Приложение 4
к приказу директора
ГБПОУ КК УТМиПТ
от 27.03.2024 г. № 66от
_____ № _____

ПОЛИТИКА
обеспечения отказоустойчивости информационных систем государственного бюджетного профессионального образовательного учреждения Краснодарского края «Успенский техникум механизации и профессиональных технологий»

1. Общие положения

1.1. Политика обеспечения отказоустойчивости информационных систем (далее – Политика) государственного бюджетного профессионального образовательного учреждения Краснодарского края «Успенский техникум механизации и профессиональных технологий» (далее – образовательная организация) определяет порядок обеспечения отказоустойчивости информационных систем (далее – ИС) Техникума.

1.2. Настоящая Политика разработана в соответствии с:

1.2.1 приказом Федеральной службы по техническому и экспортному контролю России от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

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

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

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

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

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

1.3.3 контроль состояния и качества предоставления уполномоченным лицом[1]) вычислительных ресурсов (мощностей), в том числе для передачи информации.

1.4. Обеспечение отказоустойчивости информационных систем реализуется путем:

1.4.1 контроля физического доступа к техническим средствам;

1.4.2 защиты технических средств от внешних воздействий;

1.4.3 резервирования технических средств;

1.4.4 резервного копирования и восстановления информации;

1.4.5 тестирования функций технического и программного обеспечения по реализации отказоустойчивости;

1.4.6 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) государственного бюджетного профессионального образовательного учреждения Краснодарского края «Успенский техникум механизации и профессиональных технологий»).

2.3. Порядок доступа в помещения осуществляется в соответствии с организационно распорядительным документом: «Правила доступа в помещения государственного бюджетного профессионального образовательного учреждения Краснодарского края «Успенский техникум механизации и профессиональных технологий», в которых ведется обработка защищаемой информации, в том числе персональных данных».

2.4. Учет доступа в помещения может реализовываться путем:

2.4.1использования систем контроля и управления доступом;

2.4.2 использования систем охраны помещений;

2.4.3 использования систем видеонаблюдения;

[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.

2.4.4 опечатывания помещений и контроля выдачи ключей от помещений;

2.4.5 реализации иных мер, предусмотренных контрольно-пропускным режимом.

2.5. Должна обеспечиваться защита технических средств от внешних воздействий[3)], включающая:

2.5.1 обеспечение выполнения норм и правил пожарной безопасности – для всех помещений, в которых размещаются технические средства;

2.5.2 обеспечение необходимых для эксплуатации технических средств, условий по степени запыленности воздуха – для всех помещений, в которых размещаются технические средства;

2.5.3 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 путем:

3.1.1 выполнения требований раздела 2 настоящей Политики;

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

3.1.3 резервирования каналов связи, используемых в виртуальной инфраструктуре;

3.1.4 резервирования информационных ресурсов (систем) и средств 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 активов государственного

[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.

бюджетного профессионального образовательного учреждения Краснодарского края «Успенский техникум механизации и профессиональных технологий»).

3.2. Под резервированием понимается повышение характеристик надежности технических средств посредством введения аппаратной избыточности за счет включения запасных (резервных) элементов и связей, дополнительных по сравнению с минимально необходимым для выполнения заданных функций в данных условиях работы.

Предусматривается три вида резервирования:

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

облегченный (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:

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

4.1.2 виртуальные машины (контейнеры);

4.1.3 параметры настройки, конфигурации и журналы аудита средств защиты информации.

4.2. Резервное копирование может осуществляться следующими способами:

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

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

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

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

4.4. Зеркалирование жестких 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:

4.6.1 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;

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

4.6.3 полное резервное копирование – создается полная копия всех данных.

4.7. В случае хранения резервных копий на съемных носителях информации они должны быть учтены и храниться в соответствии с Политикой использования информационных активов государственного бюджетного профессионального образовательного учреждения Краснодарского края «Успенский техникум механизации и профессиональных технологий». Съемный носитель с резервной копией должен быть подписан и содержать следующую информацию:

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

4.7.2 схему резервного копирования;

4.7.3 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 образовательной организации.

