Министерство образования и науки Нижегородской области
Государственное бюджетное профессиональное образовательное учреждение
«Арзамасский коммерческо-технический техникум»

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 6FEC4E52BDF8E756BB4124C0B475A34D
Владелец: Горшков Евгений Андреевич
Действителен: с 11.06.2025 до 04.09.2026

УТВЕРЖДАЮ
Директор ГБПОУ АКТТ
_____ Е.А. Горшков
Приказ от 03.09.2025 г. № 138 § 3

ИЗМЕНЕНИЯ в ПОЛОЖЕНИЕ
об обработке и защите персональных данных в Государственном бюджетном профессиональном образовательном учреждении «Арзамасский коммерческо-технический техникум»

г. Арзамас
2025 г.

1. Внести следующие изменения в Положение об обработке и защите персональных данных в Государственном бюджетном профессиональном образовательном учреждении «Арзамасский коммерческо-технический техникум» (далее – Положение):

1.1. Внести пункт 6.1.19 в раздел 6 «Обязанности и права Техникума как оператора персональных данных» Положения в следующей редакции:

«6.1.19. Техникум обеспечивает необходимую защиту автоматизированного рабочего места (сокращённо – АРМ), предназначенного для осуществления хранения и обработки персональных данных субъектов, путем реализации комплекса организационных и технических мероприятий, направленных на предотвращение несанкционированного доступа, изменения, блокирования, копирования, распространения и иных неправомерных действий с персональными данными.».

1.2. Внести пункт 7.2.3 в раздел 7 «Права и обязанности субъекта персональных данных» Положения в следующей редакции:

«7.2.3. Субъект, который является работником Техникума и участвует в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации, относящейся к персональным данным, и имеющий доступ к автоматизированному рабочему месту, должен соблюдать ряд обязанностей, определенных в Приложении № 1 к настоящему Положению.».

1.3. Внести пункт 8.10 в раздел 8 «Хранение и использование персональных данных, доступ к ним» Положения в следующей редакции:

«8.10. Защита, хранение и учет машиночитаемых носителей персональных данных обеспечивается в соответствии с инструкцией, которая является Приложением № 2 к настоящему Положению.».

1.4. Внести пункт 9.12 в раздел 9 «Порядок обеспечения защиты персональных данных» Положения в следующей редакции:

«9.12. Техникум обеспечивает своевременное реагирование на возникающие инциденты информационной безопасности в информационных системах данных в соответствии с Приложением № 3 к настоящему Положению.».

1.5. Внести пункт 9.13 в раздел 9 «Порядок обеспечения защиты персональных данных» Положения в следующей редакции:

«9.13. В целях защиты персональных данных в Техникуме организуется антивирусный контроль и парольная защита автоматизированных рабочих мест согласно Приложений № 4 и № 5 соответственно.».

1.6. Внести пункт 9.14 в раздел 9 «Порядок обеспечения защиты персональных данных» Положения в следующей редакции:

«9.14. Для предотвращения нарушений прав субъектов персональных данных определяется порядок допуска лиц в помещения, в которых распложены элементы информационных систем персональных данных и ведется их обработка в рабочее и нерабочее время, а также в нештатных ситуациях, в соответствии с Приложением № 6 к настоящему Положению.».

1.7. Дополнить Положение Приложением № 1 «Обязанности ответственного работника автоматизированного рабочего места (АРМ)» в следующей редакции:

« Приложение № 1

Обязанности ответственного работника автоматизированного рабочего места (АРМ)

1. Общие обязанности сотрудников по обеспечению информационной безопасности при работе на АРМ.

Каждый сотрудник, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению и данным автоматизированного рабочего места (АРМ), несет персональную ответственность за свои действия и обязан:

— строго соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами АРМ;

— знать и строго выполнять правила работы со средствами защиты информации, установленными на АРМ;

— хранить в тайне свой пароль (пароли). В соответствии с «Инструкцией по организации парольной защиты» с установленной периодичностью менять свой пароль (пароли);

— выполнять требования «Инструкции по организации антивирусной защиты» в части касающейся действий пользователей;

— немедленно ставить в известность администратора защиты информации при подозрении компрометации паролей;

— вызывать ответственного специалиста организации при обнаружении:

— фактов совершения в его отсутствие попыток несанкционированного доступа (НСД) к АРМ;

— несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств АРМ;

— отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию АРМ, выхода из строя или неустойчивого функционирования узлов АРМ или периферийных устройств (дисковода, и т.п.), а также перебоев в системе электроснабжения;

— некорректного функционирования установленных на АРМ технических средств защиты;

— непредусмотренных отводов кабелей и подключенных устройств;

— присутствовать при работах по внесению изменений в аппаратно-программную конфигурацию закрепленного за ним АРМ в подразделении.

Пользователям категорически ЗАПРЕЩАЕТСЯ:

— использовать компоненты программного и аппаратного обеспечения АРМ в неслужебных целях;

— самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств АРМ или устанавливать дополнительно любые программные и аппаратные средства;

— осуществлять обработку информации в присутствии посторонних (не допущенных к данной информации) лиц;

— записывать и хранить информацию (содержащую сведения конфиденциального характера) на неучтенных носителях информации (гибких магнитных дисках и т.п.);

— оставлять включенной без присмотра ПЭВМ, не активизировав средства защиты от несанкционированного доступа к данным (временную блокировку экрана);

— оставлять без личного присмотра на рабочем месте (или где бы то ни было) машинные носители, распечатки и другие носители, содержащие защищаемую информацию (сведения конфиденциального характера);

— умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к возникновению кризисной ситуации. Об обнаружении такого рода ошибок - ставить в известность администратора безопасности информации.».

