Приложение 9
к приказу директора
ГБПОУ КК УТМиПТ
от 27.03.2024 г. № 66

ИНСТРУКЦИЯ
администратора информационных систем государственного бюджетного профессионального образовательного учреждения Краснодарского края «Успенский техникум механизации и профессиональных технологий»

1. Общие положения

1.1. Администратор информационных систем является функциональной ролью (наделенной набором функций, требований, прав и обязанностей), назначаемой работнику государственного бюджетного профессионального образовательного учреждения Краснодарского края «Успенский техникум механизации и профессиональных технологий» (далее – образовательная организация).

1.2. Администратор информационных систем назначается приказом директора образовательной организации.

1.3. Администратор информационных систем функционально подчиняется директору образовательной организации.

1.4. На время отсутствия администратора информационных систем его обязанности исполняет лицо, назначенное в установленном порядке соответствующим приказом директора образовательной организации. Данное ответственное лицо наделяется правами и несет ответственность за надлежащее исполнение возложенных на него обязанностей.

1.5. Администратор информационных систем в своей работе руководствуется следующими нормативно-правовыми и организационно-распорядительными документами в области обработки и защиты информации:

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

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

1.5.3 Постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

1.5.4 приказом Федеральной службы по техническому и экспортному контролю Российской Федерации (далее - ФСТЭК России) от 1 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

1.5.5 приказом ФСТЭК 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»;

1.5.6 настоящей инструкцией администратора информационных систем образовательной организации (далее – Инструкция);

1.5.7 иными организационно-распорядительными документами, правовыми актами образовательной организации, руководящими и нормативными документами регуляторов Российской Федерации в области обработки и обеспечения безопасности информации (в том числе персональных данных).

1.6. Иные должностные лица образовательной организации по мере необходимости могут быть ознакомлены с основными положениями настоящей Инструкции.

1.7. В случае увольнения, администратор информационных систем обязан передать директору образовательной организации, все носители защищаемой информации, дополнительные идентификаторы, ключи от помещений и хранилищ, которые находились в его распоряжении в связи с выполнением им служебных обязанностей во время работы.

2. Обязанности администратора информационных систем в части инвентаризации, учета, эксплуатации и предоставления прав доступа к информационным ресурсам (системам)

2.1. Администратор информационных систем в части обеспечения процесса инвентаризации, учета, эксплуатации и предоставления прав доступа к информационным ресурсам (системам), находящим в его зоне ответственности, обязан:

2.1.1 обеспечивать настройку программного обеспечения в соответствии с требованиями эксплуатационной документации;

2.1.2 осуществлять настройку активного сетевого оборудования, в том числе параметры фильтрации и маршрутизации информационных потоков в соответствии с установленными правилами;

2.1.3 обеспечивать проведение инвентаризации и учета информационных систем, а также средств обработки информации, находящихся в зоне его ответственности, в соответствии с утвержденными формами учета;

2.1.4 обеспечивать процесс ведения и поддержки в актуальном состоянии технических паспортов информационных систем, закрепленных за ним;

2.1.5 обеспечивать процесс составления и поддержки в актуальном состоянии описания технологических процессов обработки информации в информационных системах, закрепленных за ним;

2.1.6 контролировать процесс формирования аутентификационной информации (имен пользователей и паролей доступа), руководствуясь при этом политикой использования аутентификационной информации образовательной организации;

2.1.7 обеспечивать, при наличии технических возможностей, процессы определения логических имен (и) или адресов устройств (MAC-адреса, IP-адреса), доступ которых разрешается к информационному ресурсу (системе), при определении прав доступа к данному информационному ресурсу (системе);

2.1.8 вести и дополнять (в соответствии с заявками работников образовательной организации) реестр программного обеспечения (далее – Реестр), разрешенного к использованию в информационных системах образовательной организации. Перед внесением изменений в Реестр необходимо осуществить согласование с администратором информационной безопасности на предмет отсутствия известных уязвимостей в программном обеспечении, планируемом к внесению в Реестр;

