

ПОЛИТИКА
использования информационных активов
государственного бюджетного профессионального
образовательного учреждения Краснодарского края
«Успенский техникум механизации и профессиональных
технологий»

1. Общие положения

1.1. Настоящая политика использования информационных активов (далее – Политика) государственного бюджетного профессионального образовательного учреждения Краснодарского края «Успенский техникум механизации и профессиональных технологий» (далее – образовательная организация) определяет процедуры идентификации (инвентаризации), учета, эксплуатации информационных активов образовательной организации, а также порядок предоставления доступа к ним.

1.2. Настоящая Политика разработана в соответствии с:

1.2.1 Федеральным законом Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

1.2.2 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»;

1.2.3 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»;

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

2. Инвентаризация и учет информационных активов

2.1. Проведение инвентаризации и учета информационных активов является необходимым аспектом обеспечения безопасности информации.

2.2. В общем случае под информационными активами понимаются:

2.2.1 информационные ресурсы, содержание защищаемую информацию (в базах данных, в файловом виде в каталогах);

2.2.2 информационные системы, в которых осуществляется обработка защищаемой информации, в совокупности со средствами обработки такой информации и с учетом технологии ее обработки.

2.3. Информационные ресурсы могут являться как самостоятельными сущностями (например, общие сетевые папки или файлы, хранящиеся на сетевых хранилищах данных), так и составными компонентами информационных систем (например, базы данных информационных систем). В случае если информационные ресурсы являются составными компонентами информационных систем – такие информационные ресурсы подлежат инвентаризации, учету (и другим действиям по управлению информационными ресурсами, в соответствии с положением настоящей Политики) в составе данных информационных систем.

2.4. Средства обработки информации, в составе информационных систем, могут включать:

2.4.1 автоматизированные рабочие места пользователей (далее – АРМ), в том числе мобильные АРМ (ноутбуки);

2.4.2 сервера информационных систем (виртуальные и физические);

2.4.3 съемные носители информации;

2.4.4 активное сетевое оборудование;

2.4.5 средства защиты информации¹);

2.4.6 системное и прикладное программное обеспечение.

2.5. Для каждого информационного актива устанавливается однозначное соответствие между следующими его характеристиками:

2.5.1 тип информационного актива;

2.5.2 собственник информационного актива;

2.5.3 местоположение (месторасположение) информационного актива и его пользователя;

2.5.4 категория информации, обрабатываемой информационным активом и (или) содержащаяся в информационном активе (для информационных ресурсов). В качестве категорий такой информации могут выступать служебная информация, персональные данные и т.д.;

2.5.5 критичность информационного актива;

2.5.6 принадлежность к информационной системе;

2.5.7 администратор информационного актива (лицо, ответственное за обеспечение его функционирования).

2.6. Формы учета информационных активов приведены в приложениях 1-6 к настоящей Политике.

¹) Требования к учету и эксплуатации средств криптографической защиты информации регламентированы Политикой использования средств криптографической защиты информации министерства образования, науки и молодежной политики Краснодарского края.

Учет средств антивирусной защиты информации и средств защиты информации от несанкционированного доступа, устанавливаемых на АРМ пользователей и сервера, может осуществляться функционалом централизованного администрирования данных средств.

2.7. Для каждого информационного ресурса (системы) Администратором данного ресурса (системы), при содействии Администратора информационной безопасности разрабатывается Технический паспорт информационной системы и Описание технологического процесса обработки информации в информационной системе (форма Технического паспорта информационной системы приведена в приложении 7, форма Описания технологического процесса обработки информации в информационной системе приведена в приложении 8).

2.8. Под Собственником информационного актива подразумевается субъект (должностное лицо в рамках юридического лица), осуществляющий владение и использование указанного актива и реализующий полномочия в пределах, установленных законодательством (в том числе, предоставления прав доступа к информационному активу).

2.9. Под критичностью информационного актива понимается степень возможного ущерба в случае нарушения:

2.9.1 конфиденциальности информации, обрабатываемой информационным активом и (или) содержащейся в информационном активе (для информационных ресурсов):

2.9.1.1 неправомерный доступ;

2.9.1.2 копирование;

2.9.1.3. предоставление;

2.9.1.4 распространение.

2.9.2 целостности информации, обрабатываемой информационным активом и (или) содержащейся в информационном активе (для информационных ресурсов):

2.9.2.1 неправомерное уничтожение;

2.9.2.2 неправомерное модифицирование.

2.9.3 доступности информации, обрабатываемой информационным активом и (или) содержащейся в информационном активе (для информационных ресурсов):

2.9.3.1 неправомерное блокирование.

2.10. При определении критичности информационных активов необходимо оперировать следующими критериями:

2.10.1 высокая критичность – если в результате нарушения одного из свойств безопасности (конфиденциальности, целостности, доступности) возможны существенные негативные последствия в социальной, политической, международной, экономической, финансовой или иных областях деятельности и (или) информационная система и (или) пользователь (обладатель информации) не могут выполнять возложенные на них функции;

2.10.2 средняя критичность – если в результате нарушения одного из свойств безопасности (конфиденциальности, целостности, доступности) возможны умеренные негативные последствия в социальной, политической, международной, экономической, финансовой или иных областях деятельности и (или) информационная система и (или) оператор (обладатель информации) не могут выполнять хотя бы одну из возложенных на них функций;

2.10.3 низкая критичность – если в результате нарушения одного из свойств безопасности (конфиденциальности, целостности, доступности) возможны незначительные негативные последствия в социальной, политической, международной, экономической, финансовой или иных областях деятельности и (или) информационная система и (или) оператор (обладатель информации) могут выполнять возложенные на них функции с недостаточной эффективностью или выполнение функций возможно только с привлечением дополнительных сил и средств.

2.11. Под классом защищенности информационной системы по требованиям безопасности информации (далее – класс защищенности) понимается класс защищенности государственной информационной системы и (или) уровень защищенности персональных данных, обрабатываемых информационным активом.

3. Порядок эксплуатации информационных активов

3.1. Порядок использования автоматизированных рабочих мест и серверов.

3.2.1. Работнику для работы в информационной системе и (или) для доступа к информационному ресурсу предоставляется АРМ, введенный в домен образовательной организации.

3.2.2. Каждый работник, обеспеченный АРМ, получает аутентификационную информацию (персональное сетевое имя (имя пользователя), пароль и адрес электронной почты), который предназначается для хранения рабочих файлов. Сведения о правах доступа пользователей к информационным ресурсам отражаются ответственными лицами (согласно разделу 4 настоящей Политики) в матрице доступа.

3.2.3. Работа с информационными активами работникам разрешена только на закрепленных за ними АРМ, в определенное время и только с разрешенным программным обеспечением и сетевыми ресурсами.

