МИНИСТЕРСТВО ОБРАЗОВАНИЯ, НАУКИ И МОЛОДЕЖНОЙ ПОЛИТИКИ КРАСНОДАРСКОГО КРАЯ
ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ КРАСНОДАРСКОГО КРАЯ
«СЛАВЯНСКИЙ ЭЛЕКТРОТЕХНОЛОГИЧЕСКИЙ ТЕХНИКУМ»

ПРИКАЗ

от 30.12.2023 № 954

г. Славянск-на-Кубани

Об организационных мероприятиях по обработке и обеспечению безопасности персональных данных, обрабатываемых в государственном бюджетном профессиональном учреждении Краснодарского края «Славянский электротехнологический техникум»

Во исполнение требований Федерального закона от 27 июля 2008 г. № 152-ФЗ «О персональных данных», в соответствии с постановлениями Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», от 21 марта 2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных», необходимых для обеспечения безопасности персональных данных, обрабатываемых в учреждении, установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности, п р и к а з ы в а ю:

1. Назначить ответственного за организацию обработки персональных данных в техникуме заместителя директора по АХР Е.А. Козырь.

2. Утвердить:

1) правила обработки персональных данных в государственном бюджетном профессиональном учреждении Краснодарского края «Славянский электротехнологический техникум» (приложение 1);

2) правила рассмотрения запросов субъектов персональных данных или их представителей в государственном бюджетном профессиональном учреждении Краснодарского края «Славянский электротехнологический техникум» (приложение 2);

3) правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в государственном бюджетном профессиональном учреждении Краснодарского края «Славянский электротехнологический техникум» (приложение 3).

4) правила доступа в помещения государственном бюджетном профессиональном учреждении Краснодарского края «Славянский электротехнологический техникум», в которых ведется обработка защищаемой информации, в том числе персональных данных (приложение 4);

5) перечень персональных данных, обрабатываемых в государственном

бюджетном профессиональном учреждении Краснодарского края «Славянский электротехнологический техникум» (приложение 5);

6) перечень должностей государственном бюджетном профессиональном учреждении Краснодарского края «Славянский электротехнологический техникум», замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным (приложение 6);

7) перечень информационных ресурсов и систем в государственном бюджетном профессиональном учреждении Краснодарского края «Славянский электротехнологический техникум» (приложение 7);

8) оценку вреда, который может быть причинен субъектам персональных данных в государственном бюджетном профессиональном учреждении Краснодарского края «Славянский электротехнологический техникум» (приложение 8);

9) типовую форму согласия сотрудника государственного бюджетного профессионального учреждения Краснодарского края «Славянский электротехнологический техникум» (приложение 9);

10) типовую форму согласия на обработку персональных данных (приложение 10);

11) типовую форму разъяснения субъекту персональных данных, юридических последствий отказа предоставить свои персональные данные (приложение 11);

12) типовую форму обязательства сотрудника государственного бюджетного профессионального учреждения Краснодарского края «Славянский электротехнологический техникум», непосредственно осуществляющего обработку персональных данных (приложение 12);

13) типовую форму согласия сотрудника государственного бюджетного профессионального учреждения Краснодарского края «Славянский электротехнологический техникум» на передачу (предоставление, распространение) персональных данных (приложение 13);

3. Разместить Э.В. Берёзкину, преподавателю информатики, ответственному редактору сайта, нормативный документ, указанный в пункте 2 настоящего приказа, на сайте техникума.

4. Контроль за исполнением настоящего приказа возложить на заместителя директора по АХР Е.А. Козырь.

Директор А.А. Осмачкин

Проект внесен:
Заместитель директора по АХР Е.А. Козырь

Приложение 1

УТВЕРЖДЕНЫ
приказом ГБПОУ КК СЭТ
от 30.12.2023 № 954

ПРАВИЛА
обработки персональных данных в государственном бюджетном профессиональном учреждении Краснодарского края «Славянский электротехнологический техникум»

1. Общие положения

1.1. Настоящие Правила обработки персональных данных в государственном бюджетном профессиональном учреждении Краснодарского края «Славянский электротехнологический техникум» (далее – Правила) устанавливают процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных, а также определяют для каждой цели обработки персональных данных содержание обрабатываемых персональных данных, категории субъектов, персональные данные которых обрабатываются, сроки их обработки и хранения, порядок уничтожения при достижении целей обработки или при наступлении иных законных оснований.

1.2. Настоящие Правила разработаны в соответствии с:

Конституцией Российской Федерации;

Трудовым кодексом Российской Федерации;

Федеральным законом Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (далее – Федеральный закон «О персональных данных»);

Федеральным законом Российской Федерации от 25 декабря 2008 г. № 273-ФЗ «О противодействии коррупции» (далее – Федеральный закон «О противодействии коррупции»);

постановлением Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» (далее – Постановление Правительства Российской Федерации № 687);

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» (далее – Постановление Правительства Российской Федерации № 1119).

2. Термины и определения

2.1. Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

2.2. Специальные категории персональных данных – персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни субъектов персональных данных.

2.3. Биометрические персональные данные – персональные данные, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются оператором для установления личности субъекта персональных данных (за исключением сведений, относящихся к специальным категориям персональных данных).

2.4. Персональные данные, разрешенные субъектом персональных данных для распространения, – персональные данные, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных путем дачи согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения в порядке, предусмотренном Федеральным законом «О персональных данных».

2.5. Иные персональные данные – любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных), за исключением персональных данных, относящихся к специальным, биометрическим или персональным данным, разрешенными субъектом персональных данных для распространения.

2.6. Оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

2.7. Обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

2.8. Автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники.

2.9. Распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

2.10. Предоставление персональных данных – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

2.11. Блокирование персональных данных – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

2.12. Уничтожение персональных данных – действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

2.13. Трансграничная передача персональных данных – передача персональных данных на территорию иностранного государства, органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

3. Принципы обработки персональных данных

3.1. Обработка персональных данных в государственном бюджетном профессиональном учреждении Краснодарского края «Славянский электротехнологический техникум» (далее – Техникум) осуществляется в соответствии с настоящими Правилами, а также требованиями, установленными законодательством Российской Федерации с учетом необходимости обеспечения защиты прав и свобод субъектов персональных данных, в том числе защиты права на неприкосновенность частной жизни, личную и семейную тайну, на основе следующих принципов:

обработка персональных данных осуществляется Техникумом в связи с осуществлением функций, возложенных на него, а также реализацией служебных или трудовых отношений;

обработка персональных данных в Техникуме осуществляется лицом (лицами), уполномоченным (и) приказом Техникума на обработку персональных данных и несущим(и) ответственность в соответствии с законодательством Российской Федерации за нарушение режима защиты этих персональных данных (далее – лицо, уполномоченное на обработку персональных данных);

обработка персональных данных ограничивается достижением конкретных, заранее определенных и законных целей;

не допускается обработка персональных данных, несовместимая с целями сбора персональных данных;

не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой;

обработке подлежат только персональные данные, которые отвечают целям их обработки;

содержание и объем обрабатываемых персональных данных

соответствует заявленным целям обработки;

не допускается избыточность обрабатываемых персональных данных по отношению к заявленным целям их обработки;

при обработке персональных данных обеспечиваются точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных;

принимаются необходимые меры, либо обеспечивается их принятие по удалению или уточнению неполных, или неточных персональных данных;

хранение персональных данных осуществляется в форме, позволяющей определить субъекта персональных данных, не дольше, чем того требуют цели обработки персональных данных;

если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем, по которому является субъект персональных данных, обрабатываемые персональные данные уничтожаются, либо обезличиваются по достижении целей обработки или, в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

3.2. Лицо, уполномоченное на обработку персональных данных, обязано:

знать и выполнять требования законодательства в области персональных данных;

хранить в тайне известные ему персональные данные, информировать лицо, ответственное за организацию обработки персональных данных в Техникуме, о фактах нарушения порядка обращения с персональными данными, о попытках несанкционированного доступа к ним;

соблюдать требования настоящих Правил, порядок учета и хранения персональных данных, исключать доступ к ним посторонних лиц;

обрабатывать только те персональные данные, к которым получен доступ в силу исполнения служебных обязанностей;

прекратить обработку персональных данных, ставших известными ему в связи с исполнением должностных обязанностей в случае расторжения с ним служебного контракта.

3.3. Лицу, уполномоченному на обработку персональных данных, запрещается:

использовать сведения, содержащие персональные данные, в неслужебных целях, а также в служебных целях – при ведении переговоров по телефонной сети, в открытой переписке, статьях и выступлениях;

передавать персональные данные по незащищенным каналам связи (телетайп, факсимильная связь, электронная почта) без использования сертифицированных Федеральной службой безопасности России (далее – ФСБ) средств криптографической защиты информации;

выполнять на дому работы, связанные с использованием персональных данных, выносить документы и другие носители информации, содержащие персональные данные, за пределы места (помещения) их хранения;

нарушать режим защиты персональных данных.

3.4. Обработка персональных данных в Техникуме осуществляется как с использованием средств автоматизации (в информационных системах), так и без использования таких средств и включает: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление и изменение, связанные с необходимостью их актуализации), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

3.5. Сбор, запись, систематизация, накопление и уточнение (обновление, изменение) персональных данных осуществляется лицом, уполномоченным на обработку персональных данных, путем:

получения оригиналов необходимых документов;

копирования оригиналов документов;

внесения сведений в учетные формы (на материальных и электронных носителях);

внесения персональных данных в установленном порядке в информационные системы, используемые в Техникуме.

3.6. Трансграничная передача персональных данных в Техникуме не осуществляется.

3.7. Принятие решений, порождающих юридические последствия в отношении субъектов персональных данных или иным образом затрагивающих их права и законные интересы, на основании исключительно автоматизированной обработки их персональных данных, не осуществляется.

3.8. Перечень информационных систем, в которых осуществляется обработка персональных данных, представлен в приложении 1.

3.9. Субъектами персональных данных, чьи персональные данные обрабатываются в Техникуме являются:

- работники техникума;
- обучающиеся (поступающие);
- иные субъекты персональных данных (законные представители обучающихся и т.д.).

4 Условия и порядок обработки персональных данных

4.1. Под персональными данными работников и обучающихся понимается информация, необходимая руководству техникума в связи с трудовыми отношениями и отношениями, возникающими в связи с предоставлением образовательных услуг и касающаяся конкретного работника и обучающегося, а также сведения о фактах, событиях и обстоятельствах жизни работников и обучающихся, позволяющие идентифицировать их личность. Персональные данные являются конфиденциальной информацией, охраняемой в установленном законом порядке.

4.2. Персональные данные добровольно передаются работником и обучающимся непосредственно держателю этих данных и потребителям внутри техникума исключительно для обработки и использования в работе.

4.3. К числу массовых потребителей персональных данных вне техникума относятся государственные и негосударственные учреждения и организации:

налоговые инспекции;

правоохранительные органы;

органы статистики;

страховые агентства;

военкоматы;

органы социального страхования;

пенсионные фонды;

подразделения органов местного самоуправления.

4.4. Внутри техникума к разряду потребителей персональных данных относятся работники структурных подразделений, которым эти данные необходимы для выполнения должностных обязанностей.

специалист по кадрам;

специалисты экономической службы;

руководители структурных подразделений и д.т.

4.5. У специалиста по кадрам хранятся личные дела работников, работающих в настоящее время. Для этого используются специально оборудованные шкафы или сейфы, которые запираются. Личные дела располагаются в алфавитном порядке.

После увольнения работника документы по личному составу передаются на хранение в архив техникума.

4.6. Личные дела обучающихся хранятся в аналогичном порядке в учебной части техникума и после завершения обучения передаются на хранение в архив техникума.

4.7. К персональным данным относятся:

биографические сведения работника или обучающегося;

образование;

специальность;

занимаемая должность;

наличие судимостей;

адрес места жительства;

номера телефонов;

состав семьи;

место работы или учебы членов семьи и родственников;

характер взаимоотношений в семье;

размер заработной платы или стипендии;

содержание трудового договора;

содержание договора об образовании;

содержание декларации, подаваемой в налоговую инспекцию;

подлинники и копии приказов по личному составу и по учебной деятельности;

личные дела, личные карточки (форма Т-2) и трудовые книжки работников;

личные дела обучающихся;

основания к приказам по личному составу и по учебной деятельности;

дела, содержащие материалы по повышению квалификации и переподготовке работников, их аттестации, служебным расследованиям;

копии отчетов, направляемые в органы статистики;

анкета;

копии документов об образовании;

результаты медицинского обследования на предмет годности к осуществлению трудовых обязанностей либо к обучению;

фотографии и иные сведения, относящиеся к персональным данным работника и обучающегося.

фамилия, имя, отчество (в том числе предыдущие фамилии, имена и (или) отчества, в случае их изменения);

число, месяц, год рождения;

место рождения;

информация о гражданстве (в том числе предыдущее гражданства, иные гражданства);

вид, серия, номер документа, удостоверяющего личность, наименование органа, выдавшего его, дата выдачи;

адрес места жительства (адрес регистрации, фактического проживания, дата регистрации по месту жительства);

номер контактного телефон или сведения о других способах связи;

реквизиты страхового свидетельства государственного пенсионного страхования;

идентификационный номер налогоплательщика;

реквизиты страхового полиса обязательного медицинского страхования;

реквизиты свидетельства государственной регистрации актов гражданского состояния;

семейное положение, состав семьи и сведения о близких родственниках (в том числе бывших), необходимых для заполнения анкеты;

сведения о трудовой деятельности;

сведения о воинском учете и реквизиты документов воинского учета;

сведения об образовании, в том числе о послевузовском профессиональном образовании (наименование и год окончания образовательного учреждения, наименование и реквизиты документа об образовании, квалификация, направление подготовки или специальность по документу об образовании);

сведения об ученой степени с указанием подтверждающих документов;

информация о владении иностранными языками, степень владения;

информация о наличии или отсутствии судимости;

государственные награды, иные награды и знаки отличия;

сведения о профессиональной переподготовке и (или) повышении

квалификации;

информация о ежегодных оплачиваемых отпусках, учебных отпусках, отпусках без сохранения денежного содержания и по уходу за ребенком;

номер индивидуального лицевого счета, в том числе родственников для перечисления денежных средств по исполнительным документам;

номер банковской карты.

4.8. Предоставление персональных может осуществляться без письменного согласия субъекта персональных данных в соответствии со статьей 88 Трудового кодекса Российской Федерации в случаях, предусмотренных законодательством Российской Федерации:

статьями 9, 11 Федерального закона Российской Федерации от 1 апреля 1996 г. № 27-ФЗ «Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования»;

пунктом 4 статьи 13 Федерального закона Российской Федерации от 7 февраля 2011 г. № 3-ФЗ «О полиции»;

пунктом 7 ст. 17 Федерального закона от 24 июля 1998 г. № 125-ФЗ «Об обязательном социальном страховании от несчастных случаев на производстве и профессиональных заболеваний»;

статьями 12 и пункта 2 статьи 14 Федерального закона Российской Федерации от 21 июля 1997 г. № 118-ФЗ «О судебных приставах»;

пунктом 2.1 статьи 4 Федерального закона Российской Федерации от 17 января 1992 г. № 2202-1 «О прокуратуре Российской Федерации»;

частью 2 пункта 1 статьи 64 и части 10 статьи 65 Федерального закона Российской Федерации от 2 октября 2007 г. № 229-ФЗ «Об исполнительном производстве».

4.9. Распространение персональных данных осуществляется только с согласия субъекта персональных данных с целью информационного обеспечения (для формирования телефонных справочников и опубликования информации на сайте Техникума).

4.10. Обработка персональных данных в соответствии с Федеральным законом «О персональных данных», Федерального закона «О противодействии коррупции», Трудового кодекса Российской Федерации, осуществляется без согласия субъектов персональных данных для достижения целей, возложенных законодательством Российской Федерации на Техникум функции, полномочий и обязанностей.

4.11. Обработка персональных данных осуществляется при условии получения согласия указанных субъектов персональных данных при передаче (распространении, предоставлении) персональных данных третьим лицам в случаях, не предусмотренных положениями Трудового кодекса Российской Федерации и Федерального закона «О противодействии коррупции».

4.12. В случаях, предусмотренных пунктом 4.11 раздела 4, настоящих Правил, согласие субъекта персональных данных оформляется в письменной форме, если иное не установлено Федеральным законом «О персональных данных».

4.13. Обработка персональных данных осуществляется сотрудниками техникума согласно утвержденного списка.

4.14. Сбор, запись, систематизация, накопление и уточнение (обновление, изменение) персональных данных осуществляется путем:

непосредственного получения оригиналов (с целью их копирования и последующего возврата субъекту персональных данных) необходимых документов (заявление, трудовая книжка, анкета, иные документы);

внесения сведений в учетные формы (на бумажных и электронных носителях);

формирования персональных данных в ходе кадровой работы;

внесения персональных данных в информационные системы техникума.

4.15. Запрещается получать, обрабатывать и приобщать к личному делу персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, интимной жизни.

4.16. При сборе персональных данных сотрудниками техникума осуществляющих сбор (получение) персональных данных обязан разъяснить указанным субъектам персональных данных юридические последствия отказа предоставить их персональные данные, в случае если предоставление персональных данных является обязательным в соответствии с действующим законодательством Российской Федерации.

4.17. Передача (распространение, предоставление) и использование персональных данных осуществляется лишь в случаях и порядке, предусмотренных действующим законодательством Российской Федерации и настоящими Правилами.

4.18. Персональные данные, внесенные в личные дела относятся к сведениям конфиденциального характера (за исключением сведений, которые в установленных федеральными законами случаях могут быть опубликованы в средствах массовой информации).

5. Условия и порядок обработки персональных данных

ботка персональных данных включает в себя их получение, хранение, комбинирование, передачу, а также актуализацию, блокирование, защиту, уничтожение.

5.2. Получение, хранение, комбинирование, передача или любое другое использование персональных данных работника и обучающегося может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности работников и обучающихся, контроля количества и качества выполняемой работы, качества обучения и обеспечения сохранности имущества.

5.3. Все персональные данные работников и обучающихся получаются от них самих. Если персональные данные работника или обучающегося возможно получить только у третьей стороны, то работник или обучающийся должен

быть уведомлен об этом заранее, и от него должно быть получено письменное согласие. Руководство техникума сообщает работнику или обучающемуся о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа работника или обучающегося дать письменное согласие на их получение.

Не допускается получение и обработка персональных данных работника или обучающегося об их политических, религиозных и иных убеждениях и частной жизни, а также об их членстве в общественных объединениях или о профсоюзной деятельности, за исключением случаев, предусмотренных действующим законодательством.

5.4. При принятии решений относительно работника на основании его персональных данных не допускается использование данных, полученных исключительно в результате их автоматизированной обработки или электронного получения.

5.5. В случаях, непосредственно связанных с вопросами трудовых отношений, получение и обработка данных о частной жизни работника возможны только с его письменного согласия.

5.6. Пакет анкетно-биографических и характеризующих материалов (далее пакет) работника формируется после издания приказа о его приеме на работу. Пакет обязательно содержит личную карточку утвержденной формы, а также может содержать документы, содержащие персональные данные работника, в порядке, отражающем процесс приема на работу.

Все документы хранятся в папках в алфавитном порядке фамилий работников.

Пакет пополняется на протяжении всей трудовой деятельности работника в техникуме. Изменения, вносимые в личную карточку утвержденной формы, должны быть подтверждены соответствующими документами (например, копия свидетельства о браке).

Специалист по кадрам, ответственный за документационное обеспечение кадровой деятельности, принимает от устраивающегося на работу работника документы, проверяет полноту и правильность их заполнения, соответствие указываемых сведений с представленными документами.

5.7. Пакет анкетно-биографических и характеризующих материалов (далее пакет) обучающегося формируется после издания приказа о его зачислении на учёбу. В пакете собираются документы, содержащие персональные данные обучающегося, в порядке, отражающем процесс зачисления на учёбу.

Все документы хранятся в папках в алфавитном порядке фамилий обучающихся.

Пакет пополняется на протяжении всего периода обучения в техникуме. Изменения, должны быть подтверждены соответствующими документами (например, копия свидетельства о браке).

Работники техникума, ответственные за приём документов от поступающих на обучение, принимает от поступающих документы, проверяет полноту их заполнения и правильность указываемых сведений в соответствии с предъ-

явленными документами.

5.8. Под блокированием персональных данных понимается временное прекращение операций по их обработке по требованию субъекта персональных данных при выявлении им недостоверности обрабатываемых сведений или неправомерных действий в отношении его данных.

5.9. При обработке персональных данных работников или обучающихся директор техникума вправе определять способы обработки, документирования, хранения и защиты персональных данных работников и обучающихся с использованием современных информационных технологий.

6. Процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации в сфере защиты персональных данных

6.1. Процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации в сфере защиты персональных данных, включают в себя выполнение обязанностей и реализацию комплекса мер по обеспечению безопасности персональных данных, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами и включают в себя:

назначение лица, ответственного за обработку персональных данных в Техникуме;

сбор согласий (в соответствии с установленной типовой формой) на обработку персональных данных, в случаях, установленных действующим законодательством Российской Федерации и настоящими Правилами;

оценку вреда, который может быть причинен субъектам персональных данных Министерства;

обезличивание, уточнение и уничтожение персональных данных, в случаях, когда это необходимо;

определение правил рассмотрения запросов субъектов персональных данных или их представителей;

определение правил работы с обезличенными данными в случае обезличивания персональных данных;

определение порядка доступа в помещения, в которых ведется обработка персональных данных;

осуществление внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным Федеральным законом «О персональных данных», принятыми в соответствии с ним нормативными правовыми актами и локальными актами Техникума;

определение угроз безопасности персональных данных, при их обработке в информационных системах Техникума;

определение уровня защищенности персональных данных, обрабатываемых в информационных системах Техникума;

применение организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных;

исключение несанкционированного, в том числе случайного, доступа к персональным данным, а также иных неправомерных действий в отношении персональных данных;

применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

оценка эффективности принимаемых мер по обеспечению безопасности персональных данных;

учет машинных носителей персональных данных;

обнаружение фактов несанкционированного доступа к персональным данным и принятием мер;

восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

установление правил доступа к персональным данным, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационных системах;

контроль за принимаемыми мерами по обеспечению безопасности персональных данных.

7. Полномочия лица, ответственного за организацию обработки персональных данных в техникуме

7.1. Лицо, ответственное за организацию обработки персональных данных в Техникуме, определяется приказом директора учреждения, получает указания непосредственно от него и подотчетно ему.

7.2. Лицо, ответственное за организацию обработки персональных данных в, обязано:

— организовывать принятие мер, необходимых для обеспечения защиты обрабатываемых персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий;

— осуществлять внутренний контроль, за соблюдением требований законодательства в области персональных данных, в том числе требований к защите персональных данных;

— обеспечить доведение до сведения лиц, непосредственно связанных с реализацией настоящих Правил, положений законодательства в области персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных;

— организовать прием и обработку обращений (запросов) субъектов персональных данных или их представителей, а также осуществлять контроль

за приемом и обработкой таких обращений (запросов);

— в случае нарушения требований к защите персональных данных принимать необходимые меры по восстановлению нарушенных прав субъектов персональных данных.

7.3. Лицо, ответственное за организацию обработки персональных данных, вправе:

7.1.1. В установленном порядке привлекать к реализации мер, направленных на обеспечение безопасности персональных данных, в том числе для проведения внутренних проверок.

7.1.2. Иметь доступ к информации, касающейся обработки персональных данных в техникуме и включающей:

— цели обработки персональных данных;

— категории обрабатываемых персональных данных;

— категории субъектов, персональные данные которых обрабатываются;

— правовые основания обработки персональных данных;

— перечень действий с персональными данными, общее описание используемых способов обработки персональных данных;

— описание мер, предусмотренных статьями 18.1 и 19 Федерального закона «О персональных данных», в том числе сведения о наличии шифровальных (криптографических) средств и наименования этих средств;

— дату начала обработки персональных данных;

— срок или условия прекращения обработки персональных данных;

— сведения о наличии или об отсутствии трансграничной передачи персональных данных в процессе их обработки;

— сведения об обеспечении безопасности персональных данных в соответствии с требованиями к защите персональных данных, установленными Правительством Российской Федерации.

8. Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных

Лица, виновные в нарушении положений законодательства в области персональных данных, привлекаются к дисциплинарной, материальной, гражданско-правовой, административной и (или) уголовной ответственности в порядке, установленном федеральными законами.

Приложение 2

УТВЕРЖДЕНЫ
приказом ГБПОУ КК СЭТ
от 30.12.2023 № 054

ПРАВИЛА
рассмотрения запросов субъектов персональных данных или их представителей в государственном бюджетном профессиональном учреждении Краснодарского края «Славянский электротехнологический техникум»

1. Общие положения

1.1. Настоящие Правила определяют порядок учета (регистрации), рассмотрения запросов субъектов персональных данных или их представителей (далее – запросы) в государственном бюджетном профессиональном учреждении Краснодарского края «Славянский электротехнологический техникум» (далее – Техникум).

1.2. Настоящие Правила разработаны в соответствии с:

Трудовым кодексом Российской Федерации;

Федеральным законом от 27 июня 2006 г. № 152-ФЗ «О персональных данных» (далее – Федеральный закон «О персональных данных»);

Федеральным законом от 2 мая 2006 г. № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации» (далее – Федеральный закон «О порядке рассмотрения обращений граждан Российской Федерации»);

постановлением Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

1.3. Настоящие Правила распространяются на сотрудников Техникума, осуществляющих работу с персональными данными.

2. Права субъектов персональных данных

2.1. Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

подтверждение факта обработки персональных данных;

правовые основания и цели обработки персональных данных;

цели и применяемые способы обработки персональных данных;

наименование и место нахождения оператора, сведения о лицах (за исключением работников оператора, то есть помимо работников оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с Техникумом или на основа-

нии Федерального закона, в соответствии с которым осуществляется предоставление персональных данных;

обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен Федеральным законом;

сроки обработки персональных данных, в том числе сроки их хранения;

порядок осуществления субъектом персональных данных прав, предусмотренных Федеральным законом;

информацию об осуществленной или о предполагаемой трансграничной передаче данных;

наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению Техникума, если обработка поручена или будет поручена такому лицу;

иные сведения.

2.2. Право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с частью 8 статьи 14 Федерального закона «О персональных данных».

2.3. Субъект персональных данных вправе требовать от Техникума уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные Федеральным законом «О персональных данных» меры по защите своих прав.

2.4. Сведения, указанные в части 7 статьи 14 Федерального закона «О персональных данных», должны быть предоставлены субъекту персональных данных в доступной форме и в них не должно содержаться персональных данных, относящихся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных.

2.5. Сведения, указанные в части 7 статьи 14 Федерального закона «О персональных данных», предоставляются субъекту персональных данных или его представителю Техникумом, при обращении субъекта персональных данных, либо при получении запроса субъекта персональных данных или его представителя.

3. Правила рассмотрения запросов субъектов

3.1. Запрос субъекта персональных данных должен содержать:

номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя;

сведения о дате выдачи указанного документа и выдавшем его органе;

сведения, подтверждающие участие субъекта персональных данных в отношениях с Техникумом, либо сведения, иным образом подтверждающие факт обработки персональных данных Техникумом, подпись субъекта персональных данных или его представителя.

3.2. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации, согласно форме, приведенной в приложении 1.

3.3. Рассмотрение запросов является обязанностью уполномоченных сотрудников Техникума.

3.4. Сотрудники обеспечивают:

проверку достоверности сведений, указанных в запросе;

объективное, всестороннее и своевременное рассмотрение запроса;

принятие мер, направленных на восстановление или защиту нарушенных прав, свобод и законных интересов субъектов персональных данных;

направление письменных ответов по существу запроса.

3.5. Запрос прочитывается и проверяется на повторность, при необходимости сверяется с находящейся в архиве предыдущей перепиской. В случае, если сведения, указанные в части 7 статьи 14 Федерального закона «О персональных данных», а также обрабатываемые персональные данные были предоставлены для ознакомления субъекту персональных данных по его запросу, субъект персональных данных вправе обратиться повторно в Техникум или направить повторный запрос в целях получения сведений, указанных в части 7 статьи 14 Федерального закона «О персональных данных», и ознакомления с такими персональными данными в соответствии с частью 4 статьи 14 Федерального закона «О персональных данных» не ранее чем через тридцать дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен предусмотренным Федеральным законом.

3.6. Срок предоставления ответов на поступившие запросы от субъектов персональных данных или их представителей в соответствии с частью 1 статьи 20 Федерального закона «О персональных данных» составляет тридцать дней.

3.7. Субъект персональных данных вправе обратиться повторно в Техникум или направить повторный запрос в целях получения сведений, указанных в части 7 статьи 14 Федерального закона № 152-ФЗ «О персональных данных», а также в целях ознакомления с обрабатываемыми персональными данными до истечения срока, указанного в настоящем пункте, в случае, если такие сведения и (или) обрабатываемые персональные данные не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения. Повторный запрос, наряду с необходимыми сведениями, должен содержать обоснование направления повторного запроса.

3.8. Техникум вправе отказать субъекту персональных данных в выполнении повторного запроса, не соответствующего условиям, предусмотренным частями 4 и 5 статьи 14 Федерального закона «О персональных данных». Такой отказ должен быть мотивированным.

3.9. Техникум обязан сообщить субъекту персональных данных или его представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также предоставить возможность ознакомления с этими персональными данными при обращении

субъекта персональных данных или его представителя, либо дать письменный ответ, согласно форме, приведенной в приложении 2, в течение тридцати дней с даты получения запроса субъекта персональных данных или его представителя.

3.10. В случае отказа в предоставлении информации о наличии персональных данных о соответствующем субъекте персональных данных или персональных данных субъекту персональных данных или его представителю при их обращении, либо при получении запроса субъекта персональных данных или его представителя, уполномоченные должностные лица Техникума обязаны дать в письменной форме мотивированный ответ, содержащий ссылку на положение части 8 статьи 14 Федерального закона «О персональных данных» или иного Федерального закона, являющегося основанием для такого отказа, согласно форм отказов, приведенных в приложении 3, 4.

3.11. Техникум обязан предоставить безвозмездно субъекту персональных данных или его представителю возможность ознакомления с персональными данными, относящимися к этому субъекту персональных данных.

3.12. В соответствии с частью 3 статьи 20 Федерального закона «О персональных данных» Техникум:

в срок, не превышающий семи рабочих дней со дня предоставления субъектом персональных данных или его представителем сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными, сотрудники техникума обязаны внести в них необходимые изменения;

в срок, не превышающий семи рабочих дней со дня представления субъектом персональных данных или его представителем сведений, подтверждающих, что такие персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки, сотрудники Техникума обязаны уничтожить такие персональные данные.

3.13. Техникум обязан уведомить субъекта персональных данных или его представителя о внесенных изменениях и предпринятых мерах и принять разумные меры для уведомления третьих лиц, которым персональные данные этого субъекта были переданы.

3.14. В случае выявления неправомерной обработки персональных данных при обращении субъекта персональных данных или его представителя, либо по запросу субъекта персональных данных или его представителя, либо уполномоченного органа по защите прав субъектов персональных данных, сотрудники Техникума обязаны осуществить блокирование неправомерно обрабатываемых персональных данных, относящихся к этому субъекту персональных данных с момента такого обращения или получения указанного запроса на период проверки.

3.15. В случае выявления неточных персональных данных при обращении субъекта персональных данных или его представителя, либо по их запросу или по запросу уполномоченного органа по защите прав субъектов персональных данных, сотрудники Техникума обязаны осуществить блокирование персональных данных, относящихся к этому субъекту персональных данных, с момента такого обращения или получения указанного запроса на период проверки, если

блокирование персональных данных не нарушает права и законные интересы субъекта персональных данных или третьих лиц.

3.16. В случае подтверждения факта неточности персональных данных сотрудники Техникума на основании сведений, представленных субъектом персональных данных или его представителем, либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов обязаны уточнить персональные данные в соответствии с частью 2 статьи 20 Федерального закона «О персональных данных» в течение семи рабочих дней со дня представления таких сведений и снять блокирование персональных данных.

3.17. В случае выявления неправомерной обработки персональных данных сотрудники Техникума в срок, в соответствии с частью 3 статьи 20 Федерального закона «О персональных данных», не превышающий трех рабочих дней с даты этого выявления, обязаны прекратить неправомерную обработку персональных данных, а в случае, если обеспечить правомерность обработки персональных данных невозможно, сотрудники техникума в срок не превышающий десяти рабочих дней с даты выявления неправомерной обработки персональных данных обязаны уничтожить такие персональные данные или обеспечить их уничтожение. Об устранении допущенных нарушений или об уничтожении персональных данных техникум обязан уведомить субъекта персональных данных или его представителя. В случае, если обращение субъекта персональных данных или его представителя, либо запрос уполномоченного органа по защите прав субъектов персональных данных были направлены уполномоченным органом по защите прав субъектов персональных данных, также в указанный орган.

3.18. Для проверки фактов, изложенных в запросах, при необходимости организуются служебные проверки в соответствии с законодательством Российской Федерации.

3.19. По результатам служебной проверки составляется мотивированное заключение, которое должно содержать объективный анализ собранных материалов. Если при проверке выявлены факты совершения сотрудниками техникума действия (бездействия), содержащего признаки административного правонарушения или состава преступления, информация передается незамедлительно в правоохранительные органы. Служебная проверка проводится в соответствии с установленными в техникума правилами.

Приложение 1
к правилам рассмотрения
запросов субъектов
персональных данных или их
представителей в
государственном бюджетном
профессиональном учреждении
Краснодарского края
«Славянский
электротехнологический
техникум»

ФОРМА

Директору ГБПОУ КК СЭТ

_____
Ф.И.О. субъекта персональных данных

_____
Номер основного документа, удостоверяющего личность

_____
Наименование выдавшего органа

_____
Дата выдачи

Заявление (запрос) о доступе субъекта персональных данных к своим персональным данным

Прошу подтвердить факт обработки моих персональных данных и предоставить мне для ознакомления информацию, составляющую мои персональные данные, на основании:

_____

(указать сведения, подтверждающие участие субъекта персональных данных в отношениях с оператором (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных оператором)

_____ _____ _____
дата подпись расшифровка подписи

Приложение 2
к правилам рассмотрения
запросов субъектов
персональных данных или их
представителей в
государственном бюджетном
профессиональном учреждении
Краснодарского края
«Славянский
электротехнологический
техникум»

ФОРМА

**Ответ на запрос о предоставлении субъекту
его персональных данных**

Уведомление

Уважаемый(ая) _____
(фамилия, имя, отчество)

В ответ на Ваш запрос от _____
(дд.мм.гг.)

сообщаем, что в государственном бюджетном профессиональном учреждении Краснодарского края «Славянский электротехнологический техникум» (далее – Оператор), расположенный по адресу: 353560, Краснодарский край г. Славянск-на-Кубани, ул. Краснодарская, д. 248, осуществляется обработка следующих Ваших персональных данных:

_____

_____
(перечислить персональные данные)

Указанные персональные данные получены

_____

_____
(непосредственно от Вас / указать источник получения персональных данных)

Персональные данные обрабатываются и используются Оператором в целях и на основании

_____

_____
(перечислить цели и правовые основания обработки)

Ваши персональные данные обрабатываются (нужное подчеркнуть) автоматизированным/неавтоматизированным/смешанным способом.

Перечень лиц (за исключением работников Оператора), которые имеют доступ к Вашим персональным данным или которым могут быть раскрыты Ва-

ши персональные данные на основании договора с оператором или на основании федерального закона:

_____

_____

(перечислить юридические и физические лица)

Сроки обработки и хранения персональных данных определяются целями обработки (персональные данные обрабатываются до тех пор, пока соответствуют целям обработки).

_____	_____	_____
дата	подпись	расшифровка подписи

Настоящее уведомление на руки получил(а):

_____	_____	_____
дата	подпись	расшифровка подписи

Приложение 3
к правилам рассмотрения
запросов субъектов
персональных данных или их
представителей в
государственном бюджетном
профессиональном учреждении
Краснодарского края
«Славянский
электротехнологический
техникум»

ФОРМА

Отказ в выполнении повторного запроса
субъекта персональных данных

Уведомление

Уважаемый(ая) _____
(фамилия, имя, отчество)

На основании _____

_____
(ссылка на положение части 4 или 5 статьи 14 Федерального закона от 27 июля 2006 года № 152-ФЗ "О персональных данных" или на иной федеральный закон, являющийся основанием для такого отказа)

государственное бюджетное профессиональное учреждение Краснодарского края «Славянский электротехнологический техникум» вынуждено отказать Вам в выполнении повторного запроса на доступ к Вашим персональным данным.

_____ _____ _____
дата подпись расшифровка подписи

Настоящее уведомление на руки получил(а):

_____ _____ _____
дата подпись расшифровка подписи

Приложение 4
государственном бюджетном
профессиональном учреждении
Краснодарского края
«Славянский
электротехнологический
техникум»

ФОРМА

Отказ в предоставлении доступа субъекта персональных данных к его персональным данным

Уведомление

Уважаемый(ая) _____
(фамилия, имя, отчество)

На основании _____

(ссылка на положение части 8 статьи 14 Федерального закона от 27 июля 2006 года № 152-ФЗ "О персональных данных" или на иной федеральный закон, являющийся основанием для такого отказа)

государственное бюджетное профессиональное учреждение Краснодарского края «Славянский электротехнологический техникум» вынуждено отказать Вам в предоставлении доступа к Вашим персональным данным.

_____ _____ _____
дата подпись расшифровка подписи

Настоящее уведомление на руки получил(а):

_____ _____ _____
дата подпись расшифровка подписи

Приложение 3

УТВЕРЖДЕНЫ
приказом ГБПОУ КК СЭТ
от 30.12.2023 № 954

ПРАВИЛА
осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в государственном бюджетном профессиональном учреждении Краснодарского края «Славянский электротехнологический техникум»

1. Общие положения

1.1. Настоящие правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в государственном бюджетном профессиональном учреждении Краснодарского края «Славянский электротехнологический техникум» (далее – Правила) определяют порядок осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным законодательством Российской Федерации и принятыми в соответствии с ним нормативными правовыми актами.

1.2. Настоящие Правила разработаны в соответствии с:

Федеральным законом от 27 июня 2006 г. № 152-ФЗ «О персональных данных» (далее – Федеральный закон «О персональных данных»);

постановлением Правительства Российской Федерации от 15 августа 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

постановлением Правительства Российской Федерации от 21 марта 2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и другими нормативными правовыми актами;

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

1.3. Настоящими Правилами в своей работе должны руководствоваться:

сотрудники государственного бюджетного профессионального учреждении Краснодарского края «Славянский электротехнологический техникум» (далее – Техникум), осуществляющие внутренний контроль соответствия обработки персональных данных требованиям к защите персональных данных.

2. Структура процессов по внутреннему контролю

2.1. Контроль выполнения требований по защите персональных данных в структурных подразделениях Техникума осуществляется с целью определения наличия несоответствий между требуемым уровнем защиты персональных данных и его фактическим состоянием, а также выработки мер по их устранению и недопущению в дальнейшем.

2.2. Контроль выполнения требований по защите персональных данных в структурных подразделениях Техникума осуществляет ответственный за организацию обработки персональных данных в Техникуме.

2.3. Общий контроль выполнения требований по обеспечению безопасности персональных данных осуществляет ответственный за выполнение мероприятий по контролю исполнения в структурных подразделениях Техникума требований документов по обеспечению безопасности персональных данных.

2.4. Контроль проводится в форме плановых и внеплановых проверок. Внеплановые проверки могут быть контрольными и по частным вопросам.

2.5. Контрольные проверки проводятся для установления полноты выполнения рекомендаций плановых проверок.

2.6. Проверки по частным вопросам охватывают отдельные направления по защите персональных данных и могут проводиться в случаях, когда стали известны факты несанкционированного доступа, утечки либо утраты персональных данных субъектов персональных данных или нарушения требований по защите персональных данных.

2.7. Сроки проведения контрольных проверок доводятся руководителям проверяемых структурных подразделений техникума не позднее, чем за 24 часа до начала проверки.

2.8. Проверки по частным вопросам могут проводиться без уведомления руководителей структурных подразделений техникума.

2.9. Периодичность и сроки проведения плановых проверок структурных подразделений \ устанавливаются планом проверок на календарный год. Сроки проведения плановых проверок доводятся руководителям проверяемых подразделений не позднее, чем за 10 суток до начала проверки.

3. Порядок подготовки к проверке

3.1. Общий контроль выполнения требований по обеспечению безопасности персональных данных в структурных подразделениях Техникума осуществляется в соответствии с Планом проведения внутренних проверок соответствия обработки персональных данных требованиям к защите персональных данных (форма представлена в приложении 1), утвержденным директором техникума.

3.2. Ответственный за выполнение мероприятий по контролю исполнения структурных подразделений требований документов по обеспечению безопасности персональных данных подготавливает предложения по составу комиссии или группы проверяющих лиц.

3.3. Контроль в структурных подразделениях, осуществляемый ответственными за обеспечение контроля процессов обеспечения безопасности персональных данных структурных подразделений техникума, осуществляется в соответствии с Планом проведения внутренних проверок соответствия обработки персональных данных требованиям к защите персональных данных структурных подразделений (форма представлена в приложении 2). Данные Планы утверждаются руководителями структурных подразделений и согласовываются с ответственным за выполнение мероприятий по контролю исполнения структурных подразделений, требований документов по обеспечению безопасности персональных данных.

