Приложение 10
к приказу директора
ГБПОУ КК УТМиПТ
от 27.03.2024 г. № 66

# ИНСТРУКЦИЯ
## администратора информационной безопасности государственного бюджетного профессионального образовательного учреждения Краснодарского края «Успенский техникум механизации и профессиональных технологий»

1. Общие положения

1.1. Администратор информационной безопасности является функциональной ролью (определенным 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 информационной безопасности назначается приказом директора.

1.3. Администратор информационной безопасности функционально подчиняется директору образовательной организации.

1.4. На время отсутствия администратора информационной безопасности (отпуск, болезнь, прочее) его обязанности исполняет лицо, назначенное в установленном порядке приказом директора образовательной организации. Данное ответственное лицо наделяется правами и несет ответственность за надлежащее исполнение возложенных на него обязанностей.

1.5. Администратор информационной безопасности в своей работе руководствуется следующими нормативными правовыми актами 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 11 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 приказом Федеральной службы безопасности Российской Федерации (далее – ФСБ России) от 10 июля 2014 г. № 378 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»;

1.5.7 положением о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005), утвержденным приказом ФСБ России от 9 февраля 2005 г. № 66;

1.5.8 инструкцией об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну, утвержденной приказом Федерального агентства правительственной связи и информации Российской Федерации (далее – ФАПСИ) от 13 июня 2001 г. № 152;

1.5.9 методическими рекомендациями по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности, утвержденными руководством 8 Центра ФСБ России от 31 марта 2015 г. № 149/7/2/6-432;

1.5.10 настоящей инструкцией администратора информационной безопасности государственного бюджетного профессионального образовательного учреждения Краснодарского края «Успенский техникум механизации и профессиональных технологий» (далее - Инструкция);

1.5.11 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 информационной безопасности 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 информационной безопасности в части инвентаризации, учета, эксплуатации и предоставления прав доступа к информационным ресурсам (системам) и средствам защиты информации

2.1. Администратор информационной безопасности в части обеспечения инвентаризации, учета, эксплуатации средств защиты информации и предоставления прав доступа к информационным ресурсам (системам) обязан:

2.1.1 проводить инвентаризацию и учет средств защиты информации и эксплуатационной документации, в том числе учет прав доступа в соответствии с установленными формами учета;

2.1.2 обеспечивать содействие администратору информационных систем (ресурсов) при разработке им технических паспортов на информационные системы и описаний технологического процесса обработки информации в информационных системах;

2.1.3 вести регистрацию, учет, выдачу съемных носителей информации, а также дополнительных идентификаторов доступа к информационным системам. В составе комиссии по обеспечению информационной безопасности (далее – комиссия по ОИБ), осуществлять уничтожение съемных носителей информации и дополнительных средств аутентификации в установленных случаях;

2.1.4 осуществлять контроль подключения периферийного оборудования (в том числе съемных носителей информации, usb-модемов) к АРМ и серверам путем контроля использования интерфейсов ввода (вывода) посредством функционала средства защиты информации от несанкционированного доступа;

2.1.5 согласовывать заявки пользователей на доступ к информационным ресурсам (системам), полученные от руководителей структурных подразделений образовательной организации;

2.1.6 предоставлять и изменять права доступа пользователям к информационным ресурсам (системам) посредством функционала средства защиты информации от несанкционированного доступа. Изменение прав доступа должно осуществляться только в соответствии с матрицами доступа к информационным ресурсам (системам) и средствам обработки информации, получаемым от руководителей структурных подразделений образовательной организации. При назначении прав доступа пользователей допускается группировка учетных записей по ролям.

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

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

2.2.2 предоставлять и изменять права доступа пользователям к средствам защиты информации с учетом минимально необходимых полномочий для выполнения ими своих служебных обязанностей, при этом у пользователей

должны отсутствовать права на деактивацию и изменение параметров безопасности средств защиты информации;

2.2.3 незамедлительно блокировать учетные записи пользователей в случаях выявления нарушений сотрудником требований организационно-распорядительных документов образовательной организации, регламентирующих процессы обработки и обеспечения безопасности информации, а также в случае увольнения пользователя.