3.2.4. Доступ привилегированных пользователей (Администраторов) к информационным ресурсам и (или) системам осуществляется с использованием дополнительных средств аутентификации (факторов).

3.2.5. До ввода аутентификационной информации, пользователями (в том числе привилегированными) запрещаются любые действия с информационным ресурсом и (или) информационной системой.

3.2.6. Самостоятельная установка работниками программного обеспечения на АРМ строго запрещена. Установка и удаление любого программного обеспечения производится только ответственными сотрудниками (Администраторами).

3.2.7. Самостоятельное изменение работниками аппаратной конфигурации АРМ, а также подключение к АРМ мобильных устройств передачи информации (сотовые телефоны, usb-модемы, и прочее) запрещено. Изменение (модификация) аппаратной конфигурации АРМ и серверов производится только ответственными сотрудниками (Администраторами).

3.2.8. АРМ и сервера подлежат опечатыванию/опломбированию (с целью недопущения бесконтрольного изменения аппаратных конфигураций). Опечатывание осуществляется Администратором информационной безопасности. Пользователи АРМ и администраторы серверов обязаны следить за сохранностью данных пломб и в случае их нарушений – незамедлительно сообщать о данном событии Администратору информационной безопасности.

3.2.9. На АРМ и серверах ответственными сотрудниками осуществляется установка пароля на доступ к базовой системе ввода-вывода (BIOS).

3.2.10. На АРМ и серверах ответственными сотрудниками обеспечивается синхронизация системного времени.

3.2.11. На АРМ пользователей должно быть запрещено использование технологий беспроводной передачи данных (в частности, 802.11x Wi-Fi, 802.15.1 Bluetooth, 802.22 WRAN, IrDA и иных беспроводных соединений), а также веб-камер и микрофонов. Использование данных технологий допускается в исключительных случаях, обоснованных служебной необходимостью, и должно быть согласовано пользователем в формате служебной записки с руководителем структурного подразделения и Администратором информационной безопасности. Допускается использование веб-камер и микрофонов для проведения видео- (аудио-) конференций на АРМ, не имеющим непосредственный доступ к информационным системам эксплуатирующийся в образовательной организации.

3.2.12. При работе АРМ и серверов должен обеспечиваться контроль работоспособности (неотключения) программного обеспечения средств защиты информации. Настройка программного обеспечения и средства защиты информации должна осуществляться в соответствии с требованиями эксплуатационной документации на них.

3.2.13. Порядок внесения изменений в состав программного обеспечения и аппаратных характеристик АРМ и серверов информационных систем приведен в разделе 5 настоящей Политики. Все изменения документально фиксируются.

3.2.14. При необходимости отлучиться от АРМ, сотрудник обязан, во избежание осуществления несанкционированного доступа к ресурсам АРМ, принудительно заблокировать АРМ посредством функционала операционной системы или используемого средства защиты информации от несанкционированного доступа.

3.2.15. Передача сотрудниками электронных документов как внутри, так и между подразделениями Техникума производится с использованием учтенных съемных носителей информации, а также посредством общих папок и средств электронной почты. Иные способы передачи запрещены.

3.2. Порядок использования электронной почты.

3.2.1. Электронная почта используется для обеспечения обмена работниками информацией в рамках информационных систем образовательной организации и общедоступных сетей.

3.2.2. Электронная почта образовательной организации предназначена исключительно для использования в служебных целях.

3.2.3. Каждый работник имеет право на просмотр либо иное использование, в интересах образовательной организации, сообщений служебной электронной почты, которые направлены или получены им, соответственно, с его или на его адрес электронной почты.

3.2.4. Все почтовые сообщения, переданные или принятые с использованием служебной электронной почты, принадлежат образовательной организации и являются неотъемлемой частью производственного процесса.

3.2.5. Любые сообщения служебной электронной почты могут быть прочитаны, использованы в интересах образовательной организации, либо удалены уполномоченными на это работниками.

3.2.6. При работе с электронной почтой сотрудник должен учитывать следующие принципиальные положения:

3.2.6.1 электронная почта не является средством гарантированной доставки отправленного сообщения до адресата;

3.2.6.2 электронная почта не является средством передачи информации, обеспечивающим конфиденциальность передаваемой информации. Передачу конфиденциальной информации вне локальной сети необходимо осуществлять только в зашифрованном виде;

3.2.6.3 электронная почта не является средством передачи информации, гарантированно идентифицирующим отправителя сообщения.

3.2.7. Работникам запрещено вести частную переписку с использованием средств служебной электронной почты (к частной переписке относится переписка, не связанная с исполнением работником своих должностных обязанностей). Использование служебной электронной почты для частной переписки работником, является нарушением трудовой дисциплины.

3.2.8. Работникам, на предоставленных им АРМ, запрещается использовать сторонние сервисы электронной почты (gmail.com и другие).

3.2.9. Работникам запрещается использование своего адреса электронной почты для подписки на рассылки и другие сервисы, а также при регистрации на любых сайтах, расположенных в сети Интернет, если они прямо не связаны с должностными обязанностями работника.

3.2.10. В целях повышения уровня безопасности при работе со служебной электронной почтой, при получении входящей корреспонденции:

3.2.10.1 необходимо избегать перехода по ссылкам, содержащихся во входящих электронных сообщениях, полученных от недостоверных источников;

3.2.10.2 открывать вложения электронной почты, полученные от недостоверных источников;

3.2.10.3 проверять адреса отправителей электронной почты с целью предотвращения подделки адреса отправителя путем замены адреса на схожий, но с подменными символами (например, путем замены букв цифрами – замена «www.google.com» на «www.g00gle.com», где вместо буквы «о» используется цифра «0» и прочее);

3.2.10.4 проверять имена и домены отправителя сообщения, ссылки на Интернет-ресурсы, расширения вложенных файлов.

3.2.11. Исходящие электронные сообщения работников образовательной организации должны содержать следующие поля:

3.2.11.1 адрес получателя;

3.2.11.2 тема электронного сообщения;

3.2.11.3 текст электронного сообщения (при необходимости, могут быть вложены различные файлы);

3.2.11.4 подпись отправителя.

3.2.12. Подписываясь в ознакомлении с настоящей Политикой, работник дает согласие на ознакомление и иное использование в интересах образовательной организации его переписки, осуществляемой с использованием служебной электронной почты, и соглашается с тем, что любое использование его переписки, осуществляемой с использованием служебной электронной почты, не может рассматриваться как нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений.

3.2.13. Использование личных мобильных устройств (планшеты, сотовые телефоны) работников возможно только для доступа к сервисам служебной электронной почты. Использование мобильных устройств, для иных целей (доступа к информационным активам) – запрещено.

3.3. Порядок работы в сети Интернет.

