Приложение

УТВЕРЖДЕНА
постановлением администрации
муниципального образования
Северский муниципальный район
Краснодарского края
от _____№_____

ПОЛИТИКА
обеспечения отказоустойчивости информационных систем администрации муниципального образования Северский район Краснодарского края

1. Общие положения

1.1. Политика обеспечения отказоустойчивости информационных систем администрации муниципального образования Северский муниципальный район Краснодарского края (далее – Политика) определяет порядок обеспечения отказоустойчивости информационных систем (далее – ИС) администрации муниципального образования Северский муниципальный район Краснодарского края (далее - Администрация).

1.2. Настоящая политика разработана в соответствии с:

Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных»;

приказом Федеральной службы по техническому и экспортному контролю России от 18 февраля 2013 года № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

методическим документом Федеральной службы по техническому и экспортному контролю России от 11 февраля 2014 года «Меры защиты информации в государственных информационных системах».

1.3. Под обеспечением отказоустойчивости информационных систем, в общем случае понимается:

обеспечение целостности информации, программного обеспечения (в том числе, средств защиты информации);

обеспечение доступности информационных систем и средств обработки информации (автоматизированных рабочих мест (далее – АРМ), серверов, активного сетевого оборудования, средств защиты информации) и защищаемой информации;

контроль состояния и качества предоставления уполномоченным

лицом[1)] вычислительных ресурсов (мощностей), в том числе, для передачи информации.

1.4. Обеспечение отказоустойчивости информационных систем реализуется путём:

контроля физического доступа к техническим средствам;

защиты технических средств от внешних воздействий;

резервирования технических средств;

резервного копирования и восстановления информации;

тестирования функций технического и программного обеспечения по реализации отказоустойчивости;

контроля взаимодействия с поставщиками услуг (уполномоченными лицами).

2. Контроль физического доступа и защита технических средств

2.1. Для помещений, в которых размещаются компоненты информационных систем (средства обработки информации), должна обеспечиваться контролируемая зона[2)].

2.2. Границы контролируемой зоны информационных систем отражаются в Технических паспортах информационных систем (в соответствии с политикой использования информационных ресурсов (систем) Администрации).

2.3. Порядок доступа в помещения осуществляется в соответствии с организационно распорядительным документом «Порядок доступа работников Администрации, в помещения, в которых ведётся обработка персональных данных», в которых ведётся обработка защищаемой информации, в том числе персональных данных.

2.4. Учёт доступа в помещения может реализовываться путём:

использования систем контроля и управления доступом;

использования систем охраны помещений;

использования систем видеонаблюдения;

опечатывания помещений и контроля выдачи ключей от помещений;

реализации иных мер, предусмотренных контрольно-пропускным

---

1) Уполномоченное лицо - лицо, обрабатывающее информацию, являющуюся информационным ресурсом, по поручению обладателя информации (заказчика) или оператора и (или) предоставляющее им вычислительные ресурсы (мощности) для обработки информации, в том числе на основании заключенного договора.

2) Контролируемая зона – пространство (территория, здание, часть здания), в котором исключено неконтролируемое пребывание работников и лиц, не имеющих постоянного допуска (не являющихся работниками), а также посторонних транспортных, технических и иных материальных средств. Границами контролируемой зоны могут являться периметр охраняемой территории, ограждающие конструкции охраняемого здания или охраняемой части здания, если оно размещено на неохраняемой территории.

режимом.

2.5. Должна обеспечиваться защита технических средств от внешних воздействий[3)], включающая поддержание необходимого температурно-влажностного режима - для серверных помещений (путём использования систем кондиционирования).

2.6. Должно исключаться наличие в серверных помещениях труб отопления;

обеспечение выполнения норм и правил пожарной безопасности – для всех помещений размещения технических средств;

обеспечение необходимых для эксплуатации технических средств, условий по степени запылённости воздуха – для всех помещений размещения технических средств;

обеспечение выполнения норм и правил устройства и технической эксплуатации электроустановок, а также соблюдение параметров электропитания и заземления технических средств (в том числе, использование для АРМ; серверов; активного сетевого оборудования; средств защиты информации, выполненных в виде программно-аппаратных комплексов, кратковременных резервных источников питания (достаточных для обеспечения правильного (корректного) завершения работы технического средства, устройства в случае отключения основного источника питания) и (или) долговременных резервных источников питания в случае длительного отключения основного источника питания и необходимости продолжения выполнения техническим средством установленных функциональных задач[4]).