4.9. Учет проведения резервного копирования должен осуществляться автоматизированными средствами (в случае наличия технической возможности) или в «Журнале учета проведения резервного копирования» (форма журнала приведена в Приложении 2). 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 учетом критичности информационного ресурса.

[6)] Ежедневно/ежемесячно/ежеквартально и тому подобное.

4.10. Восстановление защищаемой информации из резервных копий осуществляется в случае ее 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 учета восстановления информации» (форма журнала приведена в Приложении 3 к настоящей Политике).

4.15. Ответственность за резервирование и восстановление защищаемой информации несет Администратор 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 образовательной организации.

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

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

5.3.1 определение информации, подлежащей резервному копированию;

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

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

5.4. Администратор информационной безопасности несет ответственность за:

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

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

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

5.4.4 проведение резервного копирования и восстановление, а также их учет;

5.4.5 сохранность резервных копий;

5.4.6 периодическую проверку корректности функционирования средств обеспечения отказоустойчивости технических средств;

5.4.7 периодическую проверку функций средств резервного копирования и восстановления защищаемой информации;

5.4.8 осуществление планирования и реализацию контрольных мероприятий по проверке степени выполнения положений настоящей Политики работниками образовательной организации;

5.4.9 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);

5.4.10 организацию процесса управления инцидентами информационной безопасности в части положений настоящей Политики (в соответствии с Политикой управления событиями безопасности информации образовательной организации).

5.5. Администратор информационных систем несет ответственность за:

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

5.5.2 мониторинг состояния и качества предоставления уполномоченным лицом услуг по передаче информации, предоставлению вычислительных мощностей;

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

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

5.5.5 уведомление Администратора информационной безопасности о фактах повреждения защищаемой информации и необходимости ее восстановления;

5.5.6 сохранность резервных копий;

5.5.7 периодическую проверку корректности функционирования средств обеспечения отказоустойчивости технических средств;

5.5.8 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.

Приложение 1
к политике обеспечения
отказоустойчивости
информационных систем

ПЕРЕЧЕНЬ
информационных ресурсов, подлежащих резервному копированию

№ п/п	Наименование информационной ресурса/системы	Обладатель информации	Способ резервного копирования, средство	Период резервного копирования	Место размещения/хранения резервных копий	Срок восстановления информации	Лицо, ответственное за резервное копирование и восстановление информации
1	2	3	4	5	6	7	8

Дата _____20__ г.

Составитель _____ Ф.И.О.
(подпись)

Приложение 2
к политике обеспечения
отказоустойчивости
информационных систем

ФОРМА ЖУРНАЛА
проведения резервного копирования информации

№ п/п	Наименование информационной ресурса/системы	Схема резервного копирования	Время и дата резервного копирования	Произвел резервное копирование	
				Ф.И.О.	подпись[1)]
1	2	3	4	5	6

Дата _____20__ г.

Составитель _____ Ф.И.О.
(подпись)

[1)] Заполняется в случае ведения журнала на бумажном носителе.

Приложение 3
к политике обеспечения
отказоустойчивости
информационных систем

ФОРМА ЖУРНАЛА
проведения восстановления информации

№ п/п	№ инцидента ИБ[1)]	Наименование информационной ресурса/системы	Источник резервной копии с указанием схемы резервного копирования	Время и дата восстановления	Произвел восстановление	
					Ф.И.О.	подпись[2)]
1	2	3	4	5	6	7

Дата ______20__ г.

Составитель _____ Ф.И.О.
(подпись)

[1)] Номер инцидента сообщается Администратором информационной безопасности согласно «Журналу учета инцидентов информационной безопасности».

[2)] Заполняется в случае ведения журнала на бумажном носителе.