3.3.1. Доступ к сети Интернет предоставляется работникам образовательной организации только в целях выполнения служебных обязанностей, требующих непосредственного подключения к внешним информационным ресурсам и (или) повышения эффективности выполнения своих служебных обязанностей.

3.3.2. Работникам запрещается:

3.3.2.1 использовать предоставленный доступ в сеть Интернет в личных целях;

3.3.2.2. использовать специализированные аппаратные и программные средства, позволяющие получить несанкционированный доступ к сети Интернет.

3.3.3. При работе с ресурсами сети Интернет запрещается:

3.3.3.1 публиковать, загружать и распространять материалы, содержащие конфиденциальную информацию, за исключением случаев, когда это входит в должностные обязанности и способ передачи является безопасным, заранее согласованный с Администратором информационной безопасности;

3.3.3.2 публиковать, загружать и распространять информацию, полностью или частично, защищенную авторскими или другим правами, без разрешения владельца;

3.3.3.3 публиковать, загружать и распространять вредоносное ПО, предназначенное для нарушения, уничтожения либо ограничения функциональности любых аппаратных и программных средств, для осуществления несанкционированного доступа;

3.3.3.4 публиковать, загружать и распространять серийные номера к коммерческому программному обеспечению и программное обеспечение для их генерации, пароли и прочие средства для получения несанкционированного

доступа к платным Интернет-ресурсам, а также ссылки на вышеуказанную информацию;

3.3.3.5 публиковать, загружать и распространять материалы, содержащие угрожающую, клеветническую, непристойную информацию, а также информацию, оскорбляющую честь и достоинство других лиц, материалы, способствующие разжиганию национальной розни, подстрекающие к насилию, призывающие к совершению противоправной деятельности и так далее;

3.3.3.6 обращаться к ресурсам сети Интернет, содержащим развлекательную (в том числе музыкальные, видео, графические и другие файлы, не связанные с производственной деятельностью), эротическую или порнографическую информацию;

3.3.3.7 использование анонимных прокси-серверов;

3.3.3.8 фальсификация (попытки фальсификации) своего IP-адрес, а также прочей служебной информации.

3.4. Порядок использования съемных носителей информации.

3.4.1. Под съемными носителями информации понимается, оптические диски, флэш-накопители, SD-карты, внешние накопители на жестких дисках и иные устройства хранения информации.

3.4.2. Под использованием съемных носителей информации понимается их подключение к инфраструктуре АРМ и серверам с целью приема/передачи информации.

3.4.3. Допускается использование только учтенных носителей информации, которые являются собственностью образовательной организации и подвергаются регулярной ревизии и контролю.

3.4.4. Допускается использование (пользователю) съемных носителей информации в тех информационных системах, к которым он имеет санкционированный доступ.

3.4.5. Учет съемных носителей информации, встроенных в корпуса АРМ и серверов, ведется в составе таких технических средств.

3.4.6. Учет съемных носителей информации и факт их выдачи осуществляется в Журнале учета съемных носителей информации (форма журнала учета съемных носителей информации приведена в приложении № 8, форма журнала учета выдачи съемных носителей информации приведена в приложении № 9), который ведется Администратором информационной безопасности. При этом съемные носители информации должны быть соответствующим образом промаркированы.

3.4.7. Хранение съемных носителей информации должно осуществляться в сейфах, запираемых металлических шкафах. Перечень мест хранения съемных носителей информации должен быть заранее определен, при этом в каждом структурном подразделении определяются ответственные лица за обеспечение сохранности съемных носителей информации (форма учета мест хранения съемных носителей информации приведена в приложении № 12).

3.4.8. Съемные носители информации, пришедшие в негодность, или отслужившие установленный срок, подлежат уничтожению. Уничтожение съемных носителей с защищаемой информацией осуществляется комиссией образовательной организации по обеспечению информационной безопасности,

назначаемой приказом директора образовательной организации. По результатам уничтожения носителей составляется акт и сведения заносятся в соответствующий журнал (форма журнала учета и форма акта уничтожения приведены в приложениях 10-11 соответственно).

3.4.9. В следующих случаях должно быть обеспечено надежное уничтожение (стирание) информации, исключающее возможность восстановления защищаемой информации, со съемного носителя:

3.4.9.1 после его приобретения;

3.4.9.2 при его первичном подключении к информационному активу;

3.4.9.3 при передаче для постоянного использования от одного пользователя другому пользователю;

3.4.9.4 при передаче в сторонние организации (в том числе перед и после возвращения из ремонта или перед передачей в утилизацию).

3.4.10. Надежное уничтожение информации обеспечивается Администратором информационной безопасности посредством функционала сертифицированного ФСТЭК России средства защиты информации.

3.4.11. Работники обязаны:

3.4.11.1 использовать носители информации исключительно для выполнения своих служебных обязанностей;

3.4.11.2 обеспечивать физическую безопасность носителей информации;

3.4.11.3 извещать Администратора информационной безопасности о фактах утраты (кражи) носителей информации.

3.4.12. При использовании предоставленных работникам съемных носителей информации запрещено:

3.4.12.1 использовать носители информации в личных целях;

3.4.12.2 передавать носители информации другим лицам;

3.4.12.3 оставлять съемные носители информации без присмотра, если не предприняты действия по обеспечению их физической безопасности.

3.4.13. Любое взаимодействие (обработка, прием/передача информации) с информационными системами посредством использования неучтенных (личных) носителей информации, рассматривается как несанкционированное (за исключением случаев заранее оговоренных и согласованных с Администратором информационной безопасности).

3.4.14. Информация об использовании работниками информационных активов протоколируется и, при необходимости, может быть предоставлена руководителям структурных подразделений.

4. Порядок предоставления доступа к информационным активам

4.1. Права доступа работникам к информационным активам предоставляются на время и в объеме минимально необходимых полномочий для выполнения ими своих должностных обязанностей.

4.2. К работе с информационными активами допускаются лица, назначенные на соответствующую должность и прошедшие инструктаж по вопросам информационной безопасности (ознакомившиеся с организационно-

распорядительной документацией, регламентирующей процессы обработки и защиты информации, в том числе персональных данных).

4.3. Необходимость доступа работника к информационным активам определяет руководитель структурного подразделения на основании должностных обязанностей сотрудника.

4.4. Основанием для предоставления прав доступа работнику к информационным активам является заявка руководителя структурного подразделения, согласованная²⁾ с Владелец информационного актива и Администратором информационной безопасности (форма заявки приведена в приложении 13).

4.5. Права доступа работников к информационным активам (информационным ресурсам, информационным системам) назначаются Администратором информационного актива (после передачи ему согласованной заявки) и назначенные права доступа отражаются ответственным лицом в матрице доступа³⁾ (формы матриц доступа к информационным активам приведены в приложениях 14-17).