2.1.9 обеспечивать установку, обновление и удаление программного обеспечения, а также изменение состава аппаратной конфигурации АРМ и серверов. Контролировать, чтобы устанавливаемое программное обеспечение входило в Реестр, разрешенного к использованию в информационных системах образовательной организации, а также, чтобы установка программного обеспечения допускалась только с эталонных копий дистрибутивов;

2.1.10 следить за сроками действия лицензий на программное обеспечение;

2.1.11 обеспечивать контроль работоспособности программного обеспечения (в том числе средств защиты информации) на АРМ и серверах информационных систем;

2.1.12 обеспечивать запрет пользователям на доступ к управлению средствами защиты информации;

2.1.13 обеспечивать процессы контроля подключения периферийного оборудования (в том числе съемных носителей информации, usb-модемов и прочих) к АРМ и серверам, в том числе путем контроля использования интерфейсов ввода-вывода. В качестве мер контроля использования интерфейсов[1]) ввода-вывода могут выступать такие меры как опечатывание интерфейсов ввода-вывода, использование механических запирающих устройств, удаление драйверов, обеспечивающих работу интерфейсов ввода-вывода;

2.1.14 обеспечивать процессы опечатывания/опломбирования АРМ и сервера, а также установку пароля для входа в базовую систему ввода-вывода (BIOS) на всех АРМ и серверах;

2.1.15 обеспечивать процесс ведения матриц доступа к информационным ресурсам (системам), закрепленным за ним. Предоставлять матрицы доступа (для обобщения и по запросу) администратору информационной безопасности;

2.1.16 обеспечивать процессы предоставления и изменения прав доступа пользователям к информационным ресурсам (системам). Изменение прав доступа должно осуществляться только в соответствии с согласованными заявками на изменение прав доступа к информационным ресурсам (системам).

---

[1]) Данные меры должны реализовываться администратором информационных систем в случае отсутствия на АРМ/сервере средства защиты информации от несанкционированного доступа.

При определении прав доступа пользователей допускается группировка учетных записей по ролям.

2.2. Предоставление прав доступа пользователей к информационным ресурсам (системам) может осуществляться:

2.2.1 функционалом операционных систем (в том числе функционалом файловой системы NTFS);

2.2.2 функционалом Active Directory;

2.2.3 функционалом прикладного программного обеспечения.

2.3. При предоставлении прав доступа пользователям к информационным ресурсам (системам) должны соблюдаться следующие основные требования:

2.3.1 предоставлять доступ (пользователям) к информационным ресурсам только в минимально необходимом объеме для выполнения ими своих служебных обязанностей;

2.3.2 блокировать права доступа в случаях выявления нарушений пользователем требований организационно-распорядительных документов образовательной организации, регламентирующих процессы обработки и обеспечения безопасности информации, а также в случае увольнения пользователя.

3. Обязанности администратора информационных систем в части обеспечения надежности информационных систем

3.1. Администратор информационных систем в части обеспечения надежности информационных систем, находящихся в его зоне ответственности, обязан:

3.1.1 обеспечивать процессы поддержания базовой конфигурации информационных систем, закрепленных за ним (мест установки и параметров настройки программного обеспечения и технических средств), в том числе защиту архивных файлов, параметров настройки программного обеспечения и иных данных, не подлежащих изменению в процессе обработки информации;

3.1.2 обеспечивать процессы контроля пороговых значений основных показателей функционирования технических средств (степени загрузки: процессорных мощностей, дискового пространства, оперативной памяти, каналов связи и прочее). Данный контроль может осуществляться как средствами операционных систем, так и дополнительным специализированным программным обеспечением;

3.1.3 обеспечивать процесс ведения перечня информационных ресурсов, подлежащих резервному копированию;

3.1.4 обеспечивать процессы резервного копирования и восстановления информации, а также их учета;

3.1.5 обеспечивать сохранность резервных копий;