1.8. Дополнить Положение Приложением № 2 «Инструкция по защите, хранению и учету машинных носителей персональных данных в ГБПОУ АКТТ» в следующей редакции:

«

Приложение № 2

Инструкция по защите, хранению и учету машинных носителей персональных данных в ГБПОУ АКТТ

1. Общие положения

1.1. Настоящая Инструкция по защите машинных носителей персональных данных в Государственном бюджетном профессиональном образовательном учреждение «Арзамасский коммерческо-технический техникум» (далее - Инструкция) определяет в ГБПОУ АКТТ порядок учета, хранения, выдачи, уничтожения и ограничения использования машинных носителей персональных данных, используемых в ГБПОУ АКТТ.

1.2. Сокращения, термины и определения:

1.2.1. Перечень сокращений:

ФАПСИ - Федеральное агентство правительственной связи и информации при Президенте Российской Федерации;

ФСТЭК России - Федеральная служба по техническому и экспортному контролю;

ФСБ России - Федеральная служба безопасности Российской Федерации;

Роскомнадзор - Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций;

АРМ - Автоматизированное рабочее место;

ИСПДн - Информационная система персональных данных;

ПДн - Персональные данные;

СВТ - Средства вычислительной техники;

СКЗИ - Средство криптографической защиты информации.

1.2.2. Перечень терминов:

Администратор безопасности информационной системы персональных данных (администратор безопасности) - работник, ответственный за обеспечение безопасности персональных данных в информационной системе персональных данных.

Информационная система - совокупность, содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

Инцидент информационной безопасности - одно или несколько нежелательных, или не ожидаемых событий информационной безопасности, которые со значительной вероятностью приводят к компрометации бизнес-операций и создают угрозы для информационной безопасности.

Машинный носитель данных - материальный носитель, используемый для передачи и хранения защищаемой информации в электронном виде.

Машинный носитель персональных данных - машинный носитель информации, на которых хранятся и (или) обрабатываются персональные данные.

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

СКЗИ - шифровальные (криптографические) средства защиты информации конфиденциального характера.

К СКЗИ 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.

1.3. Перечень нормативных правовых актов, на основании которых разработана настоящая Инструкция:

— Федеральный закон от 27.07.2006 N 152-ФЗ «О персональных данных»;

— Постановление Правительства РФ от 01.11.2012 N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

— Приказ 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»;

— Приказ 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»;

— Приказ Роскомнадзора от 28.10.2022 N 179 «Об утверждении Требований к подтверждению уничтожения персональных данных».

1.4. Работники, допущенные к обработке персональных данных в ГБПОУ АКТТ в связи с необходимостью выполнения ими трудовых (служебных) обязанностей, (далее - работники) должны быть ознакомлены с настоящей Инструкцией до начала обработки персональных данных под подпись. Обязанность по организации ознакомления работника с настоящей Инструкцией возлагается на ответственного за организацию обработки ПДн.

2. Организация учета машинных носителей персональных данных

2.1. Все используемые в ГБПОУ АКТТ машинные носители персональных данных подлежат регистрации и учету, а именно:

- несъёмные машинные носители (жесткие диски, находящиеся в системных блоках серверов, в том числе во внешних RAID-массивах серверов, и системных блоках АРМ ИСПДн);

- съёмные машинные носители (флеш-память, SSd-диски, оптические носители персональных данных и пр. технические средства, предназначенные для запоминания информации, и оперативно подключаемые к АРМ или серверу в целях записи на них информации из памяти АРМ (или сервера) либо считывания с них информации в память АРМ (или сервера).

2.2. Применение в ГБПОУ АКТТ незарегистрированных машинных носителей персональных данных запрещается.

2.3. Приобретенные машинные носители информации перед использованием передаются администратору безопасности для регистрации.

2.4. Ответственным за регистрацию, хранение, выдачу машинных носителей персональных данных, ведение учетной документации и контроль уничтожения машинных носителей персональных данных в установленном порядке является администратор безопасности.

2.5. Ответственность по организации процедуры уничтожения машинных носителей персональных данных возлагается на ответственного за организацию обработки ПДн.

2.6. При смене администратора безопасности составляется акт приема - сдачи учетной документации и машинных носителей персональных данных.

3. Порядок учета машинных носителей персональных данных

3.1. Основной учет машинных носителей персональных данных производится по Журналу учета машинных носителей персональных данных в ГБПОУ АКТТ (Приложение №1 к настоящей Инструкции).

Ведение и надежное хранение Журнала машинных носителей персональных данных в ГБПОУ АКТТ осуществляет администратор безопасности.

Срок хранения завершенного Журнала учета машинных носителей персональных данных в ГБПОУ АКТТ определяется утвержденной номенклатурой ГБПОУ АКТТ.

Уничтожение Журнала учета машинных носителей персональных данных в ГБПОУ АКТТ по истечении срока хранения (не менее 3-х лет) осуществляется в установленном порядке в ГБПОУ АКТТ.

3.2. Учет осуществляется с использованием регистрационных (заводских) номеров.

3.3. Учетный номер каждого зарегистрированного носителя - уникальный.

3.4. Учетный номер наносится на машинный носитель персональных данных способом, обеспечивающим сохранность маркировки в процессе эксплуатации носителя и не приводящим его в негодность:

- учетный номер оптического носителя персональных данных

наносится несмываемыми чернилами на его нерабочую поверхность и заверяется подписью администратора безопасности (на нерабочей стороне может указываться дополнительная информация, используемая в процессе применения);

- учетный номер жесткого диска наносится непосредственно на корпус носителя (при эксплуатации жесткого диска в составе СВТ, на корпус таких СВТ может наклеиваться этикетка с указанием количества и учетных номеров, установленных в нем носителей информации);

- учетный номер флеш-памяти, ssd-дисков может наносится посредством специальной наклейки, номер заверяется подписью администратора безопасности.

4. Выдача машинных носителей персональных данных

4.1. Работники получают учтенный машинный носитель персональных данных от администратора безопасности для выполнения работ на конкретный срок.

4.2. Выдача машинных носителей персональных данных работнику производится по Журналу учета машинных носителей персональных данных в ГБПОУ АКТТ под подпись.