4.6. Права доступа работников к информационным активам (средствам защиты информации) назначаются Администратором информационной безопасности и отражаются в матрице доступа.

4.7. В случае наличия на АРМ работника средства защиты информации от несанкционированного доступа, доступ к информационным активам также назначается Администратором информационной безопасности. В таком случае согласованная заявка на предоставление прав доступа работникам передается также и Администратору информационной безопасности.

4.8. Изменение и (или) блокирование прав доступа к информационным активам может осуществляться в следующих случаях:

4.8.1 выявление нарушений работникам исполнения, установленных нормативно-методическими документами образовательной организации, требований по обработке и обеспечению безопасности информации (в том числе персональных данных);

4.8.2 в период отпуска работника – по заявке руководителя структурного подразделения;

4.8.3 в случае изменения должностных обязанностей работника (перевода на другую должность);

4.8.4 в случае увольнения работника (все изменения в правах доступа, связанные с увольнением работника, выполняются администраторами незамедлительно после окончания последнего сеанса работы данного пользователя⁴⁾). Помимо блокирования учетной записи уволенного работника, также должно быть осуществлена минимизация прав доступа к информационному активу для такой учетной записи.

²⁾ Согласование может осуществляться посредством служебной электронной почты.

³⁾ Матрица доступа может вестись в электронном виде.

⁴⁾ Ответственность за своевременное уведомление администраторов о увольнении работников несут руководители структурных подразделений, в чьем подчинении находятся увольняемые работника.

4.9. В случае увольнения работника также изымаются предоставленные ему съемные носители информации и аппаратные идентификаторы.

5. Порядок внесения изменений в состав программного обеспечения и технических средств

5.1. Все изменения программного обеспечения и технических средств (АРМ, серверов) должны быть санкционированы и проводиться только на основании заявок руководителей структурных подразделений образовательной организации.

5.2. Все изменения в состав локально-вычислительной сети структурных подразделений образовательной организации осуществляется – Администратором информационных систем.

5.3. Право внесения изменений в конфигурацию программно-аппаратных средств информационной системы, обрабатывающей защищаемую информацию, предоставляется:

5.3.1 в отношении системных и прикладных программных средств, а также в отношении аппаратных средств АРМ пользователей и серверов – Администратору информационных систем;

5.3.2 в отношении программных и программно-аппаратных средств защиты информации – Администратору информационной безопасности;

5.3.3 в отношении программно-аппаратных средств телекоммуникаций (активного сетевого оборудования) – Администратору информационных систем.

5.4. Запрещено изменение конфигурации аппаратно-программных средств, защищенных АРМ и серверов кем-либо, кроме уполномоченных работников.

5.5. Установка (обновление) программного обеспечения информационных активов производится с эталонных копий программных средств, хранящихся у администраторов информационных систем (эталонные копии программных средств защиты информации хранятся у Администратора информационной безопасности).

5.6. Обновление программного обеспечения осуществляется, в том числе по результатам проведения внутреннего инструментального аудита информационной безопасности (в соответствии с «Политикой аудита информационной безопасности государственного бюджетного профессионального образовательного учреждения Краснодарского края «Успенский техникум механизации и профессиональных технологий»).

5.7. Все добавляемые программные и аппаратные компоненты должны быть предварительно проверены на работоспособность, а также отсутствие вредоносного программного кода.

5.8. Действия по изменению программного обеспечения фиксируются в Реестре разрешенного к использованию в информационных системах государственного бюджетного профессионального образовательного учреждения Краснодарского края «Успенский техникум механизации и профессиональных технологий» (форма реестра приведена в приложении 18).

Реестр ведется Администратором информационной безопасности при содействии Администратора информационных систем.

6. Порядок действий в ходе эксплуатации информационной системы, аттестованной по требованиям безопасности информации

6.1. Аттестованная информационная система по требованиям безопасности информации – информационная система, успешно прошедшая процедуру оценки соответствия требований, предъявляемым к установленному классу защищенности информационной системы (далее – аттестация), на которую, в установленном порядке, организацией имеющей лицензию Федеральной службы по техническому и экспортному контролю (далее – ФСТЭК России) на деятельность по технической защите информации (далее – Лицензиат ФСТЭК России), выдан Аттестат соответствия информационной системы требованиям по безопасности информации (далее – Аттестат соответствия).

6.2. Администратор информационной безопасности и Администратор информационных систем обеспечивают поддержание базовой конфигурации информационных систем и системы защиты информации (структуры системы защиты, состава, мест установки и параметров настройки средств защиты информации, программного обеспечения и технических средств) в соответствии с аттестатом соответствия информационной системы требованиям безопасности информации.

6.3. Виды возможных изменений в состав и структуру аттестованной по требованиям безопасности информации информационной системы и необходимые действия со стороны ее Владельца:

№ п/п	Вид изменений	Порядок необходимых действий
1	2	3
1	Повышение класса защищенности информационной системы.	Необходимо проведение аттестации (повторно) информационной системы с выдачей Аттестата соответствия.
2	Увеличение состава угроз информационной системы, связанное с добавлением новых информационных технологий в информационную систему.	1. Необходимо проведение дополнительных аттестационных испытаний информационной системы (контроль эффективности) в рамках действующего аттестата соответствия. 2. Владелец информационной системы отправляет уведомительное письмо Лицензиату ФСТЭК России, выдавшем Аттестат соответствия, в котором указываются планируемые изменения, а также их причину (форма письма приведена в приложении 19). 3. По результатам анализа планируемых изменений, Лицензиат ФСТЭК России
3	Изменение состава средств защиты информации, указанных в аттестате соответствия, на новые, не указанные в аттестате.	
4	Добавление в состав аттестованной информационной системы новых АРМ и/или серверов.	
5	Переустановка средств защиты информации с аттестованных АРМ и (или) серверов на новые АРМ и (или)	

