Министерство образования Кировской области

Кировское областное государственное

профессиональное образовательное бюджетное учреждение

«Вятский колледж профессиональных технологий, управления и сервиса»

(КОГПОБУ «ВятКТУиС»)

УТВЕРЖДАЮ

Директор колледжа

_____ Т.Ф. Корепанова

«29» декабря 2015 г.

П О Л И Т И К А

конфиденциальности и информационной безопасности

в КОГПОБУ«ВятКТУиС»

Киров

2015

В настоящем документе используются следующие термины и их определения.

Автоматизированная система – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Безопасность персональных данных – состояние защищенности персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных.

Вирус (компьютерный, программный) – исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению.

Вредоносная программа – программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных.

Доступ к информации – возможность получения информации и ее использования.

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Информационная система персональных данных (ИСПДн) – информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

Информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Использование персональных данных – действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические

последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц.

Источник угрозы безопасности информации – субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации.

Конфиденциальность персональных данных – обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания.

Неавтоматизированная обработка персональных данных – обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы, считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.

Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных.

Носитель информации – физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

Обработка персональных данных – действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

Оператор (персональных данных) – государственный орган, муниципальный орган, юридическое или физическое лицо, организующее и (или) осуществляющее обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

Персональные данные – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

Политика «чистого стола» – комплекс организационных мероприятий, контролирующих отсутствие записывания на бумажные носители ключей и атрибутов доступа (паролей) и хранения их вблизи объектов доступа.

Пользователь информационной системы персональных данных – лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования.

Правила разграничения доступа – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

Угрозы безопасности персональных данных – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.

Целостность информации – способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

Обозначения и сокращения

АВС – антивирусные средства
АРМ – автоматизированное рабочее место
ИБ – информационная безопасность
ИСПДн – информационная система персональных данных
КЗ – контролируемая зона
НСД – несанкционированный доступ
ПДн – персональные данные
ПО – программное обеспечение
СЗИ – средства защиты информации
СКЗИ – средства криптографической защиты информации
УБПДн – угрозы безопасности персональных данных
ЭЦП– электронная цифровая подпись

1. Общие положения

Правовую основу настоящей Политики составляют законы Российской Федерации и другие законодательные акты, определяющие права и ответственность граждан, сотрудников и государства в сфере безопасности, а также нормативные, отраслевые и ведомственные документы, по вопросам безопасности информации, утвержденные органами государственного управления различного уровня в пределах их компетенции.

Целью настоящей Политики является обеспечение безопасности объектов защиты колледжа от всех видов угроз, внешних и внутренних, умышленных и непреднамеренных, минимизация ущерба от возможной реализации угроз безопасности.

1. Задачами настоящей политики являются:

1) описание организации системы управления информационной безопасностью в колледже;

2) определение Политик информационной безопасности, а именно:

-Парольная политика

-Антивирусная политика

-Политика защиты АРМ

-Политика безопасности при работе с электронной почтой

-Политика безопасности при работе в сети Интернет

-Политика безопасности при архивировании, восстановлении и резервном копировании

-Политика безопасности при работе с криптографическими средствами защиты информации и Электронной цифровой подписью

-Политика безопасности ИСПДн в нештатных ситуациях (чрезвычайных ситуациях)

3) регламентация

-Порядка доступа сотрудников техникума в помещение, в котором ведется обработка персональных данных

-Порядка хранения и обращения материальных носителей

Информационная безопасность (ИБ) состоит из трех основных компонентов:

а) конфиденциальность: защита конфиденциальной информации от несанкционированного раскрытия или перехвата;

б) целостность: обеспечение точности и полноты информации и компьютерных программ;

в) доступность: обеспечение доступности информации и жизненно важных сервисов для пользователей, когда это требуется.

3) Управление информационной безопасностью позволяет коллективно использовать информацию, обеспечивая при этом ее защиту и защиту вычислительных ресурсов.

Общее руководство обеспечением ИБ осуществляет директор колледжа. Ответственность за организацию мероприятий по обеспечению ИБ и контроль за соблюдением требований ИБ несет сотрудник, отвечающий за функционирование автоматизированной системы и выполняющий функции администратора безопасности (далее администратор безопасности). Руководители структурных подразделений учреждения ответственны за обеспечение выполнения требований ИБ в своих подразделениях.

4) Настоящий документ закрепляет основные организационные решения по управлению информационной безопасностью в сетях колледжа и определяет основные меры по защите информации, описывает цели и задачи информационной безопасности, определяет совокупность правил, требований и руководящих принципов в области ИБ, которыми руководствуется учреждение в своей деятельности, а также устанавливает должностных лиц, являющихся ответственными за реализацию политики ИБ и поддержание ее в актуальном состоянии.

Требования настоящей Политики обязательны для выполнения всеми должностными лицами колледжа.

Для сотрудников колледжа требования данного документа, в части их касающейся, должны быть зафиксированы в их должностных инструкциях и трудовых договорах.

2. Основные принципы обеспечения информационной безопасности в учреждении

Общие принципы безопасного функционирования учреждения подразумевают:

- Постоянный и всесторонний анализ информационного пространства с целью выявления уязвимостей информационных активов.

- *Своевременность обнаружения проблем,* потенциально способных повлиять на ИБ колледжа, корректировка моделей угроз и нарушителя

- *Прогнозируемость развития проблем*. Учреждение должно выявлять причинно-следственную связь возможных проблем и строить на этой основе точный прогноз их развития.

- *Адекватность защитных мер.* Разработка и внедрение защитных мер, адекватных характеру выявленных угроз, с учетом затрат на их реализацию. При этом меры, принимаемые для обеспечения ИБ, не должны усложнять

достижение целей, а также повышать трудоемкость технологических процессов обработки

- *Эффективность защитных мер.* Учреждение должно эффективно реализовывать принятые защитные меры.

- *Использование опыта при принятии и реализации решений.* Учреждение должно накапливать, обобщать и использовать как свой опыт, так и опыт других организаций на всех уровнях принятия решений и их исполнения.

- *Непрерывность принципов безопасного функционирования*. Учреждение должно обеспечивать непрерывность реализации принципов безопасного функционирования.

- *Контролируемость защитных мер.* Учреждение должно применять только те защитные меры, правильность работы которых может быть проверена, при этом учреждение должно регулярно оценивать адекватность защитных мер и эффективность их реализации с учетом влияния защитных мер на функционирование учреждения.

Специальные принципы обеспечения ИБ учреждения подразумевают:

- *Определенность целей.* Функциональные цели и цели ИБ Учреждения должны быть явно определены во внутреннем документе. Неопределенность приводит к “расплывчатости” организационной структуры, ролей персонала, политик ИБ и невозможности оценки адекватности принятых защитных мер.

- *Персонификация и адекватное разделение ролей и ответственности*. Учреждение должно обладать информацией о своих сотрудниках, тщательно подбирать персонал. Ответственность должностных лиц учреждения за решения, связанные с обработкой информации, должна быть персонифицирована. Она должна быть адекватной и фиксироваться в положениях, контролироваться и совершенствоваться.

- *Адекватность ролей функциям и процедурам и их сопоставимость с критериями и системой оценки.* Роли должны адекватно отражать исполняемые функции и процедуры их реализации, принятые в учреждении. При назначении взаимосвязанных ролей должна учитываться необходимая последовательность их выполнения. Роль должна быть согласована с критериями оценки эффективности ее выполнения. Основное содержание и качество исполняемой роли реально определяются применяемой к ней системой оценки.

- *Наблюдаемость и оцениваемость обеспечения ИБ*. Любые предлагаемые защитные меры должны быть устроены так, чтобы результат их применения был явно наблюдаем (прозрачен) и мог быть оценен подразделением организации, имеющим соответствующие полномочия.