4.3. Выдача работникам съёмных машинных носителей персональных данных разрешается исключительно для реализации технологических процессов в ИСПДн, необходимых для выполнения трудовых (служебных) обязанностей, и осуществляется с оформлением Заявления на право использования съёмного машинного носителя информации (Приложение №2 к настоящей Инструкции).

4.4. По завершении работ или установленного срока использования работник сдает машинный носитель персональных данных администратору безопасности, о чем делается соответствующая запись в Журнале учета машинных носителей персональных данных в ГБПОУ АКТТ.

5. Использование и передача машинных носителей персональных данных

5.1. На машинные носители персональных данных записываются исключительно ПДн и программные средства обработки ПДн, содержащиеся в ИСПДн.

5.2. Машинные носители персональных данных, допускающие повторную запись информации, при передаче между пользователями, в сторонние организации для ремонта или утилизации проходят процедуру уничтожения (стирания) персональных данных с оформлением Акта об уничтожении персональных данных в соответствии с приказом ГБПОУ АКТТ «О создании комиссии по уничтожению персональных данных в ГБПОУ АКТТ с целью уничтожения остаточной информации. Процедуру организует и контролирует администратор безопасности. Акт об уничтожении персональных данных хранится у ответственного за организацию обработки ПДн.

5.3. Ремонт машинных носителей персональных данных, содержащие персональные данные, сторонней организацией запрещен.

5.4. ПДн, используемые в различных целях, записываются на разные машинные носители персональных данных.

5.5. Вынос машинных носителей персональных данных за пределы установленных мест обработки ПДн допустим только с письменного разрешения директор ГБПОУ АКТТ.

5.6. Передача носителей, содержащих ПДн, которые обрабатываются в ИСПДн, сторонним организациям или третьим лицам производится по приказу директора ГБПОУ АКТТ через администратора безопасности. Администратор безопасности производит в этом случае необходимые отметки в Журнале учета машинных носителей персональных данных в ГБПОУ АКТТ.

6. Хранение машинных носителей персональных данных

6.1. Хранение машинных носителей персональных данных осуществляется в условиях, препятствующих несанкционированному ознакомлению, копированию, изменению или уничтожению информации, содержащейся на машинных носителях.

6.2. Машинные носители персональных данных хранятся в служебных помещениях, съёмные машинные носители персональных данных - в сейфах (металлических шкафах), оборудованных внутренними замками с двумя или более дубликатами ключей и приспособлениями для опечатывания замочных скважин или кодовыми замками.

В случае если на съёмном машинном носителе персональных данных хранятся только персональные данные в зашифрованном с использованием СКЗИ виде, допускается хранение таких носителей вне сейфов (металлических шкафов).

6.3. Хранение машинных носителей персональных данных осуществляется в условиях, исключающих утрату их функциональности и хранимой информации (оптические носители хранятся в конвертах или специальных коробках, обеспечивающих сохранность рабочей поверхности носителя от загрязнения и механических повреждений).

6.4. Порядок хранения машинных носителей персональных данных, предназначенных к списанию (уничтожению), в том числе нечитаемых вследствие выхода из строя из-за неисправности (износа), не изменяется.

6.5. Ответственным за сохранность машинного носителя персональных данных является пользователь ИСПДн, получивший машинный носитель персональных данных в соответствии с разделом 4 настоящей Инструкции.

7. Действия при выходе из строя, порче или утрате машинных носителей персональных данных

7.1. В случае выхода из строя, утраты или порчи пользователем машинного носителя персональных данных немедленно ставится в известность администратор безопасности. Администратор безопасности докладывает об инциденте ответственному за организацию обработки ПДн.

7.2. Факт выхода из строя машинного носителя персональных данных устанавливается утвержденной приказом ГБПОУ АКТТ комиссией (в состав комиссии включается администратор безопасности, системный администратор ИСПДн и ответственный за организацию обработки персональных данных) с оформлением Акта технической экспертизы состояния машинного носителя информации (Приложение №3 к настоящей Инструкции), утверждаемого директором ГБПОУ АКТТ.

Неисправный носитель заменяется исправным, после чего администратором безопасности делаются соответствующие отметки в документах учета.

7.3. По факту утраты или порчи машинного носителя персональных данных, несанкционированного и (или) нецелевого использования учтенных машинных носителей информации проводится служебная проверка в установленном порядке по решению директора ГБПОУ АКТТ.

Администратором безопасности делаются соответствующие отметки в документах учета.

7.4. Машинные носители персональных данных, пришедшие в негодность или с истекшим сроком эксплуатации, подлежат уничтожению в установленном порядке.

8. Уничтожение машинных носителей персональных данных

8.1. Уничтожение машинных носителей персональных данных производится способом, гарантирующим невозможность восстановления информации, содержавшейся на носителе. Такими способами являются: механическое, электрическое, электромагнитное, химическое или термическое воздействие на носитель, применение специального программного обеспечения для уничтожения информации на носителе. Способ уничтожения выбирается администратором безопасности в зависимости от типа носителя и возможностей ГБПОУ АКТТ.

8.2. Уничтожение машинных носителей персональных данных производится в присутствии членов комиссии, утвержденной приказом директора «О создании комиссии по уничтожению персональных данных ГБПОУ АКТТ».

8.3. В случае проведения процедуры уничтожения машинного носителя информации сторонней организацией на основании заключенного гражданско-правового договора с учетом требований приказа директора «О создании комиссии по уничтожению персональных данных в ГБПОУ АКТТ» уничтожение машинного носителя информации оформляется Актом, который находится на хранении у администратора безопасности.

8.4. Утилизация лома уничтоженных носителей производится в соответствии с правилами уничтожения СВТ.