3.4. Проверяющие лица обязаны получить у руководителей проверяемых структурных подразделений техникума информацию об условиях обработки персональных данных, необходимую для достижения целей проверки. Перед началом проверки они должны изучить материалы предыдущих проверок данного структурного подразделения.

4. Порядок проведения проверки

4.1. Руководитель проверяемого структурного подразделения обязан оказывать содействие комиссии по проверке или группе проверяющих лиц и в случае необходимости определяет должностное лицо, ответственное за сопровождение проверки.

4.2. Допуск проверяющих лиц к конкретным информационным ресурсам, защищаемым сведениям и техническим средствам должен исключать ознакомление проверяющих лиц с конкретными персональными данными.

4.3. Должны быть согласованы конкретные вопросы по объему, содержанию, срокам проведения проверки, а также каких сотрудников структурных подразделений техникума необходимо привлечь к проверке и какие помещения следует посетить.

4.4. Общий порядок проведения проверки включает:

выявление сотрудников, задействованных в обработке персональных данных;

проверка факта ознакомления сотрудников проверяемого структурного подразделения с нормативными документами, регламентирующими вопросы обработки и защиты персональных данных;

получение при содействии сотрудников проверяемого структурного подразделения документов, касающихся обработки и защиты персональных данных в данном структурном подразделении; анализ полученной документации;

непосредственная проверка выполнения установленного порядка обработки и защиты персональных данных и требований законодательства Российской Федерации в области защиты персональных данных.

4.5. В ходе осуществления контроля выполнения требований по защите персональных данных в структурном подразделении рассматриваются следующие показатели работ по защите персональных данных:

наличие согласий на обработку персональных данных субъектов персональных данных, в случаях, предусмотренных законодательствам Российской Федерации;

соответствие состава и сроков обработки целям обработки ПДн;

соответствие Перечня лиц, имеющих доступ в помещения, в которых ведется обработка персональных данных реальному составу сотрудников;

наличие нормативных документов по защите персональных данных;

знание нормативных документов и уровень подготовки сотрудников, имеющих доступ к персональным данным;

полнота и правильность выполнения требований нормативных документов сотрудниками, имеющими доступ к персональным данным;

наличие документов, подтверждающих учет и сохранность материальных носителей персональных данных.

4.6. В ходе осуществления контроля выполнения требований по защите персональных данных в структурном подразделении дополнительно рассматриваются следующие показатели работ по защите персональных данных:

соответствие информации, указанной в уведомлении об обработке персональных данных, реальному положению дел;

наличие и корректность перечня информационных систем;

наличие документа, подтверждающего:

правильность определения уровня защищенности персональных данных, обрабатываемых в информационных системах, а также классов защищенности информационных систем;

наличие документа, подтверждающего факт определения угроз безопасности персональных данных, а также его актуальность (срок актуальности документа не может превышать 3 года);

соответствие состава средств вычислительной техники информационных систем указанному в документации на информационную систему;

соответствие требованиям по организации разграничения доступа пользователей к информационным ресурсам (в том числе сетевым);

порядок защиты персональных данных при передаче по сети;

применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

оценка эффективности принимаемых мер по обеспечению безопасности персональных данных.

4.7. Во время проведения проверки, выявленные нарушения требований по обработке и защите персональных данных должны быть по возможности устранены. Проверяющие лица могут дать рекомендации по устранению на месте отмечаемых нарушений и недостатков.

4.8. Недостатки, которые не могут быть устранены на месте, включаются в итоговый документ по результатам проверки.

5. Оформление результатов проверки

5.1. Результаты проверки оформляются актом.

5.2. Акт составляется в одном экземпляре и подписывается членами комиссии. Оригинал документа с результатами проверки хранится (передается) у ответственного за выполнение мероприятий по контролю исполнения структурными подразделениями техникума требований документов по обеспечению безопасности персональных данных. Копия документа о проверке передается в проверяемое структурное подразделение.

5.3. Результаты проверок подразделений периодически обобщаются ответственным за выполнение мероприятий по контролю исполнения структурными подразделениями техникума и доводятся до сведения ответственного за организацию обработки и обеспечение безопасности персональных данных.

5.4. При необходимости принятия решений по результатам проверки структурного подразделения– ответственному за организацию обработки и обеспечение безопасности персональных данных техникума готовится соответствующая служебная записка.

6. Корректирующие мероприятия и контроль за их исполнением

6.1. Руководитель структурного подразделения анализирует акт о результатах внутренней проверки и в пятидневный срок определяет перечень мероприятий, необходимых для устранения нарушений и их причин.

6.2. Перечень мероприятий согласуется с ответственным за организацию обработки и обеспечение безопасности персональных данных.

6.3. Если корректирующие мероприятия касаются других структурных подразделений техникума, то к анализу привлекаются специалисты соответствующих структурных подразделений.

6.4. Выполнение корректирующих мероприятий и их достаточность определяется ответственным за организацию обработки и обеспечение безопасности персональных данных.

6.5. Внутренняя проверка считается оконченной после выполнения всех корректирующих мероприятий и устранения выявленных нарушений.

Приложение 1
к Правилам осуществления
внутреннего контроля соответствия
обработки персональных данных
требованиям к защите
персональных данных в государственном бюджетном профессиональном учреждении Краснодарского края «Славянский электротехнологический техникум»

ПЛАН
проведения внутренних проверок соответствия обработки персональных данных требованиям к защите персональных данных государственного бюджетного профессионального учреждения Краснодарского края «Славянский электротехнологический техникум»

№ п/п	Наименование структурного подразделения в государственном бюджетном профессиональном учреждении Краснодарского края «Славянский электротехнологический техникум»	Наименование мероприятия	Период проведения проверки	Отметка о выполнении (№ акта проверки)	Отметка о выполнении корректирующих мероприятий	Примечание
1	2	3	4	5	6	7

Приложение 2
к Правилам осуществления
внутреннего контроля соответствия
обработки персональных
данных требованиям к защите
персональных данных в государственном бюджетном профессиональном учреждении Краснодарского края «Славянский электротехнологический техникум»

ПЛАН
проведения внутренних проверок соответствия обработки персональных данных требованиям к защите персональных данных структурных подразделений в государственном бюджетном профессиональном учреждении Краснодарского края «Славянский электротехнологический техникум»

№ п/п	Наименование мероприятия	Период проведения проверки	Отметка о выполнении (№ акта проверки)	Отметка о выполнении корректирующих мероприятий	Примечание
1	2	3	4	5	6

Приложение 4

УТВЕРЖДЕНЫ
приказом ГБПОУ КК СЭТ
от 30.12.2023 № 954

ПРАВИЛА
доступа в помещения в государственном бюджетном профессиональном учреждении Краснодарского края «Славянский электротехнологический техникум», в которых ведется обработка защищаемой информации, в том числе персональных данных

1. Общие положения

1.1. Настоящие Правила устанавливают порядок доступа в помещения в государственном бюджетном профессиональном учреждении Краснодарского края «Славянский электротехнологический техникум» (далее – Техникум), в которых ведется обработка конфиденциальной и защищаемой информации, в том числе персональных данных (далее – Информация).

1.2. Правила разработаны в целях обеспечения безопасности информации, обрабатываемой в Техникуме, на средствах вычислительной техники информационных систем, на материальных носителях информации, а также для обеспечения внутриобъектового режима.

1.3. Настоящий Порядок устанавливает правила доступа в следующие помещения Техникума:

помещения, в которых происходит обработка Информации, как с использованием средств автоматизации, так и без таковых, в том числе серверные помещения;

помещения, в которых хранятся материальные носители Информации и их резервные копии;

помещения, в которых установлены средства криптографической защиты информации (далее – СКЗИ) и хранятся носители ключевой информации, в том числе средства электронной подписи (далее – Спецпомещения).

1.4. Настоящий Порядок разработан в соответствии с:

Федеральным законом Российской Федерации от 27 июня 2006 г. № 152-ФЗ «О персональных данных» (далее – Федеральный закон «О персональных данных»);

постановлением Правительства Российской Федерации от 15 августа 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

постановлением Правительства Российской Федерации от 21 марта 2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение

выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» ;

приказом Федеральной службой безопасности 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»;

приказом Федерального агентства правительственной связи и информации при Президенте Российской Федерации от 13 июня 2001 г. № 152 «Об утверждении инструкции 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».

1.5. В каждом структурном подразделении Техникума назначается ответственное лицо за доступ в Помещения.

1.6. Сотрудники, допущенные в помещения, обязаны:

выполнять требования обеспечения безопасности Информации;

соблюдать режим конфиденциальности при обращении с Информацией, носителями Информации и СКЗИ (в том числе ключевыми документами к ним);

своевременно выявлять попытки посторонних лиц получить сведения об Информации, об используемых СКЗИ или ключевых документах к ним;

предусматривать раздельное безопасное хранение действующих и резервных ключевых документов, предназначенных для применения в случае компрометации действующих криптоключей.

2. Общие требования к оборудованию помещений и регламентации доступа в них

2.1. Режим обеспечения безопасности помещений, в которых осуществляется обработка Информации (далее – Помещения) должен быть организован таким образом, чтобы препятствовать возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения.

2.2. Ограждающие конструкции Помещений, должны предполагать существенные трудности для нарушителя по их преодолению (например, металлические решетки на окнах, металлическая дверь, система контроля и управления доступом и так далее).

2.3. Помещения должны быть оснащены надежными входными дверьми с замками, а также средствами опечатывания помещений по окончании рабочего дня.

2.4. Окна Помещений, расположенных на первых или последних этажах зданий, а также окна, находящиеся около пожарных лестниц и других мест,

откуда возможно проникновение в помещения посторонних лиц, должны быть оборудованы металлическими решетками, или ставнями, или охранной сигнализацией, или другими средствами, препятствующими неконтролируемому проникновению в помещения.

2.5. В Техникума определяется перечень помещений, в которых разрешена обработка Информации. Форма перечня представлена в приложении 1.

2.6. Доступ сотрудников в Помещения должен быть организован согласно перечню лиц, допущенных в Помещения обработки Информации (форма перечня представлена в приложении 2). Перечень сотрудников, доступ которых разрешен в Помещения, размещается на внутренней стороне двери этого помещения.

2.7. В Помещениях определяются места хранения материальных носителей Информации и лиц, ответственных за их сохранность (форма перечня представлена в приложении 3).

2.8. Указанные перечни разрабатываются ответственными за доступ в Помещения лицами и утверждаются директором техникума либо лицом его замещающем.

2.9. Доступ посторонних лиц в Помещения, должен осуществляться только ввиду служебной необходимости и под контролем сопровождающего лица из числа сотрудников, допущенных в Помещение. При этом должны быть приняты меры, исключающие ознакомление посторонних лиц с защищаемой Информацией. Такими мерами являются:

размещение мониторов, исключающее или существенно затрудняющее просмотр отображаемой информации;

размещение документации на бумажных носителях, содержащих Информацию, исключающее просмотр Информации на них (документация убирается в папки, ящики тумбочек/столов, либо переворачивается лицевой стороной вниз, либо накрывается сверху непрозрачными объектами, закрывающими область текста).

2.10. В нерабочее время все окна и двери в помещениях (в том числе в смежные помещения), в которых ведется обработка Информации, должны быть надежно закрыты, материальные носители должны быть убраны в запираемые шкафы (сейфы), компьютеры выключены либо заблокированы.

2.11. При необходимости повышенного уровня обеспечения безопасности Помещений могут использоваться системы видеонаблюдения и системы контроля и управления доступом.

3. Особенности доступа в серверные помещения

3.1. Учет доступа в серверные помещения третьих лиц (осуществляющих обслуживание, техническое сопровождение, настройку серверного и активного сетевого оборудования) должен отражаться в Журнале доступа в серверные помещения (форма журнала приведена в приложении 4 к настоящей Политике).

3.2. Двери серверных помещений должны быть оборудованы устройствами, обеспечивающими постоянное закрытие дверей на замок и их открытие только для санкционированного прохода.

3.3. Уборка серверных помещений должна происходить только под контролем сопровождающего лица из числа сотрудников, допущенных в Помещение.

3.4. Нахождение в серверных помещениях посторонних лиц без сопровождающего запрещено.

3.5. При возникновении чрезвычайных ситуаций природного и техногенного характера, аварий, катастроф, стихийных бедствий, а также других ситуаций, которые могут создавать угрозу жизни и здоровью граждан, доступ в серверные помещения, в целях оказания помощи гражданам, предотвращения, ликвидации предпосылок и последствий нештатной ситуации, может осуществляться без согласования с ответственным за доступ в Помещения лицом.

3.6. Сотрудники органов Министерства Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий (далее – МЧС), аварийных служб, врачи «скорой помощи» допускаются в серверные помещения для ликвидации нештатной ситуации, иных чрезвычайных ситуаций или оказания медицинской помощи в сопровождении сотрудника, допущенного в Помещение.

Приложение 1
к Правилам доступа в помещения государственного бюджетного профессионального учреждения Краснодарского края «Славянский электротехнологический техникум», в которых ведется обработка защищаемой информации, в том числе персональных данных

ФОРМА

ПЕРЕЧНЬ
помещений, в которых разрешена обработка конфиденциальной информации (в том числе персональных данных)

№ п/п	Наименование структурного подразделения	№ кабинета	Ответственное лицо (Ф.И.О., должность)	Подпись
1	2	3	4	5

Приложение 2
к Правилам доступа в помещения государственного бюджетного профессионального учреждения Краснодарского края «Славянский электротехнологический техникум», в которых ведется обработка защищаемой информации, в том числе персональных данных

ФОРМА

ПЕРЕЧНЬ
лиц, допущенных в помещения обработки конфиденциальной информации (в том числе персональных данных)

№ п/п	Наименование структурного подразделения	№ кабинета	Ф.И.О. сотрудника	Должность
1	2	3	4	5

Приложение 3
к Правилам доступа в помещения государственного бюджетного профессионального учреждения Краснодарского края «Славянский электротехнологический техникум», в которых ведется обработка защищаемой информации, в том числе персональных данных

ФОРМА

ПЕРЕЧНЬ
мест хранения материальных носителей конфиденциальной информаций (в том числе персональных данных) и лиц, ответственных за их сохранность

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

Приложение 4
к Правилам доступа в помещения государственного бюджетного профессионального учреждения Краснодарского края «Славянский электротехнологический техникум», в которых ведется обработка защищаемой информации, в том числе персональных данных

ФОРМА

ЖУРНАЛ
доступа в серверное помещение

№ п/п	Номер помещения	Название организации (проводящей работы) Ф.И.О. и должность сотрудника	Перечень проводимых работ и оборудования, к которому осуществляется доступ	Основание проводимых работ	Дата и время		Ф.И.О. должность сотрудника, сопровождающего третье лицо	Подпись
					начала работ	завершения работ		
1	2	3	4	5	6	7	8	9

Приложение 5

УТВЕРЖДЕН
приказом ГБПОУ КК СЭТ
от 30.12.2023 № 954

ПЕРЕЧЕНЬ
персональных данных, обрабатываемых в государственном бюджетном профессиональном учреждении Краснодарского края «Славянский электротехнологический техникум»

1.1. Перечень персональных данных:
биографические сведения работника или обучающегося;
образование;
специальность;
занимаемая должность;
наличие судимостей;
адрес места жительства;
номера телефонов;
состав семьи;
место работы или учебы членов семьи и родственников;
характер взаимоотношений в семье;
размер заработной платы или стипендии;
содержание трудового договора;
содержание договора об образовании;
содержание декларации, подаваемой в налоговую инспекцию;
подлинники и копии приказов по личному составу и по учебной деятельности;
личные дела, личные карточки (форма Т-2) и трудовые книжки работников;
личные дела обучающихся;
основания к приказам по личному составу и по учебной деятельности;
дела, содержащие материалы по повышению квалификации и переподготовке работников, их аттестации, служебным расследованиям;
копии отчетов, направляемые в органы статистики;
анкета;
копии документов об образовании;
результаты медицинского обследования на предмет годности к осуществлению трудовых обязанностей либо к обучению;
фотографии и иные сведения, относящиеся к персональным данным работника и обучающегося.
фамилия, имя, отчество (в том числе предыдущие фамилии, имена и (или) отчества, в случае их изменения);
число, месяц, год рождения;

место рождения;

информация о гражданстве (в том числе предыдущее гражданства, иные гражданства);

вид, серия, номер документа, удостоверяющего личность, наименование органа, выдавшего его, дата выдачи;

адрес места жительства (адрес регистрации, фактического проживания, дата регистрации по месту жительства);

номер контактного телефон или сведения о других способах связи;

реквизиты страхового свидетельства государственного пенсионного страхования;

идентификационный номер налогоплательщика;

реквизиты страхового полиса обязательного медицинского страхования;

реквизиты свидетельства государственной регистрации актов гражданского состояния;

семейное положение, состав семьи и сведения о близких родственниках (в том числе бывших), необходимых для заполнения анкеты;

сведения о трудовой деятельности;

сведения о воинском учете и реквизиты документов воинского учета;

сведения об образовании, в том числе о послевузовском профессиональном образовании (наименование и год окончания образовательного учреждения, наименование и реквизиты документа об образовании, квалификация, направление подготовки или специальность по документу об образовании);

сведения об ученой степени с указанием подтверждающих документов;

информация о владении иностранными языками, степень владения;

информация о наличии или отсутствии судимости;

государственные награды, иные награды и знаки отличия;

сведения о профессиональной переподготовке и (или) повышении квалификации;

информация о ежегодных оплачиваемых отпусках, учебных отпусках, отпусках без сохранения денежного содержания и по уходу за ребенком;

номер индивидуального лицевого счета, в том числе родственников для перечисления денежных средств по исполнительным документам;

номер банковской карты.

1.2. Целями обработки перечисленных персональных данных являются:

обеспечения кадровой и учебно-воспитательной работы техникума.

1.3. Основанием для обработки перечисленных персональных данных является:

ст. 63, 65, 66, 68, 69, 72-1, 72-2, 73, 76, 83, 86, 88, 392 Трудового кодекса Российской Федерации;

ст. 9, 11 Федерального закона Российской Федерации от 1 апреля 1996 г. № 27-ФЗ «Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования»;

п. 4 ст. 13 Федерального закона Российской Федерации от 7 февраля 2011 г. № 3-ФЗ «О полиции»;

ст. 12 и п. 2 ст. 14 Федерального закона Российской Федерации от 21 июля 1997 г. № 118-ФЗ «О судебных приставах»;

п. 2.1 ст. 4 Федерального закона Российской Федерации от 17 января 1992 г. № 2202-1 «О прокуратуре Российской Федерации»;

ч. 2 п. 1 ст.64 и ч.10 ст. 65 Федерального закона Российской Федерации от 2 октября 2007 г. № 229-ФЗ «Об исполнительном производстве».

п. 220, 436 Перечня, утвержденного приказом Минкультуры Российской Федерации от 25 августа 2010 г. № 558;

распоряжение Правительства Российской Федерации от 26 мая 2005 г. № 667-р «Об утверждении формы анкеты, представляемой гражданином Российской Федерации, поступающим на государственную гражданскую службу Российской Федерации или на муниципальную службу в Российской Федерации»;

ст. 16, 17 Федерального закона Российской Федерации от 27 июля 2004 г. № 79-ФЗ «О государственной гражданской службе Российской Федерации»;

ст. 196 Гражданского Кодекса Российской Федерации;

ст. 218 Налогового кодекса Федерации;

п.1.1 – 3.2 части 1 ст. 8 Федерального закона Российской Федерации от 25 декабря 2008 г. № 273-ФЗ «О противодействии коррупции»;

федеральный закон Российской Федерации от 29 декабря 2006 г. № 255-ФЗ «Об обязательном социальном страховании на случай временной нетрудоспособности и в связи с материнством»;

федеральный закон Российской Федерации от 24 июля 2009 г. № 213-ФЗ «О страховых взносах в ПФ РФ, ФСС, ФФОМС и ТФОМС»;

ч. 1 ст. 24 Федерального закона Российской Федерации от 24 июля 2009 г. № 212-ФЗ «О страховых взносах в ПФ РФ, ФСС РФ, ФОМС»;

федеральный закон Российской Федерации от 28 марта 1998 г. № 53-ФЗ «О воинской обязанности и военной службе».

2. Перечень персональных данных граждан, обратившихся в Техникум

2.1. Перечень персональных данных:

фамилия, имя, отчество (последнее при наличии);

почтовый адрес;

адрес электронной почты;

указанный в обращении контактный телефон;

иные персональные данные, указанные в обращении, а также ставшие известными в ходе личного приема граждан или в процессе рассмотрения обращения.

2.2. Целью обработки перечисленных персональных данных является рассмотрения устных и письменных обращений граждан по вопросам, относящимся к компетенции Техникума, с последующим уведомлением граждан о результатах рассмотрения.

Приложение 6

УТВЕРЖДЕН
приказом ГБПОУ КК СЭТ
от 30.12.2023 № 954

ПЕРЕЧЕНЬ
должностей государственного бюджетного профессионального учреждения Краснодарского края «Славянский электротехнологический техникум» которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным

№ п/п	Наименование должности государственного бюджетного профессионального учреждения Краснодарского края «Славянский электротехнологический техникум»
1	2
1	Директор
2	Секретарь директора
3	Специалист отдела кадров
4	Главный бухгалтер
5	Ведущий бухгалтер
6	Юрисконсульт
7	Ведущий экономист
8	Бухгалтер
9	Заведующий курсовой подготовкой
10	Старший методист
11	Секретарь учебной части
12	Заместитель директора по АХР
13	Заместитель директора по УР
14	Заместитель директора по УПР
15	Заместитель директора по УВР
16	Комендант общежития
17	Члены приемной комиссии в период приемной компании

Приложение 7

УТВЕРЖДЕН
приказом ГБПОУ КК СЭТ
от 30.12.2023 № 954

ПЕРЕЧЕНЬ
информационных ресурсов и систем государственного бюджетного профессионального учреждения Краснодарского края «Славянский электротехнологический техникум»

1. Перечень информационных систем и ресурсов

1.1. Совокупность информационных ресурсов, доступ к которым осуществляется в государственном бюджетном профессиональном учреждение Краснодарского края «Славянский электротехнологический техникум» (далее – Техникум), образуют информационную систему Техникума.

1.2. Перечень информационных ресурсов:

№ п/п	Наименование ИС
1	2
1	Государственная информационная система «Единая межведомственная система электронного документооборота органов исполнительной власти Краснодарского края» (ГИС «ЕМСЭД КК»)
2	Государственная интегрированная информационная система управления общественными финансами (ГИИС «Электронный бюджет»)
3	Федеральная информационная система «Федеральный реестр сведений о документах об образовании и (или) о квалификации, документах об обучении» (ФИС ФРДО)
4	Федеральная информационная система обеспечения проведения государственной итоговой аттестации обучающихся, освоивших основные образовательные программы основного общего и среднего общего образования, и приема граждан в образовательные организации для получения среднего профессионального и высшего образования. (ФИС ГИА)
5	Автоматизированная система удаленного рабочего места (АС УРМ)
6	Государственная информационная система за оборотом товаров (честный знак)
7	Федеральная государственная информационная система, предназначенная для сертификации и отслеживания товаров, подконтрольных Госветнадзору (Меркурий ХС)
8	федеральная государственная информационная система предназначена для автоматизации процессов оформления и учета документов фитосанитарного надзора (ФГИС «АРГУС-ФИТО)

№ п/п	Наименование ИС
1	2
9	Федеральная государственная информационная система «САТУРН» (ФГИС САТУРН)
10	Федеральная государственная информационная система «ЗЕРНО» (ФГИС ЗЕРНО)
11	Федеральная государственная информационная система учета и контроля за обращением с отходами I и II классов опасности (ФГИС ОПВК)
12	Единая государственная информационная система социального обеспечения ЕГИССО
13	Официальный сайт для размещения информации о государственных (муниципальных) учреждениях БАС ГОВ
14	Единая информационная система «Закупки» (ИЕС ЗАКУПКИ)
15	Региональная информационная систему Краснодарского края, используемую в сфере закупок для обеспечения государственных и муниципальных нужд
16	Система «Контур. Экстерн» предназначена для осуществления документооборота между предприятиями всех форм собственности и государственными контролирующими органами.
17	Информационный ресурс для размещения наиболее полной информации об ООО "НПО "КРИСТА
18	Сервис электронной подачи документов в арбитражные суды «Мой Арбитр»

Приложение 8

УТВЕРЖДЕНА
приказом ГБПОУ КК СЭТ
от 30.12.2023 № 954

ОЦЕНКА
вреда, который может быть причинен субъектам персональных данных государственного бюджетного профессионального учреждения Краснодарского края «Славянский электротехнологический техникум»

1. Общие положения

1.1. Настоящий документ содержит оценку вреда, который может быть причинен субъектам персональных данных, (далее – Оценка возможного вреда), обрабатываемых в государственном бюджетном профессиональном учреждении Краснодарского края «Славянский электротехнологический техникум» (далее – Техникум). Методику проведения оценки возможного вреда, а также соотношение указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (далее – Федеральный закон «О персональных данных»).

1.2. Оценка возможного вреда осуществляется в соответствии с требованиями статьи 18.1 Федерального закона «О персональных данных».

1.3. В связи с отсутствием нормативных документов Правительства Российской Федерации, Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю Российской Федерации по оценке возможного вреда субъектам персональных данных, производится качественная оценка возможного вреда по методике, описанной в разделе 3 настоящего документа.

2. Термины и определения

2.1. Персональные данные – любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных).

2.2. Специальные категории персональных данных – персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни субъектов персональных данных.

2.3. Биометрические персональные данные – персональные данные, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются оператором для установления личности субъекта персональных данных (за исключением сведений, относящихся к специальным категориям персональных

данных).

2.4. Персональные данные, разрешенные субъектом персональных данных для распространения – персональные данные, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных путем дачи согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения в порядке, предусмотренном Федеральным законом «О персональных данных».

2.5. Иные персональные данные – любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных), за исключением персональных данных, относящихся к специальным, биометрическим или общедоступным персональным данным.

2.6. Оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

2.7. Распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

2.8. Предоставление персональных данных – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

2.9. Блокирование персональных данных – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

2.10. Уничтожение персональных данных – действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

2.11. Конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

2.12. Целостность информации – состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими право на такое изменение.

2.13. Доступность информации – состояние информации (ресурсов информационной системы), при которой субъекты, имеющие права доступа, могут реализовать их беспрепятственно.

3. Методики оценки возможного вреда

3.1. Вред субъекту персональных данных возникает в результате неправомерного или случайного доступа к персональным данным, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении пер-

сональных данных.

3.2. Перечисленные неправомерные действия определяются как следующие нарушения характеристик безопасности информации (персональных данных):

3.2.1. Неправомерное предоставление, распространение и копирование персональных данных являются нарушением конфиденциальности персональных данных.

3.2.2. Неправомерное блокирование персональных данных является нарушением доступности персональных данных.

3.2.3. Неправомерное уничтожение персональных данных является нарушением доступности и целостности персональных данных.

3.2.4. Неправомерное изменение персональных данных является нарушением целостности персональных данных.

3.2.5. Нарушение права субъекта персональных данных требовать от оператора персональных данных уточнения его персональных данных, их блокирования или уничтожение является нарушением целостности информации.

3.2.6. Нарушение права субъекта на получение информации, касающейся обработки его персональных данных, является нарушением доступности персональных данных.

3.2.7. Обработка персональных данных, выходящая за рамки установленных и законных целей обработки, в объеме больше необходимого для достижения установленных и законных целей и дольше установленных сроков является нарушением конфиденциальности персональных данных.

3.2.8. Неправомерное получение персональных данных от лица, не являющегося субъектом персональных данных, является нарушением конфиденциальности персональных данных.

3.3. Субъекту персональных данных может быть причинен вред в форме:

3.3.1. Морального вреда – физические или нравственные страдания, причиненные субъекту персональных данных, действиями (или бездействием) оператора персональных данных, нарушающими личные неимущественные права субъекта персональных данных, либо посягающими на принадлежащие субъекту персональных данных нематериальные блага, а также в других случаях, предусмотренных законом.

3.3.2. Убытков – расходы, которые лицо (субъект персональных данных), чье право нарушено, произвело или должно будет произвести для восстановления нарушенного права, утрата или повреждение его имущества (реальный ущерб), а также неполученные доходы, которые это лицо получило бы при обычных условиях гражданского оборота, если бы его право не было нарушено (упущенная выгода).

3.4. Оценка возможного вреда субъектам персональных данных определяется в соответствии следующими качественными критериями оценки нарушения заданных характеристик безопасности персональных данных:

3.4.1. Высокий – приводит к значительным негативным последствиям для субъекта персональных данных, а именно:

нанесение крупного ущерба субъекту персональных данных;

крупные финансовые потери для субъекта персональных данных в ре-

зультате неправомерных действий с персональными данными;

возможно нанесение тяжелого вреда здоровью субъекта или возможность реализации прямой угрозы жизни.

3.4.2. Средний – приводит к негативным последствиям для субъекта персональных данных, а именно:

причинение ущерба субъекту персональных данных;

значительные финансовые потери в результате неправомерных действий с персональными данными;

возможно нанесение вреда, не создающего угрозы жизни или здоровью субъекту персональных данных.

3.4.3. Низкий – приводит к незначительным последствиям для субъекта персональных данных, а именно:

нанесение незначительного ущерба субъекту персональных данных или отсутствие подобного вреда;

отсутствие финансовых потерь или незначительные потери для субъекта персональных данных;

отсутствие вреда здоровью или жизни субъекту персональных данных, или незначительный вред.

4. Оценка возможного вреда

4.1. Степень возможного вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона «О персональных данных», определяется по наибольшему значению возможного нарушения каждой из характеристик безопасности информации и отношении категорий субъектов персональных данных, чьи персональные данные обрабатываются в Техникуме.

4.2. Оценка возможного вреда приведена в приложении 1 к настоящему документу.

4.3. Для всех категорий субъектов персональных данных, чьи персональные данные обрабатываются в Министерстве, определена средняя степень возможного ущерба, так как:

в составе персональных данных, обрабатываемых в Техникуме, отсутствуют сведения, неправомерные действия с которыми, могут привести к причинению крупного вреда субъекту персональных данных;

угроза нанесения тяжкого вреда здоровью или угроза жизни и здоровью субъектам персональных данных отсутствует.

5. Соотношение возможного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных»

5.1. В Техникуме принимаются правовые, организационные и технические меры, необходимые и достаточные для обеспечения исполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и

принятыми в соответствии с ним нормативными правовыми актами, для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении них.

5.2. Состав мер, направленных на защиту персональных данных, определяется исходя из требований, установленных:

Федеральным законом Российской Федерации «О персональных данных».

Федеральным законом Российской Федерации от 2 мая 2006 г. № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации»;

Федеральным законом Российской Федерации от 27 июля 2010 г. № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг»;

Федеральным законом Российской Федерации от 25 декабря 2008 г. № 273-ФЗ «О противодействии коррупции»;

постановлением Правительства Российской Федерации от 21 марта 2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных»;

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

постановлением Правительства Российской Федерации от 15 августа 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

приказом Федеральной службы по техническому и экспертному контролю Российской Федерации 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»;

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

5.3. Соотношение возможного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных», приведено в приложении 2 к настоящему документу.

Приложение 1
к оценке вреда, который может
быть причинен субъектам
персональных данных
государственного бюджетного
профессионального учреждения
Краснодарского края «Славянский
электротехнологический техникум»

ОЦЕНКА
возможного вреда

№ п/п	Категория субъектов персональных данных	Категория персональных данных	Характеристика безопасности информации	Степень возможного вреда	Примечание
1	2	3	4	5	6
1	Работники техникума	ПДн, разрешенные субъектом персональных данных для распространения	Конфиденциальность		Нарушение конфиденциальности данной категории персональных данных не несет за собой вред субъектам
			Целостность	Низкая	
			Доступность	Низкая	
		Биометрические	Конфиденциальность		Данная категория персональных данных не обрабатывается
			Целостность		
			Доступность		
		Специальные	Конфиденциальность		
			Целостность		
			Доступность		
		Иные	Конфиденциальность	Средняя	
			Целостность	Средняя	
			Доступность	Низкая	
2	Обучающиеся техникума	ПДн, разрешенные субъектом персональных	Конфиденциальность		Нарушение конфиденциальности данной категории персональных данных не несет за собой вред субъектам
			Целостность		
			Доступность		

1	2	3	4	5	6
		данных для распространения			Данная категория персональных данных не обрабатывается
		Биометрические	Конфиденциальность		
			Целостность		
			Доступность		
		Специальные	Конфиденциальность		
			Целостность		
			Доступность		
		Иные	Конфиденциальность	Средняя	
			Целостность	Средняя	
			Доступность	Низкая	
3	Граждане, обратившиеся в Техникум	ПДн, разрешенные субъектом персональных данных для распространения	Конфиденциальность		Данные категории персональных данных не обрабатывается
			Целостность		
			Доступность		
		Биометрические	Конфиденциальность		
			Целостность		
			Доступность		
		Специальные	Конфиденциальность		
			Целостность		
			Доступность		
		Иные	Конфиденциальность	Средняя	
			Целостность	Средняя	
			Доступность	Низкая	

Приложение 2
к оценке вреда, который может быть причинен субъектам персональных данных субъектам персональных данных государственного бюджетного профессионального учреждения Краснодарского края «Славянский электротехнологический техникум»

СООТНОШЕНИЕ
возможного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных»

№ п/п	Перечень мер, принимаемых для обеспечения защиты персональных данных	Степень возможного вреда субъекту персональных данных, при невыполнении меры
1	2	3
1	Сбор согласий на обработку персональных данных, в случаях, установленных Федеральным законом «О персональных данных»	Средняя
2	Оценка вреда субъектам персональных данных	Средняя
3	Обезличивание, уточнение и уничтожение персональных данных, в случаях, когда это необходимо	Средняя
4	Определение правил рассмотрения запросов субъектов персональных данных или их представителей	Средняя
5	Определение правил работы с обезличенными данными в случае обезличивания персональных данных	Средняя
6	Определение порядка доступа в помещения Министерства, в которых ведется обработка персональных данных	Средняя
7	Осуществление внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным Федеральным законом «О персональных данных», принятыми в соответствии с ним нормативными правовыми актами и локальными актами Министерства	Средняя
8	Определение угроз безопасности персональных данных, при их обработке в информационных системах Министерства	Средняя
9	Определение уровня защищенности персональных данных, обрабатываемых в информационных системах Министерства	Средняя
10	Применение организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах Министерства, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные уровни за-	Средняя

1	2	3
	щищенности персональных данных	
11	Исключение несанкционированного, в том числе случайного, доступа к персональным данным, а также иных неправомерных действий в отношении персональных данных	Средняя
12	Применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации	Средняя
13	Оценка эффективности принимаемых мер по обеспечению безопасности персональных данных	Средняя
14	Учет машинных носителей персональных данных	Средняя
15	Обнаружение фактов несанкционированного доступа к персональным данным и принятие мер	Средняя
16	Восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним	Средняя
17	Установление правил доступа к персональным данным, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационных системах Министерства	Средняя
18	Контроль за принимаемыми мерами по обеспечению безопасности персональных данных	Средняя

Приложение 9

УТВЕРЖДЕНО
приказом ГБПОУ КК СЭТ
от 30.12.2023 № 954

ФОРМА

Директору ГБПОУ КК СЭТ

_____
Ф.И.О. субъекта персональных данных

_____
Номер основного документа,
удостоверяющего личность

_____
Наименование выдавшего органа

_____
Дата выдачи

СОГЛАСИЕ
сотрудника ГБПОУ КК СЭТ
на обработку персональных данных

Я, _____,
(фамилия, имя, отчество субъекта персональных данных)
проживающий по адресу: _____,
в _____
(адрес субъекта персональных данных)
соответствии с Федеральным законом от 27 июля 2007 г. № 152-ФЗ «О персональных данных» даю свое согласие государственному бюджетному профессиональному образовательному учреждению Краснодарского края «Славянский электротехнологический техникум» (далее – Оператор), расположенному по адресу: 353560, Краснодарский край, г. Славянск-на-Кубани, ул. Краснодарская, д. 248, на обработку как с использованием средств автоматизации, так и без использования таких средств, включая (сбор, запись, систематизацию, накопление, хранение, уточнение, извлечение, использование, передачу, обезличивание, блокирование, удаление, уничтожение) следующих моих персональных данных:

фамилия, имя, отчество (в том числе предыдущие фамилии, имена и (или) отчества, в случае их изменения);

число, месяц, год рождения;

место рождения;

информация о гражданстве (в том числе предыдущие гражданства, иные гражданства);

вид, серия, номер документа, удостоверяющего личность, наименование органа, выдавшего его, дата выдачи;

адрес места жительства (адрес регистрации, фактического проживания, дата регистрации по месту жительства);

номер контактного телефона или сведения о других способах связи;

реквизиты страхового свидетельства государственного пенсионного страхования;

идентификационный номер налогоплательщика;

реквизиты страхового медицинского полиса обязательного медицинского страхования;

реквизиты свидетельства государственной регистрации актов гражданского состояния;

семейное положение, состав семьи и сведения о близких родственниках (в том числе бывших), необходимые для заполнения анкеты;

сведения о трудовой деятельности;

сведения о воинском учете и реквизиты документов воинского учета;

сведения об образовании, в том числе о послевузовском профессиональном образовании (наименование и год окончания образовательного учреждения, наименование и реквизиты документа об образовании, квалификация, направление подготовки или специальность по документу об образовании);

сведения об ученой степени с указанием подтверждающих документов;

информация о владении иностранными языками, степень владения;

медицинские сведения по установленной форме об отсутствии у гражданина заболевания, препятствующего поступлению на государственную гражданскую службу или ее прохождению;

фотография;

сведения о прежнем месте работы;

информация, содержащаяся в трудовом договоре, дополнительных соглашениях к трудовому договору;

сведения о пребывании за границей (когда, где, с какой целью);

информация о классном чине государственной гражданской службы Российской Федерации (в том числе дипломатическом ранге, воинском или специальном звании, классном чине правоохранительной службы, классном чине гражданской службы субъекта Российской Федерации), квалификационном разряде государственной гражданской службы (квалификационном разряде или классном чине муниципальной службы);

информация о наличии или отсутствии судимости;

информация об оформленных допусках к государственной тайне;

государственные награды, иные награды и знаки отличия;

сведения о профессиональной переподготовке и (или) повышении квалификации;

информация о ежегодных оплачиваемых отпусках, учебных отпусках, отпусках без сохранения денежного содержания и по уходу за ребенком;

сведения о доходах, расходах, об имуществе и обязательствах имущественного характера, а также о доходах, расходах, об имуществе и обязательствах имущественного характера супругов и несовершеннолетних детей;

номер индивидуального лицевого счета, в том числе родственников для перечисления денежных средств по исполнительным документам;

номер банковской карты.

Обработка персональных данных разрешается на период трудоустройства, а также на срок, установленный нормативно-правовыми актами Российской Федерации.

Срок действия согласия – бессрочно, до момента его отзыва.

Я согласен(а), что мои персональные данные будут ограниченно доступны представителям государственных органов власти и использоваться для решения задач, связанных с оформлением трудовых отношений, обработкой и финансовым обеспечением деятельности техникума, составлением отчетности, мобилизационной работой, в том числе будут предоставлены структурным подразделениям администрации Краснодарского края, налоговым органам и Фонду социального страхования Российской Федерации, Пенсионному фонду Российской Федерации, банковским организациям и Военным комиссариатам, в целях выполнения указанных выше задач.

Я проинформирован(а), что под обработкой персональных данных понимаются действия (операции) с персональными данными в рамках выполнения Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных», конфиденциальность персональных данных соблюдается в рамках исполнения Оператором законодательства Российской Федерации.

Получение сведений о моих персональных данных третьей стороной возможно только при наличии официального запроса с указанием конкретных персональных данных и целей, для которых они будут использованы, и моего письменного согласия.

После увольнения мои персональные данные хранятся в техникуме в течение сроков хранения документов, предусмотренных действующим законодательством Российской Федерации.

Мне разъяснены юридические последствия отказа от предоставления персональных данных.

Я оставляю за собой право отозвать свое согласие посредством составления соответствующего письменного документа, который может быть направлен мной в адрес Оператора по почте заказным письмом с уведомлением о вручении либо вручен лично под расписку представителю Оператора.

Субъект персональных данных: _____/ _____

(подпись) (ФИО)

«___»_____ 20___г.

Приложение 10

УТВЕРЖДЕНО
приказом ГБПОУ КК СЭТ
от 30.11.2023 № 954

ФОРМА

Директору ГБПОУ КК СЭТ

Ф.И.О. субъекта персональных данных

_____

номер основного документа, удостоверяющего личность

_____

наименование выдавшего органа

_____

дата выдачи

СОГЛАСИЕ
на обработку персональных данных

Я, _____,
(фамилия, имя, отчество субъекта персональных данных)
проживающий по адресу: _____,
в _____
(адрес субъекта персональных данных)
соответствии с Федеральным законом от 27 июля 2007 г. №152-ФЗ «О персональных данных» даю своё согласие государственному бюджетному профессиональному образовательному учреждению Краснодарского края «Славянский электротехнологический техникум» (далее – Оператор), расположенному по адресу: 353560, Краснодарский край, г. Славянск-на-Кубани, ул. Краснодарская, д. 248, на обработку, как с использованием средств автоматизации, так и без использования таких средств, включая (сбор, запись, систематизацию, накопление, хранение, уточнение, извлечение, использование, передачу, обезличивание, блокирование, удаление, уничтожение) следующих моих персональных данных:
_____,
полученных Оператором в результате вступления со мной в правоотношения с целью
_____
_____
_____
_____.