3. Основные направления обеспечения информационной безопасности учреждения

В качестве основных направлений обеспечения информационной безопасности учреждения следует рассматривать:

- обеспечение информационной безопасности при ведении делопроизводства и осуществлении документооборота (как бумажного, так и электронного);
- обеспечение информационной безопасности при обработке информации в автоматизированной системе учреждения и информационных системах по бухгалтерским операциям;
- обеспечение информационной безопасности при осуществлении взаимодействия с пациентами;
- обеспечение информационной безопасности при проведении работ по созданию (модернизации) информационных систем учреждения;
- обеспечение информационной безопасности при соблюдении правовых и договорных требований;
- обеспечение информационной безопасности в условиях чрезвычайных ситуаций.

4. Сведения, являющие конфиденциальными

Сведения, отнесенные к категории ограниченного доступа	Основания отнесения сведений к категории ограниченного доступа
Коммерческая тайна	Федеральный закон от 29.07.2004 N 98-ФЗ "О коммерческой тайне"
	Статья 1465 Гражданского кодекса РФ (часть четвертая)
Конфиденциальность персональных данных (любой информации, относящейся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных))	Статья 7 Федерального закона от 27.07.2006 N 152-ФЗ "О персональных данных"
Тайна страхования	Статья 32 Федерального закона от 24.07.2009 N 212-ФЗ "О страховых взносах в Пенсионный фонд Российской Федерации, Фонд социального страхования Российской Федерации, Федеральный фонд обязательного медицинского страхования"
Тайна усыновления	Статья 139 Семейного кодекса РФ
Конфиденциальность информации,	Статья 5 Федерального закона от 27.07.2010 N 193-

относящейся к процедуре медиации	ФЗ "Об альтернативной процедуре урегулирования споров с участием посредника (процедуре медиации)"
Конфиденциальность информации, предоставляемой организациям (гражданам), осуществляющим производство и выпуск средств массовой информации	Статья 41 Закона РФ от 27.12.1991 N 2124-1 "О средствах массовой информации"
Ограничение доступа к информации, содержащейся в контрольных измерительных материалах, используемых при проведении государственной итоговой аттестации	Статья 59 Федерального закона от 29.12.2012 N 273-ФЗ "Об образовании в Российской Федерации"
Конфиденциальность сведений, содержащихся в индивидуальных лицевых счетах застрахованных лиц в системе обязательного пенсионного страхования	Статья 6 Федерального закона от 01.04.1996 N 27-ФЗ "Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования"
Ограничение доступа к первичным статистическим данным, содержащимся в формах федерального статистического наблюдения	Статья 9 Федерального закона от 29.11.2007 N 282-ФЗ "Об официальном статистическом учете и системе государственной статистики в Российской Федерации"

5. Основные подходы к решению проблемы защиты информации

Подходы к решению проблемы защиты информации в техникуме, в общем виде, сводятся к исключению неправомерных или неосторожных действий со сведениями, относящимися к информации ограниченного распространения, а также с информационными ресурсами, являющимися критичными для обеспечения функционирования процессов учреждения.

Для этого в колледже выполняются следующие мероприятия:

5) устанавливается круг лиц и порядок доступа к подобной информации;
6) вырабатываются меры по контролю обращения с документами, содержащими конфиденциальные сведения;
7) включаются в трудовые договоры с сотрудниками обязательства о неразглашении конфиденциальных сведений и определяются санкции за нарушения порядка работы с ними и их разглашение.

Форма подписки о неразглашении сведений конфиденциального характера подписывается при заключении трудового договора, который подписывается всеми сотрудниками учреждения при приеме на работу. Персональные данные сотрудника учреждения – информация, необходимая

работодателю в связи с трудовыми отношениями и касающаяся конкретного сотрудника.

Согласно Ст. 86 п.7 Трудового кодекса РФ защита персональных данных сотрудника от неправомерного их использования или утраты должна быть обеспечена работодателем за счет его средств в порядке, установленном федеральным законом.

Согласно Ст.88 Трудового кодекса РФ при передаче персональных данных сотрудника работодатель должен соблюдать следующие требования:

8) осуществлять передачу персональных данных сотрудника в пределах одной организации в соответствии с локальным нормативным актом организации, с которым сотрудник должен быть ознакомлен под расписку;
9) разрешать доступ к персональным данным сотрудников только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные сотрудника, которые необходимы для выполнения конкретных функций.

Согласно Ст.90 Трудового кодекса РФ лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных сотрудника, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с федеральными законами.

6. Парольная политика

6.1.Правила формирования пароля

- Персональные пароли должны выбираться пользователями информационной системы самостоятельно с учетом следующих требований:
- длина пароля должна быть не менее 8 символов;
- в составе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (“ ~ ! @ # $ % ^ & * ( ) - + _ = \ | / ? ,);
- при смене пароля новое значение должно отличаться от предыдущего не менее чем в 4 позициях;
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, известные названия, словарные и жаргонные слова и т.д.), последовательности символов и знаков (111,, abcd и т.д.), общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.), аббревиатуры, клички домашних животных, номера автомобилей, телефонов и другие значимые сочетаний букв и знаков, которые можно угадать, основываясь на информации о пользователе.

6.2.Ввод пароля

- Ввод пароля осуществляется непосредственно пользователем информационной системы.
- При вводе пароля пользователю необходимо исключить возможность его подсматривания посторонними лицами (человек за спиной, наблюдение человеком за движением пальцев в прямой видимости или в отраженном свете) и техническими средствами (стационарными и встроенными в мобильные телефоны видеокамерам и т.п.).
- При вводе пароля пользователю запрещается проговаривать вслух вводимые символы.
- символы вводимого пароля не отображаются на экране в явном виде;
- учёт всех попыток (успешных и неудачных) входа в систему.
- Пользователю запрещается передавать пароль для ввода другим лицам. Передача пароля для ввода другим лицам является разглашением конфиденциальной информации и влечёт за собой установленную ответственность.

6.3.Порядок смены паролей

- Смена паролей должна проводится регулярно, не реже одного раза в год.
- В случае прекращения полномочий пользователя (увольнение, либо переход на другую работу) производится немедленное удаление его паролей.
- Срочная (внеплановая) полная смена паролей должна производится в случае прекращения полномочий (увольнение или переход на другую работу) администраторов информационной системы и других сотрудников, которым по роду работы были предоставлены полномочия по управлению системой парольной защиты. Кадровая служба должна известить Администратора безопасности о состоявшемся приказе в течение 24 часов после увольнения, перевода работника.
- Смена пароля производится системным администратором в соответствии с п.3.1 настоящей инструкции.

Администратор ведет Журнал по учету нештатных ситуаций ПЭВМ, работающих с конфиденциальной информацией, принудительной смены паролей, выполнения профилактических работ, установки и модификации программных средств на компьютерах ИСПДн, в котором отмечает причины внеплановой смены паролей пользователей.

Временный пароль, заданный администратором при регистрации нового пользователя, следует изменить при первом входе в систему.

6.4. Хранение пароля

Запрещается

-записывать пароли на бумаге, в файле, электронной записной книжке и других носителях информации, в том числе на предметах («Политика чистого стола»).

-сообщать другим пользователям личный пароль и регистрировать их в системе под своим паролем.

Хранение пользователем своего пароля на бумажном носителе допускается только в личном, опечатанном владельцем пароля сейфе, либо в сейфе у Администратора безопасности в опечатанном печатью конверте.

6.5.Действия в случае утери и компрометации пароля

В случае утери или компрометации пароля пользователя должны быть немедленно предприняты меры в соответствии с п.3.3 или п.3.4 в зависимости от полномочий владельца скомпрометированного пароля.