## 3. Обязанности администратора информационной безопасности в части обеспечения функционирования информационных ресурсов (систем) и средств защиты информации

3.1. Администратор информационной безопасности в части обеспечения функционирования информационных ресурсов (систем) и средств защиты информации обязан:

3.1.1 осуществлять установку, обновление и удаление (в случае необходимости) средства защиты информации. Установка должна осуществляться в соответствии с требованиями эксплуатационной документации на них и допускается только с эталонных копий сертифицированных дистрибутивов;

3.1.2 обеспечивать поддержание в актуальном состоянии конфигурации (в соответствии с установленными Политикам безопасности) средств защиты информации;

3.1.3 обеспечивать устойчивое функционирование применяемых средств защиты информации на всех этапах их жизненного цикла (внедрение, эксплуатация, модернизация);

3.1.4 обеспечивать непрерывность функционирования средств защиты информации путем проведения периодического контроля работы программных и (или) программного-аппаратных средств защиты информации, а также резервного копирования и, в случае необходимости, восстановления конфигурационных файлов средств защиты информации (импорт и экспорт конфигурации);

3.1.5 деактивировать средства защиты информации на АРМ и серверах только для проведения профилактических мероприятий;

3.1.6 предусмотреть возможность аварийного отключения средств защиты информации в случае их критических сбоев;

3.1.7 хранить эталонные копий сертифицированных дистрибутивов средств защиты информации с соблюдением установленных правил;

3.1.8 настраивать механизм автоматического антивирусного сканирования информационных ресурсов (систем) с учетом их загрузки (сканирование информационных ресурсов (систем) должно выполняться в момент их наименьшей загрузки, например, ночью);

3.1.9 контролировать целостность программно-аппаратной среды компьютера, целостность объектов файловой системы, реестра и других файлов, не подлежащих изменению, а также восстанавливать такие файлы и

ветки реестров в случае обнаружения нарушенной целостности посредством функционала средства защиты информации от несанкционированного доступа, межсетевого экранирования уровня хоста;

3.1.10 следить за сроками действия технической поддержки на средства защиты информации;

3.1.11 согласовывать перечни информационных ресурсов, подлежащих резервному копированию;

3.1.12 контролировать 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);

3.1.13 устанавливать параметры качества паролей пользователей в настройках параметров безопасности в соответствии с требованиями Политики использования аутентификационной информации при доступе к информационным ресурсам и системам образовательной организации;

3.1.14 осуществлять, в автоматическом или ручном режиме, обновление из доверенных источников базы решающих правил системы обнаружения вторжений, антивирусной базы средства антивирусной защиты информации, базу признаков уязвимостей средства анализа защищенности;

3.1.15 обеспечивать непрерывность регистрации, учета, сбора и хранения (сроком не менее 12 месяцев) событий безопасности информации средств защиты информации в соответствии с установленными требованиями.

3.2. Непрерывность регистрации, учета, сбора и хранения событий безопасности информации обеспечивается:

3.2.1 своевременным архивированием и резервным копированием журналов аудита (статистики) средств защиты информации, а также их восстановлением в случае необходимости;

3.2.2 предоставлением доступа к журналам аудита (статистики) только уполномоченным должностным лицам;

3.2.3 контролем пороговых значений степени загрузки дискового пространства для обеспечения возможности ведения (записи) журналов аудита (статистики).

## 4. Обязанности администратора информационной безопасности в части обеспечения состояния защищенности

4.1. Администратор информационной безопасности в части обеспечения состояния защищенности информационной системы образовательной организации обязан:

4.1.1 инициировать процесс определения уровней защищенности персональных данных, обрабатываемых в информационных системах и уровнях защищенности государственных информационных систем и информировать о них администраторов соответствующих информационных систем (ресурсов);

4.1.2 осуществлять планирование и реализацию контрольных

мероприятий по проверке степени выполнения политик и правил образовательной организации по обеспечению защиты информации (в т.ч. защите персональных данных);

4.1.3 участвовать в составе комиссии по ОИБ по внутреннему аналитическому аудиту информационной безопасности и разработке (не реже 1 раза в полугодие) рекомендаций по осуществлению корректирующих воздействий;

4.1.4 проводить внутренний инструментальный контроль защищенности информационных систем с целью выявления (поиска) уязвимостей;

4.1.5 осуществлять посредством функционала средства анализа защищенности контроль соответствия Реестру разрешенного к использованию в информационных системах образовательной организации, установленному на автоматизированных рабочих местах (далее – АРМ) и серверах информационных систем программного обеспечения;

4.1.6 осуществлять контроль установки обновлений программного обеспечения;

4.1.7 осуществлять контроль устранения выявленных ранее уязвимостей;

4.1.8 разрабатывать отчеты с описанием выявленных уязвимостей и планом мероприятий по их устранению;

4.1.9 разрабатывать рекомендации по повышению уровня безопасности информационных ресурсов (систем) и средств обработки информации;

4.1.10 в случае проектирования и внедрения средств защиты информации информационных систем проводить анализ уязвимостей информационных систем;

4.1.11 устранять уязвимости в конфигурации средств защиты информации, выявленные в ходе проведения инструментального аудита;

4.1.12 осуществлять мониторинг и анализ событий безопасности информации с целью выявления инцидентов информационной безопасности;