Обработка персональных данных разрешается на период наличия указанных выше правоотношений, а также на срок, установленный нормативно-правовыми актами Российской Федерации.

Срок действия согласия – бессрочно, до момента его отзыва.

Я проинформирован(а), что под обработкой персональных данных понимаются действия (операции) с персональными данными в рамках выполнения Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных», конфиденциальность персональных данных соблюдается в рамках исполнения Оператором законодательства Российской Федерации.

Подтверждаю ознакомление с «Правилами обработки персональных данных в ГБПОУ КК СЭТ, правами и обязанностями в области защиты персональных данных.

Мне разъяснены юридические последствия отказа от предоставления персональных данных.

Я оставляю за собой право отозвать свое согласие посредством составления соответствующего письменного документа, который может быть направлен мной в адрес.

Субъект персональных данных: _____/ _____

(подпись) (ФИО)

Дата: «___»_____ 20___г.

Приложение 11

УТВЕРЖДЕНО
приказом ГБПОУ КК СЭТ
от 30.12.2023 № 954

ФОРМА

Разъяснение субъекту персональных данных юридических последствий отказа предоставить свои персональные данные

В соответствии с принципами обработки персональных данных, установленными Федеральным законом Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных», при обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, и актуальность по отношению к заявленным целям обработки персональных данных.

Кроме того, оператор должен принимать необходимые меры по уточнению неполных или неточных персональных данных.

В случае, если субъект персональных данных отказывается предоставить свои персональные данные, либо представленные персональные данные являются неточными и (или) неполными по отношению к заявленным целям обработки персональных данных государственное бюджетное профессиональное образовательное учреждение Краснодарского края «Славянский электротехнологический техникум» оставляет за собой право отказать в предоставлении своих услуг субъекту персональных данных.

Мне, _____.
(фамилия, имя, отчество)

разъяснены юридические последствия отказа предоставить свои персональные данные государственному бюджетному профессиональному образовательному учреждению Краснодарского края «Славянский электротехнологический техникум».

_____ _____ _____
дата подпись расшифровка подписи

Приложение 12

УТВЕРЖДЕНО
приказом ГБПОУ КК СЭТ
от 30.12.2023 № 954

ФОРМА

ОБЯЗАТЕЛЬСТВО
сотрудника государственного бюджетного профессионального образовательного учреждения Краснодарского края «Славянский электротехнологический техникум», непосредственно осуществляющего обработку персональных данных

Я, _____
(фамилия, имя, отчество, должность)

обязуюсь:

знать и выполнять требования законодательства в области персональных данных;

хранить в тайне известные мне персональные данные, информировать лицо, ответственное за организацию обработки персональных данных в министерстве, о фактах нарушения порядка обращения с персональными данными, о попытках несанкционированного доступа к ним;

обрабатывать только те персональные данные, к которым получен доступ в силу исполнения служебных обязанностей;

прекратить обработку персональных данных, ставших известными мне в связи с исполнением должностных обязанностей, в случае расторжения со мной государственного контракта, освобождения меня от замещаемой должности и увольнения с государственной гражданской службы.

В соответствии со статьей 7 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» я уведомлен(а) о том, что персональные данные являются информацией ограниченного доступа, и я обязан(а) не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, ставшие известными мне в связи с исполнением должностных обязанностей.

Ответственность, предусмотренная законодательством Российской Федерации, за разглашение информации ограниченного доступа, мне разъяснена.

_____ _____ _____
дата подпись расшифровка подписи

Приложение 13

УТВЕРЖДЕНО
приказом ГБПОУ КК СЭТ
от 30.12.2023 № 954

ФОРМА

Директору ГБПОУ КК СЭТ

_____
Ф.И.О. субъекта персональных данных

_____
Номер основного документа,
удостоверяющего личность

_____
Наименование выдавшего органа

_____
Дата выдачи

СОГЛАСИЕ
сотрудника ГБПОУ КК СЭТ на передачу (предоставление, распространение) персональных данных

Я, _____,
(фамилия, имя, отчество субъекта персональных данных)

соответствии с Федеральным законом от 27 июля 2007 г. № 152-ФЗ «О персональных данных» даю свое согласие государственному бюджетному профессиональному образовательному учреждению Краснодарского края «Славянский электротехнологический техникум» (далее – Оператор), расположенному по адресу: 353560, Краснодарский край, г. Славянск-на-Кубани, ул. Краснодарская, д. 248, на передачу (предоставление) следующих персональных данных:

фамилия, имя, отчество (в том числе предыдущие фамилии, имена и (или) отчества, в случае их изменения);

число, месяц, год рождения;

место рождения;

информация о гражданстве (в том числе предыдущие гражданства, иные гражданства);

вид, серия, номер документа, удостоверяющего личность, наименование органа, выдавшего его, дата выдачи;

адрес места жительства (адрес регистрации, фактического проживания, дата регистрации по месту жительства);

номер контактного телефона или сведения о других способах связи;

реквизиты страхового свидетельства государственного пенсионного страхования;

идентификационный номер налогоплательщика;

реквизиты страхового медицинского полиса обязательного медицинского страхования;

реквизиты свидетельства государственной регистрации актов гражданского состояния;

семейное положение, состав семьи и сведения о близких родственниках (в том числе бывших), необходимые для заполнения анкеты;

сведения о трудовой деятельности;

сведения о воинском учете и реквизиты документов воинского учета;

сведения об образовании, в том числе о послевузовском профессиональном образовании (наименование и год окончания образовательного учреждения, наименование и реквизиты документа об образовании, квалификация, направление подготовки или специальность по документу об образовании);

сведения об ученой степени с указанием подтверждающих документов;

информация о владении иностранными языками, степень владения;

медицинские сведения по установленной форме об отсутствии у гражданина заболевания, препятствующего поступлению на государственную гражданскую службу или ее прохождению;

фотография;

сведения о прохождении государственной гражданской службы, в том числе: дата, основания поступления на государственную гражданскую службу и назначения на должность государственной гражданской службы, дата, основания назначения, перевода, перемещения на иную должность государственной гражданской службы, наименование замещаемых должностей государственной гражданской службы с указанием структурных подразделений, размера денежного содержания, результатов аттестации на соответствие замещаемой должности государственной гражданской службы, а также сведения о прежнем месте работы;

информация, содержащаяся в служебном контракте, дополнительных соглашениях к служебному контракту;

сведения о пребывании за границей (когда, где, с какой целью);

информация о классном чине государственной гражданской службы Российской Федерации (в том числе дипломатическом ранге, воинском или специальном звании, классном чине правоохранительной службы, классном чине гражданской службы субъекта Российской Федерации), квалификационном разряде государственной гражданской службы (квалификационном разряде или классном чине муниципальной службы);

информация о наличии или отсутствии судимости;

информация об оформленных допусках к государственной тайне;

государственные награды, иные награды и знаки отличия;

сведения о профессиональной переподготовке и (или) повышении квалификации;

информация о ежегодных оплачиваемых отпусках, учебных отпусках, отпусках без сохранения денежного содержания и по уходу за ребенком;

сведения о доходах, расходах, об имуществе и обязательствах имущественного характера, а также о доходах, расходах, об имуществе и обязательствах имущественного характера супругов и несовершеннолетних детей;

номер индивидуального лицевого счета, в том числе родственников для перечисления денежных средств по исполнительным документам;

номер банковской карты,

Я согласен(а), что мои персональные данные будут ограниченно доступны представителям государственных органов власти и использоваться для решения задач, связанных с оформлением трудовых отношений, обработкой и финансовым обеспечением деятельности техникума, составлением отчетности, мобилизационной работой, в том числе будут предоставлены структурным подразделениям администрации Краснодарского края, налоговым органам и Фонду социального страхования Российской Федерации, Пенсионному фонду Российской Федерации, банковским организациям и Военным комиссариатам, в целях выполнения указанных выше задач.

Передачу (распространение) указанных персональных данных разрешаю на период государственной гражданской службы.

Срок действия согласия – бессрочно, до момента его отзыва.

Я проинформирован(а), что под обработкой персональных данных (в том числе под передачей (предоставлением)) понимаются действия (операции) с персональными данными в рамках выполнения Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных», конфиденциальность персональных данных соблюдается в рамках исполнения Оператором законодательства Российской Федерации.

Получение сведений о моих персональных данных третьей стороной возможно только при наличии официального запроса с указанием конкретных персональных данных и целей, для которых они будут использованы, и моего письменного согласия.

Я оставляю за собой право отозвать свое согласие посредством составления соответствующего письменного документа, который может быть направлен мной в адрес Оператора по почте заказным письмом с уведомлением о вручении либо вручен лично под расписку представителю Оператора.

Субъект персональных данных: _____/ _____

(подпись) (ФИО)

«___»_____ 20___г.

Хранить 5 лет до 2022 г.

Для служебного пользования

Учетный № 8.23

ЖУРНАЛ том 2 с №89
поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов

(для обладателя конфиденциальной информации)

ГБПОУ КК СЭТ

Начат 21.11.2017г

Окончен

№ п.п.	Наименование СКЗИ, эксплуатационной и технической документации к ним, ключевых документов	Серийные номера СКЗИ, эксплуатационной и технической документации к ним, номера серий ключевых документов	Номера экземпляров (криптографические номера) ключевых документов	Отметка о получении		Отметка о выдаче	
				От кого получены	Дата и номер сопроводительного письма	Ф.И.О. пользователя СКЗИ	Дата и расписка в получении
1	2	3	4	5	6	7	8
89	Ключ ЭЦП	100	1	Семенян Б.К.	Б.К. 20.11.2017		
	Семенян Б.К.				тр. 605 от 20.11.17		
90	Заявление на	101	1	Семенян	Б.К. 20.11.2017	Иванова	20.11.17
	изготовление		2		тр. 605 от 20.11.2017	Г.М.	
	СК ПЭП						
	Семенян Б.К.						
91	Ключ ЭЦП	102	1	Осмагчин А.А.	20.11.2017		
	Осмагчин А.А.				тр. 605 от 20.11.17		
92	Заявление на	103	1	Осмагчин А.А.	20.11.17	Иванова	20.11.17
	изготовление		2		тр. 605 от 20.11.17	Г.М.	
	СК ПЭП						
	Осмагчин А.А.						
93	Ключ доступа	104	1	Колоб К.А.	20.11.2017		
	S-07 инт 2349010484				тр. 605 от 20.11.17		
	234901001 pbs						
94	Регистрационная	105	1	Колоб К.А.	20.11.2017 г.	Иванова	20.11.17
	карточка запроса		2		тр. 605 от 20.11.17	Г.М.	
	на сертификат						
	ключа доступа						
	S-07 инт 2349010484						
	234901001 pbs						
95	Регистрационная	106	1	ОКЗИ Минфин	21.11.2017		
	карточка сертификата			на СК			
	ключа ЭЦП						
	Семенян Б.К.						
96	Сертификат	107	1	ОКЗИ Мин-			
	ключа ЭЦП			фина СК			
	Семенян Б.К.						
97	Регистрационная	108	1	ОКЗИ Мин	21.11.2017		
	карточка сертифи-			фина СК	дов. 1424		
	ката ключа				от 20.11.2017.		
	ЭЦП Осмагчина А.А.						
98	Сертификат	109	1	ОКЗИ Мин	21.11.2017		
	ключа Осмагчина А.А.			фина СК	дов. 1424 от 20.11.17		
99	Сертификат ключа	110	1	ОКЗИ Мин	21.11.2017		
	доступа S-07 инт			фина СК			
	2349010484						
	234901001 pbs						
100	Ключ ЭЦП	2022C8ECC	1	Акулинина С.А.	21.11.2017 г. 657 от 3.10.18		
	Акулинина С.А.						

Отметка о подключении (установке СКЗИ)			Отметка об изъятии СКЗИ из аппаратных средств, уничтожении ключевых документов			Примечание
Ф.И.О. сотрудников органа криптографической защиты, пользователя СКЗИ, произведших подключение установку	Дата подключения (установки) и подписи лиц, произведших подключение (установку)	Номера, аппаратных средств, в которые установлены или к которым подключены СКЗИ	Дата изъятия (уничтожения)	Ф.И.О. сотрудников органа криптографической защиты, пользователя СКЗИ, производивших изъятие (уничтожение)	Номер акта или расписка об уничтожении	
9	10	11	12	13	14	15
			02.10.18	Симоненко Г.Н.	1508	
				Кравченко В.В.	от 2.10.18г	
				Мазуренко С.Н.		
			21.11.2019	Акулешина С.А.	1024	
				Мазуренко С.Н.	21.11.2019	

Кравченко В.В.

№ п.п.	Наименование СКЗИ, эксплуатационной и технической документации к ним, ключевых документов	Серийные номера СКЗИ, эксплуатационной и технической документации к ним, номера серий ключевых документов	Номера экземпляров (криптографические номера) ключевых документов	Отметка о получении		Отметка о выдаче	
				От кого получены	Дата и номер сопроводительного письма	Ф.И.О. пользователя СКЗИ	Дата и расписка в получении
1	2	3	4	5	6	7	8
101	Заявление на изготовление ск ПЭП Акульшина С.А.		1 2	Акульшина С.А.	21.11.2018г. 657 от 3.10.18г.	Иванова Т.Н.	21.11.18
102	Ключ ЭЦП Осмачкин А.А.	e022C8EF3	1	Осмачкин А.А	21.11.2018г. 657 от 3.10.18г.		
103	Заявление на изготовление ск ПЭП Осмачкин А.А.		1 2	Осмачкин А.А	21.11.2018г. 657 от 3.10.18г.	Иванова Т.Н.	21.11.18
104	Ключ доступа S-07 исп 234901.0484 - 234901001 ods	e022C8ECA	1	Акульшина С.А.	21.11.2018г. 657 от 3.10.18г.		
105	Регистрационная карточка запроса на сертификат ключа доступа S-07 исп 234901.0484 - 234901001 ods		1 2	Акульшина С.А.	21.11.2018г. 657 от 3.10.18г.	Иванова Т.Н.	21.11.18
106	Регистрационная карточка сертификата ключа ЭЦП Акульшина С.А.		1	ОКЗИ Минэкономразвития КК	21.11.2018		
107	Сертификат ключа ЭЦП Акульшина С.А.		1	ОКЗИ Минэкономразвития КК	21.11.2018		
108	Регистрационная карточка сертификата ключа ЭЦП Осмачкин А.А		1	ОКЗИ Минэкономразвития КК	22.11.2018г. вх. 1778. от 22.11.2018		
109	Сертификат ключа Осмачкина А.А.		1	ОКЗИ Минэкономразвития КК	22.11.2018 вх 1778 от 22.11.2018		
110	Сертификат ключа доступа S-07 исп 234901.0484 - 234901001 ods		1	ОКЗИ Минэкономразвития КК	22.11.2018		
111	Ключ ЭЦП Акульшина С.А.	e022C8ECC	1	Акульшина С.А.	21.11.2019г. 657 от 3.10.18		
112	Заявление на изготовление ск ПЭП Акульшина С.А.		1 2	Акульшина С.А.	21.11.2019 657 от 3.10.18	Иванова Т.Н.	20.11.19

Отметка о подключении (установке СКЗИ)			Отметка об изъятии СКЗИ из аппаратных средств, уничтожении ключевых документов			Примечание
Ф.И.О. сотрудников органа криптографической защиты, пользователя СКЗИ, произведших подключение установку	Дата подключения (установки) и подписи лиц, произведших подключение (установку)	Номера, аппаратных средств, в которые установлены или к которым подключены СКЗИ	Дата изъятия (уничтожения)	Ф.И.О. сотрудников органа криптографической защиты, пользователя СКЗИ, производивших изъятие (уничтожение)	Номер акта или расписка об уничтожении	
9	10	11	12	13	14	15
			21.11.2019	Акульшина С.А.	1024	
				Мацупренко С.Н.	21.11.2019	
				Кравченко В.В.		
			21.11.2019	Акульшина С.А	1024	
				Мацупренко С.Н.	21.11.2019	
				Кравченко В.В		

№ п.п.	Наименование СКЗИ, эксплуатационной и технической документации к ним, ключевых документов	Серийные номера СКЗИ, эксплуатационной и технической документации к ним, номера серий ключевых документов	Номера экземпляров (криптографические номера) ключевых документов	Отметка о получении		Отметка о выдаче	
				От кого получены	Дата и номер сопроводительного письма	Ф.И.О. пользователя СКЗИ	Дата и расписка в получении
1	2	3	4	5	6	7	8
113	Ключ ЭЦП	e022 08EF3	1	Осмаркин А.А.	21.11.2019 №657 от 3.10.18		
	Осмаркин А.А.						
114	Заявление на		1	Осмаркин А.А.	21.11.2019 №657 3.10.18	Иванова	
	изготовление		2			Г.М.	20.11.19
	СК ПЭП						
	Осмаркин А.А.						
115	Ключ доступа	e022C8ECA	1	Акульшина С.А	21.11.2019 657 3.10.18		
	S-07 иктт 2349010484						
	234901001 pbs						
116	Регистрационная		1	Акульшина С.А	21.11.2019 657 3.10.18	Иванова	
	карточка запроса		2			Г.М.	20.11.19
	на сертификат						
	ключа доступа						
	S-07 иктт 2349010484						
	234901001 pbs						
117	Регистрационная		1	ОКЗИ Минфина	21.11.2019		
	карточка сертификата			КК			
	ключа ЭЦП						
	Акульшина С.А						
118	Сертификат		1	ОКЗИ Минфина	21.11.2019		
	ключа ЭЦП			КК			
	Акульшина С.А.						
119	Регистрационная		1	ОКЗИ Минфина	21.11.2019		
	карточка сертификата			КК	дов. б/н		
	ключа ЭЦП				от 5.11.2019		
	Осмаркин А.А						
120	Сертификат ключ		1	ОКЗИ Минфина	22.11.2019		
	Осмаркина А.А.			КК	дов. б/н		
121	Сертификат ключа		1	ОКЗИ	от 5.11.2019		
	доступа S-07 иктт			Минфина	22.11.2019		
	2349010484			КК			
	-234901001 pbs						
122	Ключ ЭЦП	e022C8FCC	1	Акульшина С.А	20.11.2020 657 от 3.10.2018		
	Акульшина С.А						
123	Заявление на		1	Акульшина С.А	20.11.2020 657 от 3.10.2018	Иванова	
	изготовление		2			Г.М.	20.11.20
	СК ПЭП Акульшина С.А.						
124	Ключ ЭЦП	e022208EF3	1	Осмаркин А.А	20.11.2020 657 от 3.10.2018		
	Осмаркин АА						
125	Заявление на		1	Осмаркин А.А	20.11.2020 657 от 3.10.2018	Иванова	
	изготовление СК ПЭП		2			Г.М.	20.11.20
	Осмаркин АА						

№ п.п.	Наименование СКЗИ, эксплуатационной и технической документации к ним, ключевых документов	Серийные номера СКЗИ, эксплуатационной и технической документации к ним, номера серий ключевых документов	Номера экземпляров (криптографические номера) ключевых документов	Отметка о получении		Отметка о выдаче	
				От кого получены	Дата и номер сопроводительного письма	Ф.И.О. пользователя СКЗИ	Дата и расписк в получении
1	2	3	4	5	6	7	8
126	Ключ доступа	e022c8eca	1	Акулышина С.А.	20.11.2020 657 от 3.10.2018		
	S-07 urn 234901048Y						
	234901001 pbs						
127	Регистрационная		1	Акулышина С.А.	20.11.2020 657 от 3.10.2018	Иванова Т.И.	20.11.20
	карточка запроса		2				
	на сертификат						
	ключа доступа						
	S-07 urn 234901048Y						
	234.901001 pbs						
128	Регистрационная		1	ОКЭП Минэкономразвития	20.11.2020		
	карточка сертификата			КК			
	ключа ЭЦП						
	Акулышина С.А.						
129	Сертификат		1	ОКЭП Минэкономразвития	20.11.2020		
	ключа ЭЦП			КК			
	Акулышина С.А.						
130	Регистрационная		1	ОКЭП Минэкономразвития	20.11.2020		
	карточка сертификата			КК			
	ключа ЭЦП			сов б/н от	11.11.2020		
	Осмачкин А.А.						
131	Сертификат ключа		1	ОКЭП Минэкономразвития	20.11.2020		
	Осмачкин А.А.			КК			
132	Сертификат		1	доверен. б/н	11.11.2020.		
	ключа доступа						
	S-07 urn 234901048Y						
	234901001 pbs						
133	Ключ ЭЦП	e022c8ecc	1	Акулышина С.А.	19.11.2021 657 от 3.10.2018		
	Акулышина С.А.						
134	Заявление на		1	Акулышина С.А.	19.11.2021 657 от 3.10.2018	Иванова Т.И.	19.11.21
	изготовление		2				
	СК ПЭП Акулышина С.А.						
135	Ключ ЭЦП	e022208ef3	1	Осмачкин А.А.	19.11.2021 657 от 3.10.2018		
	Осмачкин А.А.						
136	Заявление на		1	Осмачкин А.А.	19.11.2021 657 от 3.10.2018	Иванова Т.И.	19.11.21
	изготовление		2				
	СК ПЭП Осмачкин А.А.						
137	Ключ доступа	e022c8eca	1	Акулышина С.А.	19.11.2021 657 от 3.10.2018		
	S-07 urn 234901048Y						
	234901001 pbs						
138	Регистрационная		1	Акулышина С.А.	19.11.2021 657 от 3.10.2018	Иванова Т.И.	19.11.21
	карточка запроса		2				

на сертификат ключа доступа S-07 urn 234901048Y 234901001 pbs

№ п.п.	Наименование СКЗИ, эксплуатационной и технической документации к ним, ключевых документов	Серийные номера СКЗИ, эксплуатационной и технической документации к ним, номера серий ключевых документов	Номера экземпляров (криптографические номера) ключевых документов	Отметка о получении		Отметка о выдаче	
				От кого получены	Дата и номер сопроводительного письма	Ф.И.О. пользователя СКЗИ	Дата и распис в получени
1	2	3	4	5	6	7	8
139	Регистрационная карточка сертификата ключа ЭЦП Акульшина С.А		1	ОКЗИ Минэкономики КК	19.11.2021 657 от 3.10.2018		
140	Сертификат ключа ЭЦП Акульшина С.А.		1	ОКЗИ Минэкономики КК	19.11.2021 657 от 3.10.2018		
141	Регистрационная карточка сертификата ключа ЭЦП Осмачкин А.А.		1	ОКЗИ Минэкономики КК довер. б/н	19.11.2021 657 от 3.10.2018 15.11.2021		
142	Сертификат ключа Осмачкин А.А.		1	ОКЗИ Минэкономики КК довер. б/н	19.11.2021 657 от 3.10.2018 15.11.2021		
143	Сертификат ключа доступа S-07 urm 2349010484 234901001 pbS		1	ОКЗИ Минэкономики КК	19.11.2021 657 от 3.10.2018		
144	Ключ доступа S-07 urm 2349010484 234901001 pbS	E022C8ECA	1	Акульшина С.А	довер. 319 от 04.05.2022		
145	Реестр. карточка запроса на сертификат ключа доступа S-07 urm 2349010484 234901001 pbS		1 2	Акульшина С.А	довер. 319 от 04.05.2022		
146	Ключ ЭЦП Акульшина С.А.	E022C8ECC	1	Акульшина С.А.	18.11.2022 716 от 10.11.2022		
147	Заявление на изготовление СК ПЭП Акульшина С.А.		1 2	Акульшина С.А	18.11.2022, 716 от 10.11.2022	Осмачкин А.А.	18.11.2
148	Ключ ЭЦП Осмачкин А.А	E022208FF3	1	Осмачкин А.А	18.11.2022 716 от 10.11.2022		
149	Заявление на изготовление СК ПЭП Осмачкин А.А		1 2	Осмачкин А.А	18.11.2022 716 от 10.11.2022	Осмачкин А.А.	18.11.
150	Ключ доступа S-07 urm 2349010484 234901001 pbS	E022C8EC7	1	Акульшина С.А.	18.11.2022 716 от 10.11.2022		

№ п.п.	Наименование СКЗИ, эксплуатационной и технической документации к ним, ключевых документов	Серийные номера СКЗИ, эксплуатационной и технической документации к ним, номера серий ключевых документов	Номера экземпляров (криптографические номера) ключевых документов	Отметка о получении		Отметка о выдаче	
				От кого получены	Дата и номер сопроводительного письма	Ф.И.О. пользователя СКЗИ	Дата и расписк в получении
1	2	3	4	5	6	7	8
151	Регистрационная карточка запроса на сертификат ключа доступа S-07 Urm 2349010484 234901001 pbs		1 2	Акульшина С.А.	18.11.2022 г. 716 от 10.11.2022,	Мальцев В.М.	18.11.22
152	Регистрационная карточка сертификата ключа ЭЦП Акульшина С.А		1	ОКЗИ Минфина КК	18.11.2022 г 716 от 10.11.2022 г		
153	Сертификат ключа ЭЦП Акульшина С.А			Минфина КК	716 от 10.11.2022.		
154	Регистрационная карточка сертификата ключа ЭЦП Осмачкин А.А		1	ОКЗИ Минфина КК	18.11.2022 г 926 859 от 10.11.2022		
155	Сертификат ключа ЭЦП Осмачкин А.А.		1	ОКЗИ Минфина КК	18.11.2022 г. 716 от 10.11.2022 926 859 от 10.11.2022.		
156	Сертификат ключа доступа S-07 Urm 2349010484 234901001 pbs		1	ОКЗИ Минфина КК	18.11.2022 г. 716 от 10.11.2022		
157	Установочный комплект СКЗИ Континент-АП	Зав № СТ22-2EU3 рег № 351А3-002470	1	ОКЗИ Минфин КК	24.03.2022 926 249 от 24.03.2022 акт 07-274 от 24.03.2022 г		
158	Ключ ЭЦП Акульшина С.А	e022c8ecc	1	Акульшина С.А	17.11.2022 г. 716 от 10.11.2022 г		
159	Заявление на изготовление СК КЭП Акульшина С.А		1 2	Акульшина С.А	17.11.2022 г 716 от 10.11.2022 г	Дурницкий А.А.	17.11.2022 Дурн
160	Ключ ЭЦП Осмачкин А.А	e02208ef3	1	Осмачкин А.А	17.11.2022 г 716 от 10.11.2022 г		

№ п.п.	Наименование СКЗИ, эксплуатационной и технической документации к ним, ключевых документов	Серийные номера СКЗИ, эксплуатационной и технической документации к ним, номера серий ключевых документов	Номера экземпляров (криптографические номера) ключевых документов	Отметка о получении		Отметка о выдаче	
				От кого получены	Дата и номер сопроводительного письма	Ф.И.О. пользователя СКЗИ	Дата и ра в получ
1	2	3	4	5	6	7	8
161	Заявление на изготовление ск ПЭП Осмачкин АА		1 2	Осмачкин АА	17 11. 2023 716 от 10.11.2022 г.	Дубинчук АА	17.11.2
162	Ключ доступа E022C8ECA S-07 ИГМ 2349010484 2349010001 pbs		1	Акулевич С.А	17 11. 2023 г 716 от 10.11.2022 г		
163	Регистрационная карточка запроса на сертификат ключей доступа S-07 ИГМ 2349010484 2349010001 pbs		1 2	Акулевич С.А	17 11. 2023 716 от 10. 11. 2022 г	Дубинчук	17.11.2
164	Регистрационная карточка сертификата ключа ЭЦП Акулевич С.А		1	ОКЗГ Минфин КК	17. 11. 2023 г дов. 866 от 07. 11. 2023 г.		
165	Сертификат ключа ЭЦП Акулевич С.А.		1	ОКЗГ Минфин КК	17. 11. 2023 г дов 866 от 07. 11. 2023 г		
166	Регистрационная карточка сертификата ключа ЭЦП Осмачкин АА		1	ОКЗГ Минфин КК	17. 11. 2023 г дов 866 от 07. 11. 2023 г		
167	Сертификат ключа ЭЦП Осмачкин А-А		1	ОКЗГ Минфин КК	17. 11. 2023 г дов 866 от 07. 11. 2023 г		
168	Сертификат ключа доступа S-07 ИГМ 2349010484 pbs		1	ОКЗГ Минфин КК	17. 11. 2023 г дов 866 от 07. 11. 2023 г		

пронумеровано, прошнуровано
и скреплено гербовой
печатью 10(десять) листов

Директор А.А.Осмачкин

21 ноября 2017г.

МИНИСТЕРСТВО ОБРАЗОВАНИЯ, НАУКИ
И МОЛОДЕЖНОЙ ПОЛИТИКИ КРАСНОДАРСКОГО КРАЯ
ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ КРАСНОДАРСКОГО КРАЯ
«СЛАВЯНСКИЙ ЭЛЕКТРОТЕХНОЛОГИЧЕСКИЙ ТЕХНИКУМ»

П Р И К А З

от 10.11.2022 № 714

г. Славянск-на-Кубани

О назначении комиссии по проверке готовности к обмену электронных документов с использованием электронной цифровой подписи

В целях выполнения условий договора с министерством финансов Краснодарского края от 20 ноября 2017 года № 176/07-ЭД «Об обмене электронными документами, подписанными электронной подписью» (далее – Договор) п р и к а з ы в а ю:

1. Назначить комиссию по проверке готовности к обмену электронных документов с использованием ЭЦП в составе:
   Председатель комиссии: главный бухгалтер Акульшина С.А.
   Члены комиссии: юрисконсульт Кравченко В.В.
   ведущий бухгалтер Колот М.А.
2. Комиссии проверить и составить акт готовности ГБПОУ КК СЭТ к обмену документов с использованием ЭЦП.
3. Предыдущий приказ от 03 октября 2018 года № 665 «О назначении комиссии по проверке готовности к обмену электронных документов с использованием электронной цифровой подписи» считать утратившим силу с 10 ноября 2022 года.
4. Приказ вступает в силу со дня его подписания.

Директор А.А. Осмачкин

С приказом ознакомлены:

С.А. Акульшина
В.В. Кравченко
М.А. Колот

МИНИСТЕРСТВО ОБРАЗОВАНИЯ, НАУКИ
И МОЛОДЕЖНОЙ ПОЛИТИКИ КРАСНОДАРСКОГО КРАЯ
ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ КРАСНОДАРСКОГО КРАЯ
«СЛАВЯНСКИЙ ЭЛЕКТРОТЕХНОЛОГИЧЕСКИЙ ТЕХНИКУМ»

П Р И К А З

от 10.11.2022 № 715

г. Славянск-на-Кубани

О создании постоянно действующей комиссии для уничтожения ключевых документов

В целях выполнения условий договора с министерством финансов Краснодарского края от 20 ноября 2017 года № 176/07-ЭД «Об обмене электронными документами, подписанными электронной подписью» (далее – Договор) п р и к а з ы в а ю:

1. Создать комиссию для уничтожения ключевых документов в составе:
   Председатель комиссии: главный бухгалтер Акульшина С.А.
   Члены комиссии: юрисконсульт Кравченко В.В.
   ведущий бухгалтер Колот М.А.
2. Предыдущий приказ от 19 ноября 2018 года № 864 «О создании постоянно действующей комиссии» считать утратившим силу с 10 ноября 2022 года.
3. Приказ вступает в силу со дня его подписания.

Директор А.А. Осмачкин

С приказом ознакомлены:

С.А. Акульшина
В.В. Кравченко
М.А. Колот

МИНИСТЕРСТВО ОБРАЗОВАНИЯ, НАУКИ И МОЛОДЕЖНОЙ ПОЛИТИКИ КРАСНОДАРСКОГО КРАЯ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ КРАСНОДАРСКОГО КРАЯ «СЛАВЯНСКИЙ ЭЛЕКТРОТЕХНОЛОГИЧЕСКИЙ ТЕХНИКУМ»

П Р И К А З

от 10.11.2022 № 716

г. Славянск-на-Кубани

Об организации передачи электронных документов с использованием электронной подписи в министерство финансов Краснодарского края

В целях выполнения условий договора с министерством финансов Краснодарского края от 20 ноября 2017 года № 176/07-ЭД «Об обмене электронными документами, подписанными электронной подписью» (далее – Договор) п р и к а з ы в а ю:

1. Определить размещение автоматизированного рабочего места обмена электронными документами в кабинете № 1.4, находящееся по адресу: 353560, Краснодарский край, г. Славянск - на -Кубани, ул. Краснодарская, д. 248.
2. Возложить обязанности внештатного администратора информационной безопасности и пользователем электронной подписи на главного бухгалтера Акульшину Светлану Александровну, а в ее отсутствие – на ведущего бухгалтера Колот Марину Александровну.
3. При обмене электронными документами с министерством финансов Краснодарского края использовать электронную подпись следующих должностных лиц:

директор – Осмачкин Александр Анатольевич;
главный бухгалтер – Акульшина Светлана Александровна.

4. Внештатному администратору информационной безопасности организовать работу по изготовлению, своевременной смене, учету и выдаче ключей электронной подписи для работников, указанных в пункте 3 настоящего приказа.
5. Работникам, указанных в пунктах 2,3 настоящего приказа, при обмене электронными документами с использованием электронной подписи руководствоваться Договором и регламентом криптографической защиты информации министерства финансов Краснодарского края.
6. Максимально ограничить доступ в помещение, указанное в пункте 1 настоящего приказа.

7. Контроль за выполнением настоящего приказа оставляю за собой.

8. Предыдущий приказ от 03 октября 2018 года № 657 «Об организации передачи электронных документов с использованием электронной подписи в министерство финансов Краснодарского края» считать утратившим силу с 10 ноября 2022 года.

9. Приказ вступает в силу со дня его подписания.

Директор А.А. Осмачкин

С приказом ознакомлены:

С.А. Акульшина

М.А. Колот

МИНИСТЕРСТВО ОБРАЗОВАНИЯ, НАУКИ И МОЛОДЕЖНОЙ ПОЛИТИКИ КРАСНОДАРСКОГО КРАЯ
ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ КРАСНОДАРСКОГО КРАЯ
«СЛАВЯНСКИЙ ЭЛЕКТРОТЕХНОЛОГИЧЕСКИЙ ТЕХНИКУМ»
(ГБПОУ КК СЭТ)
ИНН 2349010484 ОГРН 1022304652490
353560 РФ, Краснодарский край,
г.Славянск-на-Кубани, ул.Краснодарская, 248
№ 871 от 17.11. 2023 г.
на № _____ от _____ 20___ г.

УТВЕРЖДАЮ
Директор ГБПОУ КК СЭТ
А.А. Осмачкин
17 ноября 2023 год

АКТ
на уничтожение ключевых документов

Комиссия, созданная приказом государственного бюджетного профессионального образовательного учреждения Краснодарского края «Славянский электротехнологический техникум» № 716 от 10.11.2022 года, в составе:

Председателя комиссии: главного бухгалтера Акульшиной С.А.,

Членов комиссии: ведущего бухгалтера Колот М.А.

юрисконсульта Кравченко В.В.

Произвела отбор нижеперечисленных ключевых документов для уничтожения:

№п/п	Наименование ключевого документа	Учетный номер	экземпляр	Серийный номер ключевого носителя
1	Ключ ЭЦП Осмачкин А.А.	148	1	e022C8EF3
2	Ключ ЭЦП Акульшина С.А.	146	1	e022C8ECC
3	Ключ доступа	150	1	e022C8ECA

Перед уничтожением, сведения указанные в акте, сверены с учетными данными журнала эксплуатационной и технической документации к ним, ключевых документов и фактическим наличием.

Уничтожение произведено полностью, методом стирания.

Председатель комиссии: _____ С.А. Акульшина

Члены комиссии: _____ М.А. Колот

_____ В.В. Кравченко

Сведения об уничтожении ключевых документов внесены в журнал поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов.

Внештатный администратор
информационной безопасности _____ С.А. Акульшина

МИНИСТЕРСТВО ОБРАЗОВАНИЯ, НАУКИ И МОЛОДЕЖНОЙ ПОЛИТИКИ КРАСНОДАРСКОГО КРАЯ
ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ КРАСНОДАРСКОГО КРАЯ
«СЛАВЯНСКИЙ ЭЛЕКТРОТЕХНОЛОГИЧЕСКИЙ ТЕХНИКУМ»

ПРИКАЗ

от 30.12.2023 № 967

г. Славянск-на-Кубани

Об утверждении плана мероприятий по защите информации в информационных системах в государственном бюджетном профессиональном учреждении Краснодарского края «Славянский электротехнологический техникум»

Во исполнение требований Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», п р и к а з ы в а ю:

1. Утвердить план мероприятий по защите информации в информационных системах в государственном бюджетном профессиональном учреждении Краснодарского края «Славянский электротехнологический техникум» (Приложение № 1).

2. Разместить Э.В. Берёзкину, преподавателю информатики, ответственному редактору сайта, нормативный документ, указанный в пункте 1 настоящего приказа, на сайте техникума.

3. Контроль за исполнением настоящего приказа возложить на заместителя директора по АХР Козырь Е.А.

Директор А.А. Осмачкин

Проект внесен:
Заместитель директора по АХР Е.А. Козырь

Приложение 1

УТВЕРЖДЕНО
приказом ГБПОУ КК СЭТ
от 30.12.2023 № 957

План
мероприятий по защите информации в информационных системах в государственном бюджетном профессиональном учреждении Краснодарского края «Славянский электротехнологический техникум»

Общие положения

1.1. План мероприятий по защите информации в информационных системах в государственном бюджетном профессиональном учреждении Краснодарского края «Славянский электротехнологический техникум» (далее - План) содержит перечень мероприятий и требований.

1.2. План разработан в соответствии с Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

1.3. План содержит следующую информацию:

- формирование требований к защите информации, содержащейся в информационных системах
- разработка системы защиты информации ИС;
- внедрение системы защиты информации ИС;
- обеспечение защиты информации в ходе эксплуатации ИС;

2. Планирование мероприятий

1.1. Для обеспечения защиты информации, содержащейся в ИС, проводятся мероприятия, которые представлены в Таблице 1.

Таблица 1. План мероприятий.

№ п/п	Мероприятие	Сроки (периодичность) выполнения	Примечание
1	2	3	4
1. Формирование требований к защите информации, содержащейся в ИС			
1.1.	Принятие решения о необходимости защиты информации, содержащейся в ИС	-	-
1.2.	Классификация ИС по требованиям защиты информации и определение уровня защищенности персональных данных (далее - ПДн) при их обработке в ИС	Перед созданием системы защиты и при необходимости в ходе эксплуатации ИС	Определение класса защищенности ИС и уровня защищенности ПДн при их обработке в ИС осуществляется при создании ИС, а также в ходе эксплуатации при изменении состава, структуры ИС или технических особенностей ее построения (при изменении программного обеспечения, топологии и т.д.).
1.3.	Определение угроз безопасности информации, реализация которых может привести к нарушению безопасности информации в ИС, и разработка на их основе модели угроз безопасности информации	Перед созданием системы защиты и в ходе эксплуатации ИС при выявлении новых уязвимостей	Разрабатывается/уточняется Модель угроз безопасности и модель нарушителя безопасности информации.
1.4.	Определение требований к системе защиты информации ИС	Перед созданием системы защиты	Разрабатывается техническое задание на создание системы защиты информации ИС.
2. Разработка системы защиты информации ИС			
2.1.	Проектирование системы защиты информации ИС	До ввода в эксплуатацию и при необходимости	Разработка Проекта на систему защиты. Выбор мер по защите информации проводится исходя из класса защищенности ИС, уровня защищенности ПДн при их обработке в ИС и угроз безопасности информации, включенных в Модель угроз безопасности, а также с учетом структурнофункциональных характеристик ИС. Определяются виды и типы средств защиты информации, обеспечивающие реализацию технических мер защиты информации. Определяется структура системы защиты информации ИС, включая состав (количество) и места размещения ее элементов. Осуществляется выбор средств защиты информации, сертифицированных на соответствие требованиям по безопасности информации, с учетом их стоимости, совместимости с информационными технологиями и техническими средствами, функций безопасности этих средств и особенностей их реализации, а также класса защищенности ИС и уровня защищенности ПДн при их обработке в ИС. Определяются требования к параметрам настройки программного обеспечения, включая программное обеспечение средств защиты информации, обеспечивающие реализацию мер защиты информации, а также устранение возможных уязвимостей ИС ,приводящих к
2.2.	Разработка эксплуатационной документации на систему защиты информации ИС		

№ п/п	Мероприятие	Сроки (периодичность) выполнения	Примечание
1	2	3	4
			возникновению угроз безопасности информации.
		3. Внедрение системы защиты информации ИС	
3.1.	Установка и настройка средств защиты информации в ИС	До ввода в эксплуатацию и при необходимости	Установка и настройка средств защиты информации в соответствии с эксплуатационной документацией на систему защиты информации ИС и документацией на средства защиты информации.
3.2.	Разработка документов. определяющих правила и процедуры, реализуемые оператором для обеспечения защиты информации в ИС в ходе ее эксплуатации	До ввода в эксплуатацию и при необходимости	Разработка организационно-распорядительных документов по защите информации.
3.3.	Внедрение организационных мер защиты информации	До ввода в эксплуатацию и при необходимости	Реализация правил разграничения доступа, регламентирующих права доступа субъектов доступа к объектам доступа, и введение ограничений на действия пользователей, а также на изменение условий эксплуатации, состава и конфигурации технических средств и программного обеспечения; Проверка полноты и детальности описания в организационно-распорядительных документах по защите информации действий пользователей и администраторов ИС по реализации организационных мер защиты информации; Отработка действий должностных лиц и подразделений, ответственных за реализацию мер защиты информации.
3.4.	Предварительные испытания системы защиты информации ИС	До ввода в эксплуатацию и при необходимости	Проверка работоспособности системы защиты информации ИС, а также принятие решения о возможности опытной эксплуатации системы защиты информации ИС.
3.5.	Опытная эксплуатация системы защиты информации ИС	До ввода в эксплуатацию и при необходимости	Проверка функционирования системы защиты информации ИС, в том числе реализованных мер защиты информации, а также готовность пользователей и администраторов к эксплуатации системы защиты информации ИС.
3.6.	Анализ уязвимостей ИС и принятие мер защиты информации по их устранению	До ввода в эксплуатацию и при необходимости	Проведение анализа уязвимостей средств защиты информации, технических средств и программного обеспечения ИС. Уточнение модели угроз безопасности информации и при необходимости принятие дополнительные меры защиты информации, в случае выявления уязвимостей ИС, приводящих к возникновению дополнительных угроз безопасности информации.
3.7.	Приемочные испытания системы защиты информации ИС	До ввода в эксплуатацию и при необходимости	Проверка выполнения требований к системе защиты информации ИС в соответствии с техническим заданием на создание системы защиты информации ИС.