6.6.Ответственность при организации парольной защиты

Владельцы паролей должны быть ознакомлены под роспись с перечисленными выше требованиями и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение парольной информации.

Ответственность за организацию парольной защиты возлагается на администратора безопасности.

Периодический контроль за соблюдением требований парольной политики возлагается на Ответственного за организацию защиты персональных данных.

7. Антивирусная политика

7.1. Общие положения

Политика антивирусной защиты определяет требования к организации защиты информационно-вычислительной сети (далее –ИВС) от вредоносных программ, с целью предотвращения потери (искажения, перехвата) информации, заражения программного обеспечения, перегрузки и повреждения оборудования ИВС.

Политика является руководящим документом, единым для всех подразделений колледжа, обязательным для выполнения всеми работниками.

К объектам антивирусной защиты относятся:

- Серверы ИВС;

- Компьютеры (ноутбуки), принадлежащие колледжу, подключенные или периодически подключаемые к ИВС;

- Компьютеры (ноутбуки), принадлежащие техникуму, не подключенные к ИВС, но по специфике их использования предполагается копирование (перенос) информации, содержащейся в них, на ресурсы ИВС или обратно;

- Шлюз (шлюзы), соединяющий ИВС с сетью Интернет и другими сетями;

- Корпоративная система электронной почты.

7.2. Организация защиты

7.2.1. К использованию в колледже допускается сетевой лицензионный антивирус Kaspersky Workstation, установленный на АРМ.

По умолчанию обеспечивается базовый уровень безопасности, при котором задействованы следующие модули:

a. Файловый Антивирус: уровень безопасности-высокий

метод проверки-эвристический анализ (поверхностный)

режим проверки-интеллектуальный

действия над вредоносными программами: лечить; удалить, если лечение невозможно

b. Почтовый антивирус: уровень безопасности-высокий

область защиты-входящие и исходящие сообщения

метод проверки-эвристический анализ (средний)

действия над вредоносными программами: лечить; удалить, если лечение невозможно

c. Веб-антивирус уровень безопасности-высокий

метод проверки-эвристический анализ (средний)

действие – запретить загрузку

7.2.2. Доступ в сеть Интернет и локальным сетевым ресурсам предоставляется только при наличии на АРМ лицензионного антивируса Kaspersky Workstation в связи с высоким риском заражения компьютерными вирусами и программами разрушающего воздействия. Наличие корректно функционирующего антивируса Kaspersky Workstation автоматически проверяется аппаратно-программными средствами при подключении к локальной сети.

Запрещено использование сторонних средств антивирусной защиты.

Запрещено удаление антивируса Kaspersky Workstation и изменение настроек.

Разрешено использование функционала антивируса Kaspersky Workstation для проверки личных носителей данных.

7.3. В случае невыполнения требований пункта 7.2.2 доступ в локальную вычислительную сеть колледжа должен быть приостановлен до устранения несоответствий. Одновременно с этим должен быть оповещен руководитель подразделения, в котором работает пользователь АРМ, о несоблюдении политики антивирусной защиты.

7.4. Установка антивируса Kaspersky Workstation на компьютерах (серверах) осуществляется системным администратором в соответствии с «Памяткой для установки/обновления антивируса Kaspersky Workstation.». Управление настройками параметров антивируса Kaspersky Workstation осуществляется системным администратором и самостоятельному изменению не подлежит.

В колледже практикуется автоматическая установка обновлений антивирусного программного обеспечения, в том числе антивирусной фильтрации трафика электронного почтового обмена.

8. Политика защиты АРМ

Политика защиты АРМ устанавливает следующие правила:

8.1. Во время работы с конфиденциальной информацией должен предотвращаться ее просмотр не допущенными к ней лицами.

8.2. При любом оставлении рабочего места, рабочая станция должна быть заблокирована, съемные машинные носители, содержащие конфиденциальную информацию, заперты в помещении, шкафу или ящике стола или в сейфе.

8.3. Несанкционированное использование печатающих, факсимильных, копировально-множительных аппаратов и сканеров должно предотвращаться путем их размещения в помещениях с ограниченным доступом, использования паролей или иных доступных механизмов разграничения доступа.

8.4. Доступ к компонентам операционной системы и командам системного администрирования на рабочих станциях пользователей ограничен. Право на доступ к подобным компонентам предоставлено только администратору безопасности. Конечным пользователям предоставляется доступ только к тем командам, которые необходимы для выполнения их должностных обязанностей.

Доступ к информации предоставляется только лицам, имеющим обоснованную необходимость в работе с этими данными для выполнения своих должностных обязанностей.

8.5. Пользователям запрещается устанавливать неавторизованные программы на компьютеры.

Конфигурация программ на компьютерах должна проверяться ежемесячно на предмет выявления установки неавторизованных программ.

Техническое обслуживание должно осуществляться только на основании обращения пользователя к администратор безопасности.

Локальное техническое обслуживание должно осуществляться только в личном присутствии пользователя.

При проведении технического обслуживания должен выполняться минимальный набор действий, необходимых для устранения проблемы, явившейся причиной обращения, и использоваться любые возможности, позволяющие впоследствии установить авторство внесенных изменений.

8.6. Копирование конфиденциальной информации и временное изъятие носителей конфиденциальной информации (в том числе в составе АРМ) допускаются только с санкции пользователя. В случае изъятия носителей, содержащих конфиденциальную информацию, пользователь имеет право присутствовать при дальнейшем проведении работ.

8.7. Программное обеспечение должно устанавливаться со специальных ресурсов или съемных носителей и в соответствии с лицензионным соглашением с его правообладателем.

Конфигурации устанавливаемых рабочих станций должны быть стандартизованы, а процессы установки, настройки и ввода в эксплуатацию - регламентированы.

8.8. АРМ, на которых предполагается обрабатывать конфиденциальную информацию, должны быть закреплены за соответствующими сотрудниками Управления. Запрещается использование указанных АРМ другими пользователями без согласования с администратором безопасности. При передаче указанного АРМ другому пользователю, должна производиться гарантированная очистка диска (форматирование).

Администратор безопасности вправе отказать в устранении проблемы, вызванной наличием на рабочем месте программного обеспечения или оборудования, установленного или настроенного пользователем в обход действующей процедуры.

9. Порядок доступа сотрудников техникума в помещение, в котором ведется обработка персональных данных

9.1. Сотрудники колледжа, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено Федеральными законами.

9.3. Обеспечение безопасности персональных данных от уничтожения, изменения, блокирования, копирования, распространения, а также от иных

неправомерных действий в отношении персональных данных достигается, в том числе, соблюдением правил доступа в помещения, где обрабатываются персональные данные в информационной системе персональных данных и без использования средств автоматизации.

9.4. Размещение информационных систем, в которых обрабатываются персональные данные, осуществляется в кабинетах бухгалтерии, приемной директора техникума. В помещениях, в которых обрабатываются персональные данные, организуется режим обеспечения безопасности, при котором обеспечивается сохранность носителей персональных данных и средств защиты информации, а также исключается возможность неконтролируемого проникновения и пребывания в этих помещениях посторонних лиц.

9.5. При хранении материальных носителей персональных данных должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный доступ к ним.

9.6. В помещения, где размещены технические средства, позволяющие осуществлять обработку персональных данных, а также хранятся носители информации, допускаются только ответственные сотрудники КОГПОБУ «ВятКТУиС», наделенные полномочиями обработки персональных данных. Посторонние посетители допускаются только в присутствии сотрудников КОГПОБУ «ВятКТУиС».

9.7. Ответственным за организацию доступа в помещения КОГПОБУ «ВятКТУиС», в которых ведется обработка персональных данных, является ответственный за обработку персональных данных.