4.1.13 пересматривать (не реже 1 раза в год) перечень событий безопасности информации, подлежащих регистрации в информационных системах образовательной организации;

4.1.14 регистрировать инциденты информационной безопасности в журнале учета инцидентов;

4.1.15 вести карточки инцидентов информационной безопасности;

4.1.16 определять лиц, ответственных за локализацию и устранение последствий инцидентов информационной безопасности;

4.1.17 контролировать сроки локализации и устранения последствий инцидентов информационной безопасности;

4.1.18 анализировать проделанную ответственными лицами работу по локализации и устранению последствий инцидентов информационной безопасности;

4.1.19 участвовать в составе комиссии по ОИБ для расследования инцидентов информационной безопасности.

## 5. Обязанности администратора информационной безопасности в части эксплуатации, аттестованной по требованиям безопасности информации, информационной системы

5.1. Администратор информационной безопасности в части эксплуатации, аттестованной по требованиям безопасности информации, информационной системы, обязан:

5.1.1 контролировать сроки действия сертификатов соответствия, выданных ФСТЭК России и ФСБ России, на средства защиты информации и, при необходимости, уведомлять ответственных лиц о необходимости обновления (замены) средств защиты информации;

5.1.2 контролировать сроки указанные в аттестатах соответствия информационных систем требованиям по безопасности информации для проведения планового контроля эффективности принимаемых мер по обеспечению информационной безопасности;

5.1.3 разрабатывать уведомления лицензиата ФСТЭК России, выдавшего аттестат соответствия информационной системы требованиям по безопасности информации, о планируемых изменениях в аттестованных информационных системах.

## 6. Взаимодействие с прочими ответственными лицами

6.1. Администратор информационной безопасности должен взаимодействовать со следующими ответственными лицами:

6.1.1. Со всеми работниками образовательной организации в ходе:

6.1.1.1 разъяснения им возникающих вопросов по функционированию средств защиты информации;

6.1.1.2 содействия им при устранении последствий вирусных заражений;

6.1.1.3 проведения аудита информационной безопасности;

6.1.1.4 расследования инцидентов информационной безопасности.

6.1.2. С администратором информационных ресурсов (систем), в части:

6.1.2.1 согласования прав доступа пользователей информационных ресурсов (систем);

6.1.2.2 составления Реестра программного обеспечения, разрешенного к использованию в информационных системах образовательной организации (перед внесением изменений в Реестр администратор информационной безопасности его согласовывает на предмет отсутствия известных уязвимостей в программном обеспечении, планируемом к внесению в Реестр);

6.1.2.3 получения от него (по запросу) журналов аудита событий безопасности информации (или прав на просмотр журналов аудита);

6.1.2.4 информирования его о выявленных несовместимостях версий средств защиты информации с прикладным программным обеспечением (возможных сбоях);

6.1.2.5 согласования процессов установки средства защиты информации;

6.1.2.6 оказания помощи в выполнении ими своих служебных

обязанностей;

6.1.2.7 устранения выявленных уязвимостей.

6.1.3. С ответственным пользователем средств криптографической защиты информации при:

6.1.3.1 согласовании процессов установки средства криптографической защиты информации;

6.1.3.2 оказании помощи в выполнении ими своих служебных обязанностей;

6.1.3.3 устранении выявленных уязвимостей.

6.1.4. Со сторонними организациями при:

6.1.4.1 проведении ими аттестации информационных систем по требованиям безопасности информации;

6.1.4.2 выполнении ими работ по заключенным государственным контрактам.

## 7. Права администратора информационной безопасности

7.1. Администратор информационной безопасности имеет право:

7.1.1. требовать от пользователей безусловного выполнения требований организационно-распорядительных документов образовательной организации, регламентирующих вопросы обеспечения обработки и защиты информации;

7.1.2 требовать от пользователей представления письменных объяснений по фактам нарушений требований организационно-распорядительных документов образовательной организации, регламентирующих вопросы обеспечения обработки и защиты информации;

7.1.3 вносить обоснованные предложения о привлечении к ответственности пользователей, допустивших нарушение установленных требований организационно-распорядительных документов образовательной организации, регламентирующих вопросы обеспечения обработки и защиты информации;

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

7.1.5 в рамках своих функциональных обязанностей инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения информационной безопасности;

7.1.6 вносить предложения руководству по совершенствованию процессов управления информационной безопасности.

## 8. Ответственность администратора информационной безопасности

8.1. Администратор информационной безопасности несет ответственность за:

8.1.1 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 информационной безопасности, находящихся в зоне его ответственности;

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

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

8.1.4 неработоспособность или ненадлежащее функционирование средств защиты информации.