№ п/п	Мероприятие	Сроки (периодичность) выполнения	Примечание
1	2	3	4
3.8.	Аттестация ИС по требованиям защиты информации и ввод ее в действие	До ввода в эксплуатацию и при необходимости	Проводится совместно с лицензиатами ФСТЭК России.
4.	**Обеспечение защиты информации в ходе эксплуатации аттестованной ИС**		
4.1.	Планирование мероприятий по защите информации в ИС	Вместе с вводом ИС в эксплуатацию	Разработка, утверждение и актуализация плана мероприятий по защите информации в ИС.
4.2.	Анализ угроз безопасности информации в ИС	Не реже одного раза в квартал; При внедрении новых узлов и/или технологий в ИС; При появлении информации о новых уязвимостях	В ходе анализа угроз безопасности информации в ИС в ходе ее эксплуатации осуществляются: выявление, анализ и устранение уязвимостей ИС; анализ изменения угроз безопасности информации в ИС; оценка возможных последствий реализации угроз безопасности информации в ИС.
4.3.	Управление (администрирование) системой защиты информации ИС	Постоянно в ходе эксплуатации ИС	В ходе управления (администрирования) системой защиты информации ИС осуществляются: управление учетными записями пользователей и поддержание в актуальном состоянии правил разграничения доступа в ИС; управление средствами защиты информации ИС; управление обновлениями программных и программно-аппаратных средств, в том числе средств защиты информации, с учетом особенностей функционирования ИС; мониторинг и анализ события безопасности зарегистрированных в ИС; обеспечение функционирования системы защиты информации информационной системы в ходе ее эксплуатации, включая ведение эксплуатационной документации и организационно-распорядительных документов по защите информации.
4.4.	Управление конфигурацией аттестованной ИС и ее системой защиты информации	Постоянно в ходе эксплуатации ИС	В ходе управления конфигурацией ИС и ее системы защиты информации осуществляются: определение компонентов ИС и ее системы защиты информации, подлежащих изменению в рамках управления конфигурацией; управление изменениями ИС и ее системы защиты информации: разработка параметров настройки, обеспечивающих защиту информации, анализ потенциального воздействия планируемых изменений на обеспечение защиты информации, санкционирование внесения изменений в ИС и ее систему защиты информации, документирование действий по внесению изменений в ИС и сохранение данных об изменениях конфигурации; контроль действий по внесению изменений в ИС и ее систему защиты информации.

№ п/п	Мероприятие	Сроки (периодичность) выполнения	Примечание
1	2	3	4
4.5.	Выявление инцидентов и реагирование на них	Постоянно в ходе эксплуатации ИС; Не реже одного раза в год проведение внутреннего аудита информационной безопасности	В ходе реагирования на инциденты осуществляются: обнаружение и идентификация инцидентов, в том числе отказов в обслуживании, сбоев(перезагрузок) в работе технических средств, программного обеспечения и средств защиты информации, нарушений правил разграничения доступа, неправомерных действий по сбору информации, внедрений вредоносных компьютерных программ (вирусов) и иных событий, приводящих к возникновению инцидентов; своевременное информирование пользователями и администраторами лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в информационной системе; анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий; планирование и принятие мер по устранению инцидентов, в том числе по восстановлению ИС и ее сегментов в случае отказа в обслуживании или после сбоев, устранению последствий нарушения правил разграничения доступа, неправомерных действий по сбору информации, внедрения вредоносных компьютерных программ (вирусов) и иных событий, приводящих к возникновению инцидентов.
4.6.	Информирование и обучение персонала ИС	Не реже одного раза в два года	В ходе информирования и обучения персонала ИС осуществляются: информирование персонала ИС о появлении актуальных угроз безопасности информации, о правилах безопасной эксплуатации ИС; доведение до персонала ИС требований по защите информации, а также положений организационно-распорядительных документов по защите информации с учетом внесенных в них изменений; обучение персонала ИС правилам эксплуатации отдельных средств защиты информации; проведение практических занятий и тренировок с персоналом ИС по блокированию угроз безопасности информации и реагированию на инциденты; контроль осведомленности персонала ИС об угрозах безопасности информации и уровня знаний персонала по вопросам обеспечения защиты информации.
4.7.	Контроль за обеспечением уровня защищенности информации, содержащейся в ИС	Не реже одного раза в два года	В ходе контроля за обеспечением уровня защищенности информации, содержащейся в ИС, осуществляются: контроль (анализ) защищенности информации с учетом особенностей функционирования ИС; анализ и оценка функционирования ИС и ее системы защиты информации, включая анализ и устранение уязвимостей и иных недостатков в функционировании системы защиты информации ИС; документирование процедур и результатов контроля за обеспечением уровня защищенности

№ п/п	Мероприятие	Сроки (периодичность) выполнения	Примечание
1	2	3	4
			информации, содержащейся в ИС; принятие решения по результатам контроля за обеспечением уровня защищенности информации, содержащейся в ИС, о необходимости доработки(модернизации) ее системы защиты информации. Контроль за обеспечением уровня защищенности информации, содержащейся в ИС, проводится самостоятельно и (или) с привлечением организации, имеющей лицензию на деятельность по технической защите конфиденциальной информации.
5.	**Обеспечение защиты информации при выводе из эксплуатации аттестованной ИС или после принятия решения об окончании обработки информации**		
5.1.	Архивирование информации, содержащейся в ИС	При выводе из эксплуатации аттестованной ИС или после принятия решения об окончании обработки информации	Архивирование информации, содержащейся в ИС, должно осуществляться при необходимости ее дальнейшего использования.
5.2.	Уничтожение (стирание) данных и остаточной информации с машинных носителей информации и (или) уничтожение машинных носителей информации	При выводе из эксплуатации аттестованной ИС или после принятия решения об окончании обработки информации	Уничтожение (стирание) данных и остаточной информации с машинных носителей информации производится при необходимости передачи машинного носителя информации другому пользователю ИС. При выводе из эксплуатации машинных носителей информации, на которых осуществлялись хранение и обработка информации, осуществляется физическое уничтожение этих машинных носителей информации.

МИНИСТЕРСТВО ОБРАЗОВАНИЯ, НАУКИ И МОЛОДЕЖНОЙ ПОЛИТИКИ КРАСНОДАРСКОГО КРАЯ
ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ КРАСНОДАРСКОГО КРАЯ
«СЛАВЯНСКИЙ ЭЛЕКТРОТЕХНОЛОГИЧЕСКИЙ ТЕХНИКУМ»

ПРИКАЗ

от 30.12.2023 № 956

г. Славянск-на-Кубани

Об утверждении правил доступа сотрудников, обучающихся и посетителей в помещения государственного бюджетного профессионального учреждения Краснодарского края «Славянский электротехнологический техникум»

В целях обеспечения безопасности и соблюдения режима ограниченного доступа в помещения государственного бюджетного профессионального учреждения Краснодарского края «Славянский электротехнологический техникум» (далее - Техникум) приказываю:

1. Утвердить прилагаемые Правила доступа сотрудников, обучающихся и посетителей в помещения государственного бюджетного профессионального учреждения Краснодарского края «Славянский электротехнологический техникум» (Приложение № 1).

2. Ответственного за организацию обработки персональных данных в техникуме заместителя директора по АХР Е.А. Козырь в месячный срок обеспечить ознакомление работников путем размещения на сайте и стендах учреждения.

3. Разместить Э.В. Берёзкину, преподавателю информатики, ответственному редактору сайта, нормативный документ, указанный в пункте 1 настоящего приказа, на сайте техникума.

4. Контроль за исполнением настоящего приказа возложить на заместителя директора по АХР Е.А. Козырь.

Директор А.А. Осмачкин

Проект внесен:
Заместитель директора по АХР Е.А. Козырь

Приложение № 1

УТВЕРЖДЕНО
приказом ГБПОУ КК СЭТ
от 30.12.2023 № 956

Правила доступа сотрудников, обучающихся и посетителей в помещения государственного бюджетного профессионального учреждения Краснодарского края «Славянский электротехнологический техникум»

1. Общие положения

1.1. Настоящие правила разработаны с целью организации режима обеспечения безопасности помещений государственного бюджетного профессионального учреждения Краснодарского края «Славянский электротехнологический техникум» (далее - Техникум), препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения, и устанавливает правила доступа в помещения министерства в рабочее и нерабочее время, а также в нештатных ситуациях.

1.2. Настоящие правила распространяются на сотрудников и студентов техникума.

1.3. Ответственность за соблюдение положений настоящих правил несут сотрудники техникума.

1.4. Бесконтрольный доступ посторонних лиц в помещения запрещен.

2. Система контроля и управления доступом

2.1. Система контроля и управления доступом состоит из следующих технических средств:

преграждающие управляемые устройства в составе преграждающих конструкций и исполнительных устройств (турникеты, двери с электромагнитными замками или электромеханическими защелками и т.д.).

2.2. Система контроля и управления доступом (далее - СКУД) должна обеспечивать выполнение следующих основных функций:

открывание преграждающих управляемых устройств при считывании идентификационного признака, доступ по которому разрешен в данную зону доступа (помещение) в заданный временной интервал или по команде оператора системы контроля и управления доступом;

запрет открывания преграждающих управляемых устройств при считывании идентификационного признака, доступ по которому не разрешен в данную зону доступа (помещение) в заданный временной интервал;

санкционированное изменение (добавление, удаление) идентификационных

защита от несанкционированного доступа к программным средствам устройств управления для изменения (добавления, удаления) идентификационных признаков;

сохранение настроек базы данных идентификационных признаков при отключении электропитания;

ручное, полуавтоматическое или автоматическое открывание преграждающих управляемых устройств для прохода при аварийных ситуациях, пожаре, технических неисправностях в соответствии с настоящими правилами и правилами противопожарной безопасности;

автоматическое закрытие преграждающих управляемых устройств через определенное время после считывания разрешенного идентификационного признака;

регистрация и протоколирование текущих событий;

возможность формирования статистической отчетности.

2.3. Должно быть обеспечено постоянное закрытие дверей СКУД и открытие только для санкционированного прохода.

3. Электронные пропуска.

3.1. Электронный пропуск является основным документом сотрудников и студентов для прохода в помещения техникума.

3.2. Электронный пропуск выдается под личную подпись в ведомости выдачи электронных пропусков получателем.

3.3. Выдача электронных пропусков осуществляется по документам, удостоверяющим личность.

3.4. Замена электронного пропуска возможна в случае изменения фамилии, имени, отчества или в случае утери или порчи.

В случае утери, утраты или порчи электронного пропуска его владелец обязан незамедлительно проинформировать техникум, пропуск из СКУД незамедлительно удаляется.

Взамен утерянного, утраченного или испорченного электронного пропуска выдается новый.

3.5. При увольнении и отчислении, электронный пропуск сдается заместителю директора по АХР.

4. Правила доступа в помещения в рабочее время

4.1. Доступ иных лиц в помещения осуществляется:

в рабочие дни с 7.30 до 18.00;

4.2. Допуск в помещения осуществляется:

по электронным пропускам;

по служебной записке работника с регистрацией в журнале посетителей;

по согласованию с работниками техникума при предъявлении документа, удостоверяющего личность, с регистрацией в журнале посетителей.

4.3. Доступ иных лиц в помещения может осуществляться под контролем лиц, имеющих право допуска в помещения.

4.4. Проход по электронным пропускам осуществляется через турникет в

автоматическом режиме. При проходе по электронным пропускам сотрудник поста охраны осуществляет визуальный контроль.

4.5. При несрабатывании электронного пропуска при проходе через турникет сотрудник поста охраны имеет право остановить лицо, осуществляющее проход, для выяснения причин несрабатывания электронного пропуска.

4.6. Пропуск иностранных делегаций осуществляется в соответствии со служебной запиской, согласованной с руководителем техникума

4.7. Пропуск в помещения техникума инвалидов (включая инвалидов, использующих кресла-коляски и собак-проводников) осуществляется в соответствии со статьей 15 Федерального закона от 24 ноября 1995 г. № 181-ФЗ «О социальной защите инвалидов в Российской Федерации».

Проход инвалидов обеспечивается сотрудником поста охраны и в его сопровождении.

Для дублирования необходимой для инвалидов звуковой и зрительной информации в здания и сооружения министерства пропускаются сурдопереводчики и тифлосурдопереводчики, сопровождающие инвалидов, по документам, удостоверяющим личность.

Пропуск собак-проводников осуществляется при наличии документа, подтверждающего ее специальное обучение, выданного по установленной форме.

4.8. В случаях, предусмотренных законодательством Российской Федерации, контроль лиц, проходящих в помещения техникума, может осуществляться с применением технических средств осмотра, а их личных вещей - путем осмотра сотрудником поста охраны.

4.9. Крупногабаритные предметы (размером свыше 50х50х50 см) предъявляются сотруднику поста охраны для осмотра.

4.10. Не подлежат вносу (выносу) в помещения техникума огнестрельное, холодное, пневматическое, газовое оружие, боеприпасы и спецсредства (за исключением служебного оружия в случаях, предусмотренных законодательством Российской Федерации), наркотические и психотропные средства, пиротехнические устройства, взрывчатые, отравляющие, другие вещества и материалы, представляющие опасность для жизни и здоровья людей.

4.11. Проход технического персонала для уборки помещений техникума, осуществляется по электронным пропускам или спискам.

5. Правила доступа в помещения в нерабочее время

Доступ работников в помещения в нерабочее время допускается по согласованию с директором техникума.

Нахождение в помещениях посторонних лиц в нерабочее время запрещается

6. Правила доступа в помещения в нештатных ситуациях

6.1. В случае возникновения нештатной ситуации работникам необходимо незамедлительно сообщать о происшествии руководителю техникума или заместителю директора по АХР.

6.2. При возникновении чрезвычайных ситуаций (пожар, взрыв, авария) и по сигналу гражданской обороны лица, находящиеся в помещениях техникума, покидают их без проверки, документов, удостоверяющих личность, через основные и запасные выходы.

7. Ответственность

Передавать электронный карты сторонним лицам строго запрещено.

МИНИСТЕРСТВО ОБРАЗОВАНИЯ, НАУКИ И МОЛОДЕЖНОЙ ПОЛИТИКИ КРАСНОДАРСКОГО КРАЯ
ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ КРАСНОДАРСКОГО КРАЯ
«СЛАВЯНСКИЙ ЭЛЕКТРОТЕХНОЛОГИЧЕСКИЙ ТЕХНИКУМ»

ПРИКАЗ

от 30.12.2023 № 955

г. Славянск-на-Кубани

Об утверждении положения об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных государственного бюджетного профессионального учреждения Краснодарского края «Славянский электротехнологический техникум»

Во исполнение требований части 5 статьи 19 Федерального закона от 27.07.2006 N 152-ФЗ "О персональных данных", постановления Правительства Российской Федерации от 01.11.2012 N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных", приказа Федеральной службы по техническому и экспортному контролю от 11.02.2013 N 17 "Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах", приказа ФСТЭК России от 18.02.2013 N 21 "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных", приказом Федеральной службы безопасности Российской Федерации от 10.07.2014 N 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" п р и к а з ы в а ю:

1. Утвердить положение об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных государственного бюджетного профессионального учреждения Краснодарского края «Славянский электротехнологический техникум» (Приложение № 1).

2. Разместить Э.В. Берёзкину, преподавателю информатики, ответственному редактору сайта, нормативный документ, указанный в пункте 1 настоящего приказа, на сайте техникума.

3. Контроль за исполнением настоящего приказа возложить на заместителя директора по АХР Е.А. Козырь.

Директор А.А. Осмачкин

Проект внесен:
Заместитель директора по АХР Е.А. Козырь

Приложение 1

УТВЕРЖДЕНО
приказом ГБПОУ КК СЭТ
от 30.12.2023 № 955

Положение об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных государственного бюджетного профессионального учреждения Краснодарского края «Славянский электротехнологический техникум»

1. Общие положения

1.1. Угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных в техникуме (далее - Актуальные угрозы безопасности ИСПДн), определены в соответствии с частью 5 статьи 19 Федерального закона от 27.07.2006 N 152-ФЗ "О персональных данных", постановлением Правительства Российской Федерации от 01.11.2012 N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных", приказом Федеральной службы по техническому и экспортному контролю (далее - ФСТЭК России) от 11.02.2013 N 17 "Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах", приказом ФСТЭК России от 18.02.2013 N 21 "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных", приказом Федеральной службы безопасности Российской Федерации (далее - ФСБ России) от 10.07.2014 N 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", Методикой определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденной заместителем директора ФСТЭК России 14.02.2008, 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, утверждёнными руководством 8-го Центра ФСБ России от 31.03.2015 N 149/7/2/6-432, Базовой моделью угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденной заместителем директора ФСТЭК России 15.02.2008, и Банком

данных угроз безопасности информации, размещенным на официальном сайте ФСТЭК России (http://bdu.fstec.ru).

1.2. Актуальные угрозы безопасности ИСПДн содержат перечень актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных (далее - ИСПДн) техникума.

1.3. Актуальные угрозы безопасности ИСПДн подлежат адаптации в ходе разработки органами власти частных моделей угроз безопасности персональных данных для каждой информационной системы (далее - ИС).

1.4. При разработке частных моделей угроз безопасности персональных данных проводится анализ структурно-функциональных характеристик ИС, эксплуатируемой при осуществлении колледжем функций и полномочий, а также применяемых в ней информационных технологий и особенностей ее функционирования, в том числе с использованием Банка данных угроз безопасности информации.

1.5. В частной модели угроз безопасности персональных данных указываются:

описание ИСПДн и ее структурно-функциональных характеристик;

описание угроз безопасности персональных данных с учетом совокупности предположений о способах, подготовке и проведении атак;

описание возможных уязвимостей ИС, способов реализации угроз безопасности информации и последствий нарушений безопасности информации.

1.6. Объектами информатизации в колледже выступают ИС, имеющие сходную структуру и одноточечное подключение к сетям общего пользования и (или) информационно-телекоммуникационной сети "Интернет" (далее - сеть "Интернет") через выделенную инфраструктуру - межведомственную сеть передачи данных Краснодарского края.

1.7. В зависимости от конкретного объекта информатизации ИС в техникуме делятся на два вида:

локальная ИС, рабочие места и базы данных которой расположены в пределах одного здания;

распределенная ИС, рабочие места которой расположены в пределах одного здания, а базы данных хранятся и обрабатываются в Центре обработки данных техникума.

1.8. Базы данных информации, с использованием которых осуществляются сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение) персональных данных граждан Российской Федерации, находятся на территории Российской Федерации.

1.9. Ввод персональных данных в ИС и вывод данных из ИС осуществляются с использованием бумажных и электронных носителей информации. В качестве электронных носителей информации используются учтенные съемные носители информации и оптические диски. Доступ к ИСПДн ограничен перечнем сотрудников колледжа, являющихся владельцем ИС.

1.10. Передача персональных данных в другие организации и в территориальные органы федеральных органов исполнительной власти по сетям общего пользования и (или) сети "Интернет" осуществляется с использованием сертифицированных шифровальных (криптографических) средств защиты информации (далее - СКЗИ).

1.11. Контролируемой зоной ИС являются здания техникума. В пределах контролируемой зоны находятся рабочие места пользователей, серверы, сетевое и телекоммуникационное оборудование ИС. Вне контролируемой зоны находятся линии передачи данных и телекоммуникационное оборудование, используемое для информационного обмена по сетям общего пользования и (или) сети "Интернет".

1.12. В зданиях техникума:

должен быть организован пропускной режим;

должно быть исключено неконтролируемое пребывание посторонних лиц и неконтролируемое перемещение (вынос за пределы здания) компьютеров и оргтехники;

помещения со средствами вычислительной техники должны быть оборудованы запирающимися дверями и опечатывающими устройствами;

дополнительно может быть организовано видеонаблюдение в коридорах, вестибюлях и холлах.

1.13. Защита персональных данных в ИС техникума и сетях общего пользования, подключаемых к сети "Интернет", обеспечивается средствами защиты информации (далее - СЗИ).

2. Характеристики безопасности информационных систем персональных данных

2.1. Основными свойствами безопасности информации являются:

конфиденциальность - обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания;

целостность - состояние защищенности информации, характеризуемое способностью ИС обеспечивать сохранность и неизменность информации при попытках несанкционированных воздействий на нее в процессе обработки или хранения;

доступность - состояние информации, при котором субъекты, имеющие права доступа, могут реализовать их беспрепятственно.

2.2. Под актуальными угрозами безопасности персональных данных понимается совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к персональным данным при их обработке в ИС, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия.

2.3. В зависимости от состава обрабатываемых персональных данных и типа актуальных угроз необходимый уровень защищенности персональных данных для каждой ИСПДн определяется индивидуально.

2.4. Для ИСПДн органов власти актуальны угрозы безопасности персональных данных третьего типа, не связанные с наличием НДВ в системном и прикладном программном обеспечении (далее - ПО), используемом в ИС.

3. Применение средств криптографической защиты информации в информационных системах персональных данных

3.1. Актуальность применения в ИСПДн органов власти СКЗИ определяется необходимостью защиты персональных данных, в том числе при информационном обмене по сетям связи общего пользования и (или) сети "Интернет".

3.2. СКЗИ предназначены для защиты информации от действий со стороны лиц, не имеющих право доступа к этой информации.

3.3. Принятыми организационно-техническими мерами в колледже должна быть исключена возможность несанкционированного доступа потенциального нарушителя к ключевой информации СКЗИ.

3.4. При эксплуатации СКЗИ должны соблюдаться требования эксплуатационно-технической документации на СКЗИ и требования действующих нормативных правовых актов в области реализации и эксплуатации СКЗИ.

3.5. Для обеспечения безопасности персональных данных при их обработке в ИСПДн используются СКЗИ, прошедшие в установленном порядке процедуру оценки соответствия.

3.6. Объектами защиты в ИСПДн являются:

персональные данные;

средства криптографической защиты информации;

среда функционирования СКЗИ (далее - СФ);

информация, относящаяся к криптографической защите персональных данных, включая ключевую, парольную и аутентифицирующую информацию СКЗИ;

документы, дела, журналы, картотеки, издания, технические документы, рабочие материалы и т. п., в которых отражена защищаемая информация, относящаяся к ИСПДн и их криптографической защите, включая документацию на СКЗИ и на технические и программные компоненты среды функционирования СКЗИ;

носители защищаемой информации, используемые в ИС в процессе криптографической защиты персональных данных, носители ключевой, парольной и аутентифицирующей информации СКЗИ и порядок доступа к ним;

используемые информационной системой каналы (линии) связи, включая кабельные системы;

помещения, в которых находятся ресурсы ИС, имеющие отношение к криптографической защите персональных данных.

3.7. Реализация угроз безопасности персональных данных, обрабатываемых в ИСПДн, определяется возможностями источников атак. На основании исходных данных об объектах защиты и источниках атак в таблице 1 для колледжа определены обобщенные возможности источников атак.

Таблица 1

Обобщенные возможности источников атак	Да/Нет
1	2
1. Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак только за пределами контролируемой зоны	Да
2. Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак в пределах контролируемой зоны, но без физического доступа к аппаратным средствам (далее - АС), на которых реализованы СКЗИ и среда их функционирования	Да
3. Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак в пределах контролируемой зоны с физическим доступом к АС, на которых реализованы СКЗИ и среда их функционирования	Нет
4. Возможность привлекать специалистов, имеющих опыт разработки и анализа СКЗИ (включая специалистов в области анализа сигналов линейной передачи и сигналов побочного электромагнитного излучения и наводок СКЗИ)	Нет
5. Возможность привлекать специалистов, имеющих опыт разработки и анализа СКЗИ (включая специалистов в области использования для реализации атак недокументированных возможностей прикладного программного обеспечения)	Нет
6. Возможность привлекать специалистов, имеющих опыт разработки и анализа СКЗИ (включая специалистов в области использования для реализации атак недокументированных возможностей аппаратного и программного компонентов среды функционирования СКЗИ)	Нет

3.8. В соответствии с обобщенными возможностями источников атак (**таблица 1**) определены две актуальные уточнённые возможности нарушителей и направления атак (соответствующие актуальные угрозы для ИС) (таблица 2).

Таблица 2

Уточнённые возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
1	2	3
1. Проведение атаки при нахождении в пределах контролируемой зоны	Неактуально	- проводятся работы по подбору персонала; - представители технических, обслуживающих и других вспомогательных служб при работе в помещениях (стойках), где расположены СКЗИ, и сотрудники, не являющиеся пользователями СКЗИ, находятся в этих помещениях только в присутствии сотрудников по эксплуатации; -сотрудники, являющиеся пользователями ИСПДн, но не являющиеся пользователями СКЗИ, проинформированы о правилах работы в ИСПДн и ответственности за несоблюдение правил обеспечения безопасности информации; - пользователи СКЗИ проинформированы о правилах работы в ИСПДн, правилах работы с СКЗИ и ответственности за несоблюдение правил обеспечения безопасности информации помещения в которых располагаются СКЗИ, оснащены входными дверьми с надежными замками, обеспечено постоянное закрытие дверей помещений на замок, их открытие осуществляется только для санкционированного прохода;

		- утверждены правила доступа в помещения, где располагаются СКЗИ, в рабочее и нерабочее время, а также в нештатных ситуациях; утвержден перечень лиц, имеющих право доступа в помещения, где располагаются СКЗИ; -осуществляется разграничение и контроль доступа пользователей к защищаемым ресурсам; - осуществляется регистрация и учет действий пользователей с ПДн; - осуществляется контроль целостности средств защиты; на АРМ и серверах, на которых установлены СКЗИ, используются сертифицированные СЗИ от несанкционированного доступа (далее - НСД); -используются сертифицированные средства антивирусной защиты
2. Проведение атак на этапе эксплуатации СКЗИ на следующие объекты: документацию на СКЗИ и компоненты	Неактуально	- проводятся работы по подбору персонала; - документация на СКЗИ хранится у ответственного за СКЗИ в металлическом сейфе; - помещения, в которых располагаются документацияна СКЗИ, СКЗИ и компоненты СФ, оснащены входными дверьми с надежными замками, обеспечено постоянное закрытие дверей помещений на замок, и их открытие осуществляетсятолько для санкционированного прохода; -утвержден перечень лиц, имеющих право доступа в помещения

3. Получение в рамках предоставленных полномочий, а также в результате наблюдений следующей информации: сведений о физических мерах защиты объектов, в которых размещены ресурсы информационной системы; сведений о мерах по обеспечению контролируемой зоны объектов, в которых размещены ресурсы информационной системы; сведений о мерах по разграничению доступа в помещения, в которых находятся СВТ, на которых реализованы СКЗИ и СФ	Актуально	
4. Использование штатных средств ИСПДн, ограниченное мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий	Актуально	
5. Физический доступ к СВТ, на которых реализованы СКЗИ и СФ	Неактуально	Проводятся работы по подбору персонала; помещения, в которых располагаются располагаются СКЗИ и СФ, оснащены входными дверьми с замками, обеспечивается постоянное закрытие дверей помещений на замок и их открытие только для санкционированного прохода.

6. Возможность воздействовать на аппаратные компоненты СКЗИ и СФ, ограниченная мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий	Неактуально	-Проводятся работы по подбору персонала; - помещения, в которых располагаются СКЗИ и СФ, оснащены входными дверьми с замками, обеспечивается постоянное закрытие дверей помещений на замок и их открытие только для санкционированного прохода; Представители технических, обслуживающих и других вспомогательных служб при работе в помещениях (стойках), где расположены компоненты СКЗИ и СФ, и сотрудники, не являющиеся пользователями СКЗИ, находятся в этих помещениях только в присутствии сотрудников по эксплуатации
7. Возможность располагать сведениями, содержащимися в конструкторской документации на аппаратные и программные компоненты СФ	Неактуально	Не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности
8. Возможность Воздействовать на любые компоненты СКЗИ и СФ	Неактуально	Не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности

4. Определение актуальных угроз безопасности персональных данных в информационных системах персональных данных

4.1. На основе проведенного анализа банка данных угроз безопасности информации (www.bdu.fstec.ru) с учётом структурно-функциональных характеристик типовых ИС, а также применяемых в них информационных технологий и особенностей функционирования, в ИС органов власти могут быть актуальны следующие угрозы безопасности ИСПДн:

У БИ.3 Угроза анализа криптографических алгоритмов и их реализации;

У БИ.4 Угроза аппаратного сброса пароля BIOS;

У БИ.6 Угроза внедрения кода или данных;

УБИ.7 Угроза воздействия на программы с высокими привилегиями;

УБИ.8 Угроза восстановления аутентификационной информации;
УБИ.9 Угроза восстановления предыдущей уязвимой версии BIOS;
УБИ.12 Угроза деструктивного изменения конфигурации/среды окружения программ;
УБИ.13 Угроза деструктивного использования декларированного функционала BIOS;
УБИ.14 Угроза длительного удержания вычислительных ресурсов пользователями;
УБИ.15 Угроза доступа к защищаемым файлам с использованием обходного пути;
УБИ.16 Угроза доступа к локальным файлам сервера при помощи URL;
УБИ.17 Угроза доступа/перехвата/изменения HTTP cookies;
УБИ.18 Угроза загрузки нештатной операционной системы;
УБИ.19 Угроза заражения DNS-кеша;
УБИ.22 Угроза избыточного выделения оперативной памяти;
УБИ.23 Угроза изменения компонентов системы;
УБИ.26 Угроза искажения XML-схемы;
УБИ.27 Угроза искажения вводимой и выводимой на периферийные устройства информации;
УБИ.28 Угроза использования альтернативных путей доступа к ресурсам;
УБИ.30 Угроза использования информации идентификации/ аутентификации, заданной по умолчанию;

УБИ.31 Угроза использования механизмов авторизации для повышения привилегий;
УБИ.32 Угроза использования поддельных цифровых подписей BIOS;
УБИ.33 Угроза использования слабостей кодирования входных данных;
УБИ.34 Угроза использования слабостей протоколов сетевого/ локального обмена данными;
УБИ.36 Угроза исследования механизмов работы программы;
УБИ.37 Угроза исследования приложения через отчёты об ошибках;
УБИ.39 Угроза исчерпания запаса ключей, необходимых для обновления BIOS;
УБИ.41 Угроза межсайтового скриптинга;
УБИ.42 Угроза межсайтовой подделки запроса;
УБИ.45 Угроза нарушения изоляции среды исполнения BIOS;
УБИ.49 Угроза нарушения целостности данных кеша;
УБИ.51 Угроза невозможности восстановления сессии работы на ПЭВМ при выводе из промежуточных состояний питания;
УБИ.53 Угроза невозможности управления правами пользователей BIOS;
УБИ.59 Угроза неконтролируемого роста числа зарезервированных вычислительных ресурсов;
УБИ.62 Угроза некорректного использования прозрачного прокси-сервера за счёт плагинов браузера;
УБИ.63 Угроза некорректного использования функционала программного обеспечения;
УБИ.67 Угроза неправомерного ознакомления с защищаемой информацией;
УБИ.68 Угроза неправомерного/некорректного использования интерфейса взаимодействия с приложением;

УБИ.69 Угроза неправомерных действий в каналах связи;
УБИ.71 Угроза несанкционированного восстановления удалённой защищаемой информации;
УБИ.72 Угроза несанкционированного выключения или обхода механизма защиты от записи в BIOS;
УБИ.74 Угроза несанкционированного доступа к аутентификационной информации;
УБИ.86 Угроза несанкционированного изменения аутентификационной информации;
УБИ.87 Угроза несанкционированного использования привилегированных функций BIOS;
УБИ.88 Угроза несанкционированного копирования защищаемой информации;
УБИ.89 Угроза несанкционированного редактирования реестра;
УБИ.90 Угроза несанкционированного создания учётной записи пользователя;
УБИ.91 Угроза несанкционированного удаления защищаемой информации;
УБИ.93 Угроза несанкционированного управления буфером;
УБИ.94 Угроза несанкционированного управления синхронизацией и состоянием;
УБИ.95 Угроза несанкционированного управления указателями;
УБИ.98 Угроза обнаружения открытых портов и идентификации привязанных к нему сетевых служб;
УБИ.99 Угроза обнаружения хостов;
УБИ.100 Угроза обхода некорректно настроенных механизмов аутентификации;
УБИ.102 Угроза опосредованного управления группой программ через совместно используемые данные;
УБИ.103 Угроза определения типов объектов защиты;
УБИ.104 Угроза определения топологии вычислительной сети;
УБИ.107 Угроза отключения контрольных датчиков;
УБИ.109 Угроза перебора всех настроек и параметров приложения;
УБИ.111 Угроза передачи данных по скрытым каналам;
УБИ.113 Угроза перезагрузки аппаратных и программно-аппаратных средств вычислительной техники;
УБИ.114 Угроза переполнения целочисленных переменных;
УБИ.115 Угроза перехвата вводимой и выводимой на периферийные устройства информации;
УБИ.116 Угроза перехвата данных, передаваемых по вычислительной сети;
УБИ.117 Угроза перехвата привилегированного потока;
УБИ.118 Угроза перехвата привилегированного процесса;
УБИ.121 Угроза повреждения системного реестра;
УБИ.122 Угроза повышения привилегий;
УБИ.123 Угроза подбора пароля BIOS;
УБИ.124 Угроза подделки записей журнала регистрации событий;
УБИ.127 Угроза подмены действия пользователя путём обмана;
УБИ.128 Угроза подмены доверенного пользователя;
УБИ.129 Угроза подмены резервной копии программного обеспечения BIOS;
УБИ.130 Угроза подмены содержимого сетевых ресурсов;
УБИ.131 Угроза подмены субъекта сетевого доступа;
УБИ.132 Угроза получения предварительной информации об объекте защиты;

УБИ.139 Угроза преодоления физической защиты;
УБИ.140 Угроза приведения системы в состояние "отказ в обслуживании";
УБИ.143 Угроза программного выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации;
УБИ.144 Угроза программного сброса пароля BIOS;
УБИ.145 Угроза пропуска проверки целостности программного обеспечения;
УБИ.149 Угроза сбоя обработки специальным образом изменённых файлов;
УБИ.152 Угроза удаления аутентификационной информации;
УБИ.153 Угроза усиления воздействия на вычислительные ресурсы пользователей при помощи сторонних серверов;
УБИ.154 Угроза установки уязвимых версий обновления программного обеспечения BIOS;
УБИ.155 Угроза утраты вычислительных ресурсов;
УБИ.156 Угроза утраты носителей информации;
УБИ.157 Угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации;
УБИ.158 Угроза форматирования носителей информации;
УБИ.159 Угроза "форсированного веб-браузинга";
УБИ.160 Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации;
УБИ.162 Угроза эксплуатации цифровой подписи программного кода;
УБИ.163 Угроза перехвата исключения/сигнала из привилегированного блока функций;
УБИ.167 Угроза заражения компьютера при посещении неблагонадёжных сайтов;
УБИ.168 Угроза "кражи" учётной записи доступа к сетевым сервисам;
УБИ.170 Угроза неправомерного шифрования информации;
УБИ.171 Угроза скрытного включения вычислительного устройства в состав бот-сети;
УБИ.172 Угроза распространения "почтовых червей";
УБИ.173 Угроза "спама" веб-сервера;
УБИ.174 Угроза "фарминга";
УБИ.175 Угроза "фишинга";
УБИ.176 Угроза нарушения технологического/производственного процесса из-за временных задержек, вносимых средством защиты;
УБИ.177 Угроза неподтверждённого ввода данных оператором в систему, связанную с безопасностью;
УБИ.178 Угроза несанкционированного использования системных и сетевых утилит;
УБИ.179 Угроза несанкционированной модификации защищаемой информации;
УБИ.180 Угроза отказа подсистемы обеспечения температурного режима;
УБИ.181 Угроза перехвата одноразовых паролей в режиме реального времени;
УБИ.182 Угроза физического устаревания аппаратных компонентов;
УБИ.183 Угроза перехвата управления автоматизированной системой управления технологическими процессами;
УБИ.185 Угроза несанкционированного изменения параметров настройки средств защиты информации;

УБИ.186 Угроза внедрения вредоносного кода через рекламу, сервисы и контент;
УБИ.187 Угроза несанкционированного воздействия на средство защиты информации;
УБИ.189 Угроза маскирования действий вредоносного кода;
УБИ.190 Угроза внедрения вредоносного кода за счет посещения зараженных сайтов в сети Интернет;
УБИ.191 Угроза внедрения вредоносного кода в дистрибутив программного обеспечения;
УБИ.192 Угроза использования уязвимых версий программного обеспечения;
УБИ.193 Угроза утечки информации за счет применения вредоносным программным обеспечением алгоритмов шифрования трафика;
УБИ.197 Угроза хищения аутентификационной информации из временных файлов cookie;
УБИ.198 Угроза скрытной регистрации вредоносной программной учетных записей администраторов;
УБИ.201 Угроза утечки пользовательских данных при использовании функций автоматического заполнения аутентификационной информации в браузере;
УБИ.203 Угроза утечки информации с не подключенных к сети Интернет компьютеров;
УБИ.204 Угроза несанкционированного изменения вредоносной программой значений параметров программируемых логических контроллеров;
УБИ.205 Угроза нарушения работы компьютера и блокирования доступа к его данным из-за некорректной работы установленных на нем средств защиты.

У .2. Угрозами безопасности персональных данных при их обработке с использованием СКЗИ являются:

4.2.1. создание способов, подготовка и проведение атак без привлечения специалистов в области разработки и анализа СКЗИ;

4.2.2. создание способов, подготовка и проведение атак на различных этапах жизненного цикла СКЗИ. К этапам жизненного цикла СКЗИ относятся: разработка (модернизация) указанных средств, их производство, хранение, транспортировка, ввод в эксплуатацию (пусконаладочные работы), эксплуатация;

4.2.3. проведение атаки, находясь вне пространства, в пределах которого осуществляется контроль за пребыванием и действиями лиц и (или) транспортных средств (далее - контролируемая зона). Границей контролируемой зоны может быть: периметр охраняемой территории организации, ограждающие конструкции охраняемого здания, охраняемой части здания, выделенного помещения;

4.2.4. проведение на этапах разработки (модернизации), производства, хранения, транспортировки СКЗИ и этапе ввода в эксплуатацию СКЗИ (пусконаладочные работы) следующих атак:

внесение несанкционированных изменений в СКЗИ и (или) в компоненты аппаратных и программных средств, совместно с которыми штатно функционируют СКЗИ, в совокупности представляющие среду функционирования СКЗИ, которые способны повлиять на выполнение предъявляемых к СКЗИ требований, в том числе с использованием вредоносных программ;

4.2.5. проведение атак на этапе эксплуатации СКЗИ на:

персональные данные;

ключевую, аутентифицирующую и парольную информацию СКЗИ;

программные компоненты СКЗИ;

аппаратные компоненты СКЗИ;

программные компоненты СФ, включая программное обеспечение BIOS;

аппаратные компоненты СФ;

данные, передаваемые по каналам связи;

4.2.6. получение из находящихся в свободном доступе источников (включая информационно-телекоммуникационные сети, доступ к которым не ограничен определенным кругом лиц, в том числе информационно-телекоммуникационную сеть "Интернет") информации об ИС, в которой используется СКЗИ. При этом может быть получена следующая информация:

общие сведения об ИС, в которой используется СКЗИ (назначение, состав, оператор, объекты, в которых размещены ресурсы ИС);

сведения об информационных технологиях, базах данных, АС, ПО, используемых в ИС совместно с СКЗИ, за исключением сведений, содержащихся только в конструкторской документации на информационные технологии, базы данных, АС, ПО, используемые в ИС совместно с СКЗИ;

содержание находящейся в свободном доступе документации на аппаратные и программные компоненты СКЗИ и СФ;

общие сведения о защищаемой информации, используемой в процессе эксплуатации СКЗИ;

сведения о каналах связи, по которым передаются защищаемые СКЗИ персональные данные (далее - канал связи);

4.2.7. применение находящихся в свободном доступе или используемых за пределами контролируемой зоны АС и ПО, включая аппаратные и программные компоненты СКЗИ и СФ;

4.2.8. получение в рамках предоставленных полномочий, а также в результате наблюдений следующей информации:

сведений о физических мерах защиты объектов, в которых размещены ресурсы ИС;

сведений о мерах по обеспечению контролируемой зоны объектов, в которых размещены ресурсы ИС;

сведений о мерах по разграничению доступа в помещения, в которых находятся СВТ, на которых реализованы СКЗИ и СФ;

4.2.9. использование штатных средств, ограниченное мерами, реализованными в ИС, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий.