9.8. Внутренний контроль за соблюдением порядка доступа в помещение, в котором ведется обработка персональных данных, проводится лицом, ответственным за организацию обработки персональных данных.

10. Политика безопасности при работе с электронной почтой

Данная политика безопасности применяется к любому письму, отправляемого или получаемого посредством системы корпоративной электронной почты колледжа.

В соответствии с требованием п.8.7.4. «Безопасность электронной почты» ГОСТ Р ИСО/МЭК ТО 177799 – 2005 устанавливаются следующие правила:

10.1. Электронная почта используется только для выполнения работником его служебных обязанностей.

10.2. В техникуме предполагается использование корпоративной электронной почты. Работа с другими сервисами электронной почты допускается только при согласовании с системным администратором.

Любое почтовое сообщение, включая вложения, созданное, отправленное или принятое с использованием корпоративной системы электронной почты – принадлежит колледжу, не конкретному пользователю.

Техникум оставляет за собой право получать доступ к любому письму, посланному или принятому с использованием корпоративной электронной почты, без дополнительного уведомления пользователя.

10.3. Запрещается

-рассылка цепных сообщений, спама, исполняемых файлов, файлов развлекательного характера.

-использование электронной почты колледжа для любой деятельности с целью получения личной материальной выгоды.

-пересылка и получение электронной почты, содержащей лицензионное программное обеспечение и другие действия, позволяющие обойти лицензионные соглашения или нарушить авторские права

-посылать письма, содержащие конфиденциальную информацию.

-создание и пересылка зашифрованных писем или писем, содержащих шифрованные участки, вложения, а также предпринимать любые другие действия затрудняющие анализ тела письма и его вложений.

-создавать, отсылать письма дискредитирующей кого-либо информации, непристойного или вызывающего содержания, которая может быть воспринята, как преследование или умаление; в случае получения такого письма пользователем, оно должно быть немедленно удалено.

10.4. При работе с электронной почтой на компьютере обязательно должно быть установлено антивирусное программное обеспечение.

10.5. Запрещается использование чужих адресов электронной почты, а также разрешение использования своего адреса кому-либо еще.

10.6. При получении письма с вложением, каждый пользователь должен следовать процедуре, описанной в данной политике безопасности.

10.7.Контроль за исполнением данной политики безопасности выполняет ответственный за информационную безопасность.

Процедура работы с полученными письмами с вложениями

При получении любого письма с вложением, пользователь должен ответить для себя на следующие вопросы:

1. Пришло ли письмо со знакомого Вам адреса?
2. Ожидали ли Вы письмо с вложением с этого адреса?
3. Говорит ли Вам о чем-нибудь тема письма и название файла-вложения?
4. Если на все вопросы ответ отрицательный, письмо должно быть немедленно удалено.

11. Политика безопасности при работе в сети Интернет

11.1.Колледж предоставляет услуги доступа к сети Интернет своим работникам, как инструмент для более эффективного выполнения своих функциональных обязанностей. Доступ к сети предоставляется только тем сотрудникам, кому он необходим для выполнения функциональных обязанностей согласно должностной инструкции.

11.2.Пользователям запрещается

-использовать Интернет для доступа, создания, отображения или передачи дискредитирующей кого-либо информации, непристойного или вызывающего содержания, которая может быть воспринята, как преследование или умаление.

-посещать сайты порнографического и развлекательного характера; колледж контролирует обращение к сайтам, и может без предупреждения закрывать к ним доступ; если пользователь обнаружил, что он случайно попал на данные сайты, следует немедленно прекратить к ним доступ и сообщить адрес сайта администратору сервиса доступа к сети Интернет для внесения данного сайта в список блокируемых.

-использовать сеть Интернет для скачивания и распространения нелицензированного программного обеспечения или любых других данных, распространение которых запрещено законом.

-преднамеренное распространение компьютерных вирусов, сетевых червей или другого злонамеренного кода.

-сознательно нарушать или мешать работе любых компьютерных систем или сетей, обходить любую систему, предназначенную для защиты информации, отнесенной к коммерческой тайне.

-использовать корпоративный доступ к сети Интернет для любой деятельности с целью получения личной материальной выгоды.

-использовать название колледжа, своей должности и служебных обязанностей, адреса корпоративной электронной почты при общении через сеть Интернет (чаты, группы новостей, форумы и т.д.) или создании учетных записей на сайтах Интернет, за исключением сотрудников, имеющих право представлять колледж в средствах массовой информации.

-распространять информацию, отнесенную к коммерческой тайне или содержащую персональные данные сотрудников техникума, на общественных серверах в сети Интернет и в локальной сети колледжа.

-использование сети Интернет для получения программного обеспечения или любой другой информации развлекательного характера, игр, социальных сетей, а также игр через сеть Интернет.

11.3.Любое полученное из сети Интернет программное обеспечение или файлы становятся собственностью колледжа, если это не нарушает чужих прав

на интеллектуальную собственность или условий распространения программного обеспечения.

11.4.Контроль за использованием ресурсов сети Интернет осуществляет ответственный за информационную безопасность в лице системного администратора.

Колледж имеет право контролировать использование ресурсов сети Интернет, включая списки посещаемых пользователями сайтов.

11.5.Пользователи не могут рассчитывать на конфиденциальность для колледжа передаваемой через сеть Интернет информации.

12. Политика безопасности при архивировании, восстановлении и резервном копировании

12.1. Общие положения

Операционное резервное копирование и восстановление данных представляет процесс резервного копирования, создания копии данных на случай потери в результате выхода из строя оборудования, ошибки оператора и т.п.

Архивирование – это процесс создания копии файла или набора файлов на специально выделенном накопителе, предназначенном для длительного хранения.

Восстановление после катастроф включает все действия по организации, управлению и автоматизации процесса восстановления после потери (разрушения) информационной инфраструктуры и данных. Это включает процессы перемещения данных в специально отведенные безопасные места, процессы восстановления информационной инфраструктуры и процессы восстановления данных в установленные сроки

Требования к архивированию, резервному копированию и восстановлению данных определяется уровнем риска сервиса, требованием к доступности сервиса и устанавливаются следующие:

-режим работы сервиса Интернет круглосуточный, время восстановления 2 часа (не по вине провайдера, предоставляющего доступ к сети)

-режим работы электронной почты круглосуточный, время восстановления 4 часа (не по вине провайдера, предоставляющего доступ к сети)

-режим работы файлового архива круглосуточный, время восстановления 4 часа.

Контроль за исполнением данной политики безопасности выполняет ответственный за информационную безопасность института в лице заведующего отделом информационных технологий.

12.2.Порядок резервного копирования защищаемой информации на твердые носители

Для предотвращения потерь информации при кратковременном отключении электроэнергии все ключевые элементы ИСПДн: ПЭВМ, сетевое и коммуникационное оборудование должны подключаться к сети электропитания через источники бесперебойного питания.

Система резервного копирования и хранения данных, должна обеспечивать хранение защищаемой информации на твердых носителях (жесткий магнитный диск, лазерный диск, флэш-карта).

Резервное копирование и хранение данных должно осуществляться на периодической основе:

- для обрабатываемых персональных данных – не реже 1 раза в неделю;
- для технологической информации – не реже 1 раза в месяц;
- эталонные копии программного обеспечения (операционные системы, штатное и специальное программное обеспечение, программные средства защиты) каждый раз при внесении изменений в эталонные копии (выход новых версий).

Носители должны храниться в несгораемом шкафу или помещении, оборудованном системой пожаротушения.

В кратчайшие сроки, не превышающие одного рабочего дня, ответственные сотрудники предпринимают меры по восстановлению работоспособности. Предпринимаемые меры при необходимости согласуются с непосредственным руководителем.