1	2	3
	серверы с последующим их добавлением в состав аттестованной информационной системы.	принимает решение о необходимости проведения дополнительных аттестационных испытаний информационной системы и определяют порядок проверки эффективности системы защиты информации в рамках вносимых изменений, о чем извещают Владельца информационной системы о принятом решении и последующих совместных действиях по внесению изменений.
6	Переустановка установленных средств защиты информации, указанных в Аттестате соответствия, на аттестованных АРМ и (или) серверах в пределах одной информационной системы.	4. Владелец информационной системы проводит работы в рамках вносимых изменений и, при необходимости, привлекает исполнителей, имеющих соответствующий уровень квалификации, из числа сотрудников организаций, обладающих необходимыми лицензиями ФСТЭК России и Федеральной службы безопасности России (далее – ФСБ) на осуществление видов деятельности, связанных с защитой информации. 5. Лицензиат ФСТЭК России проводит дополнительные аттестационные испытания АС. 6. Дополнительные аттестационные испытания информационной системы проводятся по «Программе и методикам» согласованной с владельцем информационной системы и утвержденной Лицензиатом ФСТЭК России. 7. По результатам дополнительных аттестационных испытаний, лицензиатом ФСТЭК России оформляются протокол проведенных испытаний и заключение. Положительные результаты дополнительных аттестационных испытаний дают право на обработку защищаемой информации в информационной системе с учетом внесенных изменений. 8. Копия уведомительного письма с составом планируемых изменений конфигурации информационной системы, извещение от лицензиата ФСТЭК России, «Программа и методики дополнительных аттестационных испытаний» и отчетная документация по результатам испытаний хранятся владельцем информационной системе вместе с комплектом аттестационных документов на конкретную информационную систему.
7	Понижение класса защищенности	Аттестат соответствия сохраняет свое

1	2	3
	информационной системы (уменьшение числа актуальных угроз, объема обрабатываемых данных, снижение требований к характеристикам безопасности и прочее).	действие.
8	Исключение из состава аттестованной ИС некоторых АРМ и/или серверов.	Аттестат соответствия сохраняет свое действие: 1. Владелец информационной системы пишет уведомительное письмо лицензиату ФСТЭК России, в котором указывает планируемые изменения, а также их причину. 2. Лицензиат ФСТЭК России рассматривает вносимые изменения в конфигурацию информационной системы и извещает владельца информационной системы о возможности внесения данных изменений. 3. Владелец информационной системы самостоятельно проводит работы по внесению изменений в составе аттестованной информационной системы. 4. Копия уведомительного письма с составом планируемых изменений конфигурации информационной системы и извещение от лицензиата ФСТЭК России хранятся владельцем информационной системы вместе с комплектом аттестационных документов.
9	Замена периферийного оборудования АРМ и/или серверов информационной системы: мышки, клавиатуры, блока питания, монитора, принтера, сканера и тому подобное. ⁵⁾	
10	Перемещение АРМ и/или серверов аттестованной информационной системы в пределах контролируемой зоны.	
11	Удаление, установка, переустановка на аттестованных АРМ и (или) серверах прикладного программного обеспечения, не связанного с обработкой защищаемой информации.	
12	Удаление, установка, переустановка на аттестованных АРМ и (или) серверах программного обеспечения, предназначенного для обработки защищаемой информации (без повышения класса защищенности информационной системы).	
13	Увольнение ответственных работников.	

7. Удаленный доступ работников к информационным активам

8.1. Под удаленным доступом к информационным активам образовательной организации понимаются все виды доступа, осуществляемые по внешним каналам связи (проводной (коммутируемый), широкополосный) и с использованием устройств доступа, расположенных за пределами контролируемой зоны образовательной организации.

8.2. Решение о предоставлении удаленного доступа работнику образовательной организации должно быть обосновано служебной необходимостью и согласовано с владельцем информационного актива и Администратором информационной безопасности.

8.3. Удаленный доступ к информационным активам предоставляется Администратором информационного актива на основании служебных записок,

⁵⁾ О данном изменении необходимо уведомление только в случае актуальности угроз безопасности информации, для информационной системы на которую выдан Аттестат соответствия, связанных с побочными электромагнитными излучениями и наводками (ПЭМИН). В случае неактуальности данных угроз – необходимо только внесение изменений в Технический паспорт информационной системы.

согласованных с владельцем информационного актива и Администратором информационной безопасности.

8.4. Работники образовательной организации, которым предоставляется удаленный доступ, несут персональную ответственность за использование предоставляемого доступа только по назначению с соблюдением требований безопасности, устанавливаемых настоящей Политикой и иными нормативно-методическими документами образовательной организации, регламентирующими процессы обработки и обеспечения безопасности информации, в том числе персональных данных.

8.5. Лица, получившие удаленный доступ, обязаны принимать меры по недопущению использования своих компьютеров посторонними лицами для осуществления удаленного доступа к информационным активам.

8.6. Для подтверждения подлинности удаленных соединений (пользователей и администраторов) к информационным активам должна использоваться двухфакторная аутентификация. Также для доступа должны применяться средства криптографической защиты информации, обладающие действующими сертификатами ФСБ России по требованиям, предъявляемым к средствам криптографической защиты информации.

8. Ответственность за исполнение положений настоящей Политики

8.1. Ответственность за исполнение положений настоящей Политики возлагаются на всех работников образовательной организации, осуществляющих работу на средствах вычислительной техники, при этом работники несут ответственность за уведомление Администратора информационной безопасности о любых фактах нарушения установленных требований по обеспечению информационной безопасности (инцидентах информационной безопасности).

8.2. Руководители структурных подразделений образовательной организации несут ответственность за:

8.2.1 определение мест хранения съемных носителей информации и ответственных за обеспечение их сохранности в рамках подразделений;

8.2.2 предоставление администратору информационных систем заявок на изменение прав доступа к информационным ресурсам (системам), предварительно их согласовав с владельцем информации и Администратором информационной безопасности;

8.2.3 своевременное уведомление Администратора информационных систем (ресурсов) и Администратора информационной безопасности об увольнении работников.

8.3. Обладатели информации несут ответственность за согласование доступа пользователей и Администраторов к информационным ресурсам (системам).

8.4. Администратор информационных систем несет ответственность за:

8.4.1 проведение инвентаризации и учета информационных ресурсов (систем) и средств обработки информации;

8.4.2 ведение и поддержание в актуальном состоянии технических паспортов информационных систем;

8.4.3 составление и поддержание в актуальном состоянии описаний технологического процесса обработки информации в информационной системе;

8.4.4 предоставление прав доступа пользователей к информационным ресурсам (системам) в соответствии с согласованными заявками на изменение прав доступа к информационным ресурсам (системам);

8.4.5 ведение матриц доступа к информационным ресурсам (системам) и средствам обработки информации;

8.4.6 ведение Реестра разрешенного к использованию программного обеспечения;

8.4.7 обеспечение поддержания базовой конфигурации информационных систем (мест установки и параметров настройки программного обеспечения и технических средств);

8.4.8 установку, обновление и удаление программного обеспечения на АРМ пользователей и серверах образовательной организации;

8.4.9 изменение (модификацию) аппаратной конфигурации АРМ пользователей и серверов образовательной организации;

8.4.10 опечатывание/опломбирование, а также установку паролей на BIOS АРМ и серверов образовательной организации.

8.5.Администратор информационной безопасности несет ответственность за:

8.5.1 предоставление прав доступа пользователей к информационным ресурсам и информационным системам (в соответствии с согласованными заявками на изменение прав доступа к информационным ресурсам) на тех АРМ пользователей, на которых установлено средство защиты информации от несанкционированного доступа.