3.Обеспечение отказоустойчивости технических средств

3.1. Обеспечение отказоустойчивости технических средств осуществляется путём:

выполнения требований раздела 2 настоящей Политики;

контроля пороговых значений основных показателей функционирования технических средств (степени загрузки: процессорных мощностей, дискового пространства, оперативной памяти, каналов связи и прочее);

резервирования каналов связи, используемых в виртуальной инфраструктуре;

резервирования информационных ресурсов (систем) и средств

---

3) Внешние воздействия – воздействия окружающей среды, нестабильности электроснабжения, кондиционирования и иные внешние факторы

4) В качестве кратковременных резервных источников бесперебойного питания могут применяться ИБП, в качестве долговременных резервных источников бесперебойного питания могут применяться дизельные или бензиновые генераторные установки, а также резервные линии электропитания

обработки информации (АРМ; серверов; активного сетевого оборудования, в том числе, средств защиты информации, выполненных в виде программно-аппаратных комплексов), имеющих высокую критичность (в соответствии с Политикой использования информационных ресурсов (систем) Администрации). Под резервированием понимается повышение характеристик надёжности технических средств посредством введения аппаратной избыточности за счёт включения запасных (резервных) элементов и связей, дополнительных по сравнению с минимально необходимым для выполнения заданных функций в данных условиях работы.

3.2. Предусматривается три вида резервирования:

нагруженный (горячий) резерв — резервные элементы нагружены так же, как и основные;

облегчённый (ждущий) резерв — резервные элементы нагружены меньше, чем основные;

ненагруженный (холодный) резерв — резервные элементы практически не несут нагрузки.

4. Обеспечение резервного копирования и восстановления информации

4.1. Резервному копированию подлежат:

защищаемая информация (информационные ресурсы: файлы и каталоги, базы данных информационных систем);

виртуальные машины (контейнеры);

параметры настройки, конфигурации и журналы аудита средств защиты информации.

4.2. Резервное копирование может осуществляться следующими способами:

посредством использования специализированного программного обеспечения на хранилища данных (выделенные серверы резервного копирования, ленточные библиотеки, сетевые хранилища) – тип 1 (автоматически);

посредством функционала программного обеспечения (функционала систем управления базами данных (далее - СУБД); прикладного программного обеспечения; функционала средств защиты информации) с их последующим сохранением на места размещения резервных копий (хранилища данных, съёмные носители информации) - тип 2 (автоматически или вручную);

посредством копирования защищаемой информации на места размещения резервных копий (хранилища данных, съёмные носители информации) – тип 3 (вручную).

4.3. Резервные копии запрещается хранить в одном месте с резервируемыми данными.

4.4. Зеркалирование жёстких дисков (использование технологии RAID)

не является процессом резервного копирования защищаемой информации.

4.5. Используемая схема резервного копирования должна обеспечивать производительность, достаточную для сохранения информации в установленные сроки и с заданной периодичностью[5)].

4.6. Предусматриваются следующие схемы резервного копирования:

инкрементальное резервное копирование – копируются только данные, которые были изменены со времени предыдущего резервного копирования. Последующее инкрементальное резервное копирование добавляет только данные, которые были изменены с момента предыдущего;

дифференциальное резервное копирование – копируется каждый файл, который был изменён с момента последнего полного резервного копирования, копируется всякий раз заново;

полное резервное копирование – создаётся полная копия всех данных.

4.7. В случае хранения резервных копий на съёмных носителях информации они должны быть учтены и храниться в соответствии с политикой использования информационных ресурсов (систем) Администрации. Съёмный носитель с резервной копией должен быть подписан и содержать следующую информацию:

перечень информационных ресурсов, резервные копии которых хранятся на данном носителе;

схему резервного копирования;

год, месяц, число, время создания резервной копии.

4.8. Конкретные информационные ресурсы, подлежащие резервному копированию, способ, периодичность[6)] (для каждого способа) их копирования, а также место размещения/хранения резервных копий указывается в Перечне информационных ресурсов, подлежащих резервному копированию (далее – перечень). Форма перечня приведена в приложении 1 к настоящей Политике. Не допускается хранение резервных копий в местах, не предусмотренных для этого. Характеристики процесса резервного копирования определяются администратором информационных ресурсов (систем) по согласованию с обладателями информации, содержащейся в информационном ресурсе (системе) и администратором информационной безопасности Администрации.

4.9. Учёт проведения резервного копирования должен осуществляться автоматизированными средствами (в случае наличия технической возможности) или в «Журнале учёта проведения резервного копирования». Форма журнала приведена в приложении 2 к настоящей Политике. Данный журнал может вестись в электронном виде.

---

5) При выборе схемы резервного копирования должны учитываться следующие характеристики: скорость резервного копирования, нагрузка на каналы связи, нагрузка на дисковую подсистему хранилища, время восстановления защищаемой информации, с учётом критичности информационного ресурса.

6) Ежедневно/ежемесячно/ежеквартально и тому подобное.