К использованию, для создания резервной копии в ИСПДн, допускаются материальные носители, зарегистрированные в «Журнале учета материальных носителей» (Приложение1).

Администратор информационной безопасности обязан осуществлять контроль над резервным копированием конфиденциальной информации.

Ответственность за проведение резервного копирования в ИСПДн возлагается на администратора безопасности.

Еженедельно, по окончанию работы с конфиденциальными документами (содержащими персональные данные) на компьютере, пользователь, при отсутствии администратора, обязан создавать резервную копию защищаемых документов на зарегистрированный материальный носитель (ЖМД, ГМД, CD, DVD – диски, USB накопитель, другие), создавая тем самым резервный электронный архив конфиденциальных документов.

Материальные носители (ЖМД, ГМД, CD, DVD, USB) накопитель, другие), предназначенные для создания резервной копии и хранения защищаемой информации выдаются установленным порядком ответственным за организацию обработки персональных данных, либо администратором

информационной безопасности. По окончании процедуры резервного копирования материальные носители сдаются на хранение лицу, ответственному за организацию обработки персональных данных, либо лицам, ответственным за обеспечение безопасности персональных данных в ИСПДн, либо администратору информационной безопасности. .

Перед резервным копированием пользователь или администратор информационной безопасности обязан проверить материальный носитель (ЖМД, ГМД, CD, USB накопитель) на отсутствие вирусов.

Файлы, помещаемые в электронный архив должны в обязательном порядке проходить антивирусный контроль в соответствии с п. 7 настоящего Положения.

Запрещается запись посторонней информации на материальные носители (ЖМД, ГМД, CD, USB накопитель и другие) резервной копии.

Порядок создания резервной копии:

– вставить в компьютер зарегистрированный материальный носитель (ЖМД, ГМД, CD, USB накопитель, другие) для резервного копирования;

– выбрать необходимый каталог (файл) для создания резервного архива;

– при использовании систем управления базами данных необходимо создать файл с резервной копией защищаемой информации с помощью встроенных средств системы;

– выполнить процедуру создания резервной копии;

– произвести копирование на отчуждаемый материальный носитель;

– произвести отключение отчуждаемого материального носителя и, создав не обходимые записи в журналах убрать материальный носитель в хранилище.

Хранение отчуждаемого материального носителя с резервной копией защищаемой информации осуществляется в специальном металлическом хранилище совместно с ключевой и аутентифицирующей информацией.

При восстановлении работоспособности программного обеспечения сначала осуществляется резервное копирование защищаемой информации, затем производится полная деинсталляция некорректно работающего программного обеспечения.

Восстановление программного обеспечения производится путем его инсталляции с использованием эталонных дистрибутивов, хранение которых осуществляется администратором информационной безопасности в специальном хранилище (сейфе).

При необходимости ремонта технических средств, с них удаляются опечатывающие пломбы и по согласованию с администратором информационной безопасности, лицом ответственным за организацию

обработки персональных данных и, при условии проведенной аттестации информационной системы, представителем Организации, проводившей аттестацию, оборудование передается в сервисный центр производителя. Ремонт материальных носителей персональных данных не допускается. Неисправные материальные носители персональных данных подлежат уничтожению в соответствии с порядком уничтожения материальных носителей. Работа с использованием неисправных технических средств запрещается.

При восстановлении работоспособности средств защиты информации следует выполнить их настройку в соответствии с требованиями безопасности информации, изложенными в техническом задании на создание системы защиты персональных данных. Настройку данных средств должен выполнять работник, прошедший соответствующее обучение, либо сторонняя организация, имеющая лицензию на деятельность по технической защите конфиденциальной информации.

Восстановление средств защиты информации производится с использованием эталонных сертифицированных дистрибутивов, которые хранятся в хранилище. После успешной настройки средств защиты информации необходимо выполнить резервное копирование настроек данных средств с помощью встроенных в них функций на учтенный материальный носитель.

Ответственность за проведение мероприятий по восстановлению работоспособности технических средств и программного обеспечения баз данных возлагается на администратора информационной безопасности.

Ответственность за проведение мероприятий по восстановлению средств защиты информации возлагается на администратора информационной безопасности.

13. Порядок хранения и обращения материальных носителей конфиденциальной информации

13.1. Общие положения

Все носители информации содержащие ПДн на бумажной, магнитной, магнито - оптической и иной основе, используемые в технологическом процессе обработки информации в ИСПДн, подлежат учету, хранению и обращению в соответствии с требованиями конфиденциального делопроизводства.

Организация и ведение учета накопителей и носителей ПДн, организация их хранения, обращения и уничтожения осуществляются ответственными лицами.

ПДн, должны обособляться от иной информации, в частности путем фиксации их на отдельных материальных носителях ПДн, в специальных разделах или на полях форм (бланков).

При фиксации ПДн на материальных носителях не допускается фиксация на одном материальном носителе ПДн, цели обработки которых заведомо не совместимы.

Для обработки различных категорий ПДн, осуществляемой без использования средств автоматизации, для каждой категории ПДн должен использоваться отдельный материальный носитель.

Обработка ПДн без использования средств автоматизации должна осуществляться таким образом, чтобы в отношении каждой категории ПДн можно было определить места хранения ПДн (материальных носителей) и установить перечень лиц, осуществляющих обработку ПДн либо имеющих к ним доступ.

Должно обеспечиваться раздельное хранение ПДн (материальных носителей), обработка которых осуществляется в различных целях.

При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность ПДн и исключающие несанкционированный к ним доступ.

Материальные носители персональных данных, срок использования которых истек, подлежат уничтожению; уничтожение носителей с конфиденциальной информацией осуществляется уполномоченной комиссией. По результатам уничтожения носителей составляется акт.

13.2. Порядок учета, хранения и обращения со съемными носителями персональных данных, твердыми копиями и их утилизации

Все находящиеся на хранении и в обращении съемные носители с персональными данными и иной конфиденциальной информацией подлежат учёту. Каждый такой съемный носитель должен иметь этикетку, на которой указывается его уникальный учетный номер.

Учет и выдачу съемных носителей персональных данных осуществляет Администратор безопасности. При получении делаются соответствующие записи в журнале учета. По окончании работ пользователь сдает съемный носитель для хранения, о чем делается соответствующая запись в журнале учета.

Правила использования съемных носителей персональных данных:

Запрещается

-хранить съемные носители с персональными данными вместе с носителями открытой информации, на рабочих столах, либо оставлять их без присмотра или передавать на хранение другим лицам;

-выносить съемные носители с персональными данными из служебных

помещений для работы с ними на дому, в гостиницах и т. д.

При отправке или передаче персональных данных адресатам на съемные носители записываются только предназначенные адресатам данные. Отправка персональных данных адресатам на съемных носителях осуществляется в порядке, установленном для документов для служебного пользования.

Вынос съемных носителей персональных данных для непосредственной передачи адресату осуществляется только с письменного разрешения руководителя структурного подразделения.

Порядок действий при утрате или уничтожении съемных носителей персональных данных:

-о фактах утраты съемных носителей, содержащих персональные данные, либо разглашения содержащихся в них сведений немедленно ставится в известность руководитель соответствующего структурного подразделения;

–на утраченные носители составляется акт;

-соответствующие отметки вносятся в журналы персонального учета съемных носителей персональных данных.

-съемные носители персональных данных, пришедшие в негодность, или отслужившие установленный срок, подлежат уничтожению; уничтожение съемных носителей с конфиденциальной информацией осуществляется уполномоченной комиссией. По результатам уничтожения носителей составляется акт.