8.5.2 ведение матрицы доступа к информационным ресурсам (системам) в соответствии с разграничениями, назначаемыми средством защиты информации от несанкционированного доступа;

8.5.3 ведение учета средств защиты информации и эксплуатационной документации к ним;

8.5.4 установку, обновление и удаление средств защиты информации на АРМ пользователей и серверах образовательной организации;

8.5.5 обеспечение поддержания базовой конфигурации информационных систем (мест установки и параметров настройки программных и программно-аппаратных средств защиты информации);

8.5.6 ведение матриц доступа к средствам защиты информации;

8.5.7 обеспечение содействия администратору информационных систем в части определения классов защищенности и критичности информационных систем при их учете и инвентаризации;

8.5.8 обеспечение содействия администраторам информационных систем при заполнении технических паспортов информационных систем в части перечня используемых средств защиты информации;

8.5.9 согласование заявок пользователей на предоставление прав доступа к информационным ресурсам (системам);

8.5.10 ведение учета и выдачи съемных носителей информации;

8.5.11 осуществление в составе комиссии уничтожения съемных носителей информации;

8.5.12 уведомление лицензиата ФСТЭК России, выдавшего аттестат соответствия информационной системы требованиям по безопасности информации, о планируемых изменениях в аттестованных информационных системах;

8.5.13 осуществление планирования и реализацию контрольных мероприятий по проверке степени выполнения положений настоящей Политики структурными подразделениями образовательной организации;

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

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

Приложение 1
к Политике использования
информационных активов

Форма учета информационных ресурсов и информационных систем

№ п/п	Наименование информационной ресурса/системы	Владелец	Месторасположение ¹⁾		Категория обрабатываемой информации	Критичность	Класс защищенности	Администратор ИР/ИС
			серверный сегмент	пользовательский сегмент				
1	2	3	4	5	6	7	8	9
1								
2								

Дата _____ 20__ г.

Составитель _____ Ф.И.О.
(подпись)

¹⁾ В случае отсутствия в информационной системе разделения компонентов на серверный и пользовательский сегменты (в случае нахождения их (а также в случае отсутствия одного из них) в пределах одной контролируемой зоны) – указывается одно месторасположение.

Приложение 2
к Политике использования
информационных активов

Форма учета автоматизированных рабочих мест пользователей

№ п/п	Наименование (FQDN)	Инвентарный и серийный номер	Ф.И.О., должность пользователя	Перечень ИС, с которыми осуществляется взаимодействие	Месторасположение ¹⁾
1	2	3	4	5	6
1					
2					

Дата _____ 20__ г.

Составитель _____ Ф.И.О.
(подпись)

¹⁾ Место установки технического средства: адрес, № кабинета.

Приложение 3
к Политике использования
информационных активов

Форма учета серверов

№ п/п	Наименование (FQDN)	Роль сервера ²⁾	Инвентарный и серийный номер	Тип ³⁾	Администратор ИС	Перечень ИР/ИС, функционирующих на данном сервере	Месторасполо жение	Критичность
1	2	3	4	5	6	7	8	9
1								
2								

Дата _____ 20__ г.

Составитель _____ Ф.И.О.
(подпись)

²⁾ В качестве Роли сервера может быть: контроллер домена, сервер ИС, сервер резервного копирования, сервер виртуализации, почтовый сервер, файловый сервер и так далее.

³⁾ Физический или виртуальный сервер.

Приложение 4
к Политике использования
информационных активов

Форма учета сетевого оборудования

№ п/п	Наименование (модель)	Инвентарный и серийный номер	Владелец	Месторасположение	Критичность	Администратор
1	2	3	4	5	6	7
1						
2						

Дата _____ 20__ г.

Составитель _____ Ф.И.О.
(подпись)

Приложение 5
к Политике использования
информационных активов

Форма журнала учета съемных носителей информации

№ п/п	Дата, регистрационный номер съемного носителя информации	Учетный номер, откуда поступил	Серийный номер (при наличии)	Тип съемного носителя информации	Отметка об уничтожении съемного носителя информации
1	2	3	4	5	5
1					
2					

Дата _____ 20__ г.

Составитель _____ Ф.И.О.
(подпись)

Приложение 6
к Политике использования
информационных активов

Форма учета средств защиты информации

№ п/п	Наименование средства защиты, эксплуатационной и технической документации	Регистрационные номера средства защиты, эксплуатационной и технической документации	Отметка о подключении (установке) средства защиты			Отметка об изъятии средства защиты		
			Ф.И.О. сотрудника, производившего подключение (установку)	дата подключения (установки) и подписи лиц, произведших подключение (установку)	наименование и инвентарный номер актива, в который установлено средство защиты	дата изъятия	Ф.И.О. сотрудника, производившего изъятие	расписка об изъятии
1	2	3	6	7	8	9	10	11
1								

Дата ____20__ г.

Составитель _____ Ф.И.О.
(подпись)

ТЕХНИЧЕСКИЙ ПАСПОРТ информационной системы

(наименование информационной системы)

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

1. Общие сведения об информационной системе.

1.1. Наименование и назначение информационной
(автоматизированной) системы:

Программно-технические средства ИС размещены _____

1.2. В соответствии с Актом классификации информационная система
классифицирована как:

2. Условия эксплуатации информационной системы.

2.2. Описание технологического процесса обработки информации и
режимы доступа к информационным ресурсам, включающее описание всех
типов внешних, внутренних пользователей (привилегированных,
непривилегированных), полномочий пользователей и тип доступа к
информационным ресурсам:

2.3. Сведения об аттестате соответствия информационно-телекоммуникационной инфраструктуры центра обработки данных, на базе которой функционирует информационная (автоматизированная) система, а также о модели услуг, по которой предоставляются вычислительные услуги:

3. Состав информационной системы.

3.1. Состав программно-технических средств:

3.2. Состав общесистемного и прикладного программного обеспечения:

3.3. Состав телекоммуникационного оборудования информационной (автоматизированной) системы и используемые для передачи информации линии связи:

3.4. Состав средств защиты информации, применяемых в ИС:

4. Сведения о соответствии информационной (автоматизированной) системы требованиям по безопасности информации:

5. Сведения о проведении контроля за обеспечением уровня защищенности информации.

№ п/п	Наименование организации (подразделения), проводившей контроль	Дата проведения контроля	Реквизиты документа с выводами о результатах контроля	Вывод по результатам контроля
1	2	3	4	5

[illegible]

6. Сведения об изменениях состава, условий эксплуатации информационной (автоматизированной) системы и средств защиты информации.
--

[illegible]

Администратор информационных систем

« » _____ 20__ г.