МИНИСТЕРСТВО ОБРАЗОВАНИЯ, НАУКИ И МОЛОДЕЖНОЙ ПОЛИТИКИ КРАСНОДАРСКОГО КРАЯ
ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ КРАСНОДАРСКОГО КРАЯ
«СЛАВЯНСКИЙ ЭЛЕКТРОТЕХНОЛОГИЧЕСКИЙ ТЕХНИКУМ»

ПРИКАЗ

от 30.12.2023 № 953

г.Славянск-на-Кубани

Об утверждении перечня лиц, имеющих право доступа в помещения, в которых ведется обработка персональных данных и где размещены используемые средства криптографической защиты информации, хранятся средства криптографической защиты информации и (или) носители ключевой, аутентифицирующей и парольной информации средств криптографической защиты информации

В целях выполнения требований по реализации мер, предусмотренных составом и содержанием 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, утвержденными приказом Федеральной службы безопасности Российской Федерации 10 июля 2014 года № 378, в соответствии с постановлением Правительства Российской Федерации от 21 марта 2012 г. № 211 «Об утверждении мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных», необходимых для обеспечения безопасности персональных данных, обрабатываемых в ГБПОУ КК «Славянский электротехнологический техникум», установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности, п р и к а з ы в а ю:

1. Утвердить перечень лиц, имеющих право доступа в помещения, в которых ведется обработка персональных данных и где размещены используемые средства криптографической защиты информации (далее – СКЗИ), хранятся СКЗИ и (или) носители ключевой, аутентифицирующей и парольной информации СКЗИ в соответствии с приложением к настоящему приказу.

2. Контроль за выполнением настоящего приказа возложить заместителя директора по административно-хозяйственной работе Е.А. Козырь.

3. Приказ вступает в силу со дня его подписания.

Директор А.А. Осмачкин

Проект внесен:
Заместителем директора по АХР Е.А. Козырь

Приложение

УТВЕРЖДЕН
приказом директора
ГБПОУ КК СЭТ
от 30.12.2023 № 953

ПЕРЕЧЕНЬ
лиц, имеющих право доступа в помещения, в которых ведется обработка персональных данных и где размещены используемые СКЗИ, хранятся СКЗИ и (или) носители ключевой, аутентифицирующей и парольной информации СКЗИ

№ п/п	ФИО	Должность, отдел
1	2	3
Кабинет 1.1 Кабинет директора		
1	Осмачкин Александр Анатольевич	директор
Кабинет 1.2 Приемная директора		
2	Одегова Галина Васильевна	секретарь директора
Кабинет 1.3 Отдел кадров		
3	Резанова Светлана Владимировна	специалист по кадрам
Кабинет 1.4 Бухгалтерия		
1	Акульшина Светлана Александровна	главный бухгалтер
2	Колот Марина Александровна	ведущий бухгалтер
3	Кравченко Вера Викторовна	юрисконсульт
Кабинет 1.9		
1	Романова Вера Васильевна	ведущий экономист
2	Некрасова Яна Владимировна	бухгалтер
Кабинет 5.1		
1	Сабиров Михаил Витальевич	заместитель директора по учебно-производственной работе
2	Черных Татьяна Анатольевна	старший методист
3	Товарниченко Дарья Николаевна	секретарь учебной части
Кабинет 5.4		
1	Тарасова Анна Ивановна	заместитель директора по учебной работе
Кабинет 1.6 Общежитие		
1	Козырь Елена Анатольевна	заместитель директора по административно-хозяйственной работе

В рабочее время в помещение имеют право доступа все сотрудники техникума и сотрудники охраны только в присутствии лиц, закрепленных за этим помещением.

В нерабочее время, выходные и праздничные дни в помещение имеют право доступа сотрудники техникума, закрепленные за указанным помещением.

Остальные сотрудники, в том числе сотрудники охраны, имеют право доступа в помещение только в присутствии закрепленного за этим помещением сотрудника. В исключительных случаях (пожар, наводнение и пр.) сотрудники охраны имеет право доступа в помещения без закрепленного за ним сотрудника для устранения угрозы, возникающей в результате стихийного бедствия (пожар, наводнение и пр.).

Заместитель директора по АХР Е.А. Козырь

МИНИСТЕРСТВО ОБРАЗОВАНИЯ, НАУКИ И МОЛОДЕЖНОЙ ПОЛИТИКИ КРАСНОДАРСКОГО КРАЯ
ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ КРАСНОДАРСКОГО КРАЯ
«СЛАВЯНСКИЙ ЭЛЕКТРОТЕХНОЛОГИЧЕСКИЙ ТЕХНИКУМ»

ПРИКАЗ

от 30.12.2023 № 951

г. Славянск-на-Кубани

Об утверждении состава комиссии по информационной безопасности и акта классификации пользовательского сегмента информационной системы государственного бюджетного профессионального учреждения Краснодарского края «Славянский электротехнологический техникум»

Во исполнение требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденными Приказом ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» и Требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденными Постановлением Правительства РФ от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», п р и к а з ы в а ю:

1. Утвердить состав комиссии по информационной безопасности в следующем составе:

Председатель комиссии - заместитель директора по АХР Е.А. Козырь;

Члены комиссии:

Главный бухгалтер С.А. Акульшина

Системный администратор В.Н. Стипаненко

Заведующий отделения курсовой подготовки В.С. Пухиря

2. Утвердить акт классификации пользовательского сегмента информационной системы государственного бюджетного профессионального учреждения Краснодарского края «Славянский электротехнологический техникум»

3. Разместить Э.В. Берёзкину, преподавателю информатики, ответственному редактору сайта, нормативный документ, указанный в пункте 2 настоящего приказа, на сайте техникума.

4. Контроль за исполнением настоящего приказа возложить на заместителя директора по АХР Е.А. Козырь.

Директор А.А. Осмачкин

Проект внесен:
Заместитель директора по АХР Е.А. Козырь

Приложение № 1

УТВЕРЖДЕНО
приказом ГБПОУ КК СЭТ
от 30.12.2025 № 951

АКТ
классификации пользовательского сегмента информационной системы государственного бюджетного профессионального учреждения Краснодарского края «Славянский электротехнологический техникум»

Комиссия, назначенная приказом директора государственного бюджетного профессионального учреждения Краснодарского края «Славянский электротехнологический техникум» № 951 от 30 июля 2023 года, руководствуясь Требованиями о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденными Приказом ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» и Требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденными Постановлением Правительства РФ от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», провела классификацию пользовательского сегмента информационной системы государственного бюджетного профессионального учреждения Краснодарского края «Славянский электротехнологический техникум»

Комиссия установила:

1. Масштаб пользовательского сегмента информационной системы государственного бюджетного профессионального учреждения Краснодарского края «Славянский электротехнологический техникум»: **Региональный**.

2. Уровень значимости информации, содержащейся в пользовательском сегменте информационной системы государственного бюджетного профессионального учреждения Краснодарского края «Славянский электротехнологический техникум»: **третий уровень значимости (УЗ 3)**.

3. Класс защищенности пользовательского сегмента информационной системы государственного бюджетного профессионального учреждения

Краснодарского края «Славянский электротехнологический техникум»: **третий класс защищенности (К3)**.

4. Для пользовательского сегмента информационной системы государственного бюджетного профессионального учреждения Краснодарского края «Славянский электротехнологический техникум» актуальны **угрозы 3-го типа (не связанные с наличием недекларированных возможностей в системном и прикладном программном обеспечении)**.

5. В пользовательском сегменте информационной системы государственного бюджетного профессионального учреждения Краснодарского края «Славянский электротехнологический техникум» обрабатываются специальные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора.

6. Уровень защищенности персональных данных, обрабатываемых в пользовательском сегменте информационной системы государственного бюджетного профессионального учреждения Краснодарского края «Славянский электротехнологический техникум»: **третий уровень защищенности персональных данных (УЗ 3)**.

Председатель комиссии:

Заместитель директора по АХР _____ Е.А. Козырь

Члены комиссии:

Главный бухгалтер _____ С.А. Акульшина

Системный администратор _____ В.Н. Стипаненко

Заведующий отделения курсовой подготовки _____ В.С. Пухиря

МИНИСТЕРСТВО ОБРАЗОВАНИЯ, НАУКИ И МОЛОДЕЖНОЙ ПОЛИТИКИ КРАСНОДАРСКОГО КРАЯ
ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ КРАСНОДАРСКОГО КРАЯ
«СЛАВЯНСКИЙ ЭЛЕКТРОТЕХНОЛОГИЧЕСКИЙ ТЕХНИКУМ»

ПРИКАЗ

от 30.12.2023 № 952

г. Славянск-на-Кубани

Об организационно-технических мероприятиях по обработке и обеспечению безопасности информации, обрабатываемой в государственном бюджетном профессиональном образовательном учреждении Краснодарского края «Славянский электротехнологический техникум»

Во исполнение требований федеральных законов от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», от 27 июля 2006 г. № 152-ФЗ «О персональных данных», в соответствии с приказами 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», 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», приказом Федеральной службы безопасности 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 в государственном бюджетном профессиональном образовательном учреждении Краснодарского края «Славянский электротехнологический техникум» (далее – ГБПОУ КК СЭТ, техникум), установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности, п р и к а з ы в а ю:

1. Назначить системного администратора Стипаненко В.Н. администратором информационных систем техникума;

2. Назначить руководителя отделения курсовой подготовки Пухирю В.С администратором информационной безопасности техникума, ответственным пользователем средств криптографической защиты информации техникума.

3. Во время отсутствия Пухири В.С обязанности ответственного пользователя средств криптографической защиты информации техникума возлагать на Сти-

паненко В.Н.

4. Утвердить:

1) политику использования информационных активов ГБПОУ КК СЭТ (приложение 1);

2) политику антивирусной защиты информации ГБПОУ КК СЭТ (приложение 2);

3) политику использования аутентификационной информации при доступе к информационным активам ГБПОУ КК СЭТ (приложение 3).

4) политику обеспечения отказоустойчивости информационных активов ГБПОУ КК СЭТ (приложение 4);

5) политику сетевой безопасности ГБПОУ КК СЭТ (приложение 5).

6) политику аудита информационной безопасности ГБПОУ КК СЭТ (приложение 6);

7) политику управления событиями безопасности информации ГБПОУ КК СЭТ (приложение 7);

8) политику использования средств криптографической защиты информации ГБПОУ КК СЭТ (приложение 8);

9) инструкцию администратора информационных ресурсов (систем) ГБПОУ КК СЭТ (приложение 9);

10) инструкцию администратора информационной безопасности ГБПОУ КК СЭТ (приложение 10);

11) инструкцию ответственного пользователя средств криптографической защиты информации ГБПОУ КК СЭТ (приложение 11).

5. Заместителю директора по административно-хозяйственной работе Козырь Е.А. ознакомить сотрудников техникума с настоящим приказом под подпись.

6. Специалисту по кадрам Резановой С.В. осуществлять ознакомление лиц, поступивших в техникум на работу с настоящим приказом.

7. Ответственным лицам структурных подразделений техникума ознакомить всех пользователей информационных ресурсов (систем) с Памяткой пользователя информационных ресурсов (систем) ГБПОУ КК СЭТ с отметкой на листе ознакомления (приложение 12).

8. Контроль за выполнением настоящего приказа оставляю за собой.

9. Приказ вступает в силу со дня его подписания.

Директор А.А. Осмачкин

Проект внесен:
Заместителем директора по АХР Е.А. Козырь

С приказом ознакомлены:
Дата _____

ПРИЛОЖЕНИЕ № 1

УТВЕРЖДЕНА
приказом директора
от 30.12.2023 № 952

ПОЛИТИКА
использования информационных активов
государственного бюджетного профессионального
образовательного учреждения Краснодарского края
«Славянский электротехнологический техникум»

1. Общие положения

1.1. Настоящая политика использования информационных активов (далее – Политика) государственного бюджетного профессионального образовательного учреждения Краснодарского края «Славянский электротехнологический техникум» (далее – ГБПОУ КК СЭТ, техникум) определяет процедуры идентификации (инвентаризации), учета, эксплуатации информационных активов техникума, а также порядок предоставления доступа к ним.

1.2. Настоящая Политика разработана в соответствии с:

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

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»;

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»;

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:

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

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:

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

сервера информационных систем (виртуальные и физические);

съемные носители информации;

активное сетевое оборудование;

средства защиты информации[1]);

системное и прикладное программное обеспечение.

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

тип информационного актива;

собственник информационного актива;

местоположение (месторасположение) информационного актива и его пользователя;

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.;

критичность информационного актива;

принадлежность к информационной системе;

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

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

2.7. Для каждого информационного ресурса (системы) Администратором данного ресурса (системы), при содействии Администратора информационной безопасности разрабатывается Технический паспорт информационной системы

---

[1]) Требования к учету и эксплуатации средств криптографической защиты информации регламентированы Политикой использования средств криптографической защиты информации ГБПОУ КК СЭТ.

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.

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:

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

неправомерный доступ;
копирование;
предоставление;
распространение.

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

неправомерное уничтожение;
неправомерное модифицирование.

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

неправомерное блокирование.

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

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;

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;

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 вы-

полнять 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. Сотруднику для работы в информационной системе и (или) для доступа к информационному ресурсу предоставляется АРМ, введенный в домен техникума.

3.2.2. Каждый сотрудник, 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 сотрудникам 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 сотрудниками программного обеспечения на АРМ строго запрещена. Установка и удаление любого программного обеспечения производится только ответственными сотрудниками (Администраторами).

3.2.7. Самостоятельное изменение сотрудниками 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 эксплуатирующихся в техникуме.

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 сотрудниками информацией в рамках информационных систем техникума и общедоступных сетей.

3.2.2. Электронная почта ГБПОУ КК СЭТ предназначена исключительно для использования в служебных целях.

3.2.3. Каждый сотрудник имеет право на просмотр либо иное использование, в интересах техникума, 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 техникуму и являются неотъемлемой частью производственного процесса.

3.2.5. Любые сообщения служебной электронной почты могут быть прочитаны, использованы в интересах техникума, либо удалены уполномоченными на это сотрудниками.

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

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

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

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

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

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

3.2.9. Сотрудникам 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 сотрудника.

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

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

открывать вложения электронной почты, полученные от недостоверных источников;

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);

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

3.2.11. Исходящие электронные сообщения сотрудников техникума должны содержать следующие поля:

адрес получателя;

тема электронного сообщения;

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

подпись отправителя.

3.2.12. Подписываясь в ознакомлении с настоящей Политикой, сотрудник дает согласие на ознакомление и иное использование в интересах техникума

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) сотрудников 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 сотрудникам техникума только в целях выполнения служебных обязанностей, требующих непосредственного подключения к внешним информационным ресурсам и (или) повышения эффективности выполнения своих служебных обязанностей.

3.3.2. Сотрудникам запрещается:

использовать предоставленный доступ в сеть Интернет в личных целях;

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

3.3.3. При работе с ресурсами сети Интернет запрещается:

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

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

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

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;

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;

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;

использование анонимных прокси-серверов;

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 техникума 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 соответствующем 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 техникума по обеспечению информационной безопасности, назначаемой директором ГБПОУ КК СЭТ. 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:

после его приобретения;

при его первичном подключении к информационному активу;

при передаче для постоянного использования от одного пользователя другому пользователю;

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. Сотрудники обязаны:

использовать носители информации исключительно для выполнения своих служебных обязанностей;

обеспечивать физическую безопасность носителей информации;

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

3.4.12. При использовании предоставленных сотрудникам съемных носителей информации запрещено:

использовать носители информации в личных целях;

передавать носители информации другим лицам;

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 сотрудниками информационных активов протоколируется и, при необходимости, может быть предоставлена руководителям структурных подразделений.

4. Порядок предоставления доступа к информационным активам

4.1. Права доступа сотрудникам 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 сотрудника к информационным активам определяет руководитель структурного подразделения на основании должностных (трудовых) обязанностей сотрудника.

4.4. Основанием для предоставления прав доступа сотруднику к информационным активам является заявка руководителя структурного подразделения, согласованная[2)] с Владельцем информационного актива и Администратором информационной безопасности (форма заявки приведена в приложении 13).

[2)] Согласование может осуществляться посредством служебной электронной почты.

4.5. Права доступа сотрудников 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 доступа[3)] (формы матриц доступа к информационным активам приведены в приложениях 14-17).

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

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

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

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

в период отпуска сотрудника – по заявке руководителя структурного подразделения;

в случае изменения должностных обязанностей сотрудника (перевода на другую должность, в другие подразделения);

в случае увольнения сотрудника (все изменения в правах доступа, связанные с увольнением сотрудника, выполняются администраторами незамедлительно после окончания последнего сеанса работы данного пользователя[4)]). Помимо блокирования учетной записи уволенного сотрудника, также должно быть осуществлена минимизация прав доступа к информационному активу для такой учетной записи.

4.9. В случае увольнения сотрудника 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 техникума.

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

[3)] Матрица доступа может вестись в электронном виде.

[4)] Ответственность за своевременное уведомление администраторов о увольнении сотрудников несут руководители структурных подразделений, в чьем подчинении находятся увольняемые сотрудники.

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

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

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

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 ГБПОУ КК СЭТ»).

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 ГБПОУ КК СЭТ программного обеспечения (форма реестра приведена в приложении 18). Реестр ведется Администратором информационной безопасности при содействии Администраторов 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 Администраторы 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 информационной системе.	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 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. 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
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) серверы с последующим их добавлением в состав аттестованной информационной системы.	
6	Переустановка установленных средств защиты информации, указанных в Аттестате соответствия, на аттестованных АРМ и (или) серверах в пределах одной информационной системы.	

1	2	3
		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 ФТСЭК 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 информационной системы (уменьшение числа актуальных угроз, объема обрабатываемых данных, снижение требований к характеристикам безопасности и прочее).	Аттестат соответствия сохраняет свое 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
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,	

[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.

1	2	3
	не связанного с обработкой защищаемой информации.	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.
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 сотрудников.	

7. Удаленный доступ сотрудников к информационным активам

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

8.2. Решение о предоставлении удаленного доступа сотруднику техникума 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, согласованных с владельцем информационного актива и Администратором информационной безопасности.

8.4. Сотрудники техникума, 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 техникума, 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 сотрудников техникума, осуществляющих работу на сред-

ствах вычислительной техники, при этом сотрудники 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 техникума несут ответственность за:

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

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

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

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

8.4.Администратор информационных систем несет ответственность за:

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

ведение и поддержание в актуальном состоянии технических паспортов информационных систем;

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

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

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

ведение Реестра разрешенного к использованию программного обеспечения;

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

установку, обновление и удаление программного обеспечения на АРМ пользователей и серверах техникума;

изменение (модификацию) аппаратной конфигурации АРМ пользователей и серверов техникума;

опечатывание/опломбирование, а также установку паролей на BIOS АРМ и серверов техникума.

8.5.Администратор информационной безопасности несет ответственность за:

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 пользовате-

лей, на которых установлено средство защиты информации от несанкционированного доступа.

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

ведение учета средств защиты информации и эксплуатационной документации к ним;

установку, обновление и удаление средств защиты информации на АРМ пользователей и серверах техникума;

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

ведение матриц доступа к средствам защиты информации;

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

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

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

ведение учета и выдачи съемных носителей информации;

осуществление в составе комиссии уничтожения съемных носителей информации;

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

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

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
государственного бюджетного
профессионального образовательного
учреждения Краснодарского края
«Славянский электротехнологический
техникум»

ФОРМА

Учет 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
государственного бюджетного
профессионального образовательного
учреждения Краснодарского края
«Славянский электротехнологический
техникум»

ФОРМА

Учет 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
государственного бюджетного
профессионального образовательного
учреждения Краснодарского края
«Славянский электротехнологический
техникум»

ФОРМА

Учет серверов

№ п/п	Наименование (FQDN)	Роль сервера[2)]	Инвентарный и серийный номер	Тип[3)]	Администратор ИС	Перечень ИР/ИС, функционирующих на данном сервере	Месторасположение	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
государственного бюджетного
профессионального образовательного
учреждения Краснодарского края
«Славянский электротехнологический
техникум»

ФОРМА

Учет 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
государственного бюджетного
профессионального образовательного
учреждения Краснодарского края
«Славянский электротехнологический
техникум»

ФОРМА

Журнал 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
государственного бюджетного
профессионального образовательного
учреждения Краснодарского края
«Славянский электротехнологический
техникум»

ФОРМА

Учет 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)

Приложение 7
к Политике использования
информационных активов
государственного бюджетного
профессионального образовательного
учреждения Краснодарского края
«Славянский электротехнологический
техникум»

ФОРМА

ТЕХНИЧЕСКИЙ ПАСПОРТ
информационной системы

_____
(наименование информационной системы)

Государственного бюджетного профессионального образовательного
учреждения Краснодарского края
«Славянский электротехнологический техникум»

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
1	2	3	4	5

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

№ п/п	Дата внесения изменения	Документ, на основании которого внесены изменения	Пункт технического паспорта, в который внесены изменения	Краткая характеристика изменений	Подпись лица, внесшего изменения
1	2	3	4	5	6
1	2	3	4	5	6

Администратор информационных систем
« » _____ 20__ г. _____/_____

Приложение 8
к Политике использования
информационных активов
государственного бюджетного
профессионального образовательного
учреждения Краснодарского края
«Славянский электротехнологический
техникум»

ФОРМА

ОПИСАНИЕ
технологического процесса обработки информации в

_____
(наименование информационной системы)

Государственного бюджетного профессионального образовательного
учреждения Краснодарского края
«Славянский электротехнологический техникум»

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:

пользователей информационной системы;
руководителей структурных подразделений техникума;
администратора информационных систем техникума;
администратора информационной безопасности техникума.

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 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 учтенных 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 учтенные съемные носители информации (флэш-накопители, оптические диски).

1.9. Схема информационных потоков информационной системы представлена на рисунке 1.

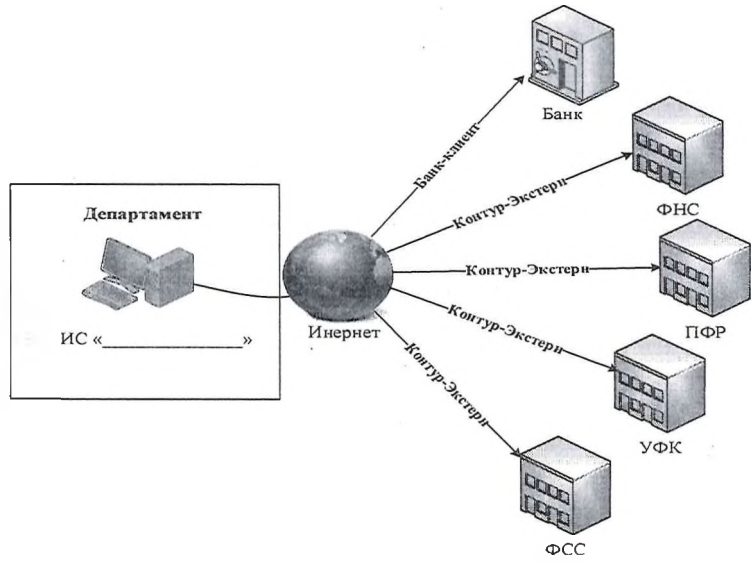

Рисунок 1 - Схема информационных потоков

2. Доступ к информационным ресурсам (системам)

2.1. Объектами доступа в информационной системе являются:

технические средства, предназначенные для обработки и передачи защищаемой информации;

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

учтенные съемные носители защищаемой информации;

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

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 техникума.

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

сотрудники, обрабатывающие защищаемую информацию;

администраторы информационных систем;

внешние пользователи (при их наличии);

временные пользователи (сотрудники 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 окончанию 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 имениях в приви-

легиях доступа к информационным ресурсам и выявленных нарушениях правил обработки защищаемой информации.

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

выходит из рабочего приложения, а затем завершает работу АРМ;

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

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

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
государственного бюджетного
профессионального образовательного
учреждения Краснодарского края
«Славянский электротехнологический
техникум»

ФОРМА

Журнал 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
государственного бюджетного
профессионального образовательного
учреждения Краснодарского края
«Славянский электротехнологический
техникум»

ФОРМА

Журнал 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
государственного бюджетного
профессионального образовательного
учреждения Краснодарского края
«Славянский электротехнологический
техникум»

ФОРМА

Акт уничтожения съемных носителей информации

Комиссия в составе:
председатель комиссии: _____.
члены 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
государственного бюджетного
профессионального образовательного
учреждения Краснодарского края
«Славянский электротехнологический
техникум»

ФОРМА

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
государственного бюджетного
профессионального образовательного
учреждения Краснодарского края
«Славянский электротехнологический
техникум»

ФОРМА

Заявка 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 сотрудника, 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)

[1)] Указывается наименование информационной системы и (или) каталога (полный пусть 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.

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

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

Приложение 14
к Политике использования
информационных активов
государственного бюджетного
профессионального образовательного
учреждения Краснодарского края
«Славянский электротехнологический
техникум»

ФОРМА

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 ИСn	наименование $объекта_1$ (путь)	наименование $объекта_n$ (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
государственного бюджетного
профессионального образовательного
учреждения Краснодарского края
«Славянский электротехнологический
техникум»

ФОРМА

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
государственного бюджетного
профессионального образовательного
учреждения Краснодарского края
«Славянский электротехнологический
техникум»

ФОРМА

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
государственного бюджетного
профессионального образовательного
учреждения Краснодарского края
«Славянский электротехнологический
техникум»

ФОРМА

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
государственного бюджетного
профессионального образовательного
учреждения Краснодарского края
«Славянский электротехнологический
техникум»

ФОРМА

**Матрица реестра программного обеспечения,
разрешенного к использованию в информационных системах
ГБПОУ КК СЭТ**

№ 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
государственного бюджетного
профессионального образовательного
учреждения Краснодарского края
«Славянский электротехнологический
техникум»

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 профессионального образовательного учреждения Краснодарского края «Славянский электротехнологический техникум» размещенного 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)

ПРИЛОЖЕНИЕ № 2

УТВЕРЖДЕНА
приказом директора
от 30.12.2023 № 952

ПОЛИТИКА
антивирусной защиты информации
государственного бюджетного профессионального
образовательного учреждения Краснодарского края
«Славянский электротехнологический техникум»

1. Общие положения

1.1. Настоящая политика антивирусной защиты информации (далее – Политика) государственного бюджетного профессионального образовательного учреждения Краснодарского края «Славянский электротехнологический техникум» (далее – ГБПОУ КК СЭТ, техникум) определяет процедуры, направленные на защиту информационных систем техникума от разрушающего воздействия компьютерных вирусов и другого вредоносного программного обеспечения.

1.2. Настоящая Политика разработана в соответствии с:

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»;

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;

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

1.3. Подсистема антивирусной защиты информации является одной из составляющих системы защиты информации ГБПОУ КК СЭТ.

1.4. Объектами защиты от воздействия вредоносных программ являются следующие компоненты информационных систем техникума:

автоматизированные рабочие места пользователей (далее – АРМ) информационных систем;

сервера информационных систем (в том числе почтовые, интернет-шлюзы, прокси-сервера и другие);

мобильные технические средства;

съемные носители информации;

иные точки доступа в информационные системы, подверженные внедрению (заражению) вредоносными компьютерными программами (вирусами).

1.5. Защита компонентов информационных систем от компьютерных вирусов осуществляется комплексом организационных мероприятий и технических мер, включающем:

регулярные профилактические работы;

анализ ситуации проявления вредоносных программ и причины их появления;

уничтожение вредоносных программ на АРМ, серверах, мобильных технических средства информационных систем и на используемых съемных носителях информации;

принятие мер по предотвращению причин появления вредоносных программ.

1.6. Технические меры, направленные на защиту информационных систем от разрушающего воздействия компьютерных вирусов и другого вредоносного программного обеспечения, реализуются за счет применения в составе подсистемы антивирусной защиты информации соответствующих антивирусных средств, удовлетворяющих установленным требованиям.

1.7. Реализацией комплекса мероприятий и мер по антивирусной защите занимается Администратор информационной безопасности техникума.

2. Организация мероприятий по антивирусной защите информации

2.1. К использованию допускаются только лицензионные средства антивирусной защиты информации, имеющие действующие сертификаты соответствия ФСТЭК России, предъявляемые к средствам антивирусной защиты, приобретенные у разработчиков (официальных поставщиков) данных средств.

2.2. Установка средств антивирусной защиты информации на автоматизированные рабочие места и сервера должна осуществляться только с сертифицированных ФСТЭК России дистрибутивов, приобретенных у разработчиков (официальных поставщиков) данных средств.

2.3. Средства антивирусной защиты информации должны использоваться на всех автоматизированных рабочих местах и серверах информационных систем и обеспечивать выполнение следующих требований:

возможность обнаружения как можно большего числа известных вредоносных программ, в том числе вирусов, деструктивного кода (макровирусов, объектов ActiveX, апплетов языка Java и других), а также максимальную готовность быстрого реагирования на появление новых видов вирусных угроз;

своевременное уведомление о необходимости обновления антивирусных баз и их последующее обновление из доверенных источников, контроль целостности обновлений антивирусных баз должен обеспечиваться функционалом антивирусного средства;

возможность автоматического распространения обновлений антивирусных баз на каждую рабочую станцию и (или) сервер;

обеспечивать соответствие системных требований средства к платформам, характеристикам и комплектации применяемой вычислительной техники;

иметь документацию, необходимую для практического применения и освоения средства, на русском языке;

обеспечение обновлений, консультаций и других форм сопровождения эксплуатации поставщиком средства.

2.4. При использовании средств антивирусной защиты информации должны выполняться следующие организационные мероприятия:

запрет использования посторонних (неучтенных) съемных носителей информации при работе в информационных системах;

запрет передачи съемных носителей информации посторонним лицам;

запрет запуска программ с внешних съемных носителей информации при работе в информационных системах.

2.5. При функционировании средств антивирусной защиты информации на компонентах информационных систем обязательно выполнение следующих требований:

антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы и другие), получаемая и передаваемая посредством каналов связи (в том числе по электронной почте), а также съемных носителей информации (CD/DVD-диски, флэш-накопители и тому подобное);

определение автоматической реакции средства антивирусной защиты информации при обнаружении компьютерных вирусов и другого вредоносного программного обеспечения;

систематическая проверка содержимого дисков АРМ, серверов;

проверка в масштабе времени, близком к реальному, объектов (файлов) из внешних источников (съемных носителей информации, сетевых подключений (в том числе к сетям общего пользования) и других внешних источников) при загрузке, открытии или исполнении таких файлов;

поддержание антивирусных баз в актуальном состоянии и их своевременное распространение на АРМ и сервера информационных систем;

запрет деактивации средств антивирусной защиты информации пользователями информационных систем;

деактивация средств антивирусной защиты информации на АРМ и серверах информационных систем только для проведения профилактических мероприятий и по согласованию с администратором информационной безопасности;

оповещение администратора информационной безопасности и в масштабе времени, близком к реальному, об обнаружении вредоносных компьютерных программ (вирусов).

3. Ответственность за исполнение положений настоящей Политики

3.1. Ответственность за исполнение положений настоящей Политики возлагаются на всех сотрудников техникума, осуществляющих работу на средствах вычислительной техники.

3.2. Пользователи информационных систем ГБПОУ КК СЭТ:

не должны каким-либо образом препятствовать функционированию (в том числе обновлению) средства антивирусной защиты информации и принимать попытки его деактивации;

должны перед получением или передачей информации осуществить ее проверку на предмет наличия компьютерных вирусов и другого вредоносного программного обеспечения. Контроль исходящей информации необходимо проводить непосредственно перед ее отправкой и (или) записью на съемный носитель, а входящей – непосредственно после ее приема перед разархивированием;

при возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и тому подобное) должны провести внеочередной антивирусный контроль АРМ и при необходимости привлечь Администратора информационной безопасности для определения факта наличия или отсутствия компьютерного вируса;

при невозможности самостоятельно устранить выявленное средствами антивирусной защиты информации вредоносное программное обеспечение – должны приостановить работу и незамедлительно уведомить Администратора информационной безопасности;

по факту обнаружения зараженных вирусом файлов должны составить служебную записку администратору информационной безопасности, в которой необходимо указать предположительный источник (отправителя, владельца и так далее) зараженного файла, тип зараженного файла, характер содержащейся в файле информации и выполненные мероприятия по его нейтрализации.

3.3. Администратор информационной безопасности должен:

руководствоваться в своей работе настоящей Инструкцией;

осуществлять функции по организации антивирусного контроля в информационных системах техникума;

содействовать пользователям информационных систем в устранении последствий вирусных заражений;

давать пояснения пользователям информационных систем по вопросам функционирования средств антивирусной защиты информации и при необходимости проводить персональные инструктажи;

осуществлять планирование и реализацию контрольных мероприятий по проверке степени выполнения положений настоящей Политики структурными подразделениями техникума;

организовывать процесс управления инцидентами информационной безопасности в части положений настоящей Политики (в соответствии с Политикой управления событиями безопасности информации).

3.4. Руководители структурных подразделений техникума, должны обеспечить в своих подразделениях выполнение организационных мероприятий согласно пункту 2.4 раздела 2 настоящей Политики.

3.5. Лица, виновные в нарушении положений настоящей Политики, могут быть привлечены к дисциплинарной, материальной, гражданской, правовой и административной ответственности.

ПРИЛОЖЕНИЕ № 3

УТВЕРЖДЕНА
приказом директора
от 30.12.2023 № 952

ПОЛИТИКА
использования аутентификационной информации
при доступе к информационным ресурсам и системам
государственного бюджетного профессионального
образовательного учреждения Краснодарского края
«Славянский электротехнологический техникум»

1. Общие положения

1.1. Политика использования аутентификационной информации при доступе к информационным ресурсам и системам (далее – Политика) государственного бюджетного профессионального образовательного учреждения Краснодарского края «Славянский электротехнологический техникум» (далее – ГБПОУ КК СЭТ, техникум) определяет требования к комплексу мер по использованию аутентификационной информации при реализации доступа к автоматизированным рабочим местам пользователей (далее – АРМ), серверам, активному сетевому оборудованию и средствам защиты информации техникума.

1.2. Под аутентификационной информацией понимается информация, используемая пользователями и администраторами информационных ресурсов (систем) и средств обработки информации для доступа к ним (имя пользователя, пароль, средства дополнительной аутентификации).

1.3. Настоящая Политика разработана в соответствии с:

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»;

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»;

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

2. Порядок формирования и использования аутентификационной информации

2.1. Для обеспечения возможности однозначного сопоставления идентификатора пользователя с запускаемыми от его имени процессами каждому пользователю формируется имя пользователя.

2.2. Для обеспечения возможности однозначного сопоставления устройства доступа (далее – АРМ пользователя) с информационными ресурсами (системами) и средствами обработки информации, к которым осуществляется доступ (объектами доступа), его имя должно соответствовать имени пользователя.

2.3. В случае привлечения третьих лиц для выполнения работ по настройке и тестированию информационных ресурсов (систем) и средств обработки информации, им предоставляются временные учетные записи с предустановленным сроком их действия (при наличии технической возможности), доступ к которым блокируется по завершению работ.

2.4. При создании учетной записи должен быть задан тип учетной записи (при наличии технической возможности). Под типами учетных записей понимается: учетная запись пользователя, учетная запись администратора, временная учетная запись, системная учетная запись.

2.5. Использование гостевых учетных записей запрещено.

2.6. Локальная учетная запись администратора операционной системы Windows (Administrator) предназначена только для служебного использования администратором при настройке систем и не может быть использована для повседневной работы.

2.7. Учетные записи пользователей не подлежат удалению в системе и могут быть только заблокированы.

2.8. Сотрудники обязаны хранить в секрете персональные пароли доступа к информационным ресурсам (системам) и средствам обработки информации и не передавать их другим лицам. Передача личного пароля пользователя третьим лицам возможно только в случаях, регламентированных в пункте 2.9 настоящей Политики.

2.9. В случае необходимости при проведении проверочных мероприятий (внутренний аналитический аудит), которые требуют знания пароля пользователя, допускается раскрытие значений своего пароля проверяющему сотруднику. По окончанию проверочных работ сотрудники самостоятельно производят немедленную смену значений «раскрытых» паролей.

2.10. В случае возникновении нештатных ситуаций, форс-мажорных обстоятельств, а также технологической необходимости использования имен и паролей сотрудников (в их отсутствие) допускается изменение паролей администратором данного информационного ресурса (системы), средства обработки информации.

2.11. Сотрудники, чьи пароли были изменены, обязаны сразу же после выяснения факта смены своих паролей, создать их новые значения в соответствии с требованиями настоящей Политики.

2.12. Хранение сотрудником (администратором, пользователем) аутентификационной информации допускается только в личном сейфе (запираемом

шкафу, ящике) либо в сейфе (запираемом шкафу, ящике) администратора соответствующей информационной системы. При этом бумажный носитель должен быть упакован в отдельный опечатанный конверт.

2.13. При доступе к средствам обработки информации (серверам, активному сетевому оборудованию, средствам защиты информации) запрещается использование аутентификационной информации, заданной производителем «по умолчанию».

2.14. После получения доступа к информационному ресурсу (системе), средству обработки информации пользователь при первом входе в систему должен сменить пароль доступа (в случае наличия технической возможности), на пароль, удовлетворяющий требованиям настоящей Политики.

2.15. При вводе аутентификационной информации (пароля) должно обеспечиваться исключение отображения вводимой парольной информации (например, осуществляется замена вводимых символов условными знаками «-», «*» или иными знаками). В случае отсутствия технической возможности реализации данного требования пользователь самостоятельно создает условия защиты, вводимой аутентификационной информации.

2.16. Запрещается передача аутентификационной информации пользователям при помощи почтовых сообщений, либо по иным открытым каналам связи.

2.17. В случае компрометации аутентификационных данных сотрудники должны незамедлительно сообщить об этом событии, являющемся инцидентом информационной безопасности, Администратору информационной безопасности.

2.18. Предусматривается периодическая плановая (в соответствии с установленным сроком) и внеплановая смена паролей.

2.19. Внеплановая немедленная смена пароля обязательна в случае его компрометации. Также, внеплановая смена пароля и (или) блокирование учетной записи пользователя производится в случае прекращения его полномочий, непосредственно после окончания последнего сеанса работы данного пользователя.

2.20. Должностным лицам запрещается разглашать пароли, ставшие известными им в ходе служебной деятельности по обеспечению функционирования информационных систем.

3. Требования к качеству аутентификационной информации и мер по обеспечению ее безопасности

3.1. К аутентификационной информации пользователей и администраторов информационных ресурсов (систем) и средств обработки информации определены следующие требования, представленные в таблице 1.

Таблица 1 – Требования к аутентификационной информации

№ п/п	Параметр качества пароля	Администратор	Пользователь
1	2	3	4

1	2	3	4
1	Минимальная длина пароля в символах	12	8
2	Максимальная длина пароля в символах	не ограничена	не ограничена
3	Содержание в пароле букв верхнего и нижнего регистра	да	да
4	Содержание в пароле специальных символов (@, #, $, &, * и тому подобное) и цифр (при наличии технической возможности)	обязательно	рекомендуется
5	Содержание в пароле личных имен, фамилий, кличек домашних животных, номеров телефонов, дат рождения, географических названий, именований АРМ и тому подобное.	запрещено	запрещено
6	Содержание в пароле общепринятых сокращений (Admin, Administrator, ViPNet, Cisco, User, UserID и так далее)	запрещено	запрещено
7	Максимальное количество неуспешных попыток аутентификации (ввода неправильного пароля) до блокировки	3	5
8	Блокировка сеанса доступа в информационную систему после времени бездействия (неактивности) пользователя (минут)	10	15
9	Блокировка программно-технического средства или учетной записи пользователя в случае достижения установленного максимального количества неуспешных попыток аутентификации	30	15
10	Блокировка учетной записи после периода неиспользования (дней)	60	90
11	Минимальное отличие нового пароля от предыдущего (в позициях)	4	3
12	Количество уникальных паролей, устанавливаемых подряд (в течение установленного срока смены паролей)	не менее 5	не менее 3
13	Максимальный срок действия пароля	60 дней	90 дней
14	Минимальный срок действия пароля	нет	нет

4. Ответственность за исполнение положений настоящей Политики

4.1. Ответственность за исполнение положений настоящей Политики возлагается на всех сотрудников техникума, осуществляющих работу на средствах вычислительной техники.

4.2. Пользователи информационных ресурсов и (или) систем техникума должны:

в случае самостоятельного формирования пароля доступа к компонентам информационных ресурсов и (или) систем руководствоваться требованиями к качеству аутентификационной информации и мер по обеспечению ее безопасности, установленными положениями настоящей Политики;

в случае получения аутентификационной информации от администратора информационного ресурса и (или) системы осуществить смену пароля пользо-

вателя при наличии технической возможности, а в случае отсутствия технической возможности обеспечить условия его сохранности;

следить за сроком действия паролей и своевременно производить их смену, а в случае отсутствия технической возможности обращаться по вопросу их смены к администраторам информационных ресурсов и (или) систем;

не допускать многократного ввода неправильного пароля и блокировки своих учетных записей;

в случае компрометации аутентификационной информации незамедлительно уведомлять администратора информационной безопасности.