14. Политика безопасности при работе с криптографическими средствами защиты информации и Электронной цифровой подписью

14.1. Общие положения

Средства криптографической защиты информации (СКЗИ) и электронной цифровой подписи (ЭЦП), предназначены для подписывания файлов налоговых деклараций и бухгалтерской отчетности ЭЦП с целью подтверждения подлинности информации и ее авторства и шифрования этих файлов при передаче по каналам связи для обеспечения конфиденциальности.

СКЗИ и средства ЭЦП могут использоваться для защиты информации в системе представления налоговых деклараций и сведений персонифицированного учета в электронном виде по телекоммуникационным каналам связи.

Для работы с СКЗИ и средствами ЭЦП привлекаются уполномоченные лица, назначенные соответствующим приказом директора техникума. Должностные лица, уполномоченные соответствующим приказом руководителя организации, эксплуатировать СКЗИ, получать и использовать ключи шифрования и ЭЦП, несут персональную ответственность за:

- сохранение в тайне конфиденциальной информации, ставшей им известной в процессе работы с СКЗИ;
- сохранение в тайне содержания закрытых ключей СКЗИ и средств ЭЦП;
- сохранность носителей ключевой информации и других документов о ключах, выдаваемых с ключевыми носителями.

В организации должны быть обеспечены условия хранения ключевых носителей и карточки отзыва ключей, исключающие возможность доступа к ним посторонних лиц, несанкционированного использования или копирования ключевой информации и паролей отзыва ключей.

Для исключения утраты ключевой информации вследствие дефектов носителей рекомендуется, после получения ключевых дисков, создать рабочие копии. Копии должны быть соответствующим образом маркированы и должны использоваться и храниться так же, как оригиналы.

Пользователь несет ответственность за то, чтобы на компьютере, на котором установлены СКЗИ и средства ЭЦП, не были установлены и не эксплуатировались программы (в том числе, - вирусы), которые могут нарушить функционирование программных СКЗИ и средств ЭЦП. При обнаружении на рабочем месте, оборудованном СКЗИ и средствами ЭЦП, посторонних программ или вирусов, нарушающих работу указанных средств, работа со средствами защиты информации на данном рабочем месте должна быть прекращена и должны быть организованы мероприятия по анализу и ликвидации негативных последствий данного нарушения.

14.2. Не допускается:

а) разглашать содержимое носителей ключевой информации или передавать сами носители лицам, к ним не допущенным, выводить ключевую информацию на дисплей и принтер;

б) вставлять ключевой носитель в ПЭВМ при проведении работ, не являющихся штатными процедурами использования ключей (шифрование/расшифровывание информации, проверка электронной цифровой подписи и т.д.), а также в дисководы других ПЭВМ;

в) записывать на ключевом носителе постороннюю информацию;

г) вносить какие-либо изменения в программное обеспечение СКЗИ и средств ЭЦП;

д) использовать бывшие в работе ключевые носители для записи новой информации без предварительного уничтожения на них ключевой информации путем переформатирования (рекомендуется физическое уничтожение носителей).

14.3.Действия в случае компрометации ключей

Под компрометацией закрытых ключей понимается их утрата (в том числе с их последующим обнаружением), хищение, разглашение, несанкционированное копирование, передача их по линии связи в открытом виде, увольнение по любой причине сотрудника, имеющего доступ к ключевым носителям или к ключевой информации на данных носите-лях, любые другие виды разглашения ключевой информации, в результате которых за-крытые ключи могут стать доступными несанкционированным лицам и (или) процессам.

Пользователь самостоятельно должен определить факт компрометации закрытого ключа и оценить значение этого события для Пользователя. Мероприятия по розыску и локализации последствий компрометации конфиденциальной информации, переданной с использованием СКЗИ, организует и осуществляет сам Пользователь.

При компрометации ключа у Пользователя, он должен немедленно прекратить связь по сети с другими абонентами и поставить в известность своего оператора системы сдачи бухгалтерской и налоговой отчетности о факте компрометации.

Для получения новых ключей уполномоченный представитель техникума должен обратиться к Оператору системы, имея при себе документы, подтверждающие его полномочия.

15. Политика безопасности в нештатных ситуациях (при чрезвычайных ситуациях)

15.1. Общие положения

В настоящем документе под аварийной ситуацией понимается некоторое происшествие, связанное со сбоем в функционировании элементов ИСПДн, предоставляемых пользователям ИСПДн. Аварийная ситуация становится возможной в результате реализации одной из угроз, приведенных в таблице «Источники угроз».

Источники угроз

Технологические угрозы	
	Пожар в здании
	Повреждение водой (прорыв системы водоснабжения, канализационных труб, систем охлаждения)
	Взрыв (бытовой газ, теракт, взрывчатые вещества или приборы, работающие под давлением)
	Химический выброс в атмосферу
Внешние угрозы	
	Массовые беспорядки

	Сбои общественного транспорта
	Эпидемия
	Массовое отравление персонала
Стихийные бедствия	
	Удар молнии
0	Сильный снегопад
1	Сильные морозы
2	Просадка грунта (подмыв грунтовых вод, подземные работы) с частичным обрушением здания
3	Затопление водой в период паводка
4	Наводнение, вызванное проливным дождем
5	Ураган, смерч
6	Подтопление здания (воздействие подпочвенных вод, вызванное внезапным и непредвиденным повышением уровня грунтовых вод)
Телекоммуникационные и ИТ угрозы	
7	Сбой системы кондиционирования
8	Сбой ИТ – систем
Угроза, связанная с человеческим фактором	
9	Ошибка персонала, имеющего доступ к серверной
0	Нарушение конфиденциальности, целостности и доступности конфиденциальной информации
Угрозы, связанные с внешними поставщиками	
1	Отключение электроэнергии
2	Сбой в работе интернет-провайдера
3	Физически разрыв внешних каналов связи

Все действия в процессе реагирования на аварийные ситуации должны документироваться ответственным за реагирование сотрудником в «Журнале учета нештатных ситуаций…..».

В кратчайшие сроки, не превышающие одного рабочего дня, ответственные за реагирование сотрудники Учреждения сотрудниками (Администратор безопасности, Оператор ИСПДн) предпринимают меры по восстановлению работоспособности. Предпринимаемые меры по возможности согласуются с вышестоящим руководством. По необходимости, иерархия может быть нарушена, с целью получения высококвалифицированной консультации в кратчайшие сроки.

15.2. Уровни реагирования на инцидент

При реагировании на инцидент, важно, чтобы пользователь правильно классифицировал критичность инцидента. Критичность оценивается на основе следующей классификации:

1. Уровень 1 – **Незначительный инцидент**. Незначительный инцидент определяется как локальное событие с ограниченным разрушением, которое не влияет на общую доступность элементов ИСПДн и средств защиты. Эти инциденты решаются ответственными за реагирование сотрудниками.

2. Уровень 2 – **Авария**. Любой инцидент, который приводит или может привести к прерыванию работоспособности отдельных элементов ИСПДн и средств защиты. Эти инциденты выходят за рамки управления ответственными за реагирование сотрудниками.

К авариям относятся следующие инциденты:

1. Отказ элементов ИСПДн и средств защиты из-за:

- повреждения водой (прорыв системы водоснабжения, канализационных труб, систем охлаждения), а также подтопления в период паводка или проливных дождей;
- сбоя системы кондиционирования.

2. Отсутствие Администратора ИСПДн и Администратора безопасности более чем на сутки из-за:

- химического выброса в атмосферу;
- сбоев общественного транспорта;
- эпидемии;
- массового отравления персонала;
- сильного снегопада;
- урагана, смерча
- сильных морозов.