ОПИСАНИЕ **технологического процесса обработки информации в**

(наименование информационной системы)

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

1. Общие сведения

1.1. Настоящее Описание технологического процесса (далее – Описание) определяет совокупность процедур при обработке информации в информационной системе (включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), блокирование, удаление, уничтожение) на компонентах информационной системы.

1.2. Настоящее Описание предназначено для следующих должностных лиц, осуществляющих обработку и защиту информации в информационной системе:

1.2.1 пользователей информационной системы;

1.2.2 руководителей структурных подразделений образовательной организации;

1.2.3 администратора информационных систем образовательной организации;

1.2.4 администратора информационной безопасности образовательной организации.

1.3. Мероприятия по защите информации осуществляются во взаимосвязи с другими мерами по обеспечению установленного режима конфиденциальности проводимых работ.

1.4. Используемые в составе системы защиты информации средства защиты информации от несанкционированного доступа должны иметь действующие сертификаты соответствия требованиям безопасности информации ФСТЭК России.

1.5. За обеспечение нормального функционирования информационной системы отвечают:

Должность, отдел, ФИО, в части

Должность, отдел, ФИО, в части

Должность, отдел, ФИО, в части

1.6. Локальная вычислительная сеть сегментирована и имеет иерархическую архитектуру и использует стек протоколов TCP/IP. Скорость передачи данных до 1000 Мбит/сек. АРМ и сервера входят в состав домена под управлением Active Directory. Для вывода на печать используются сетевые (локальные) принтеры.

1.7. Источниками данных, поступающих в информационную систему, являются данные, вводимые пользователями с клавиатуры, файлы, поступающие из смежных систем при взаимодействии с ними, файлы, загружаемые с учетных съемных носителей информации (флэш-накопители, оптические диски), со сканирующих устройств, а также файлы, генерируемые средствами защиты информации (журналы аудита).

1.8. Вывод информации может осуществляться на печатающие устройства, на учетные съемные носители информации (флэш-накопители, оптические диски).

2. Доступ к информационным ресурсам (системам)

2.1. Объектами доступа в информационной системе являются:

2.1.1 технические средства, предназначенные для обработки и передачи защищаемой информации;

2.1.2 программные средства информационных систем, предназначенные для обработки и передачи защищаемой информации;

2.1.3 учетные съемные носители защищаемой информации;

2.1.4 все виды памяти АРМ и серверов (в том числе оперативная память), в которых может находиться защищаемая информация;

2.1.5 тома и каталоги на магнитных дисках, в которых хранятся файлы, содержащие защищаемую информацию.

2.2. Субъектами доступа в информационной системе являются пользователи (в том числе привилегированные), допущенные к работам в информационных системах образовательной организации.

2.3. К работе в информационной системе образовательной организации допускаются следующие категории пользователей:

работники, обрабатывающие защищаемую информацию;

администраторы информационных систем;

внешние пользователи (при их наличии);

временные пользователи (работники сторонних организаций, осуществляющие настройку систем и подсистем).

2.4. При первичном допуске к работе в информационной системе пользователь знакомится с требованиями нормативно-методических и организационно-распорядительных документов по вопросам обеспечения безопасности информации, проходит инструктаж у Администратора информационной безопасности, получает личный идентификатор и личный текущий пароль.

2.5. Вход в операционную систему АРМ и серверов осуществляется путем ввода доменного имени и пароля пользователя/администратора на экране приветствия средства защиты информации от несанкционированного доступа.

2.6. До прохождения процедуры аутентификации пользователю запрещены любые действия с АРМ.

2.7. После успешной аутентификации и по окончании загрузки операционной системы пользователь получает установленные Администратором информационной безопасности права доступа к устройствам (в том числе сетевым), информационным ресурсам, каталогам, файлам и программам.

2.8. Доступ к информационным ресурсам осуществляется на основании функциональных обязанностей пользователей и в соответствии с «Матрицей разграничения прав доступа пользователей к защищаемым информационным ресурсам». При этом пользователю задаются минимально необходимые полномочия, достаточные для выполнения своих функциональных обязанностей.

3. Обработка информации

3.1. Защищаемая информация обрабатывается на автоматизированном рабочем месте пользователя, с использованием средств защиты информации. В случае необходимости переноса файлов на другие АРМ/сервера, относящиеся к той же информационной системе используются учтенные съемные носители информации (флэш-накопители, оптические диски), общие сетевые папки. Вывод информации на неучтенные съемные носители информации ЗАПРЕЩАЕТСЯ.

3.2. В процессе своей работы пользователь обязан выполнять принятые соглашения по обеспечению безопасности информации в рамках предоставленных привилегий по доступу к информационным ресурсам, контролировать целостность и неизменность программной среды АРМ, не допускать ее «загрязнения» посторонними программными средствами, своевременно извещать руководителя своего структурного подразделения о требуемых изменениях в привилегиях доступа к информационным ресурсам и выявленных нарушениях правил обработки защищаемой информации.

3.3. По окончании работы пользователь информационных ресурсов (систем):

3.3.1 выходит из рабочего приложения, а затем завершает работу АРМ;

3.3.2 закрывает служебное помещение (в случае ухода последним) и опечатывает его (при оснащении входной двери приспособлениями для опечатывания помещений);

3.3.3 включает средства охранной сигнализации (сдает помещение под охрану) – если таковые имеются;

3.3.4 сдает ключи от служебных помещений и хранилищ (сейфов) под роспись в журнале учета.

3.4. Администратор информационной безопасности проводит периодический анализ системных журналов средств защиты информации от несанкционированного доступа на предмет нарушений порядка работ пользователями и попыток несанкционированного доступа к информационным ресурсам (системам).

Дата _____ 20__ г.

Составитель _____ Ф.И.О.
(подпись)

Приложение 9
к Политике использования
информационных активов

Форма журнала учета выдачи съемных носителей информации

№ п/п	Регистрационный номер съемного носителя информации	Тип съемного носителя информации	Дата выдачи	Расписка в получении (ФИО и подпись)	Место хранения съемного носителя информации	Расписка в обратном приеме (ФИО, подпись и дата)
1	2	3	4	5	5	6

Дата _____ 20__ г.

Составитель _____ Ф.И.О.
(подпись)

Приложение 10
к Политике использования
информационных активов

Форма журнала учет уничтожения съемных носителей информации

№ п/п	Тип съемного носителя информации	Учетный номер носителя информации	Обоснование уничтожения носителя информации	Дата уничтожения	Номер акта уничтожения	Ф.И.О. и подпись исполнителя	Ф.И.О. и подпись администратора ИБ
1	2	3	4	5	6	7	8

Дата _____ 20__ г.

