразу после обнаружения инцидента | Администратору не позднее 8 часов после инцидента | 2 часа в рабочее время (12 часов в нерабочее) | 1 день |
|  | Ошибки пользователей системы при эксплуатации ТС, программных средств, средств и систем защиты информации, повлекшие нарушение работоспособности ТС и ПО | Нарушена работа одного пользователя | Администратору сразу после обнаружения инцидента | Администратору в первый рабочий день после инцидента | 20 минут | 2 дня |
| Нарушена работа группы пользователей | Администратору сразу после обнаружения инцидента | Администратору сразу после обнаружения инцидента | 20 минут | 1 день |
|  | Дефекты, сбои, отказы, аварии ТС, программных средств и систем информационной системы | Сбой ТС информационной системы | Администратору сразу после обнаружения инцидента | Администратору сразу после обнаружения инцидента | 1 час | 2 дня |
| Отказ ТС информационной системы, затронувший работу группы пользователей | Администратору сразу после обнаружения инцидента | Администратору не позднее 8 часов после инцидента | 1 час в рабочее время (8 часов в нерабочее) | 1 день |
| Отказ ТС информационной системы, затронувший работу одного пользователя | Администратору сразу после обнаружения инцидента | Администратору в первый рабочий день после инцидента | 1 час | 2 дня |
| Авария ТС информационной системы | Администратору сразу после обнаружения инцидента | Администратору не позднее 8 часов после инцидента | 1 час | 1 день |
|  | Сбои, отказы и аварии систем обеспечения информационной системы | Сбой систем обеспечения информационной системы | Ответственному за материально- техническое обеспечение сразу после инцидента | Ответственному за материально- техническое обеспечение в первый рабочий день после инцидента | 1 час | 1 день |
| Отказ систем обеспечения информационной системы, затронувший работу группы пользователей | Ответственному за материально- техническое обеспечение и Администратору сразу после обнаружения инцидента | Ответственному за материально- техническое обеспечение и Администратору сразу после обнаружения инцидента | 1 час | 1 день |
| Отказ систем обеспечения информационной системы, затронувший работу одного пользователя | Ответственному за материально- техническое обеспечение сразу после инцидента | Ответственному за материально- техническое обеспечение в первый рабочий день после инцидента | 1 час | 2 дня |
| Авария систем обеспечения информационной системы | Ответственному за материально- техническое обеспечение, Администратору сразу после обнаружения инцидента | Ответственному за материально- техническое обеспечение, Администратору не позднее 8 часов после инцидента | 1 час | 1 день |
|  | Природные явления, стихийные бедствия, несущие угрозу жизни человека |  | Руководителю, заместителям руководителя, которые оповещают всех своих сотрудников сразу после получения информации | Руководителю, заместителям руководителя, которые оповещают всех своих сотрудников сразу после получения информации | 10 минут | 30 минут |
|  | Природные явления, стихийные бедствия, не несущие угрозу жизни человека |  | Руководителю, заместителям Руководителя, Администратору | Руководителю, заместителям Руководителя, Администратору | 10 минут | 1 час |