3. Уровень 3 – **Катастрофа**. Любой инцидент, приводящий к полному прерыванию работоспособности всех элементов ИСПДн и средств защиты, а также к угрозе жизни пользователей ИСПДн, классифицируется как катастрофа. Обычно к катастрофам относят обстоятельства непреодолимой силы (пожар, взрыв), которые могут привести к неработоспособности ИСПДн и средств защиты на сутки и более.

К катастрофам относятся следующие инциденты:

- пожар в здании;
- взрыв;
- просадка грунта с частичным обрушением здания;
- массовые беспорядки в непосредственной близости от учреждения.

15.3.Меры обеспечения непрерывности работы и восстановления ресурсов при возникновении аварийных ситуаций

15.3.1.Технические меры

К техническим мерам обеспечения непрерывной работы и восстановления относятся программные, аппаратные и технические средства и системы, используемые для предотвращения возникновения аварийных ситуаций, такие как:

4. системы жизнеобеспечения;
5. системы обеспечения отказоустойчивости;
6. системы резервного копирования и хранения данных;
7. системы контроля физического доступа.

Системы жизнеобеспечения ИСПДн включают:

8. пожарные сигнализации и системы пожаротушения;
9. системы вентиляции и кондиционирования;
10. системы резервного питания.

Все критичные помещения (помещения, в которых размещаются элементы ИСПДн и средства защиты) должны быть оборудованы средствами пожарной сигнализации и пожаротушения.

Порядок предотвращения потерь информации и организации системы жизнеобеспечения ИСПДн описан в Порядке резервирования и восстановления работоспособности технический систем и программного обеспечения, баз данных и средств защиты информации.

15.3.2.Организационные меры

Ответственные за реагирование сотрудники ознакомляют всех сотрудников, находящихся в их зоне ответственности, с данной инструкцией в срок, не превышающий трех рабочих дней с момента выхода нового сотрудника на работу.

По окончанию ознакомления сотрудник расписывается в листе ознакомления. Подпись сотрудника должна соответствовать его подписи в документе, удостоверяющем его личность.

Должно быть проведено обучение должностных лиц, имеющих доступ к ресурсам ИСПДн, порядку действий при возникновении аварийных ситуаций. Должностные лица должны получить базовые знания в следующих областях:

- оказание первой медицинской помощи;
- пожаротушение;
- эвакуация людей;
- защита материальных и информационных ресурсов;
- методы оперативной связи со службами спасения и лицами, ответственными за реагирование сотрудниками на аварийную ситуацию;
- выключение оборудования, электричества, водоснабжения, газоснабжения.

Операторы ИСПДн и Администраторы безопасности должны быть дополнительно обучены методам частичного и полного восстановления работоспособности элементов ИСПДн.

Навыки и знания должностных лиц по реагированию на аварийные ситуации должны регулярно проверяться. При необходимости должно проводиться дополнительное обучение должностных лиц порядку действий при возникновении аварийной ситуации.

16. Ликвидация последствий нарушения политик информационной безопасности

Администратор информационной безопасности, используя данные, полученные в результате применения инструментальных средств контроля (мониторинга) безопасности информации ИС, должен своевременно обнаруживать нарушения информационной безопасности, факты осуществления НСД к защищаемым информационным ресурсам и предпринимать меры по их локализации и устранению.

В случае обнаружения факта нарушения информационной безопасности или осуществления НСД к защищаемым информационным ресурсам ИС рекомендуется уведомить администратора информационной безопасности и/или руководителя структурного подразделения, и далее следовать их указаниям.

Действия администратора безопасности при признаках нарушения политик информационной безопасности регламентируются следующими внутренними документами:

-Политикой информационной безопасности;
-Должностными обязанностями администратора безопасности;

После устранения инцидента необходимо составить акт о факте нарушения и принятых мерах по восстановлению работоспособности ИС, а также зарегистрировать факт нарушения в журнале учета нарушений, ликвидации их причин и последствий.

17. Ответственность нарушителей Политики безопасности

Ответственность за выполнение правил Политики безопасности несет каждый сотрудник колледжа в рамках своих служебных обязанностей и полномочий.

На основании ст. 192 Трудового кодекса РФ сотрудники, нарушающие требования политики безопасности, могут быть подвергнуты дисциплинарным взысканиям, включая замечание, выговор и увольнение с работы.

Все сотрудники несут персональную ответственность за прямой действительный ущерб, причиненный учреждению в результате нарушения ими правил политики(Ст. 238 Трудового кодекса РФ).

За неправомерный доступ к компьютерной информации, создание, использование или распространение вредоносных программ, а также нарушение правил эксплуатации ЭВМ, следствием которых явилось нарушение работы ЭВМ (автоматизированной системы обработки информации), уничтожение, блокирование или модификация защищаемой информации, сотрудники Управления несут ответственность в соответствии со статьями 272, 273 и 274 Уголовного кодекса Российской Федерации.

18. Порядок подготовки персонала по вопросам информационной безопасности и допуска его к работе

Организация просвещения сотрудников техникума в области информационной безопасности возлагается на Ответственного за организацию обработки персональных данных. Обучение сотрудников правилам обращения с конфиденциальной информацией, проводится путем:

10) проведения инструктивных занятий с сотрудниками;
11) самостоятельного изучения сотрудниками внутренних нормативных документов.

Допуск персонала к работе с защищаемыми информационными ресурсами осуществляется только после его ознакомления с настоящими политиками, так же соответствующими инструкциями. Согласие на соблюдение правил и требований настоящих политик подтверждается подписями

сотрудников. Правила допуска к работе с информационными ресурсами лиц, не являющихся сотрудниками колледжа, определяются на договорной основе с этими лицами или с организациями, представителями которых являются эти лица.

19. Период действия и порядок внесения изменений

Настоящая политика вводится в действие и признается утратившей силу на основании приказа директора техникума.

Изменения в политику вносятся приказом директора техникума.

Инициаторами внесения изменений в политику информационной безопасности являются:

12) Директор колледжа;
13) Администратор безопасности;
14) Руководители структурных подразделений

Плановая актуализация настоящей политики производится ежегодно и имеет целью приведение в соответствие определенных политикой защитных мер реальным условиям и текущим требованиям к защите информации.

Внеплановая актуализация политики информационной безопасности производится в обязательном порядке в следующих случаях:

15) при изменении политики РФ в области информационной безопасности, указов и законов РФ в области защиты информации;
16) при изменении внутренних нормативных документов (инструкций, положений, руководств), касающихся информационной безопасности;
17) при происшествии и выявлении инцидента (инцидентов) по нарушению информационной безопасности, повлекшего ущерб техникуму.

Ответственными за актуализацию политики информационной безопасности (плановую и внеплановую) несет администратор безопасности.

Контроль за исполнением требований настоящей политики и поддержанием ее в актуальном состоянии возлагается на администратора информационной безопасности.

20. Заключительные положения

Настоящая политика рассмотрена и одобрена на общем собрании трудового коллектива (протокол от 03.04.2014 №_13_).

Внесены изменения в связи с переименованием Кировского областного государственного образовательного бюджетного учреждения среднего профессионального образования «Вятский государственный техникум

профессиональных технологий, управления и сервиса» (КОГОБУ СПО «ВятТТУиС») в Кировское областное государственное профессиональное образовательное бюджетное учреждение «Вятский колледж профессиональных технологий, управления и сервиса»(КОГПОБУ «ВятКТУиС») (приказ от 25.12.2015 г. №169).

Данная Политика вступает в силу с момента ее утверждения и действует до замены новой или издании приказа об отмене ее действия.

21.Нормативная документация:

1. Доктрина информационной безопасности Российской Федерации (утверждена Президентом РФ от 9 сентября 2000 г. № Пр-1895).