3.1.6 обеспечивать проверку работоспособности средств резервного копирования и восстановления информации не реже одного раза в течение 6 месяцев;

3.1.7 обеспечивать процесс устранения уязвимостей информационных систем, выявленных администратором информационной безопасности;

3.1.8 обеспечивать непрерывность регистрации, учета, сбора и хранения (сроком не менее 12 месяцев) событий безопасности информации в соответствии с установленными требованиями;

3.1.9 обеспечивать процессы мониторинга и анализа событий безопасности информации с целью выявления инцидентов информационной безопасности;

3.1.10 уведомлять директора образовательной организации о необходимости обеспечения защиты технических средств от внешних воздействий.

4. Взаимодействие с прочими ответственными лицами

4.1. Администратор информационных систем должен взаимодействовать со следующими ответственными лицами:

4.1.1. С обладателями информации, содержащейся в информационном ресурсе (системе), в части:

4.1.1.1 определения степени критичности информационных систем;

4.1.1.2 определения состава, порядка резервного копирования и восстановления защищаемой информации;

4.1.1.3 согласования прав доступа пользователей информационных систем.

4.1.2. С администратором информационной безопасности, в части:

4.1.2.1 согласования прав доступа пользователей информационных систем;

4.1.2.2 получения от него информации об установленных уровнях защищенности персональных данных, обрабатываемых в информационных системах и уровнях защищенности государственных информационных систем;

4.1.2.3 составления реестра программного обеспечения, разрешенного к использованию в информационных системах образовательной организации;

4.1.2.4 содействия в ходе проведения аудита информационной безопасности;

4.1.2.5 содействия в ходе расследования инцидентов информационной безопасности;

4.1.2.6 предоставления ему (по запросу) журналов аудита событий безопасности информации;

4.1.2.7 информирования его о выявленных нарушениях функционирования средств защиты информации;

4.1.2.8 информирования его об инцидентах информационной безопасности;

4.1.2.9 участия при проведении работ по восстановлению работоспособности средств и систем защиты информации, в рамках своих обязанностей;

4.1.2.10 согласования процессов установки средств защиты информации;

4.1.2.11 оказания помощи в выполнении ими своих служебных обязанностей.

4.1.3. Со сторонними организациями при:

4.1.3.1 проведении ими аттестации информационных систем по требованиям безопасности информации;

4.1.3.2 выполнении ими работ по заключенным государственным контрактам.

5. Права администратора информационных систем

5.1. Администратор информационных систем имеет право:

5.1.1 требовать от пользователей безусловного соблюдения установленной технологии обработки защищаемой информации и выполнения организационно-распорядительных документов образовательной организации, регламентирующих вопросы обработки и защиты информации;

5.1.2 требовать от руководства оказания содействия в исполнении своих должностных обязанностей и прав;

5.1.3 в рамках своих функциональных обязанностей инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения информационной безопасности информационных ресурсов (систем), находящихся в зоне его ответственности;

5.1.4 вносить предложения руководству по совершенствованию процессов управления информационной безопасностью.

6. Ответственность администратора информационных систем

6.1. Администратор информационных систем несет ответственность за:

6.1.1 ненадлежащее исполнение или неисполнение своих должностных обязанностей, предусмотренных настоящей Инструкцией, другими регламентирующими документами в соответствии с действующим законодательством Российской Федерации, трудовым законодательством Российской Федерации, за полноту и качество проводимых им работ по обеспечению функционирования информационных систем, находящихся в зоне его ответственности;

6.1.2 правонарушения, совершенные в процессе своей деятельности в пределах, определенных действующим административным, уголовным и гражданским законодательством Российской Федерации;

6.1.3 разглашение сведений конфиденциального характера и другой защищаемой информации образовательной организации, определенных действующим административным, уголовным и гражданским законодательством Российской Федерации;

6.1.4 нарушение работоспособности или ненадлежащее функционирование находящихся в зоне его ответственности информационных систем (ресурсов) образовательной организации.