4.10. Восстановление защищаемой информации из резервных копий осуществляется в случае её утраты или повреждения вследствие несанкционированного доступа к ней, воздействия вирусов, программных ошибок, ошибок работников или аппаратных сбоев.

4.11. Срок восстановления защищаемой информации (время, в течение которого должно быть выполнено восстановление информации, обеспечивающее требуемые условия непрерывности функционирования информационного ресурса (системы) и доступности информации) определяется обладателем информационного ресурса (системы) и отражается администратором информационного ресурса (системы) в Перечне информационных ресурсов, подлежащих резервному копированию. Восстановление данных из резервных копий должно осуществляться в максимально сжатые сроки, ограниченными техническими возможностями.

4.12. Восстановление информации осуществляется по заявке от обладателя информационного ресурса (системы).

4.13. В зависимости от характера и уровня повреждения информационного ресурса (системы) восстанавливается либо весь массив резервных данных, либо отдельные поврежденные или уничтоженные файлы и папки.

4.14. Все действия по восстановлению защищаемой информации должны быть учтены в «Журнале учёта восстановления информации» (форма журнала приведена в приложении 3 к настоящей Политике).

4.15. Ответственность за резервирование и восстановление защищаемой информации несет администратор информационной безопасности совместно с администратором информационных систем.

4.16. О факте повреждения защищаемой информации и необходимости восстановления защищаемой информации наряду с администратором информационного ресурса уведомляется администратор информационной безопасности. Данный факт регистрируется как инцидент информационной безопасности.

4.17. Резервное копирование параметров настройки, конфигурации, а также журналов аудита средств защиты информации, осуществляется администратором информационной безопасности.

5. Ответственность за исполнение положений настоящей Политики

5.1. Ответственность за исполнение положений настоящей Политики возлагается на всех работников Администрации.

5.2. Пользователи информационных ресурсов Администрации несут ответственность за обеспечение резервного копирования служебных данных, располагающихся на своих АРМ, вне сетевых файловых хранилищ. Резервное хранение таких данных осуществляется строго на учтённые съёмные носители информации.

5.3. Обладатели информации, содержащейся в информационных ресурсах (системах) несут ответственность за:

определение информации, подлежащей резервному копированию;

определение способов и периодов резервного копирования данных, а также необходимых сроков их восстановления;

согласование иных характеристик процесса резервного копирования по представлению лица, ответственного за резервное копирование и восстановление информации.

5.4. Администратор информационной безопасности несет ответственность за:

своевременное уведомление (в формате служебной записки) начальников структурных подразделений Администрации о необходимости обеспечения защиты технических средств (находящихся в зоне его ответственности) от внешних воздействий;

контроль пороговых значений основных показателей функционирования технических средств, находящихся в зоне его ответственности;

определение информации, подлежащей резервному копированию и определение характеристик резервного копирования данных (в зоне своей ответственности);

проведение резервного копирования и восстановление, а также их учёт;

сохранность резервных копий;

периодическую проверку корректности функционирования средств обеспечения отказоустойчивости технических средств;

периодическую проверку функций средств резервного копирования и восстановления защищаемой информации;

осуществление планирования и реализацию контрольных мероприятий по проверке степени выполнения положений настоящей Политики работниками Администрации;

контроль выполнения уполномоченным лицом требований о защите информации, установленных законодательством Российской Федерации и условиями договора (соглашения), на основании которого уполномоченное лицо обрабатывает информацию или предоставляет вычислительные ресурсы (мощности);

организацию процесса управления инцидентами информационной безопасности в части положений настоящей политики (в соответствии с политикой управления событиями безопасности информации).

5.5. Администратор информационных систем несет ответственность за:

контроль пороговых значений основных показателей функционирования технических средств (степени загрузки: процессорных мощностей, дискового пространства, оперативной памяти, каналов связи и прочее);

мониторинг состояния и качества предоставления уполномоченным

лицом услуг по передаче информации, предоставлению вычислительных мощностей;

предоставление на согласование владельцам информационных ресурсов (систем) и администратору информационной безопасности перечней информационных ресурсов, подлежащих резервному копированию;

проведение резервного копирования и восстановление информации (в рамках его зоны ответственности), а также их учёт;

уведомление администратора информационной безопасности о фактах повреждения защищаемой информации и необходимости её восстановления;

сохранность резервных копий;

периодическую проверку корректности функционирования средств обеспечения отказоустойчивости технических средств;

периодическую проверку функций средств резервного копирования и восстановления защищаемой информации.

5.6. Лица, виновные в нарушении положений настоящей Политики, могут быть привлечены к дисциплинарной, материальной, гражданско-правовой и административной ответственности.

Начальник управления информатизации
и информационной безопасности Н.Н.Сергиевская