9. Контроль применения машинных носителей персональных данных

9.1. Контроль наличия машинных носителей персональных данных, правил и условий их хранения осуществляется посредством периодических проверок, утвержденной приказом директора комиссией, (в состав комиссии включается ответственный за организацию обработки персональных данных и администратор безопасности). Результаты проверки наличия машинных носителей персональных данных оформляются Актом проверки наличия и состояния машинных носителей информации (Приложение №4 к настоящей Инструкции).

9.2. Проверке подлежат: соответствие количества учтенных носителей фактическому, наличие и состояние учетной документации, соответствие серийных (заводских) и учетных номеров, условия хранения и использования носителей.

9.3. Акт проверки хранится у администратора безопасности.

10. Ответственность

10.1. Работники ГБПОУ АКТТ несут ответственность за ненадлежащее исполнение или неисполнение своих обязанностей, предусмотренных настоящей Инструкцией в соответствии с законодательством Российской Федерации.

Приложение № 1 к Инструкции

Журнал учета машинных носителей персональных данных в ГБПОУ АКТТ

Учетный номер ___
Журнал начат ____
Журнал окончен ___
Листов (_____)

№ п/п	Учетный (инвентарный) номер	Дата постановки на учет	Наименование, модель, емкость носителя	Заводской (серийный) номер	Тип носителя (съемный /несъемный)	Место установки (для несъемных носителей)	Ф.И.О. лица, эксплуатирующего носитель	Дата получения носителя и подпись	Дата возврата носителя и подпись администратора	Отметка об уничтожении носителя	Примечание
1	2	3	4	5	6	7	8	9	10	11	12

Лист ___

Правила по формированию и ведению журнала учета машинных носителей персональных данных в ГБПОУ АКТТ

1. Формирование журнала

Журнал ведется на бумажном носителе (формируется из листов формата А4, ориентация листа - альбомная).

Титульный лист журнала изготавливается на отдельном листе.

Все листы журнала (за исключением листов титульного), нумеруются.

Весь журнал прошнуровывается (сшивается) и подписывается с обратной стороны руководителей ГБПОУ «АКТТ» с указанием количества прошитых и пронумерованных листов в журнале.

2. Ведение журнала

Перед началом использования журнала на лицевой стороне обложки указывается номер журнала по номенклатуре дел (журналов) на текущий год и дата начала ведения журнала.

Графы журнала заполняются следующим образом:

- Графа 1 - учетный порядковый номер записи;
- Графа 2 - учетный (инвентарный) номер носителя;
- Графа 3 - дата постановки на учет;
- Графа 4 - наименование, модель, емкость носителя;
- Графа 5 - заводской (серийный) номер носителя;
- Графа 6 - указывается тип носителя (съемный, несъёмный);
- Графа 7 - для несъемных носителей указывается АРМ пользователя.
- Графа 8 - Ф.И.О. работника
- Графа 9 - дата получения носителя и подпись пользователя;
- Графа 10 - дата возврата носителя и подпись администратора безопасности;
- Графа 11 - отметку делает администратор безопасности после уничтожения носителя;
- Графа 12 - любая информация, относящаяся к носителю.

Все записи в журнале делаются четко и разборчиво. В случае если вносимые данные не помещаются на одной строке (в одной ячейке), то используется несколько строк.

Приложение № 2 к Инструкции

Форма заявления на право использования съёмного машинного носителя информации

Разрешаю
Директор ГБПОУ АКТТ
«___» _____ 20 ___ г.

Заявления на право использования съёмного машинного носителя информации

Прошу разрешить для выполнения служебных (трудовых) обязанностей использование и подключение к АРМ (инв. №_) съёмного машинного носителя персональных данных:

Должность	
ФИО полностью	
Цель использования в соответствии с служебными (трудовыми) обязанностями	
Технологический процесс, для реализации которого необходимо использование машинного носителя персональных данных	

Я предупрежден(а), что записывать, хранить на съёмных машинных носителях информации информацию ограниченного доступа допускается исключительно для реализации технологических процессов (регламентов, порядков работы и т.п.), необходимых для выполнения служебных (трудовых) обязанностей.

Подпись/ФИО/

Дата

_____

Согласовано:

Руководитель структурного подразделения */подпись/ ФИО/*

Выдан съёмный машинный носитель информации:

Учетный (регистрационный) № __

Администратор безопасности _____/_____/

Приложение № 3 к Инструкции

Форма акта технической экспертизы состояния машинного носителя информации

УТВЕРЖДАЮ
Директор ГБПОУ АКТТ
«__» _____ 20 ___ г.

Акт технической экспертизы состояния машинного носителя информации

Комиссия в составе:
Председатель *(ФИО)*
Члены комиссии *(ФИО)*

На основании *(приказа о назначении комиссии)*
Произвела наружный осмотр и контроль, сверила с данными регистрационного учета следующие носители информации:

№ п/п	Учетный (инвентарный) номер носителя	Наименование, модель, емкость носителя	Серийный (заводской) номер носителя	Место установки	Неисправность
1	2	3	4	5	6

В результате осмотра и контроля комиссия установила: (*проявление неисправности, метод определения неработоспособности носителя информации*)

В количестве (указать количество)

Характер записанной информации *(конфиденциальный/не конфиденциальный)*

Возможность дальнейшего использования носителя информации *(подлежит/не подлежит ремонту)*

Заключение комиссии: (*носитель информации подлежит/не подлежит ремонту*)

Подписи членов комиссии

Председатель	*должность*	*Подпись/ФИО*
Члены комиссии	*должность*	*Подпись/ФИО*

Приложение № 4 к Инструкции

Форма акта проверки наличия и состояния машинных носителей информации

УТВЕРЖДАЮ
Директор ГБПОУ АКТТ
«____» _____ 20 ___ г.

Акт проверки наличия и состояния машинных носителей информации

Комиссия в составе:
Председатель (*ФИО*)
Члены комиссии (*ФИО*)

На основании (*приказа о назначении комиссии*)

Провела проверку наличия и состояния машинных носителей информации в ГБПОУ АКТТ.