Составитель _____ Ф.И.О.
(подпись)

Приложение 11
к Политике использования
информационных активов

**Форма акта уничтожения съемных носителей
информации**

Комиссия в составе:

председатель

комиссии:

произвела отбор съемных носителей информации и установила, что в соответствии с требованиями руководящих документов по защите информации указанные носители и информация, записанная на них в процессе эксплуатации, в соответствии с действующим законодательством Российской Федерации, подлежит гарантированному уничтожению и составила настоящий акт о том, что произведена утилизация носителей конфиденциальной информации в составе:

№ п/п	Тип носителя	Регистрационный номер носителя	Примечание
1	2	3	4

Всего подлежит уничтожению _____ (_____) носителей.
(цифрами) (прописью)

Хранящаяся на указанных носителях информация уничтожена путем:

Перечисленные носители уничтожены путем

Председатель комиссии:

_____/_____
личная подпись инициалы фамилия

Члены комиссии:

_____/_____
личная подпись инициалы фамилия

Приложение 12
к Политике использования
информационных активов

**Перечень мест хранения съемных носителей
информации и лиц, ответственных за их сохранность**

№ п/п	Наименование структурного подразделения	Место хранения (номер помещения)	Ответственное лицо (ФИО, должность)	Подпись
1	2	3	4	5

Дата _____ 20__ г.

Составитель _____ Ф.И.О.
(подпись)

Приложение 13
к Политике использования
информационных активов

**Форма заявки на изменение прав доступа к
информационным ресурсам и системам**

От

_____ «__» _____ 20__ г.
(Ф.И.О., должность)

Сведения о пользователе, которому необходимо изменение прав доступа:

Наименование отдела:	
Ф.И.О. и должность работника, которому необходимо изменение прав доступа к информационным ресурсам:	
Имя АРМ пользователя (FQDN), IP-адрес:	

Основание для изменения прав доступа:

Перечень необходимых прав доступа к информационным системам (ресурсам):

№ п/п	Наименование ИР/ИС ¹⁾	Владелец ИР/ИС	Учетное имя пользователя ²⁾	Необходимое изменение прав доступа
1	2	3	4	5
1				
2				
Необходимость использования съемных носителей информации ³⁾ :				

Перечень информационных ресурсов сети Интернет, доступ к которым необходим в связи со служебной необходимостью:

1. _____.
2. _____.
3. _____.

Согласовано:

Владелец ИР/ИС: _____ / _____
(наименование информационной системы) (Ф.И.О.) (подпись)

Владелец ИР/ИС: _____ / _____
(наименование информационной системы) (Ф.И.О.) (подпись)

Администратор информационной безопасности: _____ / _____
(наименование информационной системы) (Ф.И.О.) (подпись)

¹⁾ Указывается наименование информационной системы и (или) каталога (полный путь с указанием IP-адреса), доступ к которым необходимы.

²⁾ В случае отсутствия – выдается администратором информационной системы.

³⁾ Указывается «ДА» или «НЕТ». В случае наличия необходимости – дополнительно указывается серийный номер съемного носителя информации.

Приложение 14
к Политике использования
информационных активов

**Матрица доступа к информационным активам (объектам
файловой системы (файлам, каталогам), информационным
системам, ресурсам сети Интернет)**

№ п/п	Наименование подразделения	Ф.И.О., должность пользователя	Имя АРМ пользователя	Учетная запись Active Directory	Наименование информационной системы, учетная запись пользователя, его роль (права доступа)		Объекты файловой системы (права доступа)		Перечень необходимых ресурсов сети Интернет, для выполнения должностных обязанностей
					наименование ИС ₁	наименование ИС _п	наименование объекта ₁ (путь)	наименование объекта _п (путь)	
1	2	3	4	5	6	7	8	9	10

Дата _____ 20__ г.

Составитель _____ Ф.И.О.
(подпись)

Приложение 15
к Политике использования
информационных активов

**Матрица доступа к информационным активам
(средствам защиты информации)**

№ п/п	Наименование средства защиты информации	Ф.И.О., должность администратора	Роль	Доступ к журналам аудита средства	Доступ к настройкам средства	Доступ к возможности деактивации функционала средства	Сведения, доступные пользователям ИС о конфигурации средства
1	2	3	4	5	6	7	8

Дата _____ 20__ г.

Составитель _____ Ф.И.О.
(подпись)

Приложение 16
к Политике использования
информационных активов

**Матрица доступа к информационным активам
(серверам информационных систем)**

№ п/п	Наименование (FQDN)	Роль сервера	Инвентарный и серийный номер	Тип	IP-адрес	Ф.И.О., должность администратора	Учетная запись	Полномочия администратора по доступу к серверу
1	2	3	4	5	6	7	8	9

Дата _____20__ г.

Составитель _____ Ф.И.О.
(подпись)

Приложение 17
к Политике использования
информационных активов

**Матрица доступа к информационным активам
(активному сетевому оборудованию)**

№ п/п	Наименование (модель)	Инвентарный и серийный номер	IP-адрес	Ф.И.О., должность администратора	Доступ к настройкам средства	Доступ к просмотру настройкам средства	Доступ к журналам аудита средства
1	2	3	4	5	6	7	8

Дата _____ 20__ г.

Составитель _____ Ф.И.О.
(подпись)

Приложение 18
к Политике использования
информационных активов

**Матрица реестра программного обеспечения,
разрешенного к использованию в информационных
системах государственного бюджетного
профессионального образовательного учреждения
Краснодарского края «Успенский техникум
механизации и профессиональных технологий»**

№ п/п	Дата включения в реестр	Производитель ПО	Название ПО	Версия
1	2	3	4	5
Системное программное обеспечение				
Прикладное программное обеспечение общего назначения				
Прикладное программное обеспечение специализированного назначения ¹⁾				

Дата _____ 20__ г.

Составитель _____ Ф.И.О.
(подпись)

¹⁾ Под прикладным программным обеспечением специализированного назначения понимается программное обеспечение, используемое для обработки защищаемой информации.

Приложение 19
к Политике использования
информационных активов

**Форма уведомление лицензиата ФСТЭК России
о планируемых изменениях информационной
системы, аттестованной по требованиям
безопасности**

Руководителю организации
Почтовый адрес организации

Уважаемый Руководитель!

Уведомляем Вас о внесении следующих изменений в состав и настройку информационной системы «Название ИС», аттестат № «Номер аттестата соответствия» от «Дата выдачи аттестата соответствия», государственного бюджетного профессионального образовательного учреждения Краснодарского края «Успенский техникум механизации и профессиональных технологий» размещенной по адресу: Места размещения компонентов информационной системы.

№ п/п	Состав и причина изменений	Дата внесения изменений
1	2	3
1		
2		
3		

Дата _____ 20__ г.

Составитель _____ Ф.И.О.
(подпись)