4.3. Администратор информационных систем техникума обязан:

создавать учетные записи пользователей и обеспечивать управление их жизненным циклом в соответствии с требованиями к качеству аутентификационной информации и мерами по обеспечению ее безопасности, установленными положениями настоящей Политики;

своевременно осуществлять блокировку/разблокировку учетной записи пользователя, а также внеплановую смену пароля в случае запросов пользователей (с незамедлительным информированием Администратора информационной безопасности об инциденте информационной безопасности).

4.4. Администраторы информационной безопасности обязан:

руководствоваться положениями настоящей Политики при задании аутентификационной информации на доступ к средствам защиты информации;

устанавливать и централизованно распространять требования к качеству аутентификационной информации и мерам по обеспечению ее безопасности в соответствии с требованиями, установленными положениями настоящей Политики;

управлять (создавать, изменять, удалять, блокировать, разблокировать) учетными записями пользователей, зарегистрированных в подсистеме управления доступом средства защиты информации от несанкционированного доступа;

осуществлять планирование и реализацию контрольных мероприятий по проверке степени выполнения положений настоящей Политики структурными подразделениями техникума;

организовывать процесс управления инцидентами информационной безопасности в части положений настоящей Политики (в соответствии с Политикой управления событиями безопасности информации).

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

ПРИЛОЖЕНИЕ № 4

УТВЕРЖДЕНА
приказом директора
от 30.12.2023 № 952

ПОЛИТИКА
обеспечения отказоустойчивости информационных систем
государственного бюджетного профессионального
образовательного учреждения Краснодарского края
«Славянский электротехнологический техникум»

1. Общие положения

1.1. Политика обеспечения отказоустойчивости информационных систем (далее – Политика) государственного бюджетного профессионального образовательного учреждения Краснодарского края «Славянский электротехнологический техникум» (далее – ГБПОУ КК СЭТ, техникум) определяет порядок обеспечения отказоустойчивости информационных систем (далее – ИС) техникума.

1.2. Настоящая Политика разработана в соответствии с:

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»;

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»;

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

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

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

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

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

---

[1]) Уполномоченное лицо - лицо, обрабатывающее информацию, являющуюся информационным ресурсом, по поручению обладателя информации (заказчика) или оператора и (или)

1.4. Обеспечение отказоустойчивости информационных систем реализуется путем:

контроля физического доступа к техническим средствам;

защиты технических средств от внешних воздействий;

резервирования технических средств;

резервного копирования и восстановления информации;

тестирования функций технического и программного обеспечения по реализации отказоустойчивости;

контроля взаимодействия с поставщиками услуг (уполномоченными лицами).

2. Контроль физического доступа и защита технических средств

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

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

2.3. Порядок доступа в помещения осуществляется в соответствии с организационно распорядительным документом: «Правила доступа в помещения ГБПОУ КК СЭТ, в которых ведется обработка защищаемой информации, в том числе персональных данных».

2.4. Учет доступа в помещения может реализовываться путем:

использования систем контроля и управления доступом;

использования систем охраны помещений;

использования систем видеонаблюдения;

опечатывания помещений и контроля выдачи ключей от помещений;

реализации иных мер, предусмотренных контрольно-пропускным режимом.

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

поддержание необходимого температурно-влажностного режима - для серверных помещений (путем использования систем кондиционирования). Должно исключаться наличие в серверных помещениях труб отопления;

предоставляющее им вычислительные ресурсы (мощности) для обработки информации, в том числе на основании заключенного договора.

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

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

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

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

обеспечение выполнения норм и правил устройства и технической эксплуатации электроустановок, а также соблюдение параметров электропитания и заземления технических средств (в том числе использование для АРМ; серверов; активного сетевого оборудования; средств защиты информации, выполненных в виде программно-аппаратных комплексов, кратковременных резервных источников питания (достаточных для обеспечения правильного (корректного) завершения работы технического средства, устройства в случае отключения основного источника питания) и (или) долговременных резервных источников питания в случае длительного отключения основного источника питания и необходимости продолжения выполнения техническим средством установленных функциональных задач4).

3. Обеспечение отказоустойчивости технических средств

3.1. Обеспечение отказоустойчивости технических средств осуществляется путем:

выполнения требований раздела 2 настоящей Политики;

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

резервирования каналов связи, используемых в виртуальной инфраструктуре;

резервирования информационных ресурсов (систем) и средств обработки информации (АРМ; серверов; активного сетевого оборудования, в том числе средств защиты информации, выполненных в виде программно-аппаратных комплексов) имеющих высокую критичность (в соответствии с Политикой использования информационных активов ГБПОУ КК СЭТ).

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

Предусматривается три вида резервирования:

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

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

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

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

4. Обеспечение резервного копирования и восстановления информации

4.1. Резервному копированию подлежат:

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

виртуальные машины (контейнеры);

параметры настройки, конфигурации и журналы аудита средств защиты информации.

4.2. Резервное копирование может осуществляться следующими способами:

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

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

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

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

4.4. Зеркалирование жестких дисков (использование технологии RAID) не является процессом резервного копирования защищаемой информации.

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

4.6. Предусматриваются следующие схемы резервного копирования:

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

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

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

полное резервное копирование – создается полная копия всех данных.

4.7. В случае хранения резервных копий на съемных носителях информации они должны быть учтены и храниться в соответствии с Политикой использования информационных активов ГБПОУ КК СЭТ. Съемный носитель с резервной копией должен быть подписан и содержать следующую информацию:

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

схему резервного копирования;

год, месяц, число, время создания резервной копии.

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

4.9. Учет проведения резервного копирования должен осуществляться автоматизированными средствами (в случае наличия технической возможности) или в «Журнале учета проведения резервного копирования» (форма журнала приведена в Приложении 2). Данный журнал может вестись в электронном виде.

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

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

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

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

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

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

4.15. Ответственность за резервирование и восстановление защищаемой информации несет Администратор информационных систем.

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

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

5. Ответственность за исполнение положений настоящей Политики

5.1. Ответственность за исполнение положений настоящей Политики возлагается на всех сотрудников техникума.

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

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

определение информации, подлежащей резервному копированию;

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

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

5.4. Администратор информационной безопасности несет ответственность за:

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

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

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

проведение резервного копирования и восстановление, а также их учет;

сохранность резервных копий;

периодическую проверку корректности функционирования средств обеспечения отказоустойчивости технических средств;

периодическую проверку функций средств резервного копирования и восстановления защищаемой информации;

осуществление планирования и реализацию контрольных мероприятий по проверке степени выполнения положений настоящей Политики сотрудниками техникума;

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

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

5.5. Администратор информационных систем несет ответственность за:

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

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

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

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

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

сохранность резервных копий;

периодическую проверку корректности функционирования средств обеспечения отказоустойчивости технических средств;

периодическую проверку функций средств резервного копирования и восстановления защищаемой информации.

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

Приложение 1
к политике обеспечения
отказоустойчивости
информационных систем
государственного бюджетного
профессионального образовательного
учреждения Краснодарского края
«Славянский электротехнологический
техникум»

ФОРМА

ПЕРЕЧЕНЬ
информационных ресурсов, подлежащих резервному копированию

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

Дата _____20__ г.

Составитель _____ Ф.И.О.
(подпись)

Приложение 2
к политике обеспечения
отказоустойчивости
информационных систем
государственного бюджетного
профессионального образовательного
учреждения Краснодарского края
«Славянский электротехнологический
техникум»

ФОРМА

ЖУРНАЛ
проведения резервного копирования информации

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

Дата _____20__ г.

Составитель _____ Ф.И.О.
(подпись)

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

Приложение 3
к политике обеспечения
отказоустойчивости
информационных систем
государственного бюджетного
профессионального образовательного
учреждения Краснодарского края
«Славянский электротехнологический
техникум»

ФОРМА

ЖУРНАЛ
проведения восстановления информации

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

Дата _____20__ г.

Составитель _____ Ф.И.О.
(подпись)

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

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

ПРИЛОЖЕНИЕ № 5

УТВЕРЖДЕНА
приказом директора
от 30.12.2023 № 952

ПОЛИТИКА
сетевой безопасности государственного бюджетного профессионального образовательного учреждения Краснодарского края «Славянский электротехнологический техникум»

1. Общие положения

1.1. Политика сетевой безопасности (далее – Политика) государственного бюджетного профессионального образовательного учреждения Краснодарского края «Славянский электротехнологический техникум» (далее – ГБПОУ КК СЭТ, техникум) регулирует вопросы обеспечения сетевой безопасности локально-вычислительной сети техникума, как части комплекса мер по обеспечению безопасности информации в ГБПОУ КК СЭТ.

1.2. Настоящая Политика разработана в соответствии с:

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»;

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»;

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

1.3. Настоящая Политика определяет требования сетевой безопасности, технологии и механизмы обеспечения безопасности сетевой инфраструктуры, а также принципы управления сетевой безопасностью.

2. Общие требования по обеспечению сетевой безопасности

2.1. Локально-вычислительная сеть (далее – ЛВС) является составной частью информационных систем техникума, обеспечивающая его функционирование.

2.2. ЛВС подлежит защите от воздействий (как внутренних, так и внешних), которые могут привести к:

нарушению непрерывности функционирования информационных процессов;

нарушению конфиденциальности защищаемой информации;

целостности защищаемой информации и правил разграничения доступа к информационным ресурсам.

нарушению доступности защищаемой информации и сервисов информационных систем.

2.3. Средства, используемые в составе ЛВС для обеспечения необходимого уровня безопасности информации, должны обеспечивать:

доступность, целостность и конфиденциальность информационных ресурсов;

защиту каналов передачи данных и управления, доступность данных каналов;

защиту сетевого трафика от перехвата;

защищенный удаленный доступ в информационную систему;

простоту используемых технологий защиты информации и их эксплуатации;

прозрачность используемых средств и механизмов защиты для пользователей.

2.4. С целью обеспечения выполнения указанных требований в составе ЛВС должны применяться следующие технологии сетевой безопасности:

межсетевое экранирование;

обнаружение и предотвращение вторжений;

криптографическая защита информации.

2.5. С целью минимизации возможных точек доступа к сетям связи общего пользования (в том числе сети интернет) использование технологий беспроводной передачи данных в техникуме запрещено:

2.6. Для регистрации сетевых узлов (автоматизированных рабочих мест, серверов и активного сетевого оборудования) в сети используются физические адреса (MAC-адреса) и IP-адреса. Для каждого сетевого узла задается IP-адрес маршрутизатора (адрес шлюза по умолчанию), через который он может связываться с компьютерами в других локальных сетях и сети Интернет. Присваивание этих параметров производится автоматически функционалом DHCP-сервера.

2.7. Доступ к средствам (устройствам) сетевой безопасности предоставляется сотрудникам, наделенным соответствующими полномочиями.

3. Межсетевое экранирование

3.1. Средствами межсетевого экранирования должен реализовываться следующий функционал:

идентификация сетевых устройств по IP-адресам и (или) MAC-адресам;

аутентификация сетевых устройств, по одному из протоколов: Remote Authentication Dial-In User Service (RADIUS); Terminal Access Controller Access Control Systems (TACACS); Lightweight Directory Access Protocol (LDAP); Kerberos;

фильтрация информационных потоков по протоколам (например, TCP, UDP, IP), портам и адресам назначения, а также определение маршрутов пере-

дачи информации (требования к фильтрации устанавливаются в соответствии с заявками пользователей на доступ к информационным ресурсам (системам) в порядке, установленном Политикой использования информационных активов ГБПОУ КК СЭТ, а также потребностями администраторов, обусловленными необходимостью администрирования информационных ресурсов (систем) и средств обработки информации);

завершение сетевых соединений (например, открепление пары порт/адрес (TCP/IP)) по их завершении и (или) по истечении заданного Администратором временного интервала неактивности сетевого соединения);

3.2. С целью выполнения указанных требований могут применяться:

программные и программно-аппаратные средства межсетевого экранирования уровня периметра сети – на внешней границе информационной системы;

программные средства межсетевого экранирования уровня хоста – на внутренних узлах сегментов информационных систем (автоматизированных рабочих местах (далее – АРМ) и серверах информационных систем);

иное активное сетевое оборудование (коммутаторы, маршрутизаторы и прочее), реализующие необходимый функционал.

3.3. Используемые средства межсетевого экранирования должны иметь соответствующие действующие сертификаты соответствия, выданные ФСТЭК России.

3.4. Средства межсетевого экранирования могут интегрироваться со средствами антивирусной защиты информации с целью обеспечения антивирусной защиты информации периметра ЛВС.

4. Обнаружение и предотвращение вторжений

4.1. Система обнаружения и предотвращения вторжений (далее - СОВ) позволяет распознавать вредоносную активность внутри сети. СОВ должны иметь в своем составе следующие компоненты:

регистрации событий безопасности (датчики);

анализа событий безопасности и распознавания компьютерных атак (анализаторы);

базу решающих правил (базу сигнатур), содержащую информацию о характерных признаках компьютерных атак.

4.2. Средствами обнаружения вторжений должен реализовываться следующий функционал:

отслеживание атак в режиме реального времени;

использование сигнатурных и эвристических методов для анализа сетевого трафика;

создавать профили (наборы сигнатур, релевантных для защиты определенных сервисов);

задавать правила, определяющие действия для выбранного типа трафика (IP, ICMP, TCP, UDP)

протоколирование нештатных ситуаций, а также попыток проведения вторжений и предотвращение угроз в журнале регистраций событий, а также предоставление отчетов;

защита от атак на сетевые протоколы на различных уровнях модели OSI;

возможность анализа собранных данных СОВ о сетевом трафике в режиме, близком к реальному масштабу времени;

централизованное управление (администрирование) компонентами средств, установленными в различных сегментах информационных систем;

обновление (из доверенных источников) базы решающих правил;

контроль целостности обновлений базы решающих правил;

уведомление о необходимости обновления и непосредственном обновлении базы решающих правил.

4.3. Средства предотвращения вторжений должны иметь в своем составе следующие компоненты:

блокирование атак в режиме реального времени;

обрыв соединения и оповещение администратора безопасности;

протоколирование нештатных ситуаций в журнале регистраций событий и предоставление отчетов.

4.4. С целью выполнения указанных требований могут применяться:

программные и программно-аппаратные средства обнаружения вторжений уровня периметра сети – на внешней границе информационной системы;

программные средства обнаружения вторжений уровня хоста – на внутренних узлах сегментов информационных систем.

4.5. Используемые средства обнаружения вторжений должны иметь соответствующие действующие сертификаты соответствия, выданные ФСТЭК России.

5. Криптографическая защита информации

5.1. Средства криптографической защиты информации, передаваемой по каналам связи, должны применяться в случае, если:

передача защищаемой информации, в том числе персональных данных, осуществляется по каналам связи, не защищенным от перехвата нарушителем передаваемой по ним информации или от несанкционированных воздействий на эту информацию (например, при передаче защищаемой информации по информационно-телекоммуникационным сетям общего пользования; удаленном доступе к информационным ресурсам (системам) и средствам обработки информации, в том числе для администрирования).

хранение защищаемой информации осуществляется на носителях информации, несанкционированный доступ к которым со стороны нарушителя не может быть исключен с помощью некриптографических методов и способов.

5.2. Используемые средства криптографической защиты информации, передаваемой по каналам связи, должны иметь соответствующие действующие сертификаты соответствия, выданные ФСБ России.

5.3. С целью выполнения указанных требований могут применяться:

программно-аппаратные средства криптографической защиты информации, передаваемой по каналам связи (криптографические шлюзы) – на внешней границе информационной системы;

программные средства и (или) программно-аппаратные средств криптографической защиты информации (в том числе средства электронной подписи) – на внутренних узлах сегментов информационных систем (автоматизированных рабочих местах (далее – АРМ) и серверах информационных систем).

5.4. Эксплуатация средств криптографической защиты информации, должна осуществляться в соответствии с Политикой использования средств криптографической защиты информации ГБПОУ КК СЭТ.

6. Ответственность за исполнение положений настоящей Политики

6.1. Администрирование локально-вычислительной сети включает в себя реализацию следующих основных функций:

планирование, создание и сопровождение кабельной системы ЛВС техникума;

организацию и сопровождение системы локальных сетей (VLAN), коммутаторов уровня доступа, магистральных коммутаторов и маршрутизаторов ЛВС техникума;

составление и поддержку адресного плана техникума;

организацию и сопровождение внешних каналов связи, внешней маршрутизации ЛВС техникума с сетями Региональной мультисервисной сети органов государственной власти Краснодарского края, сетью Интернет;

взаимодействие с операторами связи;

организацию и поддержку доменной службы имен;

организацию и поддержку домена службы каталогов (MS Active Directory) техникума, регистрацию объектов доменов и сопровождение их учетных записей;

организацию и поддержку сетевых информационных ресурсов техникума в форме файловых серверов, серверов баз данных;

разработку и реализацию мероприятий по защите ресурсов ЛВС от несанкционированного доступа;

обеспечение резервного копирования и восстановления общих информационных ресурсов техникума и информационных ресурсов структурных подразделений техникума (по их запросам).

6.2. Администратор информационных систем несет ответственность за:

знание структуры локально-вычислительной сети;

ведение учета назначенных сетевым узлам IP-адресов;

настройку параметров активного сетевого оборудования в соответствии с положениями настоящей Политики;

настройку параметров фильтрации и маршрутизации информационных потоков в соответствии с установленными правилами;

обеспечение резервирования критически важного активного сетевого оборудования и принятие мер по восстановлению работоспособности данного оборудования;

незамедлительное информирование о произошедших инцидентах, связанных с нарушением информационной безопасности (или при возникновении по-

дозрения о возможности появления инцидента, связанного с нарушением информационной безопасности) администратора информационной безопасности.

6.3. Пользователь несет личную ответственность за весь информационный обмен между его компьютером и другими компьютерами в ЛВС и за ее пределами. В случае если с данного компьютера производился несанкционированный доступ к информации на других компьютерах и в случаях других серьезных нарушений правил пользования сетью, по решению Администратора информационной безопасности, АРМ пользователя отключается от сети, учетная запись пользователя блокируется.

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

ПРИЛОЖЕНИЕ № 6

УТВЕРЖДЕНЫ
приказом директора
от 30.12.2023 № 952

Приложение 3
к политике аудита информационной безопасности государственного бюджетного профессионального образовательного учреждения Краснодарского края
«Славянский электротехнологический техникум»

ФОРМА

ПЛАН
проведения ежегодного внутреннего аналитического аудита информационной безопасности государственного бюджетного профессионального образовательного учреждения Краснодарского края «Славянский электротехнологический техникум»

№ п/п	Объекты проверки	Результаты проверки	Примечание[1)]
1	2	3	4
1	**Назначение ответственных лиц**		
1.1	Проверка назначения администратора информационных систем		
1.2	Проверка назначения администратора информационной безопасности		
2	**Инвентаризация и учет информационных ресурсов (систем), средств обработки информации**		

[1)] Если требование не применимо к проверяемому подразделению – в графе «результаты проверки» делается соответствующая запись. В графе «примечание» указываются комментарии по результату оценки объекта проверки.

1	2	3	4
2.1	Проверка наличия заполненных форм учета информационных ресурсов (систем), средств обработки информации и степени их актуальности:		
2.1.1	Учет информационных ресурсов и информационных систем		Проверяется, в том числе, корректность установленных классов защищенности (подтвержденных актами классификации) и обоснованность критичности
2.1.2	учета автоматизированных рабочих мест		
2.1.3	учета серверов		
2.1.4	учета сетевого оборудования		
2.1.5	учета съемных носителей информации		
2.1.6	учета средств защиты информации		
2.2	Проверка наличия разработанных технических паспортов на информационные системы и степени их актуальности		
2.3	Проверка наличия разработанных описаний технологического процесса обработки информации в информационной системе и степени их актуальности		
3	**Эксплуатация и предоставление прав доступа к информационным ресурсам (системам), средствам обработки информации**		
3.1	Проверка наличия заявок на предоставление (изменение) прав доступа к информационным ресурсам (системам), средствам обработки информации, матрицы доступа и их соответствие реально имеющимся правам		
3.2	Проверка перечня используемых для доступа к АРМ учетных записей пользователей с фактическими использованными для доступа к АРМ		
3.3	Выборочная проверка отсутствия активных (незаблокированных) учетных записей уволенных сотрудников		
3.4	Выборочная проверка наличия минимальных прав доступа у заблокированных учетных записей		
3.5	Проверка на АРМ пользователей и серверах наличия информации (в том числе в истории интернет-браузеров), не относящейся к служебным обязанностям		
3.6	Проверка состава, используемого на АРМ пользователей и сервере программного обеспечения (в соответствии с Реестром разрешенного к использованию ПО)		
3.7	Проверка наличия печатей (пломб) на АРМ и серверах		
3.8	Проверка наличия установленных на АРМ и серверах паролей на доступ к BIOS		
3.9	Проверка возможности использования на АРМ пользователей технологий		

1	2	3	4
	беспроводной передачи данных, веб-камер и микрофонов		
3.10	Проверка работоспособности на АРМ и серверах средств защиты информации		
3.11	Проверка наличия действующих сертификатов соответствия ФСТЭК России, выданных на используемые средства защиты информации		
3.12	Проверка настроек программного обеспечения и средств защиты информации требованиям эксплуатационной документации		Проверяется, в том числе, актуальность антивирусных баз
3.13	Проверка АРМ и серверов на предмет подключения к ним мобильных устройств передачи информации (в ретроспективе), а также неучтенных съемных носителей информации		
4	**Учет и использование съемных носителей информации**		
4.1	Проверка журнала учета выдачи съемных носителей информации с фактическим наличием у сотрудников данных съемных носителей		
4.2	Проверка наличия перечня мест хранения съемных носителей, назначения ответственных за них лиц и степени их актуальности		
4.3	Проверка съемных носителей информации на предмет наличия информации, не связанной с исполнением служебных обязанностей		
4.4	Проверка выполнения уничтожения (стирания) информации со съемных носителей информации		
4.5	Проверка выполнения порядка уничтожения съемных носителей информации		
5	**Эксплуатация аттестованных по требованиям безопасности информации информационных систем**		
5.1	Проверка наличия аттестата соответствия на информационные системы, выданного лицензиатом ФСТЭК России, и срока его действия		
5.2	Проверка выполнения порядка действий в ходе эксплуатации аттестованной информационной системы		Проверяется в случае обнаружения расхождений между техническим паспортом информационной системы сведениями, указанными в аттестационной документации, и реальным состоянием информационной системы
6	**Использование аутентификационной информации при доступе к информационным ресурсам (системам), средствам обработки информации**		
6.1	Проверка формата задания имен доступа пользователей установленным требованиям		

1	2	3	4
6.2	Проверка отсутствия гостевых учетных записей для доступа к АРМ, серверам, активному сетевому оборудованию, средствам защиты информации		
6.3	Выборочная проверка реализации требований, установленных к качеству аутентификационной информации и мер по обеспечению ее безопасности		После проверок исполнения требований к качеству пароля (приводящие к его санкционированной компрометации), пользователь должен продемонстрировать установленный пароль на доступ, после чего незамедлительно его сменить
6.4	Отсутствие сохраненных паролей доступа как на средствах программного обеспечения, так и на бумажных носителях (вне отведенных для этого мест)		
6.5	Проверка исполнения требований, предъявляемых к учету и использованию дополнительных средств аутентификации		При их использовании
7	**Организация доступа в помещения обработки информации и выполнение требований, установленных к таким помещениям**		
7.1	Проверка наличия перечня помещений, в которых разрешена обработка конфиденциальной информации (в том числе персональных данных) и степени его актуальности		
7.2	Проверка наличия перечня лиц, допущенных в помещения обработки конфиденциальной информации, степени его актуальности		Проверка наличия перечней для каждого помещения, а также в ходе проведения аудита проверяется степень исполнения данного требования при доступе в помещения
7.3	Проверка реализации требований, предъявляемых к помещениям обработки конфиденциальной информации:		
7.3.1	наличие ограждающих конструкций, предполагающих существенные трудности для нарушителей по их преодолению (металлические решетки на окнах, металлическая дверь, система контроля и управления доступом и так далее)		
7.3.2	надежные входные двери с замками, а также средствами опечатывания помещений		
7.3.3	окна помещений, расположенных на первых или последних этажах зданий, а также окна, находящиеся около пожарных лестниц и других мест, откуда возможно проникновение в помещения посторонних лиц, оборудованы металлическими		

1	2	3	4
	решетками или ставнями, или охранной сигнализацией, или другими средствами, препятствующими неконтролируемому проникновению в помещения		
7.4	Проверка наличия перечня мест хранения материальных носителей персональных данных и ответственных лиц, степени актуальности данного перечня		
7.5	Проверка реализации дополнительных требований, предъявляемых к спецпомещениям:		
7.5.1	оборудованы устройствами, обеспечивающими постоянное закрытие дверей на замок и их открытие только для санкционированного прохода		
7.6	Проверка наличия журнала учета хранилищ СКЗИ и ключей от них, а также степени его актуальности		
8	**Защита технических средств от внешних воздействий**		
8.1	Способ реализации учета доступа в помещения		Указывается реализованный способ
8.2	Проверка наличия средств обеспечения температурно-влажностного режима серверных помещений		
8.3	Проверка наличия средств обеспечения бесперебойного резервного питания для АРМ		
8.4	Проверка наличия средств обеспечения бесперебойного резервного питания для серверов		
8.5	Проверка наличия средств обеспечения бесперебойного резервного питания для активного сетевого оборудования		
9	**Обеспечение отказоустойчивости технических средств**		
9.1	Проверка резервирования средств обработки информации, имеющих высокую критичность и способа резервирования		Указать способ резервирования
9.1.1	АРМ		
9.1.2	серверов		
9.1.3	активного сетевого оборудования, в том числе средств защиты информации, выполненных в виде программно-аппаратных комплексов		
9.2	Проверка наличия контроля основных показателей функционирования технических средств (степени загрузки: процессорных мощностей, дискового пространства, оперативной памяти, каналов связи и прочее)		Указать, какие показатели контролируются какими средствами
10	**Резервное копирование защищаемой информации**		
10.1	Проверка наличия заполненного перечня информационных ресурсов, подлежащих резервному копированию, его полноту и степень актуальности		

1	2	3	4
10.2	Проверка ведения журнала проведения резервного копирования информации		
10.3	Проверка ведения журнала восстановления информации		
10.4	Проверка мест хранения резервных копий		
11	**Учет и использование средств криптографической защиты информации**		
11.1	Проверка условий эксплуатации СКЗИ, в том числе выполнение требований эксплуатационной документации на СКЗИ		
11.2	Проверка журнала поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов, степени его актуальности		
11.3	Проверка технического (аппаратного) журнала, степени его актуальности		
11.4	Проверка порядка уничтожения криптографических ключей (ключевой информации)		
12	**Обработка персональных данных**		
12.1	Проверка наличия размещенных на информационном интернет-портале техникума «Правил обработки персональных данных»		
12.2	Проверка степени актуальности уведомления об обработке персональных данных, поданных в Роскомнадзор		
12.3	Проверка наличия перечня обрабатываемых персональных данных и степени его актуальности		
12.4	Проверка наличия перечня должностей, замещение которых предусматривает осуществление обработки персональных данных, степени его актуальности		
12.5	Проверка наличия перечня информационных систем, в которых осуществляется обработка персональных данных		
12.6	Проверка соблюдения требований по учету и реагированию на запросы субъектов персональных данных		
12.7	Соблюдение условий и порядка обработки персональных данных граждан, обратившихся в техникум		
12.8	Соблюдение процедур, направленных на предотвращение и выявление нарушений законодательства РФ в сфере персональных данных		
13	**Нормативно-методическое обеспечение системы защиты информации**		
13.1	Проверка наличия модели угроз безопасности информации и степени ее актуальности с учетом используемых технологий обработки информации (срок актуальности документа не может превышать 3 лет)		
13.2	Проверка наличия Эскизного проекта системы обеспечения информационной безопасности		

1	2	3	4
13.3	Проверка ознакомления сотрудников с нормативными документами, регламентирующими процессы обработки и защиты информации (в том числе персональных данных)		Может проводиться в формате тестирования или анкетирования с установленным перечнем контрольных вопросов

Дата _____20__ г.

Составитель _____ Ф.И.О.
(подпись)

Приложение 4
к политике аудита информационной безопасности государственного бюджетного профессионального образовательного учреждения Краснодарского края «Славянский электротехнологический техникум»

ФОРМА

ПЛАН
проведения периодического внутреннего аналитического аудита информационной безопасности

(наименование структурного подразделения)

государственного бюджетного профессионального образовательного учреждения Краснодарского края «Славянский электротехнологический техникум»

№ п/п	Объекты проверки	Результаты проверки	Примечание
1	2	3	4
1.1	Проверка перечня используемых для доступа к АРМ учетных записей пользователей с фактическими, использованными для доступа к АРМ		
1.2	Проверка на АРМ пользователей информации (в том числе в истории Интернет-браузеров), не относящейся к служебным обязанностям		
1.3	Проверка состава, используемого на АРМ пользователей программного обеспечения (в соответствии с Реестром разрешенного к использованию ПО)		
1.4	Проверка наличия печатей (пломб) на АРМ		
1.5	Проверка наличия установленных на АРМ паролей на доступ к BIOS		
1.6	Проверка возможности использования на АРМ пользователей технологий беспроводной передачи данных, веб-камер и микрофонов		
1.7	Проверка работоспособности на АРМ и серверах средств защиты информации		
1.8	Проверка настроек программного обеспечения и средств защиты информации		Проверяется в том числе

1	2	3	4
	требованиям эксплуатационной документации		актуальность антивирусных баз
1.9	Проверка АРМ и серверов на предмет подключения к ним мобильных устройств передачи информации (в ретроспективе), а также неучтенных съемных носителей информации		
2	**Учет и использование съемных носителей информации**		
1.2	Проверка наличия перечня мест хранения съемных носителей, назначения ответственных за них лиц и степени их актуальности		
2.2	Проверка съемных носителей информации на предмет наличия информации, не связанной с использованием служебных обязанностей		
1.3	Проверка выполнения уничтожения (стирания) информации со съемных носителей информации		
2.3	Проверка выполнения порядка уничтожения съемных носителей информации		
3	**Использование аутентификационной информации при доступе к информационным активам**		
3.1	Выборочная проверка реализации требований, установленных к качеству аутентификационной информации и мер по обеспечению ее безопасности		После проверок исполнения требований к качеству пароля (приводящие к его санкционированной компрометации), пользователь должен продемонстрировать установленный пароль на доступ, после чего незамедлительно его сменить
3.2	Отсутствие сохраненных паролей доступа как средствами программного обеспечения, так и на бумажных носителях (вне отведенных для этого местах)		
4	**Организация доступа в помещения обработки информации и выполнение требований, установленных к таким помещениям**		
4.1	Проверка наличия перечня лиц, допущенных в помещения обработки конфиденциальной информации, степени его актуальности		Проверка наличия перечня для каждого помещения, а также в ходе проведения аудита - проверяется степени исполнения данного требования при доступе в помещения

1	2	3	4
4.2	Проверка наличия перечня мест хранения материальных носителей персональных данных и ответственных, степени актуальности данного перечня		
5	**Учет и использование средств криптографической защиты информации**		
5.1	Проверка условий эксплуатации СКЗИ, в том числе выполнение требований эксплуатационной документации на СКЗИ		
5.2	Проверка ознакомления сотрудников с нормативными документами, регламентирующими процессы обработки и защиты информации (в том числе персональных данных)		Может проводить в формате тестирования или анкетирования с установленным перечнем контрольных вопросов

Дата _____20__ г.

Составитель _____ Ф.И.О.
(подпись)

Приложение 5
к политике аудита информационной безопасности государственного бюджетного профессионального образовательного учреждения Краснодарского края «Славянск электротехнологический техникум»

ФОРМА

ПЛАН
устранения недостатков, выявленных в ходе проведения внутреннего аналитического аудита информационной безопасности

№ п/п	Нарушение / недостаток	Мероприятия по устранению	Срок исполнения	Ответственные за исполнение
1	2	3	4	5

Дата _____20__ г.

Составитель _____ Ф.И.О.
(подпись)

ПРИЛОЖЕНИЕ № 7

УТВЕРЖДЕНА
приказом директора
от 30.12.2023 № 952

ПОЛИТИКА
управления событиями безопасности информации
государственного бюджетного профессионального
образовательного учреждения Краснодарского края
«Славянский электротехнологический техникум»

1. Общие положения

1.1. Политика управления событиями безопасности информации (далее – Политика) государственного бюджетного профессионального образовательного учреждения Краснодарского края «Славянский электротехнологический техникум» (далее – ГБПОУ КК СЭТ, техникум) устанавливает единый системный подход к процессу управления событиями (их регистрация, учет, сбор, хранение и обработка) безопасности информации в техникуме.

1.2. Настоящая Политика разработана в соответствии с:

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»;

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».

1.3. Управление событиями безопасности информации осуществляется с целью своевременного выявления фактов, оказывающих негативное воздействие на информационные системы техникума (выявления инцидентов информационной безопасности).

1.4. Под событием безопасности информации понимается любое проявление состояния информационной системы и системы ее защиты, указывающие на возможность:

нарушение конфиденциальности, целостности или доступности информации, обрабатываемой в информационной системе;

нарушение доступности компонентов информационной системы (АРМ, серверов, активного сетевого оборудования);

нарушение штатного функционирования компонентов информационных систем и средств защиты информации;

нарушения процедур, установленных организационно-распорядительными документами по защите информации.

1.5. Под инцидентом информационной безопасности понимается одно или серия событий безопасности информации, связанных с нарушением, установленных в техникуме Политик безопасности информации.

2. Регистрация, учет, сбор и хранение событий безопасности информации

2.1. Перечень событий безопасности информации, подлежащих регистрации в информационных системах техникума, приведен в приложении 1 к настоящей Политике.

2.2. Перечень событий безопасности, подлежащих регистрации, должен пересматриваться, в том числе по результатам контроля (мониторинга) обеспечения уровня защищенности информации, содержащейся в информационных системах, но не реже чем 1 раз в год.

2.3. При регистрации событий безопасности информации регистрации подлежат следующие характеристики событий безопасности информации:

тип события безопасности информации;

дата и время события безопасности информации;

идентификационная информация источника события безопасности информации;

результат события безопасности информации (успешно или неуспешно);

субъект доступа (пользователь и (или) процесс), связанный с данным событием безопасности информации.

2.4. Источниками событий безопасности информации являются:

средства регистрации событий системного и прикладного программного обеспечения;

средства регистрации событий активного сетевого оборудования;

средства системы обеспечения информационной безопасности техникума;

средства системы пожарно-охранной сигнализации и системы контроля и управления доступом;

сотрудники техникума;

работники других организаций, имеющих доступ к информационным системам техникума.

2.5. Должен обеспечиваться непрерывный сбор событий безопасности информации, генерируемых компонентами информационных систем (АРМ, серверами, активным сетевым оборудованием) и средствами защиты информации.

2.6. Регистрация, учет и хранение событий безопасности информации должны обеспечиваться ответственными лицами, срок хранения событий безопасности информации должен составлять не менее 12 месяцев.

2.7. Сведения о событиях безопасности информации подлежат защите от неправомерного доступа, уничтожения или модификации. Доступ к данным сведениям должен быть ограничен, кроме уполномоченных на это лиц.

3. Мониторинг и анализ событий безопасности информации

3.1. Мониторинг и анализ событий безопасности информации осуществляется с целью выявления инцидентов информационной безопасности.

3.2. Мониторинг событий информационной безопасности может осуществляться как с использованием средств автоматизации (средств, относящихся к средствам сбора и корреляции событий безопасности информации – SIEM), так и без использования таковых.

3.3. Мониторинг и анализ событий безопасности информации осуществляется:

в части средств системы обеспечения информационной безопасности техникума – Администратором информационной безопасности;

в части средств обеспечения функционирования информационных систем (системного и прикладного программного обеспечения, активного сетевого оборудования) – Администратором информационных систем. В результате анализа событий безопасности информации он должен информировать Администратора информационной безопасности о событиях, имеющих признаки инцидентов, а также непосредственно об инцидентах информационной безопасности.

3.4. Периодичность мониторинга и анализа событий безопасности информации зависит от степени критичности информационного ресурса (системы) или средства обработки информации и составляет:

для информационных ресурсов (систем) или средств обработки информации, имеющих высокую критичность, – ежедневно;

для информационных ресурсов (систем) или средств обработки информации, имеющих среднюю критичность, – не реже одного раза в неделю;

для информационных ресурсов (систем) или средств обработки информации, имеющих низкую критичность, – не реже одного раза в месяц.

3.5. К инцидентам информационной безопасности относятся следующие категории негативных событий (группы событий) безопасности информации:

разглашение защищаемой информации работниками, имеющими право доступа к ней, а именно:

передача защищаемой информации третьим лицам, не имеющим права доступа к ней;

передача защищаемой информации по открытым каналам связи;

обработка защищаемой информации на незащищенных технических средствах;

публикация защищаемой информации в СМИ;

копирование защищаемой информации на неучтенные съемные носители информации;

утрата съемных и (или) бумажных носителей информации или передача их лицам, не имеющим права доступа к ним.

неправомерные действия со стороны лиц, имеющих право доступа к защищаемой информации (несанкционированное изменение, копирование защищаемой информации);

ошибки обслуживающего персонала при эксплуатации информационных систем;

несанкционированный доступ к защищаемой информации лицами, не имеющими права доступа к ней, а именно:

подключение технических средств к информационным системам;

использование закладочных устройств, маскировка под зарегистрированного пользователя;

использование недекларированных возможностей программного обеспечения;

использование программных закладок и применение программных вирусов;

хищение носителей защищаемой информации; нарушение функционирования технических средств обработки защищаемой информации.

дефекты, сбои, отказы, программного обеспечения и аварии технических средств и систем обеспечения их отказоустойчивого функционирования;

природные явления, стихийные бедствия (пожары, наводнения, землетрясения, грозовые разряды).

4. Порядок управления инцидентами информационной безопасности

4.1. Общий порядок управления инцидентами информационной безопасности включает:

обнаружение и информирование об инциденте информационной безопасности;

регистрация инцидента информационной безопасности;

локализация и устранение последствий инцидента информационной безопасности;

расследование инцидента информационной безопасности и реализация действий, предупреждающих его повторное возникновение (корректирующие меры).

5. Обнаружение и информирование об инциденте информационной безопасности

5.1. При обнаружении инцидента информационной безопасности (или события безопасности информации, имеющего признаки инцидента) должен быть незамедлительно проинформирован Администратор информационной безопасности (средствами служебной электронной почты и (или) посредством телефонной связи).

5.2. В случае невозможности информирования Администратора информационной безопасности об инциденте информационной безопасности (посредством телефонной связи) о случившемся инциденте информационной безопасности должен быть уведомлен (посредством телефонной связи) начальник отдела проектной деятельности, цифровой трансформации и информационной безопасности техникума или лицо, замещающее его.

5.3. Сообщение о случившемся инциденте информационной безопасности должно содержать следующую информацию:

Ф.И.О., должность работника, выявившего инцидент информационной безопасности;

время обнаружения инцидента информационной безопасности;

описание инцидента информационной безопасности.

6. Регистрация инцидента информационной безопасности

6.1. Регистрация инцидентов информационной безопасности осуществляется Администратором информационной безопасности в журнале учета инцидентов информационной безопасности (форма журнала представлена в приложении 2 к настоящей Политике).

6.2. На каждый инцидент информационной безопасности Администратором информационной безопасности формируется карточка инцидента информационной безопасности (форма карточки приведена в приложении 3 к настоящей Политике).

6.3. До момента полного заполнения карточки инцидента информационной безопасности и, соответственно, закрытия инцидента она своевременно заполняется и ведется в электронном виде, после чего распечатывается и хранится на бумажном носителе.

6.4. На этапе регистрации инцидента подлежат заполнению следующие разделы карточки:

общие сведения об инциденте информационной безопасности;

содержание инцидента информационной безопасности;

воздействие инцидента на информационные ресурсы (системы) или средства обработки информации.

6.5. Критичность инцидента зависит от критичности информационных ресурсов (систем) или средств обработки информации, затронутых инцидентом, а также области распространения (действия) инцидента, и определяется по таблице 1:

Таблица 1 – Определение критичности информационного ресурса (системы) или средства обработки информации

Область распространения и действия инцидента ИБ	Критичность информационного ресурса (системы) или средства обработки информации		
	высокая	**средняя**	**низкая**
1	2	3	4
Выходящий за пределы техникума	Высокая	Высокая	Средняя
техникум в целом	Высокая	Высокая	Средняя
Пределы отдельного структурного подразделения	Высокая	Средняя	Низкая
Пределы одной информационного ресурса (системы)	Средняя	Низкая	Низкая

7. Локализация и устранение последствий инцидента информационной безопасности

7.1. Срок реагирования на инцидент информационной безопасности напрямую зависит от степени критичности инцидента и составляет:

для инцидентов, имеющих высокую критичность, – незамедлительное реагирование;

для инцидентов, имеющих среднюю критичность, – срок реагирования не более одного рабочего дня;

для инцидентов, имеющих низкую критичность, – срок реагирования не более пяти рабочих дней.

7.2. Под реагированием на инцидент информационной безопасности понимается назначение ответственных лиц за локализацию и устранение последствий инцидента информационной безопасности. Ответственные лица назначаются Администратором информационной безопасности по согласованию с начальником отдела проектной деятельности, цифровой трансформации и информационной безопасности, или лицом, замещающим его.