Для проверки представлена следующая документация: Журнал учета носителей персональных данных в ГБПОУ АКТТ.

В соответствии с учетной документацией в ГБПОУ АКТТ числится:

Оптические диски в количестве ___ штук:

№ п/п	Тип носителя	Учетный (инвентарный) номер	Примечание
1	2	3	4

Флеш-накопители в количестве ___ штук:

№ п/п	Тип носителя	Учетный (инвентарный) номер	Примечание

1	2	3	4

Накопители на жестких дисках в количестве ____ штук:

№ п/п	Тип носителя	Учетный (инвентарный) номер	Примечание
1	2	3	4

В ходе проверки выявлено (*соответствие/не соответствие учетных носителей информации фактически представленному*).

Заключение комиссии (*носители информации находятся в исправном/ неисправном состоянии, условия хранения и использования машинных носителей персональных данных соответствуют/ не соответствуют требованиях Инструкции по защите машинных носителей персональных данных в ГБПОУ АКТТ*)

Подписи членов комиссии

Председатель	*должность*	*Подпись/ФИО*
Члены комиссии	*должность*	*Подпись/ФИО*

».

1.9. Дополнить Положение Приложением № 3 «Регламент реагирования на инциденты информационной безопасности в информационных системах данных ГБПОУ АКТТ» в следующей редакции:

«

Приложение № 3

Регламент реагирования на инциденты информационной безопасности в информационных системах данных ГБПОУ АКТТ

1. Термины и определения

1.1. Информационная система персональных данных - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

1.2. Инцидент информационной безопасности - любое непредвиденное или нежелательное событие, которое может нарушить деятельность или информационную безопасность. Инцидентами информационной безопасности являются:

- утрата услуг, оборудования или устройств;
- системные сбои или перегрузки;
- ошибки пользователей;
- несоблюдение политики или рекомендаций по информационной безопасности;
- нарушение физических мер защиты;
- неконтролируемые изменения систем;
- сбои программного обеспечения и отказы технических средств;
- нарушение правил доступа.

1.3. 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.

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

1.5. Средство защиты информации - программное обеспечение, программно-аппаратное обеспечение, аппаратное обеспечение, вещество или материал, предназначенное или используемое для защиты информации.

2. Общие положения

2.1. Настоящий Регламент реагирования на инциденты информационной безопасности в информационных системах персональных данных ГПОУ АКТТ (далее - Регламент), разработан в соответствии с законодательством Российской Федерации о персональных данных (далее -ПДн) и нормативно-методическими документами федеральных органов исполнительной власти по вопросам безопасности ПДн при их обработке в информационных системах персональных данных (далее - ИСПДн).

2.2. Настоящий Регламент определяет:

- порядок регистрации событий безопасности;
- порядок выявления инцидентов информационной безопасности и реагированию на них;
- порядок проведения анализа инцидентов информационной безопасности, в том числе определение источников и причин возникновения инцидентов.

2.3. Регламент обязателен для исполнения всеми работниками ГБПОУ АКТТ (далее -Учреждение), непосредственно осуществляющими защиту ПДн в ИСПДн.

3. Инциденты информационной безопасности

3.1. К инцидентам ИБ относятся:

- несоблюдение требований по защите ПДн:
- использование ЭВМ в целях, не связанных с выполнением трудовых (служебных, должностных, функциональных) обязанностей;
- утрата носителя ПДн;
- утрата ключевых документов, ключей от помещений и хранилищ, личных печатей, удостоверений, пропусков.
- попытки НСД к ПДн:
- подбор чужого идентификатора и пароля, последующий доступ с использованием чужого пароля;
- изменение настроек, состава, паролей технических средств ИСПДн;
- изменение (увеличение) полномочий доступа;
- нарушение целостности установленных защитных пломб;
- копирование ПДн на неучтенные съемные носители ПДн;
- заражение рабочего места и/или сервера ИСПДн вредоносной программой;
- хищение носителей ПДн;
- хищение технических средств ИСПДн;
- умышленное нарушение работоспособности технических средств ИСПДн;

- хищение криптосредств, ключевых документов, ключей от помещений и хранилищ, личных печатей, удостоверений, пропусков;
- несанкционированное проникновение в помещения ИСПДн;
- очистка электронных журналов мониторинга.
- сбои в работе технических средств ИСПДн Общества.

3.2. К инцидентам ИБ не относятся:

- неудачные попытки вторжений, которые были обнаружены и нейтрализованы с использованием СЗИ;
- неудачные попытки заражения рабочих мест и/или серверов ИСПДн вредоносной программой, которые были обнаружены и нейтрализованы с использованием СЗИ

4. Порядок регистрации событий безопасности

4.1. Регистрация событий безопасности в ИСПДн осуществляется в следующей последовательности:

1) Определение событий безопасности, подлежащих регистрации, и сроков их хранения.
2) Определение состава и содержания информации о событиях безопасности, подлежащих регистрации.
3) Сбор, запись и хранение информации о событиях безопасности.
4) Реагирование на сбои при регистрации событий безопасности.
5) Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них.
6) Генерирование временных меток и (или) синхронизация системного времени в ИСПДн.
7) Защита информации о событиях безопасности.

4.2. События безопасности, подлежащие регистрации в ИСПДн, должны определяться с учетом способов реализации угроз безопасности ПДн для ИСПДн. К событиям безопасности, подлежащим регистрации в ИСПДн, должны быть отнесены любые проявления состояния ИСПДн и ее системы защиты, указывающие на возможность нарушения конфиденциальности, целостности или доступности ПДн, доступности компонентов ИСПДн, нарушения процедур, установленных организационно распорядительными документами по защите ПДн, а также на нарушение штатного функционирования средств защиты информации (далее - СЗИ).

4.3. События безопасности, подлежащие регистрации в ИСПДн, и сроки хранения соответствующих записей регистрационных журналов должны обеспечивать возможность обнаружения, идентификации и анализа инцидентов информационной безопасности, возникших в ИСПДн.