Законы Российской Федерации

2. Закон Российской Федерации от 5 марта 1992 г. № 2446-I «О безопасности»;
3. Гражданский кодекс Российской Федерации;
4. Федеральный закон от 10 января 2002 г. № 1-ФЗ «Об электронной цифровой подписи»;
5. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;
6. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
7. Уголовный кодекс РФ;
8. Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании» (с изменениями от 9 мая 2005 г., 1 мая, 1 декабря 2007 г.);
9. Федеральный закон от 8 августа 2001 г. № 128-ФЗ «О лицензировании отдельных видов деятельности»

Указы и распоряжения президента Российской Федерации

10. Указ Президента Российской Федерации от 20 января 1994 г. № 170 «Об основах государственной политики в сфере информатизации»;
11. Указ Президента Российской Федерации от 3 апреля 1995 г. № 334 «О мерах по соблюдению законности в области разработки производства, реализации и эксплуатации шифровальных средств, а также предоставления услуг в области шифрования информации»;
12. Указ Президента Российской Федерации от 3 июля 1995 г. № 662 «О мерах по формированию общероссийской телекоммуникационной системы и обеспечению прав собственников при хранении ценных бумаг и расчетах на фондовом рынке Российской Федерации»;

13. Указ Президента Российской Федерации от 9 января 1996 г. № 21 «О мерах по упорядочению разработки, производства, реализации, приобретения в целях продажи, ввоза в Российскую Федерацию и вывоза за ее пределы, а также использования специальных технических средств, предназначенных для негласного получения информации» (с изменениями от 30 декабря 2000 г.);

14. Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера».

Постановления и распоряжения правительства Российской Федерации

15. Постановление Правительства Российской Федерации от 3 ноября 1994 г. № 1233 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти»;

16. Постановление Правительства Российской Федерации от 26 июня 1995 г. № 608 «О сертификации средств защиты информации».

17. Постановление Правительства Российской Федерации от 21 марта 2012 г. N 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами

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

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

20. Постановление Правительства РФ от 6 июля 2008 г. N 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных»

Нормативные и руководящие документы Федеральных служб РФ

1. Решение Гостехкомиссии России от 21 октября 1997 г. № 61 «О защите информации при вхождении России в международную информационную систему «Интернет»;

2. Постановление Госстандарта Российской Федерации от 21 сентября 1994 г. № 15 «Об утверждении «Порядка проведения сертификации продукции в Российской Федерации» (с изменениями от 25 июля 1996 г., 11 июля 2002 г.);

3. Постановление Госстандарта Российской Федерации от 10 мая 2000 г. № 26 «Об утверждении Правил по проведению сертификации в Российской Федерации» (с изменениями от 5 июля 2002 г.);

4. Положение о сертификации средств защиты информации по требованиям безопасности информации (утверждено приказом председателя Государственной технической комиссии при Президенте Российской Федерации от 27 октября 1995 г. № 199);

5. Положение по аттестации объектов информатизации по требованиям безопасности информации (утверждено председателем Государственной технической комиссии при Президенте Российской Федерации 25 ноября 1994 г.);

6. Типовое положение об органе по аттестации объектов информатизации по требованиям безопасности информации (утверждено приказом председателя Государственной технической комиссии при Президенте Российской Федерации т 5 января 1996 г. № 3);

7. Руководящий документ. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации (утверждена решением Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г.);

8. Руководящий документ. Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники (утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г.);

9. Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации (утвержден решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г.);

10. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации (утвержден

решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г.);

11. Руководящий документ. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации (утвержден решением председателя Государственной технической комиссии при Президенте Российской Федерации от 25 июля 1997 г.);

12. Руководящий документ. Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей (утвержден решением председателя Государственной технической комиссии при Президенте Российской Федерации от 4 июня 1999 г. № 114);

13. Руководящий документ. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий (введен в действие Приказом Гостехкомиссии России от 19.06.02 г. № 187).

14. Приказ Федеральной службы по техническому и экспортному контролю (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

15. Приказ Федеральной службы по техническому и экспортному контролю (ФСТЭК России) от 11 февраля 2013 г. Москва № 17 Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах.

16. Требования и методы по обезличиванию персональных данных, обрабатываемых в информационных системах персональных данных, в том числе созданных и функционирующих в рамках реализации федеральных целевых программ (Утверждены Приказом Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) от 05.09.2013 № 996)

Государственные стандарты

1. ГОСТ 21552-84 «Средства вычислительной техники. Общие технические требования, приемка, методы испытаний, маркировка, упаковка, транспортирование и хранение» (утвержден постановлением Госстандарта СССР от 28 июня 1984 г. № 2206, с изменениями от июня 1987 г., ноября 1988 г., декабря 1990 г.);

2. ГОСТ 34.602-89 «Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы" (утвержден постановлением Госстандарта СССР от 24 марта 1989 г. № 661);

3. ГОСТ Р 50739-95 «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования» (принят постановлением Госстандарта России от 9 февраля 1995 г. № 49);

4. ГОСТ Р 50752-95 «Информационная технология. Защита информации от утечки за счёт побочных электромагнитных излучений при её обработке средствами вычислительной техники. Методы испытаний», Госстандарт России, 1995 г.;

5. ГОСТ Р 51188-98 «Защита информации. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство» (введен в действие постановлением Госстандарта России от 14 июля 1998 г. № 295);

6. ГОСТ Р 51275-99 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения» (введен в действие постановлением Госстандарта России от 12 мая 1999 г. № 160);

7. ГОСТ Р 51583-2000 «Защита информации. Порядок создания автоматизированных систем в защищённом исполнении. Общие положения», Госстандарт России, 2000 г.;

8. ГОСТ Р 51624-2000 «Защита информации. Автоматизированные системы в защищённом исполнении. Общие требования», Госстандарт России, 2000 г.;

9. ГОСТ Р ИСО/МЭК 17799-2005 «Информационная технология. Практические правила управления информационной безопасностью» (принят постановлением Госстандарта России от 29 декабря 2005 г. № 447-ст).

Иные документы

1. Разъяснения Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций «Вопросы, касающиеся обработки персональных данных работников, соискателей на замещение вакантных должностей, а также лиц, находящихся в кадровом резерве»

2. Информационное сообщение Федеральной службы по техническому и экспортному контролю от 4 мая 2012 г. N 240/24/1701 «О работах в области оценки соответствия продукции (работ, услуг), Используемой в целях защиты сведений, составляющих государственную тайну или относимых к охраняемой в соответствии с законодательством Российской Федерации иной информации ограниченного доступа»

3. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (Утверждена Заместителем директора ФСТЭК России 15 февраля 2008 г.

4. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных(Утверждена заместителем директора ФСТЭК России 14 февраля 2008 г.)

5. Разъяснения Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) «О вопросах отнесения фото- и видео- изображения, дактилоскопических данных и иной информации к биометрическим персональным данным и особенности их обработки»

6. Методические рекомендации по составлению Частной модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных учреждений здравоохранения, социальной сферы, труда и занятости (утверждены Директором департамента информатизации Министерства здравоохранения и социального развития Российской Федерации 23.12.2009)

Приложение 1

Форма журнала
учета съемных носителей

ЖУРНАЛ

учета съемных носителей персональных данных

_____

наименование структурного подразделения

Начат «____» _____ 200_ г.
Окончен «____» _____ 200_ г.
На _____ листах

_____ _____
Должность и ФИО ответственного за хранение Подпись

№ п./п.	Метка съемного носителя (учетный номер)	Фамилия исполнителя	(Получил, вернул, передал)	Дата записи информации	Подпись исполнителя	Примечание*
1						
2						
3						
4						
5						

* Причина и основание окончания использования (№ и дата отправки адресату или распоряжения о передаче, № и дата акта утраты, неисправность, заполнение подлежащими хранению данными)