7.3. В первую очередь осуществляется локализация инцидента информационной безопасности – предпринимаются все необходимые и доступные меры по сдерживанию/пресечению распространения негативного воздействия инцидента на информационные системы, а позже (или одновременно) проводятся работы по устранению последствий инцидента информационной безопасности. Могут назначаться различные ответственные за данные процессы лица.

7.4. Ответственные лица сообщают планируемый срок локализации и устранения последствий инцидента информационной безопасности, а также отчитываются Администратору информационной безопасности о степени выполнения работ.

7.5. Процесс локализации и устранения последствий инцидента информационной безопасности своевременно отражается в Карточке инцидента информационной безопасности.

8. Расследование инцидента информационной безопасности и реализация корректирующих мер

8.1. Процедура расследования инцидента информационной безопасности предназначена для выявления причин (условий и факторов), вызвавших инцидент информационной безопасности, и/или негативную тенденцию развития связанной с этим инцидентом ситуации, а также анализа и оценки адекватности и эффективности действий, предпринятых, по управлению инцидентом информационной безопасности.

8.2. Для проведения процедуры расследования инцидента информационной безопасности привлекается комиссия по обеспечению информационной безопасности (далее – комиссия по ОИБ), утвержденная приказом директора ГБПОУ КК СЭТ.

8.3. В процессе расследования инцидента информационной безопасности на основании анализируемых данных должен быть установлен нарушитель информационной безопасности (для внутренних категорий нарушителей – должно быть выявлено конкретное физическое лицо), чьи действия (умышленные или неумышленные) привели к возникновению инцидента информационной безопасности.

8.4. По итогам расследования инцидента информационной безопасности комиссией по ОИБ разрабатывается комплекс мер, направленных на:

недопущение (минимизацию вероятности) возможности повторения инцидента в будущем – разработка корректирующих мер;

выявление нарушителей информационной безопасности (если его не удалось установить в процессе расследования инцидента).

8.5. При разработке корректирующих мер должны учитываться их возможные воздействия на процесс функционирования информационных систем (в том числе должна быть оценена возможная степень негативного влияния на работу пользователей информационных систем), а также стоимость (экономическая обоснованность) реализации данных мер.

8.6. Результат разработки корректирующих мер (отчет) передается начальнику отдела проектной деятельности, цифровой трансформации и информационной безопасности или лицу, замещающему его, для принятия дальнейших решений по реализации данных мер.

8.7. Процесс расследования инцидента информационной безопасности и реализация корректирующих мер своевременно отражается в Карточке инцидента информационной безопасности.

8.8. После выполнения всех действий по регистрации, локализации, устранению последствий, расследования инцидента информационной безопасности и принятия корректирующих мер инцидент должен быть закрыт (разрешен), о чем делается запись в журнале учета инцидентов информационной безопасности и карточке инцидента информационной безопасности.

9. Ответственность за исполнение положений настоящей Политики

9.1. Все сотрудники техникума обязаны информировать администратора информационной безопасности об инцидентах информационной безопасности, событиях безопасности информации (имеющих признаки инцидента) и, при необходимости, принимать участие в расследовании инцидента информационной безопасности вместе с комиссией по ОИБ.

9.2. Администратор информационной безопасности несет ответственность за:

пересмотр (не реже одного раза в год) Перечня событий безопасности информации информационных систем техникума;

принятие решения по реализации корректирующих мер (в соответствии с предоставленными отчетами);

регистрацию инцидентов информационной безопасности в Журнале учета инцидентов информационной безопасности;

согласование перечня лиц, ответственных за локализацию и устранение последствий инцидентов информационной безопасности;

ведение карточек инцидентов информационной безопасности;

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

контроль сроков локализации и устранение последствий инцидентов информационной безопасности;

анализ проведенной работы по локализации и устранению ответственными лицами последствий инцидентов информационной безопасности;

участие в составе комиссии по ОИБ в рамках расследования инцидентов информационной безопасности;

обеспечение непрерывности регистрации, учета, сбора и хранения (сроком не менее 12 месяцев) событий безопасности информации в соответствии с требованиями настоящей Политики (в зоне своей ответственности);

реализацию комплекса мер по защите сведений о событиях безопасности информации от неправомерного доступа, уничтожения или модифицирования (в зоне своей ответственности);

своевременный мониторинг и анализ событий безопасности информации с целью выявления информационной безопасности (в зоне своей ответственности).

9.3. Администратор информационных систем несет ответственность за:

обеспечение непрерывности регистрации, учета, сбора и хранения (сроком не менее 12 месяцев) событий безопасности информации в соответствии с требованиями настоящей Политики (в зоне своей ответственности);

реализацию комплекса мер по защите сведений о событиях безопасности информации от неправомерного доступа, уничтожения или модифицирования (в зоне своей ответственности);

своевременный мониторинг и анализ событий безопасности информации с целью выявления информационной безопасности (в зоне своей ответственности);

участие в составе комиссии по ОИБ в рамках расследования инцидентов информационной безопасности (при необходимости, определяемой администратором информационной безопасности).

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

Приложение 1
к политике управления событиями
безопасности информации
государственного бюджетного
профессионального образовательного
учреждения Краснодарского края
«Славянский электротехнологический
техникум»

ПЕРЕЧЕНЬ
типов событий безопасности информации, подлежащих регистрации в государственном бюджетном профессиональном образовательном учреждении Краснодарского края «Славянский электротехнологический техникум»

1. Физический доступ к информационным ресурсам (системам), средствам обработки информации и средствам обеспечения их отказоустойчивости:

физический доступ работников и иных лиц в защищаемые помещения, не имеющих доступ в данные помещения;

физический доступ третьих лиц в серверные помещения (проводящих работы по обслуживанию, ремонту, сопровождению и настройке серверного, активного сетевого и прочего оборудования, располагающегося в серверных помещениях);

изменение (в том числе замена, добавление или изъятие) состава средств обработки информации);

замена и (или) модификация аппаратной конфигурации средств обработки информации;

осуществление действий со съемными носителями информации1);

осуществление действий с дополнительными идентификаторами, используемыми для доступа к информационным ресурсам (системам);

вынос за пределы организации средств вычислительной техники;

передача средств вычислительной техники между структурными подразделениями техникума;

передача средств вычислительной техники и их компонентов в сторонние организации;

осуществление действий с носителями информации, позволяющими осуществить физический доступ в здания и помещения организации (proximity-карты для систем контроля и управления доступом).

2. Использование информационных ресурсов (систем) и средств обработки защищаемой информации:

предоставление аутентификационной и ключевой информации на доступ к информационным ресурсам (системам) и средствам обработки защищаемой

---

1) Регистрация, учет, выдача, использование (подключение), утилизация (уничтожение).

информации (в том числе по использованию служебной электронной почты и сети Интернет);

изменение прав доступа к информационным ресурсам (системам) и средствам обработки защищаемой информации;

изменение и (или) компрометация аутентификационной или ключевой информации;

аутентификация и идентификация пользователей информационных ресурсов (систем) и средств обработки защищаемой информации (в том числе неуспешная);

удаленный доступ к информационным ресурсам (системам) и средствам обработки защищаемой информации (с указанием протокола доступа);

действия, совершаемые с защищаемой информацией;

завершение сеансов работы пользователей информационных ресурсов (систем) и средств обработки защищаемой информации;

вывод на печать защищаемой информации;

отключение/перезагрузка или приостановление работы средств обработки защищаемой информации;

изменение параметров настроек средств обработки защищаемой информации;

изменение состава и версий программного обеспечения (в том числе баз сигнатур средств антивирусной защиты информации и средств обнаружения вторжений);

сбои и отказы работоспособности информационных ресурсов (систем) и средств обработки защищаемой информации;

восстановление работоспособности информационных ресурсов (систем) и средств обработки защищаемой информации;

архивирование, резервирование и восстановление защищаемой информации;

выполнение операций, связанных с эксплуатацией и администрированием информационных ресурсов (систем) и средств обработки защищаемой информации).

Настоящий перечень подлежит обязательному ежегодному пересмотру.

Дата _____20__ г.

Составитель _____ Ф.И.О.
(подпись)

Приложение 2
к политике управления событиями
безопасности информации
государственного бюджетного
профессионального образовательного
учреждения Краснодарского края
«Славянский электротехнологический
техникум»

ФОРМА

ЖУРНАЛ УЧЕТА
инцидентов информационной безопасности

№ п/п	№ карточки инцидента ИБ	Дата и время возникновения инцидента ИБ	Дата и время регистрации инцидента ИБ	Ф.И.О. и должность работника, обнаружившего инцидент ИБ	Критичность инцидента ИБ	Затронутые информационные ресурсы (системы) и средств обработки информации	Ф.И.О. и должность лица, ответственного за устранение инцидента	Дата и время устранения инцидента ИБ
1	2	3	4	5	6	7	8	9
1								
2								

Дата _____20__ г.
Составитель _____ Ф.И.О.
(подпись)

Приложение 3
к политике управления событиями
безопасности информации
государственного бюджетного
профессионального образовательного
учреждения Краснодарского края
«Славянский электротехнологический
техникум»

ФОРМА

КАРТОЧКА
инцидента информационной безопасности № ____

№ п/п	Наименование характеристики инцидента ИБ:	Описание
1	2	3
1. Общие сведения об инциденте ИБ		
1.1	Номер записи согласно Журналу учета инцидентов ИБ	
1.2	Дата и время возникновения инцидента ИБ	
1.3	Дата и время регистрации инцидента ИБ	
1.4	Источник информации об инциденте ИБ	работник или техническое средство
1.5	Ф.И.О. и должность работника, обнаружившего инцидент ИБ	
1.6	Контактные данные работника, обнаружившего инцидент	
1.7	Наименование технического средства, при использовании которого обнаружен инцидент ИБ	
1.8	Описание инцидента ИБ	
2. Содержание инцидента ИБ		
2.1	Сведения о нарушении установленных организационно-распорядительными документами требований по обеспечению ИБ	«нет» «наименование документа, регламентирующего требование; № пункта документа»
2.2	Данные о нарушителе требований по обеспечению ИБ	«нет» «Фамилия И.О., должность нарушителя»
2.3	Категория инцидента ИБ	«случайный» «преднамеренный»
2.4	Тип инцидента ИБ	«свершившийся»

1	2	3
		«попытка осуществления инцидента ИБ» «подозрение на инцидент ИБ»
3. Воздействие инцидента на информационные ресурсы (системы) и средства обработки защищаемой информации		
3.1	Типы объектов (ресурсов), затронутых инцидентом	«файлы/базы данных, содержащие защищаемую информацию» «автоматизированные рабочие места» «серверы информационных систем» «активное сетевое оборудование» «средства защиты информации» «носители информации (в том числе бумажные носители)» «системное/прикладное программное обеспечение» «линии и сети передачи данных» «помещения, здания, сооружения, инженерные сети и коммуникации»
3.2	Нарушенные свойства безопасности:	«конфиденциальность» «целостность» «доступность»
3.3	Область распространения и действия инцидента ИБ	«пределы одного информационного ресурса (системы)» «пределы отдельного структурного подразделения» «ГБПОУ КК СЭТ в целом» «выходящий за пределы ГБПОУ КК СЭТ»
3.4	Критичность инцидента ИБ	«высокая» «средняя» «низкая»
4. Локализация и устранение последствий инцидента ИБ		
4.1	Информирование об инциденте ИБ	«дата и время информирования и кому сообщено»
4.2	Назначение ответственного лица за локализацию инцидента ИБ	«дата и время, Ф.И.О., должность ответственного лица»
4.3	Планируемый срок локализации инцидента ИБ	«планируемый срок, определенный ответственным лицом»
4.4	Сведения о локализации инцидента ИБ	«дата и время, описание предпринятых действий»
4.5	Назначение ответственного лица за устранение последствий инцидента ИБ	«дата и время, Ф.И.О., должность ответственных лиц»
4.6	Планируемый срок устранения последствий инцидента ИБ	«планируемый срок, определенный ответственным лицом»
4.7	Сведения об устранении последствий инцидента ИБ	«дата и время, описание предпринятых действий»
5. Расследование инцидента ИБ и реализация корректирующих мер		
5.1	Сведения о комиссии по расследованию инцидента ИБ	«комиссия по ОИБ, состав ее членов»
5.2	Сведения о причинах воз-	«описание»

1	2	3
	никновения инцидента ИБ	
5.3	Сведения о лицах, понесших ответственность за инцидент ИБ	«Ф.И.О., должность лица, вид ответственности»
5.4	Степень вероятности повторного возникновения инцидента ИБ	«нет» «минимальная» «средняя» «высокая»
5.5	Перечень корректирующих мер, направленных на предупреждение повторного возникновения инцидента	«описание»

Дата, время закрытия инцидента ИБ: _____

Ф.И.О., подпись администратора ИБ _____

Дата _____20__ г.

Составитель _____ Ф.И.О.
(подпись)

ПРИЛОЖЕНИЕ № 8

УТВЕРЖДЕНА
приказом директора
от 30.12.2023 № 952

ПОЛИТИКА
использования средств криптографической защиты информации государственного бюджетного профессионального образовательного учреждения Краснодарского края «Славянский электротехнологический техникум»

1. Общие положения

1.1. Политика использования средств криптографической защиты информации (далее – Политика) государственного бюджетного профессионального образовательного учреждения Краснодарского края «Славянский электротехнологический техникум» (далее – ГБПОУ КК СЭТ, техникум) определяет:

порядок учета, хранения и использования средств криптографической защиты информации (далее – СКЗИ), криптографических ключей и эксплуатационной документации к ним;

порядок действий по уничтожению криптографических ключей;

порядок действий при компрометации криптографических ключей.

1.2. Настоящая Политика разработана в соответствии с:

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»;

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;

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;

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.

1.3. К средствам криптографической защиты информации относятся:

реализующие криптографические алгоритмы преобразования информации аппаратные, программные и аппаратно-программные средства, системы и комплексы, обеспечивающие безопасность информации при ее обработке, хранении и передаче по каналам связи, включая СКЗИ;

реализующие криптографические алгоритмы преобразования информации аппаратные, программные и аппаратно-программные средства, системы и комплексы защиты от несанкционированного доступа к информации при ее обработке и хранении;

реализующие криптографические алгоритмы преобразования информации аппаратные, программные и аппаратно-программные средства, системы и комплексы защиты от навязывания ложной информации, включая средства имитозащиты и электронной подписи;

аппаратные, программные и аппаратно-программные средства, системы и комплексы изготовления и распределения ключевых документов для СКЗИ, независимо от вида носителя ключевой информации.

1.4. Использование СКЗИ для обеспечения безопасности информации необходимо в следующих случаях:

если защищаемая информация подлежит криптографической защите в соответствии с законодательством Российской Федерации;

если в информационных системах существуют угрозы, которые могут быть нейтрализованы только с помощью СКЗИ;

если техникумом принято решение о необходимости применения криптографической защиты информации.

1.5. К случаям, когда угрозы безопасности информации могут быть нейтрализованы только с помощью СКЗИ, относятся:

передача защищаемой информации по каналам связи, не защищенным от перехвата нарушителем передаваемой по ним информации или от несанкционированных воздействий на эту информацию (например, при передаче персональных данных по информационно-телекоммуникационным сетям общего пользования);

хранение защищаемой информации на носителях информации, несанкционированный доступ к которым со стороны нарушителя не может быть исключен без применения криптографических способов защиты информации.

1.6. Для обеспечения безопасности информации при ее обработке в информационных системах должны использоваться СКЗИ, сертифицированные ФСБ России по требованиям, предъявляемым к СКЗИ. Необходимый к использованию класс СКЗИ определяется по результатам определения угроз (возможностей потенциальных нарушителей) СКЗИ.

2. Правила ввода СКЗИ в эксплуатацию

2.1. При вводе СКЗИ в эксплуатацию должны соблюдаться следующие правила:

осмотр СКЗИ, дистрибутивов на факт наличия физических дефектов, наличие заводских пломб, наличие эксплуатационной и технической документации к поставляемому СКЗИ, отсутствие признаков компрометации;

сверка акта приема передачи поставляемых СКЗИ (при наличии);

установка и ввод в эксплуатацию СКЗИ осуществляется в соответствии с эксплуатационной и технической документацией;

по результатам настройки и установки составляется «Акт установки и ввода в эксплуатацию СКЗИ» (Форма Акта установки и ввода в эксплуатацию СКЗИ приведена в приложении 1 к настоящей Политике);

производится обучение сотрудников работе с СКЗИ;

составляется протокол принятия зачета у пользователя СКЗИ (форма протокола принятия зачета у пользователя СКЗИ приведена в приложении 2 к настоящей Политике);

оформляется лицевой счет пользователя (форма лицевого счета пользователя СКЗИ приведена в приложениях 3 к настоящей Политике);

орган криптографической защиты информации (далее - ОКЗИ) выдает заключение о допуске пользователя к самостоятельной работе с СКЗИ (форма заключения о допуске пользователя к самостоятельной работе с СКЗИ приведена в приложении 4 к настоящей Политике);

производится запись в журнал поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов (далее – Журнал учета СКЗИ). Формы Журнала учета СКЗИ для обладателя конфиденциальной информации и для ОКЗИ приведены в приложениях 5-6 соответственно;

производится запись в технический (аппаратный) журнал (форма технического (аппаратного) журнала приведена в приложении 7).

3. Организация передачи информации по каналам связи с использованием СКЗИ защищаемой информации

3.1. Безопасность хранения, обработки и передачи по каналам связи с использованием СКЗИ защищаемой информации организуется и обеспечивается на основании договоров на оказание услуг по криптографической защите информации организациями, имеющими лицензию ФСБ России на осуществление разработки, производства, распространения шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных

(криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)[1)] (далее – лицензиаты ФСБ России).

3.2. Орган криптографической защиты информации осуществляет:

установку и настройку программных и программно-аппаратных средств криптографической защиты информации;

подготовку к вводу в эксплуатацию СКЗИ в соответствии с требованиями эксплуатационной документации;

проверку готовности обладателей конфиденциальной информации к самостоятельному использованию СКЗИ и составление заключений о возможности эксплуатации СКЗИ (с указанием типа и номеров, используемых СКЗИ, номеров аппаратных, программных и аппаратно-программных средств, где установлены или к которым подключены СКЗИ, с указанием также номеров печатей, которыми опечатаны технические средства, включая СКЗИ, и результатов проверки функционирования СКЗИ);

разработку мероприятий по обеспечению функционирования и безопасности, применяемых СКЗИ в соответствии с условиями выданных на них сертификатов, а также в соответствии с эксплуатационной и технической документацией к этим средствам;

инструктаж лиц, использующих СКЗИ, по правилам работы с ними;

поэкземплярный учет используемых СКЗИ, эксплуатационной и технической документации к ним;

учет обслуживаемых обладателей конфиденциальной информации, а также физических лиц, непосредственно допущенных к работе с СКЗИ;

контроль за соблюдением условий использования СКЗИ, установленных эксплуатационной и технической документацией к СКЗИ;

расследование и составление заключений по фактам нарушения условий использования СКЗИ, которые могут привести к снижению уровня защиты информации;

разработку и принятие мер по предотвращению возможных опасных последствий нарушений условий использования СКЗИ;

разработку схемы организации криптографической защиты информации (с указанием наименования, обладателей конфиденциальной информации, типов применяемых СКЗИ и ключевых документов к ним, видов защищаемой информации, используемых совместно с СКЗИ технических средств связи, прикладного и общесистемного программного обеспечения, и средств вычислительной техники).

3.3. Установка и ввод в эксплуатацию СКЗИ производится на основании «Акта установки и ввода в эксплуатацию средства криптографической защиты

[1)] В лицензии должны быть указаны пункты:12,13,14,15,17,18,20,21,22,23,24 согласно Постановлению Правительства Российской Федерации от 16.04.2012 г. № 313.

информации», который утверждается директором ГБПОУ КК СЭТ, либо лицом, замещающим его.

3.4. Обладатель конфиденциальной информации, владеющий СКЗИ, осуществляет:

поэкземплярный учет и хранение СКЗИ согласно разделу 4 настоящей Политики;

работы по обслуживанию шифровальных (криптографических) средств, предусмотренные технической и эксплуатационной документацией на эти средства (только для обеспечения собственных нужд техникума), в соответствии с требованиями разделов 5, 8, 10 настоящей Политики.

4. Учет и хранение СКЗИ и криптографических ключей к ним

4.1. Средства криптографической защиты информации, криптографические ключи (ключевые документы), а также эксплуатационная и техническая документация к СКЗИ, подлежат поэкземплярному учету.

4.2. Поэкземплярный учет СКЗИ ведется в Журнале учета СКЗИ, при этом программные СКЗИ должны учитываться совместно с аппаратными средствами, с которыми осуществляется их штатное функционирование. Если аппаратные или аппаратно-программные СКЗИ подключаются к системной шине или к одному из внутренних интерфейсов аппаратных средств, то такие СКЗИ учитываются также совместно с соответствующими аппаратными средствами.

4.3. Все полученные экземпляры СКЗИ, эксплуатационной и технической документации к ним, ключевых документов выдаются под расписку в Журнале учета СКЗИ, лицам, несущим персональную ответственность за их сохранность. Единицей поэкземплярного учета ключевых документов считается ключевой носитель многократного использования. Если один и тот же ключевой носитель многократно используют для записи криптоключей, то его каждый раз следует регистрировать отдельно.

4.4. Если эксплуатационной и технической документацией к СКЗИ предусмотрено применение разовых ключевых носителей, или криптоключи вводят и хранят (на весь срок их действия) непосредственно в СКЗИ, то такой разовый ключевой носитель или электронная запись соответствующего криптоключа должны регистрироваться в техническом (аппаратном) журнале, который ведет администратор информационной безопасности.

4.5. Передача СКЗИ, эксплуатационной и технической, ключевых документов допускается только между пользователями СКЗИ под расписку в журнале поэкземплярного учета.

4.6. Дистрибутивы СКЗИ на носителях, эксплуатационная и техническая документация к СКЗИ хранятся у администратора информационной безопасности, в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение. Администратор информационной безопасности также обязан предусмотреть раздельное безопасное хранение

действующих и резервных ключевых документов, предназначенных для применения в случае компрометации действующих криптоключей.

4.7. Аппаратные средства, с которыми осуществляется штатное функционирование СКЗИ, а также аппаратные и аппаратно-программные СКЗИ должны быть оборудованы средствами контроля за их вскрытием (опечатаны). Место опечатывания СКЗИ, аппаратных средств должно быть таким, чтобы его можно было визуально контролировать. Пользователь СКЗИ должен периодически проверять сохранность оборудования и целостность печатей на автоматизированных рабочих местах (далее – АРМ) и серверах, в которых установлены СКЗИ. В случае обнаружения посторонних (незарегистрированных) программ или выявления факта повреждения печати работа должна быть прекращена. По данному факту проводится служебное расследование и осуществляются работы по анализу и ликвидации последствий данного нарушения (регистрируется инцидент информационной безопасности).

4.8. СКЗИ и криптографические ключи могут в случае необходимости пересылаться специальной фельдъегерской (в том числе ведомственной) связью или со специально выделенными нарочными из числа сотрудников техникума, лиц, имеющих доверенность на право получения СКЗИ при соблюдении мер, исключающих бесконтрольный доступ к СКЗИ и криптографическим ключам во время доставки.

4.9. Для пересылки СКЗИ и криптографические ключи помещаются в прочную упаковку, исключающую возможность их физического повреждения и внешнего воздействия, в особенности на записанную ключевую информацию. Криптографические ключи пересылают в отдельном пакете с пометкой «Лично». Упаковки опечатывают таким образом, чтобы исключалась возможность извлечения из них содержимого без нарушения упаковок и оттисков печати.

4.10. Для пересылки СКЗИ, эксплуатационной и технической документации к ним, криптографических ключей составляется Акт приема-передачи (опись) документов, в котором указывается: что посылается и в каком количестве, учетные номера СКЗИ, криптографических ключей или документов, а также, при необходимости, назначение и порядок использования высылаемого отправления. Акт приема-передачи (опись) документов вкладывается в упаковку.

4.11. Полученную упаковку вскрывает только лицо, для которого она предназначена. Если содержимое полученной упаковки не соответствует указанному в Акте приема-передачи (описи) документов, или сама упаковка и печать их описанию (оттиску), а также если упаковка повреждена, в результате чего образовался свободный доступ к ее содержимому, то получатель составляет акт, который высылается отправителю. Полученные с такими отправлениями СКЗИ и криптографические ключи до получения указаний отправителя применять не разрешается.

4.12. При обнаружении бракованных криптографических ключей ключевой носитель с такими ключами следует вернуть изготовителю для установления причин происшедшего и их устранения в дальнейшем.

Изготовитель в этом случае должен направить новые криптографические ключи.

4.13. Ключевые носители совместно с описью криптографических ключей должны храниться в сейфе (металлическом шкафу), как правило, в отдельной ячейке. В исключительных случаях допускается хранить ключевые носители и опись криптографических ключей совместно с другими документами, при этом ключевые носители и опись криптографических ключей должны быть помещены в отдельную папку.

4.14. При отсутствии у пользователя СКЗИ сейфа (металлического шкафа) ключевые носители по окончании рабочего дня должны сдаваться администратору информационной безопасности или иному, назначенным ответственным должностному лицу, по Журналу учета СКЗИ.

5. Порядок эксплуатации СКЗИ и криптографических ключей к ним

5.1. Средства криптографической защиты информации эксплуатируются в техникуме в соответствии с правилами пользования ими, которые указаны в эксплуатационной и технической документации к СКЗИ.

5.2. СКЗИ и криптографические ключи используются в техникуме для обеспечения конфиденциальности и целостности электронных документов, в том числе при передаче информации по открытым каналам связи.

5.3. Конфиденциальность электронных документов обеспечивается путем их шифрования. Авторство и целостность электронных документов обеспечивается путем создания в документе электронной подписи пользователя.

5.4. Электронный документ может быть подписан электронной подписью с использованием только того закрытого ключа, для которого выдан сертификат ключа подписи пользователя с областью действия.

5.5. Для шифрования электронного документа пользователь использует свой собственный закрытый криптографический ключ и открытый криптографический ключ, соответствующий действующему закрытому криптографическому ключу получателя документа.

5.6. Открытый криптографический ключ содержится в сертификате ключа подписи, который выдается пользователю в электронной форме и на бумажном носителе.

5.7. Проверка подлинности электронной подписи электронного документа осуществляется пользователем с использованием открытого криптографического ключа отправителя документа.

5.8. Расшифровывание электронного документа осуществляется с использованием закрытого криптографического ключа пользователя и открытого криптографического ключа отправителя документа.

5.9. В случае необходимости генерации закрытого криптографического ключа (и пароля доступа к нему) пользователь должен осуществить генерацию самостоятельно на собственном АРМ (при наличии технической воз-

можности[1]), либо на АРМ администратора информационной безопасности. При использовании ключевой информации рекомендуется в качестве носителей ключевой информации использовать носители, имеющие специализированные контейнеры ключевой информации, обеспечивающие невозможность их экспорта (также при генерации ключевой информации должен быть задан соответствующий параметр).

5.10. Пользователь не может подписать электронный документ своей электронной подписью или выполнить его шифрование, если истек срок действия закрытых криптографических ключей. Также пользователь не может проверить электронную подпись электронного документа или произвести его расшифровывание в случае истечения срока действия сертификата ключа подписи, необходимого для выполнения соответствующей операции.

5.11. Реализованные в СКЗИ алгоритмы шифрования и электронной цифровой подписи гарантируют невозможность восстановления закрытых криптографических ключей отправителя по его открытым ключам.

5.12. При выявлении сбоев или отказов пользователь обязан сообщить о факте их возникновения администратору информационной безопасности и предоставить ему носители криптографических ключей для проверки их работоспособности. Проверку работоспособности носителей криптографических ключей администратор информационной безопасности выполняет в присутствии пользователя.

5.13. В случае если рабочие криптографические ключи потеряли работоспособность, то по заявке пользователя администратор информационной безопасности информации вскрывает конверт с резервными криптографическими ключами, делает копию ключевого носителя, используя резервные криптографические ключи, помещает резервные криптографические ключи в конверт.

5.14. В экстренных случаях, не терпящих отлагательства, вскрытие конверта с резервными криптографическими ключами может осуществляться пользователем самостоятельно с последующим уведомлением администратора информационной безопасности о факте вскрытия конверта с криптографическими ключами. На конверте делается запись о вскрытии с указанием даты и времени вскрытия конверта и подписью пользователя. Вскрытый конверт вместе с неработоспособными криптографическими ключами сдаются администратору информационной безопасности.

5.15. Вскрытие системного блока АРМ/сервера, на котором установлено СКЗИ, для проведения ремонта или технического обслуживания должно осуществляться в присутствии администратор информационной безопасности.

5.16. Пользователю запрещается:

осуществлять несанкционированное копирование криптографических ключей;

---

[1] В случае генерации пин-кода доступа администратором должна обеспечиваться смена пользователем пин-кода, при первом использовании носителю ключевой информации (обеспечивается функционалом носителя ключевой информации)

разглашать содержимое носителей ключевой информации или передавать сами носители лицам, к ним не допущенным, выводить ключевую информацию на экран монитора и принтер;

вставлять носители криптографических ключей в устройства считывания в режимах, не предусмотренных штатным режимом работы СКЗИ, а также в устройства считывания других автоматизированных рабочих мест и серверов;

записывать на носители с криптографическими ключами постороннюю информацию;

подключать к АРМ и серверам дополнительные устройства и соединители, не предусмотренные в комплектации;

вносить какие-либо изменения в программное обеспечение СКЗИ;

использовать бывшие в работе одноразовые ключевые носители для записи новых криптографических ключей.

6. Порядок действий при компрометации криптоключей

6.1. Под компрометацией криптоключей понимается хищение, утрата, разглашение, несанкционированное копирование и другие происшествия, в результате которых криптоключи могут стать доступными несанкционированным лицам и (или) процессам.

К компрометации ключей относятся следующие события:

утрата носителей ключа;

утрата носителей ключа с последующим обнаружением;

возникновение подозрений на утечку информации или ее искажение в системе конфиденциальной связи;

нарушение целостности печатей на сейфах с носителями ключевой информации, если используется процедура опечатывания сейфов;

утрата ключей от сейфов в момент нахождения в них носителей ключевой информации;

утрата ключей от сейфов в момент нахождения в них носителей ключевой информации с последующим обнаружением;

доступ посторонних лиц к ключевой информации;

другие события утери доверия к ключевой документации.

6.2. Криптоключи, в отношении которых возникло подозрение в компрометации, а также действующие совместно с ними другие криптоключи необходимо немедленно вывести из действия. О нарушениях, которые могут привести к компрометации криптоключей, их составных частей или передававшейся (хранящейся) с их использованием конфиденциальной информации, пользователи СКЗИ обязаны сообщать администратору информационной безопасности.

6.3. Осмотр ключевых носителей многократного использования посторонними лицами не следует рассматривать как подозрение в компрометации криптоключей, если при этом исключалась возможность их копирования (чтения, размножения). В случаях недостачи, непредъявления ключевых документов, а также неопределенности их местонахождения принимаются срочные меры к их розыску.

6.4. Мероприятия по розыску и локализации последствий компрометации конфиденциальной информации, передававшейся (хранящейся) с использованием СКЗИ, организует и осуществляет обладатель скомпрометированной конфиденциальной информации. Действующие и резервные ключевые документы, предназначенные для применения в случае компрометации действующих криптоключей, должны храниться во внутреннем отсеке сейфа в различных конвертах.

6.5. Порядок действий пользователя при компрометации ключей:

Решение о факте или угрозе компрометации своего криптоключа пользователь принимает самостоятельно. При компрометации ключа пользователь должен прекратить работу с скомпрометированным ключам и оповестить Администратора информационной безопасности. При наличии возможности оповестить пользователей, с которыми осуществлялось взаимодействие посредством скомпрометированных ключей.

6.6. Порядок действий при сообщении о компрометации криптоключей:

При получении сообщения о компрометации ключа пользователя, администратор информационной безопасности ответным звонком уточняет факт компрометации, и в случае его подтверждения немедленно приостанавливает действие ключа. При наличии резервных ключей, пользователь должен перейти на комплект резервных ключей. Если резервные ключи не были предусмотрены, для восстановления системы необходимо: повторно произвести формирование ключа и обеспечить получение новых криптоключей пользователями системы.

7. Уничтожение средств криптографической защиты информации

7.1. Криптографические ключи:

7.1.1. Уничтожению подлежат криптографические ключи в случае их компрометации, вывода из эксплуатации, окончания срока действия.

7.1.2. Криптографические ключи уничтожаются путем их стирания (разрушения) по технологии, принятой для ключевых носителей многократного использования, в соответствии с требованиями эксплуатационной и технической документации на СКЗИ, путем удаления с носителя информации, способом, препятствующим восстановлению удаленной информации, или физическим уничтожением материального носителя ключевой информации.

7.2. Аппаратные СКЗИ:

7.2.1. Уничтожению подлежат аппаратные СКЗИ вышедшие из строя или выведенные из эксплуатации.

7.2.2. Аппаратные СКЗИ уничтожаются (утилизируются) в соответствии с требованиями Положения ПКЗ-2005, по решению обладателя конфиденциальной информации, владеющего СКЗИ, и по согласованию с ОКЗИ.

7.3. Программные СКЗИ:

7.3.1. Уничтожению подлежат программные СКЗИ выведенные из эксплуатации.

7.2.3. Программные СКЗИ уничтожаются путем предусмотренным эксплуатационной и технической документацией к СКЗИ. В противном случае, удалением программного обеспечения СКЗИ с носителя информации, способом, препятствующим восстановлению удаленной информации.

7.4. Программно-аппаратные СКЗИ:

7.4.1. Уничтожению подлежат программно-аппаратные СКЗИ вышедшие из строя или выведенные из эксплуатации.

7.4.2. Намеченные к уничтожению (утилизации) СКЗИ, извлекаются из аппаратных средств, с которыми они функционировали. При этом СКЗИ считаются изъятыми из аппаратных средств, если исполнена предусмотренная эксплуатационной и технической документацией к СКЗИ, процедура удаления программного обеспечения СКЗИ, и они полностью отсоединены от аппаратных средств.

7.5. Дистрибутивы СКЗИ:

7.5.1. Уничтожению подлежат дистрибутивы выведенных из эксплуатации СКЗИ, ПО СКЗИ и скомпрометированных ключевых дистрибутивов на носителях информации.

7.5.2. Дистрибутивы СКЗИ уничтожаются путем удаления с носителя информации, способом, препятствующим восстановлению удаленной информации, либо физическим уничтожением материального носителя.

7.6. Ключевые документы:

7.6.1. Уничтожению подлежат скомпрометированные или выведенные из эксплуатации ключевые документы.

7.6.2. Ключевые документы уничтожаются путем удаления с носителя ключевой информации, способом, препятствующим восстановлению удаленной информации, физическим уничтожением материального носителя ключевых документов, путем сжигания, с помощью любых бумагорезательных машин или иного физического воздействия, в сроки, указанные в эксплуатационной и технической документации к соответствующим СКЗИ. Если срок уничтожения эксплуатационной и технической документацией не установлен, то ключевые документы должны быть уничтожены не позднее 10 суток после вывода их из эксплуатации (окончания срока действия).

7.7. Эксплуатационная и техническая документация к СКЗИ:

7.7.1. Эксплуатационная и техническая документация подлежит уничтожению вместе с поставляемым СКЗИ, выведенным из эксплуатации.

7.7.2. Эксплуатационная и техническая документация к СКЗИ уничтожается путем сжигания или с помощью любых бумагорезательных машин.

7.8. СКЗИ уничтожаются комиссией, состоящей из сотрудников ОКЗИ (не менее двух представителей), и не менее двух сотрудников техникума из числа членов комиссии по обеспечению информационной безопасности, назначаемой директором ГБПОУ КК СЭТ.

7.8.1. При уничтожении СКЗИ комиссия обязана:

установить наличие оригинала и количество копий СКЗИ;

проверить внешним осмотром целостность каждого СКЗИ;

установить наличие на оригинале и всех копиях СКЗИ реквизитов путем сверки с записями в Журнале учета СКЗИ;

убедиться, что СКЗИ действительно подлежат уничтожению;

произвести уничтожение СКЗИ;

составить акт об уничтожении СКЗИ.

7.9. Акт об уничтожении СКЗИ:

7.9.1. В акте указывается, что уничтожается конкретно и в каком количестве. В конце акта делается итоговая запись (цифрами и прописью) о количестве наименований и экземпляров, уничтожаемых СКЗИ, эксплуатационной и технической документации СКЗИ.

7.9.2. В Журнале учета СКЗИ администратором информационной безопасности производится отметка об уничтожении СКЗИ с указанием даты и номера Акта.

7.9.3. Исправления в тексте акта должны быть оговорены и заверены подписями всех членов комиссии, принимавших участие в уничтожении.

7.9.4. Акт об уничтожении СКЗИ подписывается председателем комиссии, членами комиссии.

7.9.5. Акты об уничтожении СКЗИ хранятся у администратора информационной безопасности.

7.9.6. Форма акта об уничтожении СКЗИ приведена в приложении 8 к настоящей Политике.

8. Организация режима в помещениях, где установлены СКЗИ или хранятся криптографические ключи

8.1. Размещение, специальное оборудование, охрана и организация режима в помещениях, где установлены СКЗИ или хранятся криптографические ключи, должны обеспечивать сохранность СКЗИ и криптографических ключей.

8.2. При обустройстве данных помещений должны выполняться требования к размещению, монтажу СКЗИ, а также другого оборудования, функционирующего с СКЗИ.

8.3. Спецпомещения выделяют с учетом размеров контролируемых зон, регламентированных эксплуатационной и технической документацией к СКЗИ. Помещения должны иметь прочные входные двери с замками, гарантирующими надежное закрытие помещений в нерабочее время. Окна помещений, расположенных на первых или последних этажах зданий, а также окна, находящиеся около пожарных лестниц и других мест, откуда возможно проникновение в спецпомещения посторонних лиц, необходимо оборудовать металлическими решетками, ставнями, охранной сигнализацией, или другими средствами, препятствующими неконтролируемому проникновению в спецпомещения.

8.4. Размещение, специальное оборудование, охрана и организация режима в помещениях должны исключить возможность неконтролируемого проникновения или пребывания в них посторонних лиц, а также визуальное наблюдение посторонними лицами за проведением работ в помещении.

8.5. Режим охраны помещений, в том числе правила допуска работников и посетителей в рабочее и нерабочее время устанавливается директором ГБПОУ КК СЭТ, либо лицом в его заменяющим. Установленный режим охраны должен предусматривать периодический контроль за состоянием технических средств охраны, если таковые имеются, а также учитывать положения настоящей Политики.

8.6. Двери спецпомещений должны быть постоянно закрыты на замок и могут открываться только для санкционированного прохода работников и посетителей. Ключи от входных дверей нумеруют, учитывают и выдают работникам, имеющим право допуска в спецпомещения, под расписку в журнале учета хранилищ СКЗИ и ключей от них (форма журнала учета хранилищ СКЗИ и ключей от них приведена в приложении 9). Дубликаты ключей от входных дверей таких помещений следует хранить в специальном сейфе.

8.7. Окна помещений, в которых установлены СКЗИ должны быть защищены для предотвращения несанкционированного просмотра.

8.8. Помещения, по возможности, должны быть оснащены системой контроля и управления доступом, охранной сигнализацией, связанной со службой охраны здания или дежурным. Исправность сигнализации периодически должна проверяться службой охраны.

8.9. Для хранения криптографических ключей, эксплуатационной и технической документации, дистрибутивов СКЗИ должно быть предусмотрено необходимое число надежных металлических хранилищ, оборудованных внутренними замками с двумя экземплярами ключей или кодовыми замками, или приспособлениями для опечатывания замочных скважин. Один экземпляр ключа от хранилища должен находиться у администратора информационной безопасности или пользователя, ответственного за хранилище. Дубликаты ключей от хранилищ пользователи хранят в специальном сейфе. По окончании рабочего дня помещение и установленные в нем хранилища должны быть закрыты, хранилища опечатаны. Печати, предназначенные для опечатывания хранилищ, должны находиться у пользователей, ответственных за эти хранилища.

8.10. В обычных условиях помещения и находящиеся в них опечатанные хранилища могут быть вскрыты только пользователями или администратором информационной безопасности.

8.11. При обнаружении признаков, указывающих на возможное несанкционированное проникновение в эти помещения или хранилища посторонних лиц, о случившемся должно быть немедленно сообщено администратору информационной безопасности, который должен оценить возможность компрометации хранящихся криптографических ключей, составить акт и принять при необходимости меры к локализации последствий компрометации криптографических ключей и к их замене.

8.12. Размещение и монтаж СКЗИ, а также другого оборудования, функционирующего с СКЗИ, в помещениях должны свести к минимуму возможность неконтролируемого доступа посторонних лиц к указанным средствам. Техническое обслуживание такого оборудования и смена

криптографических ключей в присутствии лиц, не допущенных к работе с данными СКЗИ, не допускается.

8.13. На время отсутствия пользователей необходимое оборудование при наличии технической возможности должно быть выключено, отключено от линии связи и убрано в опечатываемые хранилища. В противном случае по согласованию с администратором информационной безопасности необходимо предусмотреть организационно-технические меры, исключающие возможность использования СКЗИ посторонними лицами в отсутствие пользователя.