4.4. В ИСПДн подлежат регистрации следующие события:

- вход (выход), а также попытки входа субъектов доступа в ИСПДн и загрузки (остановка) операционной системы;
- подключение съемных машинных носителей ПДн и вывод ПДн на носители;
- запуск (завершение) программ и процессов (заданий, задач), связанных с обработкой ПДн;

- обновление или ошибки при обновлении программных средств ИСПДн и СЗИ;
- попытки доступа программных средств к определяемым защищаемым объектам доступа (техническим средствам, узлам сети, линиям (каналам) связи, внешним устройствам, программам, томам, каталогам, файлам, записям, полям записей) и иным объектам доступа;
- попытки удаленного доступа.

4.5. Состав и содержание информации о событиях безопасности, включаемой в записи регистрации о событиях безопасности, должны, как минимум, обеспечить возможность идентификации типа события безопасности, даты и времени события безопасности, идентификационной информации источника события безопасности, результат события безопасности (успешно или неуспешно), субъекта доступа (пользователя и (или) процесса), связанного с данным событием безопасности.

4.6. При регистрации входа (выхода) субъектов доступа в ИСПДн и загрузки (остановка) операционной системы состав и содержание информации должны, как минимум, включать дату и время входа (выхода) в систему (из системы) или загрузки (остановки) операционной системы, результат попытки входа (успешная или неуспешная), результат попытки загрузки (останова) операционной системы (успешная или неуспешная), идентификатор, предъявленный при попытке доступа.

4.7. При регистрации подключения съемных машинных носителей ПДн и вывода ПДн на съемные носители состав и содержание регистрационных записей должны, как минимум, включать дату и время подключения съемных машинных носителей ПДн и вывода ПДн на съемные носители, логическое имя (номер) подключаемого съемного машинного носителя ПДн, идентификатор субъекта доступа, осуществляющего вывод ПДн на съемный носитель ПДн.

4.8. При регистрации запуска (завершения) программ и процессов (заданий, задач), связанных с обработкой ПДн состав и содержание регистрационных записей должны, как минимум, включать дату и время запуска, имя (идентификатор) программы (процесса, задания), идентификатор субъекта доступа (устройства), запросившего программу (процесс, задание), результат запуска (успешный, неуспешный).

4.9. При регистрации попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам состав и содержание регистрационных записей должны, как минимум, включать дату и время попытки доступа к защищаемому файлу с указанием ее результата (успешная, неуспешная), идентификатор субъекта доступа (устройства), спецификацию защищаемого файла (логическое имя, тип).

4.10. При регистрации попыток доступа программных средств к защищаемым объектам доступа (техническим средствам, узлам сети, линиям (каналам) связи, внешним устройствам, программам, томам, каталогам, записям, полям записей) состав и содержание информации должны, как минимум, включать дату и время попытки доступа к защищаемому объекту с указанием ее результата (успешная, неуспешная), идентификатор субъекта доступа (устройства), спецификацию защищаемого объекта доступа (логическое имя (номер).

4.11. При регистрации попыток удаленного доступа к ИСПДн состав и содержание информации должны, как минимум, включать дату и время попытки

удаленного доступа с указанием ее результата (успешная, неуспешная), идентификатор субъекта доступа (устройства), используемый протокол доступа, используемый интерфейс доступа и (или) иную информацию о попытках удаленного доступа к ИСПДн.

4.12. Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения должен предусматривать:

- возможность выбора Ответственным за обеспечение безопасности ПДн в ИСПДн и (или) Администратором ИСПДн событий безопасности, подлежащих регистрации в текущий момент времени из перечня событий безопасности, определенных в пункте 4.4 настоящего Регламента;
- генерацию (сбор, запись) записей регистрации (аудита) для событий безопасности, подлежащих регистрации (аудиту) в соответствии с составом и содержанием информации, определенными в соответствии с пунктами 4.6-4.11 настоящего Регламента;
- хранение информации о событиях безопасности в течение времени, установленного в пункте 4.3 настоящего Регламента.

4.13. Объем памяти для хранения информации о событиях безопасности должен быть рассчитан и выделен с учетом типов событий безопасности, подлежащих регистрации в соответствии с составом и содержанием информации о событиях безопасности, подлежащих регистрации, в соответствии с пунктами 4.7 - 4.11настоящего Регламента, прогнозируемой частоты возникновения подлежащих регистрации событий безопасности, срока хранения информации о зарегистрированных событиях безопасности.

4.14. В ИСПДн должно осуществляться реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти.

4.15. Реагирование на сбои при регистрации событий безопасности должно предусматривать:

- предупреждение (сигнализация, индикация) о сбоях (аппаратных и программных ошибках, сбоях в механизмах сбора информации или переполнения объема (емкости) памяти) при регистрации событий безопасности;
- реагирование на сбои при регистрации событий безопасности путем изменения Ответственным за обеспечение безопасности ПДн в ИСПДн и (или) Администратором ИСПДн параметров сбора, записи и хранения информации о событиях безопасности, в том числе отключение записи информации о событиях безопасности от части компонентов ИСПДн, запись поверх устаревших хранимых записей событий безопасности.

4.16. Мониторинг (просмотр и анализ) записей регистрации (аудита) должен проводиться для всех событий, подлежащих регистрации в соответствии и с периодичностью, установленной оператором, и обеспечивающей своевременное выявление признаков инцидентов информационной безопасности в ИСПДн.

4.17. В случае выявление признаков инцидентов информационной безопасности в ИСПДн осуществляется планирование и проведение мероприятий по реагированию на выявленные инциденты безопасности в соответствии с порядком проведения разбирательств по фактам возникновения инцидентов в ИСПДн.

4.18. Получение меток времени, включающих дату и время, используемых при генерации записей регистрации (аудита) событий безопасности в ИСПДн, достигается посредством применения внутренних системных часов ИСПДн.