9. Порядок использования защищенных каналов связи

9.1. При использовании защищенного канала связи необходимо:

обеспечить информационную безопасность каждого информационного актива в соответствии с действующим законодательством Российской Федерации (АРМ, сервера, телекоммуникационного оборудования) подключаемого к защищенному каналу связи;

обеспечить в соответствии с настоящей Политикой надлежащие условия для размещения и функционирования информационного актива, подключенного к защищенному каналу связи и исключить несанкционированный доступ в помещения, где расположены информационные активы;

для защиты информационного актива, участвующих в обмене информации, выходящих за пределы контролируемой зоны, должна проводиться периодическая проверка на отсутствие уязвимостей с использованием анализа защищенности;

обеспечить периодический контроль целостности неизменяемых файлов, используемых в программном обеспечении информационных активов;

обеспечить контроль изменения прикладной программной среды, исключение ввода в информационные активы программных средств без их предварительной гарантированной проверки;

обеспечить мероприятия по антивирусной защите.

9.2. При эксплуатации защищенного канала связи необходимо соблюдать следующие правила:

использовать защищенный канал связи только по прямому назначению;

не допускать использование защищенного канала связи в личных целях;

обеспечивать сохранность информационных ресурсов и физической целостности оборудования;

не допускать распространения спама и вредоносных компьютерных программ с АРМ Пользователя;

не допускать нарушений установленного настоящей Политикой порядка эксплуатации СКЗИ и осуществления иных несанкционированных действий.

10. Ответственность за исполнение положений настоящей Политики

10.1. Ответственность за исполнение положений настоящей Политики возлагается на всех сотрудников техникума, осуществляющих работу со средствами криптографической защиты информации.

10.2. ОКЗИ несет ответственность за:

проверку готовности обладателей конфиденциальной информации к самостоятельному использованию СКЗИ и составление заключений о возможности эксплуатации СКЗИ (с указанием типа и номеров, используемых СКЗИ, номеров аппаратных, программных и аппаратно-программных средств, где установлены или к которым подключены СКЗИ, с указанием также номеров печатей, которыми опечатаны технические средства, включая СКЗИ, и результатов проверки функционирования СКЗИ);

разработку мероприятий по обеспечению функционирования и безопасности, применяемых СКЗИ в соответствии с условиями выданных на них сертификатов, а также в соответствии с эксплуатационной и технической документацией к этим средствам;

инструктаж лиц, использующих СКЗИ, по правилам работы с ними;

поэкземплярный учет используемых СКЗИ, эксплуатационной и технической документации к ним;

учет обслуживаемых обладателей конфиденциальной информации, а также физических лиц, непосредственно допущенных к работе с СКЗИ;

контроль соблюдения условий использования СКЗИ, установленных эксплуатационной и технической документацией к СКЗИ;

расследование и составление заключений по фактам нарушения условий использования СКЗИ, которые могут привести к снижению уровня защиты информации;

разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений;

разработку схемы организации криптографической защиты информации (с указанием наименования, обладателей конфиденциальной информации, типов, применяемых СКЗИ и ключевых документов к ним, видов защищаемой информации, используемых совместно с СКЗИ технических средств связи, прикладного и общесистемного программного обеспечения, и средств вычислительной техники).

10.3. Пользователи СКЗИ техникума обязаны:

соблюдать требования настоящей Политики в отношении учета, хранения и использования средств криптографической защиты информации;

не нарушать установленные правила доступа в помещения;

незамедлительно сообщать администратору информационной безопасности обо всех выявленных нарушениях обращения с СКЗИ или фактов доступа в помещения с нарушением установленных правил;

использовать криптографические средства защиты информации только в соответствии с эксплуатационной и технической документацией.

10.4. Администратор информационной безопасности обязан:

соблюдать требования настоящей Политики в отношении учета, хранения и использования средств криптографической защиты информации;

вести поэкземплярный учет используемых СКЗИ, эксплуатационной и технической документации к ним;

не нарушать установленные правила доступа в помещения;

участвовать в служебных проверках по факту нарушения требований настоящей Политики;

осуществлять замену криптографических ключей из резервных в случаях компрометации или потери работоспособности ключевого носителя с основными криптографическими ключами;

в случае необходимости разъяснять пользователям средств криптографической защиты информации особенности и порядок работы с ними.

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

Приложение 1
к политике использования средств
криптографической
защиты информации в
государственном бюджетном
профессиональном образовательном
учреждении Краснодарского края
«Славянский электротехнологический
техникум»

ФОРМА

Акт №__
установки и ввода в эксплуатацию
средства криптографической защиты информации

г. Славянск-на-Кубани « » _____ 20__г.

Настоящий акт составлен о том, что сотрудником _____
(наименование организации)
(далее – Исполнитель) была произведена установка и настройка средства криптографической защиты информации _____ (далее – криптосредство) в ГБПОУ КК СЭТ.
Серийный номер (инвентарный номер) ПЭВМ / сервера: _____
Место установки: _____
ФИО ответственного сотрудника СКЗИ:_____
ФИО пользователя ПЭВМ:_____
Учетный номер СКЗИ: _____
Серийный номер СКЗИ: _____
Регистрационный номер криптосредства (ПАК): _____
Регистрационный номер экземпляра ключевого документа: _____

Установленное и настроенное криптосредство находится в работоспособном состоянии.

Пользователь криптосредства обязуется:

не разглашать конфиденциальную информацию, к которой он допущен, в том числе сведения о криптоключах;

соблюдать требования к обеспечению безопасности криптосредств и ключевых документов к ним;

сдать криптосредство, эксплуатационную и техническую документацию к ним, ключевые документы при увольнении или отстранения от исполнения обязанностей, связанных с использованием криптосредств;

сообщать исполнителю о попытках посторонних лиц получить сведения об используемых криптосредствах или ключевых документах к ним;

немедленно уведомлять исполнителя о фактах утраты или недостачи криптосредств, ключевых документов к ним.

Исполнитель	Пользователь криптосредства
_____/_____/	_____/_____/
подпись ФИО	подпись ФИО

Приложение 2
к политике использования средств
криптографической
защиты информации в
государственном бюджетном
профессиональном образовательном
учреждении Краснодарского края
«Славянский электротехнологический
техникум»

ФОРМА

« » _____ 20__ г.

ПРОТОКОЛ № ___
принятия зачета у пользователя средств криптографической защиты информации _____ в государственном бюджетном профессиональном образовательном учреждении Краснодарского края «Славянский электротехнологический техникум»

Зачет проведен в соответствии с Перечнем вопросов по проверке знаний у пользователей средств криптографической защиты информации, утвержденным руководителем ОКЗИ компании_____ .
(наименование организации)

Результаты зачета приведены в таблице 1.

Таблица 1 – Результат сдачи зачета

№ п/п	Фамилия, имя, отчество пользователя	Номер билета	Зачет/ незачет	Подпись пользователя
1	2	3	4	5

Должность сотрудника ОКЗИ _____Ф.И.О.
(подпись)

Приложение 3
к политике использования средств
криптографической защиты информации
в государственном бюджетном
профессиональном образовательном
учреждении Краснодарского края
«Славянский электротехнологический
техникум»

ФОРМА

Государственное бюджетное профессиональное образовательное учреждение Краснодарского края «Славянский электротехнологический техникум»

ЛИЦЕВОЙ СЧЕТ
пользователя СКЗИ

_____
(ФИО)

_____
(структурное подразделение, должность)

Наименование СКЗИ	Серийные номера СКЗИ	Регистрационные номера экземпляров ключевых документов	Дата и расписка о получении СКЗИ	Дата и расписка возвращения СКЗИ	Примечания
1	2	3	4	5	6

Должность сотрудника ОКЗИ _____ Ф.И.О.
(подпись)

Приложение 4
к политике использования средств
криптографической
защиты информации в
государственном бюджетном
профессиональном образовательном
учреждении Краснодарского края
«Славянский электротехнологический
техникум»

ФОРМА

УТВЕРЖДАЮ
Руководитель органа
криптографической защиты
информации _____
(Наименование организации)

_____ _____
(подпись) (Ф.И.О.)

«____» _____ 20__года.

ЗАКЛЮЧЕНИЕ
о возможности допуска пользователей к
самостоятельной работе со средствами
криптографической защиты информации
государственного бюджетного профессионального
образовательного учреждения Краснодарского края
«Славянский электротехнологический техникум»

Пользователи, получившие ключевой носитель, а также пользователи, назначенные приказом государственного бюджетного профессионального образовательного учреждения Краснодарского края «Славянский электротехнологический техникум», прошедшие обучение и сдавшие зачет по использованию СКЗИ, допущены к самостоятельной работе и обязуются:

не разглашать конфиденциальную информацию, к которой допущены, в том числе сведения о криптоключах;

соблюдать требования к обеспечению безопасности хранения, обработки и передачи конфиденциальной информации по каналам связи с использованием СКЗИ;

сообщать оператору о ставших ему известными попытках посторонних лиц получить сведения об используемых СКЗИ или ключевых документах к ним;

сдать установленным порядком СКЗИ, эксплуатационную и техническую документацию к ним, ключевые документы при увольнении или отстранении от исполнения обязанностей, связанных с использованием СКЗИ;

немедленно уведомлять оператора о фактах утраты или недостачи СКЗИ, ключевых документов к ним, ключей от помещений, хранилищ (сейфов), личных печатей и о других фактах, которые могут привести к разглашению защищаемых сведений конфиденциального характера, а также о причинах и условиях возможной утечки таких сведений.

Перечень лиц, прошедших обучение и сдавших зачет по средства криптографической, представлен в таблице 1.

Таблица 3 – Список пользователей СКЗИ

№ п/п	Должность	ФИО	Наименование криптосредства
1	2	3	4

Должность сотрудника ОКЗИ _____ Ф.И.О.
(подпись)

Приложение 5
к политике использования средств
криптографической защиты информации
в государственном бюджетном
профессиональном образовательном
учреждении Краснодарского края
«Славянский электротехнологический
техникум»

ФОРМА

ЖУРНАЛ
поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов (для обладателя конфиденциальной информации)

№ п/п	Наименование СКЗИ, эксплуатационной и технической документации к ним, ключевых документов	Серийные номера СКЗИ, эксплуатационной и технической документации к ним, номера серий ключевых документов	Номера экземпляров (криптографические номера) ключевых документов	Отметка о выдаче		Отметка о подключении (установке СКЗИ)			Отметка об изъятии СКЗИ из аппаратных средств, уничтожении ключевых документов			Примечание
				Ф.И.О. пользователя СКЗИ	дата и расписка в получении	Ф.И.О. работников органа криптографической защиты, пользователя СКЗИ, произведших подключение установку	дата подключения (установки) и подписи лиц, произведших подключение (установку)	номера, аппаратных средств, в которые установлены или к которым подключены СКЗИ	дата изъятия (уничтожения)	Ф.И.О. работников органа криптографической защиты, пользователя СКЗИ, производивших изъятие (уничтожение)	номер акта или расписка об уничтожении	
1	2	3	4	5	6	7	8	9	10	11	12	13

Дата _____20__ г.
Составитель _____ Ф.И.О.
(подпись)

Приложение 6
к политике использования средств
криптографической защиты информации
в государственном бюджетном
профессиональном образовательном
учреждении Краснодарского края
«Славянский электротехнологический
техникум»

ФОРМА

ЖУРНАЛ
поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов (для органа криптографической защиты информации)

№ п/п	Наименование СКЗИ, эксплуатационной и технической документации к ним, ключевых документов	Серийные номера СКЗИ, эксплуатационной и технической документации к ним, номера серий ключевых документов	Номера экземпляров (криптографические номера) ключевых документов	Отметка о получении		Отметка о выдаче		примечание
				от кого получены	дата и номер сопроводительного письма	Ф.И.О. ответственного СКЗИ	дата и расписка в получении	
1	2	3	4	5	6	7	8	9

Дата _____20__ г.
Составитель _____ Ф.И.О.
(подпись)

Приложение 7
к политике использования средств
криптографической защиты информации
в государственном бюджетном
профессиональном образовательном
учреждении Краснодарского края
«Славянский электротехнологический
техникум»

ФОРМА

Технический (аппаратный) журнал

№ п/п	Дата	Тип и серийные номера используемых СКЗИ	Записи по обслуживанию СКЗИ	Используемые криптоключи			Отметка об уничтожении (стирании)		Примечание
				тип ключевого документа	серийный, криптографический номер и номер экземпляра ключевого документа	номер разового ключевого носителя или зоны СКЗИ, в которую введены криптоключи	дата	подпись пользователя СКЗИ	
1	2	3	4	5	6	7	8	9	10

Дата _____20__ г.
Составитель _____ Ф.И.О.
(подпись)

Приложение 8
к политике использования средств
криптографической
защиты информации в
государственном бюджетном
профессиональном образовательном
учреждении Краснодарского края
«Славянский электротехнологический
техникум»

ФОРМА

АКТ №__
уничтожения СКЗИ
государственного бюджетного профессионального
образовательного учреждения Краснодарского края
«Славянский электротехнологический техникум»

Состав комиссии:

Председатель комиссии _____ _____

Члены комиссии _____ _____

_____ _____

Комиссия произвела отбор к уничтожению ключевых документов:

№ п/п	Тип и регистрационный номер СКЗИ	Тип ключевого документа	Серийный номер и номер экземпляра ключевого документа	Номер носителя ключевого документа	Дата регистрации
1	2	3	4	5	6

Всего подлежит уничтожению _____(_____)
наименований документов (цифрами) (прописью)
Ключевые документы уничтожены гарантированным стиранием ключевой информации с ключевого носителя.

Председатель комиссии _____ _____

Члены комиссии _____ _____

_____ _____

Приложение 9
к политике использования средств
криптографической защиты информации
в государственном бюджетном
профессиональном образовательном
учреждении Краснодарского края
«Славянский электротехнологический
техникум»

ФОРМА

ЖУРНАЛ УЧЕТА
хранилищ СКЗИ и ключей от них

Регистрационный номер	Наименование хранилища (сейф, металлический шкаф, кладовая, спец. хранилище)	Заводской, инвентарный номер хранилища	Местонахождение хранилища (подразделение, номер комнаты, корпуса, здания)	Что хранится (СКЗИ, ключевые документы, документация на СКЗИ)	Фамилия ответственного за хранилище	Количество комплектов ключей и их номера	Расписка ответственного за хранилище в получении ключа и дата	Расписка в обратном приеме ключа и дата	Примечание
1	2	3	4	5	6	7	8	9	10

Дата _____20__ г.
Составитель _____ Ф.И.О.
(подпись)

ПРИЛОЖЕНИЕ № 9

УТВЕРЖДЕНА
приказом директора
от 30.12.2023 № 952

ИНСТРУКЦИЯ
администратора информационных систем
государственного бюджетного профессионального
образовательного учреждения Краснодарского края
«Славянский электротехнологический техникум»

1. Общие положения

1.1. Администратор информационных систем является функциональной ролью (наделенной набором функций, требований, прав и обязанностей), назначаемой сотруднику государственным бюджетным профессиональным образовательным учреждением Краснодарского края «Славянский электротехнологический техникум» (далее – ГБПОУ КК СЭТ, техникум).

1.2. Администратор информационных систем назначается приказом директора ГБПОУ КК СЭТ.

1.3. Администратор информационных систем функционально подчиняется руководителю структурного подразделения техникума, в штате которого он состоит.

1.4. На время отсутствия администратора информационных систем его обязанности исполняет лицо, назначенное в установленном порядке соответствующим приказом. 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:

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

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

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»;

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»;

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»;

настоящей инструкцией администратора информационных систем ГБПОУ КК СЭТ (далее – Инструкция);

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

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

1.7. В случае увольнения, администратор информационных систем обязан передать руководителю подразделения, в штате которого он состоит, 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:

обеспечивать настройку программного обеспечения в соответствии с требованиями эксплуатационной документации;

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

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

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

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

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

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);

вести и дополнять (в соответствии с заявками сотрудников техникума) реестр программного обеспечения (далее – Реестр), разрешенного к использованию в информационных системах техникума. 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;

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 техникума, а также, чтобы установка программного обеспечения допускалась только с эталонных копий дистрибутивов;

следить за сроками действия лицензий на программное обеспечение;

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

обеспечивать запрет пользователям на доступ к управлению средствами защиты информации;

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;

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

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

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

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

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

---

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

функционалом Active Directory;

функционалом прикладного программного обеспечения.

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

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

блокировать права доступа в случаях выявления нарушений пользователем требований организационно-распорядительных документов техникума, 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:

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;

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;

обеспечивать процесс ведения перечня информационных ресурсов, подлежащих резервному копированию;

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

обеспечивать сохранность резервных копий;

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

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

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

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

уведомлять непосредственного руководителя 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:

определения степени критичности информационных систем;

определения состава, порядка резервного копирования и восстановления защищаемой информации;

согласования прав доступа пользователей информационных систем.

4.1.2. С администратором информационной безопасности, в части:

согласования прав доступа пользователей информационных систем;

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

составления реестра программного обеспечения, разрешенного к использованию в информационных системах техникума;

содействия в ходе проведения аудита информационной безопасности;

содействия в ходе расследования инцидентов информационной безопасности;

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

информирования его о выявленных нарушениях функционирования средств защиты информации;

информирования его об инцидентах информационной безопасности;

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

согласования процессов установки средств защиты информации;

оказания помощи в выполнении ими своих служебных обязанностей.

4.1.3. Со сторонними организациями при:

проведении ими аттестации информационных систем по требованиям безопасности информации;

выполнении ими работ по заключенным государственным контрактам.

5. Права администратора информационных систем

5.1. Администратор информационных систем имеет право:

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

требовать от руководства оказания содействия в исполнении своих

должностных обязанностей и прав;

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;

вносить предложения руководству по совершенствованию процессов управления информационной безопасностью.

6. Ответственность администратора информационных систем

6.1. Администратор информационных систем несет ответственность за:

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;

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

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

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

ПРИЛОЖЕНИЕ № 10

УТВЕРЖДЕНА
приказом директора
от 30.12.2025 № 952

ИНСТРУКЦИЯ
администратора информационной безопасности государственного бюджетного профессионального образовательного учреждения Краснодарского края «Славянский электротехнологический техникум»

1. Общие положения

1.1. Администратор информационной безопасности является функциональной ролью (определенным набором функций, требований, прав и обязанностей), назначаемой сотруднику государственного бюджетного профессионального образовательного учреждения Краснодарского края «Славянский электротехнологический техникум» (далее – ГБПОУ КК СЭТ, техникум).

1.2. Администратор информационной безопасности назначается приказом директора ГБПОУ КК СЭТ.

1.3. Администратор информационной безопасности функционально подчиняется директору техникума.

1.4. На время отсутствия администратора информационной безопасности (отпуск, болезнь, прочее) его обязанности исполняет лицо, назначенное в установленном порядке соответствующим приказом. 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:

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

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

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»;

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»;

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»;

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»;

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;

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;

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;

настоящей инструкцией администратора информационной безопасности ГБПОУ КК СЭТ (далее - Инструкция);

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

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

1.7. В случае увольнения администратор информационной безопасности обязан передать руководителю подразделения, в штате которого он состоит, 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:

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

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

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), утвержденной директором ГБПОУ КК СЭТ, осуществлять уничтожение съемных носителей информации и дополнительных средств аутентификации в установленных случаях;

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;

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

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 техникума. 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:

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

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;

незамедлительно блокировать учетные записи пользователей в случаях выявления нарушений сотрудником требований организационно-распорядительных документов техникума, 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:

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;

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

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

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);

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

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

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

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);

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;

следить за сроками действия технической поддержки на средства защиты информации;

согласовывать перечни информационных ресурсов, подлежащих

резервному копированию;

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);

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

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;

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:

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

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

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 техникума обязан:

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);

осуществлять планирование и реализацию контрольных мероприятий по проверке степени выполнения политик и правил техникума по обеспечению защиты информации (в т.ч. защите персональных данных);

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;

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

осуществлять посредством функционала средства анализа защищенности

контроль соответствия Реестру разрешенного к использованию в информационных системах техникума, установленному на автоматизированных рабочих местах (далее – АРМ) и серверах информационных систем программного обеспечения;

осуществлять контроль установки обновлений программного обеспечения;

осуществлять контроль устранения выявленных ранее уязвимостей;

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

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

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

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

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

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

регистрировать инциденты информационной безопасности в журнале учета инцидентов;

вести карточки инцидентов информационной безопасности;

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

контролировать сроки локализации и устранения последствий инцидентов информационной безопасности;

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

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:

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;

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

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 техникума в ходе:

разъяснения им возникающих вопросов по функционированию средств защиты информации;

содействия им при устранении последствий вирусных заражений;

проведения аудита информационной безопасности;

расследования инцидентов информационной безопасности.

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

согласования прав доступа пользователей информационных ресурсов (систем);

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

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

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

согласования процессов установки средства защиты информации;

оказания помощи в выполнении ими своих служебных обязанностей;

устранения выявленных уязвимостей.

6.1.3. С ответственным пользователем средств криптографической защиты информации при:

согласовании процессов установки средства криптографической защиты информации;

оказании помощи в выполнении ими своих служебных обязанностей;

устранении выявленных уязвимостей.

6.1.4. Со сторонними организациями при:

проведении ими аттестации информационных систем по требованиям безопасности информации;

выполнении ими работ по заключенным государственным контрактам.

7. Права администратора информационной безопасности

7.1. Администратор информационной безопасности имеет право:

требовать от пользователей безусловного выполнения требований организационно-распорядительных документов техникума, регламентирующих вопросы обеспечения обработки и защиты информации;

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

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

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

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

вносить предложения руководству по совершенствованию процессов управления информационной безопасности.

8. Ответственность администратора информационной безопасности

8.1. Администратор информационной безопасности несет ответственность за:

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;

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

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

неработоспособность или ненадлежащее функционирование средств защиты информации.

ПРИЛОЖЕНИЕ № 11

УТВЕРЖДЕНА
приказом директора
от 30.12.2023 № 952

ИНСТРУКЦИЯ
ответственного пользователя средств
криптографической защиты информации
государственного бюджетного профессионального
образовательного учреждения Краснодарского края
«Славянский электротехнологический техникум»
Одеговой Галины Васильевны

1.

2. Общие положения

1.1. Ответственный пользователь средств криптографической защиты информации (далее - СКЗИ) обладает функциональной ролью (определенным набором функций, требований, прав и обязанностей), назначаемой сотруднику государственного бюджетного профессионального образовательного учреждения Краснодарского края «Славянский электротехнологический техникум» (далее – ГБПОУ КК СЭТ, техникум).

1.2. Ответственный пользователь СКЗИ назначается приказом директора ГБПОУ КК СЭТ.

1.3. На время отсутствия ответственного пользователя СКЗИ (отпуск, болезнь, прочее) его обязанности исполняет лицо, назначенное в установленном порядке соответствующим приказом. Данное ответственное лицо наделяется правами и несет ответственность за надлежащее исполнение возложенных на него обязанностей.

1.4. Ответственный пользователь СКЗИ в своей работе руководствуется следующими нормативными правовыми актами и организационно-распорядительными документами в области обработки и защиты информации:

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;

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»;

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;

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;

политикой использования средств криптографической защиты информации в ГБПОУ КК СЭТ (далее – Политика СКЗИ ГБПОУ КК СЭТ);

настоящей инструкцией ответственного пользователя средств криптографической защиты информации ГБПОУ КК СЭТ (далее – Инструкция);

иными организационно-распорядительными документами, правовыми актами техникума.

1.5. Иные должностные лица техникума по мере необходимости могут быть ознакомлены с основными положениями настоящей Инструкции.

1.6. В случае увольнения, ответственный пользователь СКЗИ обязан передать руководителю подразделения, в штате которого он состоит, все СКЗИ, эксплуатационную и техническую документации к ним, ключевые документы, ключи от помещений и хранилищ, которые находились в его распоряжении в связи с выполнением им служебных обязанностей во время работы.

3. Обязанности в части учета и хранения средств криптографической защиты информации эксплуатационной и технической документации к ним, а также ключевых документов

3.1. Ответственный пользователь СКЗИ в части учета и хранения средств криптографической защиты информации эксплуатационной и технической документации к ним, а также ключевых документов, должен руководствоваться пунктом 3 Политики СКЗИ ГБПОУ КК СЭТ и обязан:

вести поэкземплярный учет СКЗИ, эксплуатационной и технической документации к ним, а также ключевых документов, в соответствии с утвержденной Формой поэкземплярного учета;

выдавать пользователям экземпляры СКЗИ, эксплуатационную и техническую документацию к ним, ключевые документы исключительно под расписку в журнале поэкземплярного учета;

вести аппаратный журнал, в котором учитываются криптоключи, которые вводят и хранят в СКЗИ на весь срок их действия (а также разовые криптоключи) – например, сохраненный в реестре сертификат электронной подписи или набор ключей (dst-файл), который используется для первичной инициализации СКЗИ;

вести журнал учета хранилищ СКЗИ и ключей от них;

хранить дистрибутивы СКЗИ, эксплуатационную и техническую документацию к ним с соблюдением условий, исключающих несанкционированный доступ к ним;

обеспечить безопасное раздельное хранение действующей и резервной ключевой информации;

передавать СКЗИ и криптографические ключи в соответствии с требованиями, установленными Политикой СКЗИ ГБПОУ КК СЭТ.

4. Обязанности в части использования СКЗИ

4.1. Ответственный пользователь СКЗИ в части использования средств криптографической защиты информации обязан:

обеспечивать размещение средств криптографической защиты информации строго в соответствии с требованиями Политики СКЗИ ГБПОУ КК СЭТ;

производить опечатывание/опломбирование программно-аппаратных средств криптографической защиты информации и установку пароля для входа в базовую систему ввода-вывода (BIOS) (при наличии технической возможности), а также следить за сохранностью защитных печатей (пломб);

производить периодический контроль сохранности СКЗИ, а также всего используемого совместно с СКЗИ программного обеспечения для предотвращения внесения программно-аппаратных закладок;

при подозрении о возможности компрометации ключевой информации оперативно осуществлять процедуру смены ключей (в соответствии с установленным порядком);

перед передачей АРМ, на котором установлено программное средство криптографической защиты информации, в ремонт – обеспечить удаление ключевой информации с данного АРМ или изъятие жестких дисков;

при организации и обеспечении работы с СКЗИ и криптографическими ключами руководствоваться формулярами к соответствующим СКЗИ;

участвовать в служебных проверках по фактам нарушения требований по обращению с СКЗИ.

5. Порядок действий при компрометации криптоключей

5.1. При получении сообщения о компрометации ключа пользователя, ответственный пользователь СКЗИ ответным звонком уточняет факт компрометации, и в случае его подтверждения немедленно приостанавливает действие ключа. При наличии резервных ключей, пользователь должен перейти на комплект резервных ключей. Если резервные ключи не были предусмотрены, для восстановления системы необходимо повторно произвести формирование ключа и обеспечить получение новых криптоключей пользователями системы.

6. Обязанности в части уничтожения СКЗИ

6.1. Ответственный пользователь СКЗИ в части уничтожения криптографических ключей должен руководствоваться Политикой СКЗИ ГБПОУ КК СЭТ и обязан:

участвовать в качестве члена комиссии от техникума при уничтожении СКЗИ;

производить отметки об уничтожении СКЗИ в журнале поэкземплярного учета и техническом (аппаратном) журнале;

обеспечить сохранность Актов об уничтожении СКЗИ.

7. Взаимодействие с прочими ответственными лицами

7.1. Ответственный пользователь СКЗИ должен взаимодействовать со следующими ответственными лицами:

7.1.1. Со всеми пользователями СКЗИ ГБПОУ КК СЭТ в ходе разъяснения им возникающих вопросов по функционированию СКЗИ и порядка работы с ними;

7.1.2. С администратором информационных систем и администратором информационной безопасности при:

согласовании процессов установки средства криптографической защиты информации;

оказании помощи в выполнении ими своих служебных обязанностей;

7.1.3. С органом криптографической защиты информации (далее – ОКЗИ) при:

инструктаже пользователей СКЗИ;

проведении ОКЗИ проверки возможности допуска пользователей к самостоятельной работе с СКЗИ;

проведении ОКЗИ проверки о возможности эксплуатации СКЗИ;

разработки мероприятий по обеспечению функционирования и безопасности, применяемых СКЗИ;

расследовании и составлении заключений по фактам нарушения условий использования СКЗИ;

выполнении ОКЗИ иных работ по заключенному государственному контракту.

8. Права ответственного пользователя СКЗИ

8.1. Ответственный пользователь СКЗИ имеет право:

требовать от пользователей СКЗИ безусловного выполнения требований Политики СКЗИ ГБПОУ КК СЭТ;

требовать от пользователей СКЗИ представления письменных объяснений по фактам нарушений требований Политики СКЗИ ГБПОУ КК СЭТ;

вносить обоснованные предложения о привлечении к ответственности пользователей СКЗИ, допустивших нарушение установленных требований Политики СКЗИ ГБПОУ КК СЭТ;

требовать от руководства оказания содействия в исполнении своих

должностных обязанностей и прав;

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

осуществлять плановые и внеплановые проверки пользователей СКЗИ, наличия ключевых документов и технической документации у пользователей (если таковые выдавались);

осуществлять, в рамках своей компетенции, взаимодействие с администратором информационной безопасности и администратором информационных систем;

осуществлять плановые и внеплановые проверки функционирования СКЗИ;

осуществлять, в рамках своей компетенции, взаимодействие с организациями-производителями СКЗИ;

при изменении состава СКЗИ получить профессиональную переподготовку, повышение квалификации и стажировку в порядке, установленном законодательством Российской Федерации.

9. Ответственность ответственного пользователя СКЗИ

9.1. Ответственный пользователь СКЗИ несет ответственность за:

ненадлежащее исполнение или неисполнение своих должностных обязанностей, предусмотренных настоящей Инструкцией, другими регламентирующими документами в соответствии с действующим законодательством Российской Федерации, трудовым законодательством Российской Федерации;

нарушение требований Политики СКЗИ ГБПОУ КК СЭТ;

за полноту и качество проводимых им работ по обеспечению функционирования СКЗИ, находящихся в зоне его ответственности;

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

разглашение сведений конфиденциального характера и другой защищаемой информации техникума, определенных действующим административным, уголовным и гражданским законодательством Российской Федерации.

С инструкцией ознакомлен:

Должность ФИО

ПРИЛОЖЕНИЕ № 12

УТВЕРЖДЕНА
приказом директора
от 30.12.2023 № 952

ПАМЯТКА
пользователя информационных систем государственного бюджетного профессионального образовательного учреждения Краснодарского края «Славянский электротехнологический техникум»

1. Пользователь автоматизированного рабочего места (персонального компьютера) содержит предоставленное ему автоматизированное рабочее место (далее – АРМ) и другую вычислительную и оргтехнику в хорошем техническом, гигиеническом и технологическом состоянии, следит за чистотой на компьютерном рабочем месте, не допускает наличие пыли на компьютерном оборудовании, вокруг него и под ним, уделяя особое внимание бесперебойности его работы.

2. Каждый работник, обеспеченный АРМ, получает аутентификационную информацию (персональное сетевое имя (имя пользователя), пароль), адрес электронной почты (в случае необходимости).

3. После получения доступа к информационной системе пользователь при первом входе в систему должен сменить пароль доступа (в случае наличия технической возможности) на пароль, удовлетворяющий требованиям Политики использования аутентификационной информации при доступе к информационным ресурсам и системам государственного бюджетного профессионального образовательного учреждения Краснодарского края «Славянский электротехнологический техникум» (далее – ГБПОУ КК СЭТ, техникум. Также смена пароля должна осуществляться в случае его компрометации.

4. Пользователь не должен допускать многократного ввода неправильного пароля и блокировки своих учётных записей.

5. Пользователь обязан следить за сроком действия паролей и своевременно производить их смену, а в случае отсутствия технической возможности – обращаться к Администратору информационных систем.

6. Пользователь обязан хранить в секрете персональные пароли доступа к информационным активам и не передавать их другим лицам (за исключением случаев, предусмотренных Политикой использования аутентификационной информации при доступе к информационным ресурсам и системам техникума).

7. Хранение пользователем аутентификационной информации (хранящейся на носителе) допускается только в личном сейфе (запираемом шкафу, ящике). При этом носитель должен быть упакован в отдельный опечатанный конверт.

8. Работа с информационными ресурсами (системами) пользователям разрешена только на закреплённых за ними АРМ, в определенное время и только с разрешённым программным обеспечением и сетевыми ресурсами.

9. Самостоятельная установка и (или) обновление пользователем программного обеспечения на АРМ запрещена. Установка и удаление любого программного обеспечения производится только ответственными сотрудниками.

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

11. Самостоятельное изменение пользователем состава локально-вычислительной сети (подключение/отключение АРМ, подключение/ отключение коммутаторов, маршрутизаторов, сетевых модемов) запрещено. Изменение состава локально-вычислительной сети осуществляется уполномоченными сотрудниками.

12. АРМ подлежат опечатыванию/опломбированию. Опечатывание осуществляется ответственными сотрудниками. Пользователь АРМ обязан следить за сохранностью данных пломб и в случае их нарушений сообщать о данном факте администратору информационной безопасности.

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

14. Пользователь не должен каким-либо образом препятствовать функционированию (в том числе обновлению) средства защиты информации и принимать попытки по их деактивации.

15. Пользователь обязан обеспечить резервное копирования служебных данных, располагающихся на своих АРМ, вне сетевых файловых хранилищ. Резервное хранение таких данных осуществляется только на учтённые съёмные носители информации.

16. Пользователю АРМ запрещается:

подключать и отключать электропитание АРМ и другой вычислительной и оргтехники без ведома уполномоченных лиц;

включать в компьютерную сеть электропитания бытовые электрические приборы, а также другое электрооборудование, не относящееся к вычислительной и оргтехнике, ЛВС;

использовать носители информации, имеющие видимые повреждения, либо не проверенные на наличие вирусов;

загромождать АРМ и другую вычислительную и оргтехнику посторонними предметами;

располагать системный блок в недоступных для обслуживания местах, в местах с плохим воздухообменом, а также в местах, способствующих запылению и перегреву вентилирующих устройств;

использовать для принтеров и многофункциональных устройств помятую или не предназначенную для них бумагу;

допускать попадание влаги и посторонних предметов в монитор, системный блок АРМ, принтер, многофункциональное устройство, клавиатуру, манипулятор мышь;

выполнять чистку включённых АРМ и оргтехники, чистить АРМ и оргтехнику моющими средствами, не предназначенными для этих целей (спиртом, ацетоном, бензином и другими);

открывать системный блок АРМ или разбирать какое-либо оборудование, относящееся к вычислительной технике, оргтехнике и ЛВС;

нарушать гарантийные пломбы (наклейки) на компьютере, мониторе, принтере, многофункциональном устройстве и любом другом компьютерном или сетевом оборудовании.

17. Передача пользователем файлов как внутри техникума, так и во внешние информационные системы производится с использованием учтённых съёмных носителей информации, а также посредством общих папок, средств электронной почты. Иные способы передачи запрещены.

18. Порядок использования электронной почты:

18.1. Пользователь имеет право на просмотр либо иное использование в интересах техникума сообщений служебной электронной почты, которые направлены ему или получены им, соответственно с его адреса или на его адрес электронной почты.

18.2. Любые сообщения служебной электронной почты могут быть прочитаны, использованы в интересах техникума, либо удалены уполномоченными на это сотрудниками.

18.3. При работе с электронной почтой пользователь должен учитывать следующие принципиальные положения:

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

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

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

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

18.5. Пользователю запрещается использовать сторонние сервисы электронной почты (mail.ru, yandex.ru, gmail.com и другие).

18.6. Пользователю 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 сотрудника.

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

необходимо избегать перехода по ссылкам, содержащимся во входящих электронных сообщениях, полученных из недостоверных источников;

открывать вложения электронной почты, полученные из недостоверных источников;

проверять адреса отправителей электронной почты с целью предотвращения подделки адреса отправителя путём замены адреса на схожий, но с подменными символами (например, путём замены букв цифрами – замена «ivanov@mail.ru» на «ivanov@ma11.ru», где вместо буквы «i» используется цифра «1»);

проверять ссылки на интернет-ресурсы в целях предотвращения подделки адреса Интернет-ресурса путём замены адреса на схожий, но с подменными символами (например, путём замены букв цифрами – замена «www.google.com» на «www.g00gle.com», где вместо буквы «о» используется цифра «0»);

проверять расширения вложенных файлов, при этом особое внимание следует обращать на так называемые «исполняемые файлы» с расширением «.exe», «.js», «.cmd», «.bat».

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

19. Порядок работы в сети Интернет:

19.1. Доступ к сети Интернет предоставляется пользователю только в целях выполнения им своих служебных обязанностей, требующих непосредственного подключения к внешним информационным ресурсам и (или) повышения эффективности выполнения ими своих служебных обязанностей.

19.2. Пользователю запрещается:

использовать предоставленный доступ в сеть Интернет в личных целях;

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

публиковать, загружать и распространять материалы, содержащие конфиденциальную информацию, за исключением случаев, когда это входит в служебные обязанности, и способ передачи является безопасным и заранее согласован с администратором информационной безопасности;

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

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

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;

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 противоправных действий и так далее;

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;

использование анонимных прокси-серверов;

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

20. Порядок использования съёмных носителей информации.

20.1. Под съёмными носителями информации понимаются оптические диски, флэш-накопители, внешние накопители на жёстких дисках и иные устройства хранения информации.

20.2. Под использованием съёмных носителей информации понимается их подключение к инфраструктуре АРМ и серверам с целью приёма/передачи информации.

20.3. Допускается использование только учтённых носителей информации, которые являются собственностью ГБПОУ КК СЭТ и подвергаются регулярной ревизии и контролю.

20.4. Хранение съёмных носителей информации должно осуществляться в сейфах, запираемых металлических шкафах.

20.5. Пользователь обязан:

использовать носители информации исключительно для выполнения своих служебных обязанностей;

обеспечивать физическую безопасность носителей информации всеми разумными способами.

20.6. При использовании съёмных носителей информации запрещено:

использовать носители информации в личных целях;

передавать носители информации другим лицам;

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

20.7. Любое взаимодействие (обработка, приём/передача информации) с информационными системами посредством использования неучтённых (личных) носителей информации, рассматривается как несанкционированное (за исключением случаев, заранее оговорённых и согласованных с администратором информационной безопасности).

21. Пользователь должен обеспечивать меры, исключающие ознакомление посторонних лиц с защищаемой информацией. Такими мерами являются:

размещение мониторов, исключающее или существенно затрудняющее просмотр отображаемой информации;

размещение документации на бумажных носителях, содержащих служебную информацию, исключающее просмотр информации на них (документация убирается в папки, ящики тумбочек/столов либо переворачивается лицевой стороной вниз, либо накрывается сверху непрозрачными объектами, закрывающими область текста).

22. Пользователь должен осуществлять проверку получаемой и передаваемой информации на предмет наличия компьютерных вирусов и другого вредоносного программного обеспечения.

23. Пользователь должен обеспечивать содействие членам комиссии по обеспечению информационной безопасности в ходе проведения аудита, а также сторонним организациям, проводящим аттестацию информационных систем по требованиям безопасности информации.

24. Пользователь должен информировать администратора информационной безопасности о следующих инцидентах информационной безопасности и событиях безопасности информации (имеющих признаки инцидента):

компрометация пароля;

нарушение пломбы АРМ;

сбои в работе средств защиты информации;

вирусное заражение;

хищение/утрата носителя информации;

нарушение установленных политик безопасности и так далее.

25. Пользователь должен выполнять указания администратора информационной безопасности.

26. Пользователь должен незамедлительно предоставлять АРМ администратору информационной безопасности, администратору информационного ресурса (системы) для контроля, а также в экстренных случаях (нестабильность в работе ЛВС, угроза вирусного заражения, несанкционированного доступа к информации).

Приложение 1
к Памятке пользователя
информационных систем
государственного бюджетного
профессионального образовательного
учреждения Краснодарского края
«Славянский электротехнологический
техникум»

ЛИСТ ОЗНАКОМЛЕНИЯ
с Памяткой пользователя информационных систем
государственного бюджетного профессионального
образовательного учреждения Краснодарского края
«Славянский электротехнологический техникум»

Подписывая настоящий лист ознакомления с Памяткой пользователя информационных систем государственного бюджетного профессионального образовательного учреждения Краснодарского края «Славянский электротехнологический техникум» (далее – ГБПОУ КК СЭТ, техникум), я подтверждаю факт ознакомления с Политиками и Правилами техникума по обеспечению защиты информации (в том числе защите персональных данных), в следующем составе:

Политика использования информационных активов ГБПОУ КК СЭТ;

Политика антивирусной защиты информации ГБПОУ КК СЭТ;

Политика использования аутентификационной информации при доступе к информационным ресурсам и системам ГБПОУ КК СЭТ;

Политика обеспечения отказоустойчивости информационных систем ГБПОУ КК СЭТ;

Политика аудита информационной безопасности ГБПОУ КК СЭТ;

Политика управления событиями безопасности информации ГБПОУ КК СЭТ;

Политика использования средств криптографической защиты информации ГБПОУ КК СЭТ;

Политика сетевой безопасности ГБПОУ КК СЭТ;

Правила обработки персональных данных в ГБПОУ КК СЭТ;

Правила рассмотрения запросов субъектов персональных данных или их представителей в ГБПОУ КК СЭТ;

Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных ГБПОУ КК СЭТ;

Правила доступа в помещения техникума, в которых ведётся обработка защищаемой информации, в том числе персональных данных.

Обязуюсь исполнять требования указанных выше Политик и Правил в части, меня касающейся.

№ п/п	Ф.И.О., должность	Дата ознакомления	Подпись
1	2	3	4
1.			
2.			
3.			
4.			
5.			
6.			
7.			
8.			
9.			
10.			
11.			
12.			
13.			
14.			
15.			
16.			