4.19. Защита информации о событиях безопасности (записях регистрации (аудита)) обеспечивается применением мер защиты информации от неправомерного доступа, уничтожения или модифицирования и в том числе включает защиту средств ведения регистрации (аудита) и настроек механизмов регистрации событий.

4.20. Доступ к записям аудита и функциям управления механизмами регистрации (аудита) должен предоставляться только уполномоченным должностным лицам:

- ответственному за обеспечение безопасности ПДн в ИСПДн;
- администратору ИСПДн.

5. Порядок выявления инцидентов информационной безопасности и реагирования на них

5.1. За выявление инцидентов информационной безопасности и реагирование на них отвечают:

- ответственный за обеспечение безопасности ПДн в ИСПДн;
- администратор ИСПДн.

5.2. Работники Учреждения, должны сообщать ответственным за выявление инцидентов информационной безопасности о любых инцидентах, в которые входят:

- факты попыток и успешной реализации несанкционированного доступа в ИСПДн, в помещения, в которых осуществляется обработка ПДн, и к хранилищам ПДн;
- факты сбоя или некорректной работы систем обработки информации;
- факты сбоя или некорректной работы СЗИ;
- факты разглашения ПДн;
- факты разглашения информации о методах и способах защиты и обработки ПДн.

5.3. Все нештатные ситуации, факты вскрытия и опечатывания технических средств, выполнения профилактических работ, установки и модификации аппаратных и программных средств обработки ПДн в ИСПДн должны быть занесены ответственными за выявление инцидентов информационной безопасности в «Журнал учета нештатных ситуаций, фактов вскрытия и опечатывания технических средств, выполнения профилактических работ, установки и модификации аппаратных и программных средств обработки персональных данных в ГБПОУ АКТТ, форма которого установлена в Приложении 1 к настоящему Регламенту или в электронные журналы операционной системы и СЗИ.

5.4. Анализ инцидентов информационной безопасности, в том числе определение источников и причин возникновения инцидентов, осуществляется согласно

порядку проведения разбирательств по фактам возникновения инцидентов информационной безопасности в ИСПДн.

5.5. Меры по устранению последствий инцидентов информационной безопасности, планированию и принятию мер по предотвращению повторного возникновения инцидентов, возлагаются на ответственных за выявление инцидентов информационной безопасности.

6. Основные этапы процесса реагирования на инциденты

6.1. Лица (администратор ИС), занимающиеся реагированием на инциденты должны обеспечить защиту ИСПДн и проинформировать пользователей, о важности мер по обеспечению информационной безопасности.

6.2. Лица, занимающиеся реагированием на инциденты, должны определить, является ли обнаруженное ими с помощью различных систем обеспечения информационной безопасности событие инцидентом или нет. Для этого могут использоваться публичные отчеты, потоки данных об угрозах, средства статического и динамического анализа образцов программного обеспечения и другие источники информации. Статический анализ выполняется без непосредственного запуска исследуемого образца и позволяет выявить различные индикаторы, например, строки, содержащие URL-адреса или адреса электронной почты. Динамический анализ подразумевает выполнение исследуемой программы в защищенной среде (Песочнице) или на изолированной машине с целью выявления поведения образца и сбора артефактов его работы.

6.3. Лица, занимающиеся реагированием на инциденты, должны идентифицировать скомпрометированные компьютеры и настроить правила безопасности таким образом, чтобы заражение не распространилось дальше по сети. Кроме того, на этом этапе необходимо перенастроить сеть таким образом, чтобы ИСПДн могли продолжать работать без зараженных машин.

6.4. Далее лица, занимающиеся реагированием на инциденты, удаляют вредоносное программное обеспечение, а также все артефакты, которые оно могло оставить на зараженных компьютерах в ИСПДн.

6.5. Ранее скомпрометированные компьютеры вводятся обратно в сеть. При этом лица, занимающиеся реагированием на инциденты, некоторое время продолжают наблюдать за состоянием этих машин и ИСПДн в целом, чтобы убедиться в полном устранении угрозы.

6.6. Лица, занимающиеся реагированием на инциденты, анализируют произошедший инцидент, вносят необходимые изменения в конфигурацию программного обеспечения и оборудования, обеспечивающего информационной безопасности, и формируют рекомендации для того, чтобы в будущем предотвратить подобные инциденты. При невозможности полного предотвращения будущей атаки составленные рекомендации позволят ускорить реагирование на подобные инциденты.

7. Порядок проведения разбирательств по фактам возникновения инцидентов информационной безопасности

7.1. Для проведения разбирательств по фактам возникновения инцидентов информационной безопасности создаётся комиссия, состоящая не менее чем из трех человек с обязательным включением в её состав:

- ответственного за обеспечение безопасности ПДн в ИСПДн;
- администратора ИСПДн.

7.2. Председатель комиссии организует работу комиссии, решает вопросы взаимодействия комиссии с руководителями и работниками структурных подразделений организации, готовит и ведёт заседания комиссии, подписывает протоколы заседаний. По окончании работы комиссии готовится заключение по результатам проведённого разбирательства, которое передается на рассмотрение Директору Учреждения.

7.3. При проведении разбирательства устанавливаются:

- наличие самого факта совершения инцидента информационной безопасности, служащего основанием для вынесения соответствующего решения;
- время, место и обстоятельства возникновения инцидента, а также оценка его последствий;
- конкретный работник, совершивший инцидент информационной безопасности или повлекший своими действиями возникновения инцидента;
- наличие и степень вины работника, совершившего инцидент информационной безопасности или повлекшего своими действиями возникновение инцидента;
- цели и мотивы, способствовавшие совершению инцидента информационной безопасности.

7.4. В целях проведения разбирательства все работники обязаны по первому требованию членов комиссии предъявить для проверки все числящиеся за ними материалы и документы, дать устные или письменные объяснения об известных им фактах по существу заданных им вопросов.

7.5. Работник, совершивший инцидент информационной безопасности или повлекший своими действиями возникновения инцидента, обязан по требованию комиссии представить объяснения в письменной форме не позднее трех рабочих дней с момента получения соответствующего требования. Комиссия вправе поставить перед работником перечень вопросов, на которые работник обязан ответить. В случае отказа работника от письменных объяснений, комиссией составляется акт.

7.6. Работник имеет право, по согласованию с председателем комиссии, знакомиться с материалами разбирательства, касающимися лично его, и давать по поводу них свои комментарии, предоставлять дополнительную информацию и документы. По окончании разбирательства работнику для ознакомления предоставляется итоговый акт с выводами комиссии.

7.7. В случае давления на работника со стороны других лиц (не из состава комиссии) в виде просьб, угроз, шантажа и др., по вопросам, связанным с проведением разбирательства, работник обязан сообщить об этом председателю комиссии.

7.8. До окончания работы комиссии и вынесения решения членам комиссии запрещается разглашать сведения о ходе проведения разбирательства и ставшие известные им обстоятельства.

7.9. В процессе проведения разбирательства комиссией выясняются:

- перечень разглашенных сведений;
- причины разглашения сведений;
- лица, виновные в разглашении сведений;
- размер (экспертную оценку) причиненного ущерба;
- недостатки и нарушения, допущенные работниками при работе с ПДн;
- иные обстоятельства, необходимые для определения причин разглашения ПДн, степени виновности отдельных лиц, возможности применения к ним мер воздействия.

7.10. По завершении разбирательства комиссией составляется заключение. В заключении указываются:

- основание для проведения в разбирательства;
- состав комиссии и время проведения разбирательства;
- сведения о времени, месте и обстоятельствах возникновения инцидента информационной безопасности;
- сведения о работнике, совершившем инцидент информационной безопасности или повлекшем своими действиями возникновения инцидента (должность, фамилия, имя, отчество, год рождения, время работы в Учреждении, а также в занимаемая должность);
- цели и мотивы работника, способствовавшие совершению инцидента информационной безопасности;
- причины и условия возникновения инцидента информационной безопасности;
- данные о характере и размерах причиненного в результате инцидента ущерба;
- предложения о мере ответственности работника, совершившего инцидент информационной безопасности или повлекшего своими действиями возникновения инцидента.

7.11. На основании заключения выносится решение о применении мер ответственности к работнику, совершившему инцидент или повлекшему своими действиями возникновению инцидента, также о возмещении ущерба виновным работником (или его законным представителем), которое доводится до указанного работника в письменной форме под расписку.

7.12. Все материалы разбирательства относятся к информации ограниченного доступа и хранятся в течение 5 лет. Копии заключения и распоряжения по результатам разбирательства приобщаются к личному делу работника, в отношении которого оно проводилось.

8. Ответственность

8.1. Все работники, осуществляющие защиту ПДн, обязаны ознакомиться с данным Регламентом под подпись.

8.2. Работники несут персональную ответственность за выполнение требований настоящего Регламента.

9. Срок действия и порядок внесения изменений

9.1. Настоящий Регламент вступает в силу с момента его утверждения и действует бессрочно.

9.2. Настоящий Регламент подлежит пересмотру не реже одного раза в три года.

9.3. Изменения и дополнения в настоящий Регламент вносятся приказом Директора.

Приложение 1 к Регламенту

ФОРМА

Журнал учета нештатных ситуаций, фактов вскрытия и опечатывания технических средств, выполнения профилактических работ, установки и модификации аппаратных и программных средств обработки информации в ГБПОУ АКТТ

п/п	Дата	Краткое описание выполненной работы (нештатной ситуации)	ФИО Ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных, подпись	ФИО Администратора информационной системы, подпись	Примечание
1	2	3	4	5	6

».

1.10. Дополнить Положение Приложением № 4 «Инструкция по проведению антивирусного контроля» в следующей редакции:

«

Приложение № 4

Инструкция по проведению антивирусного контроля

1. Настоящая Инструкция предназначена для пользователей, хранящих и обрабатывающих информацию на автоматизированных рабочих местах (АРМ) локально-вычислительной сети Государственного бюджетного профессионального образовательного учреждения «Арзамасский коммерческо-технический техникум».

2. Антивирусный контроль проводится в целях обеспечения антивирусной защиты на АРМ ЛВС.

3. Установку и настройку антивирусных пакетов, а также периодическую проверку всех программ, установленных на АРМ пользователей осуществляет специалист организации (указать должность).

4. На АРМ запрещается установка программного обеспечения, не связанного с выполнением функций, предусмотренных технологическим процессом обработки информации.

5. К применению на АРМ допускаются только лицензионные антивирусные средства.

6. Пользователь АРМ при работе с гибкими магнитными носителями информации обязан перед началом работы осуществить проверку гибких магнитных дисков (ГМД) на предмет отсутствия компьютерных вирусов.

7. Во время работы запрещается отключать средства антивирусной защиты.

8. Пользователь ЛВС должен ежедневно проверять жесткие магнитные диски (ЖМД) АРМ на наличие вредоносных программ.

9. При обнаружении компьютерного вируса пользователь обязан немедленно осуществить лечение зараженных файлов путем выбора соответствующего пункта меню антивирусной программы и поставить в известность специалиста организации.

10. Техник проводит, в случае необходимости, повторное лечение зараженных файлов путем выбора соответствующего пункта меню антивирусной программы и после этого вновь проводит антивирусный контроль.

11. В случае обнаружения на ГМД нового вируса, не поддающегося лечению, пользователь обязан прекратить использование ГМД.

12. В случае обнаружения на ЖМД не поддающегося лечению вируса, техник обязан поставить в известность администратора безопасности информации, прекратить работу на АРМ и в возможно короткие сроки обновить пакет антивирусных программ.

13. Периодическое обновление антивирусных пакетов на сервере осуществляют администраторы безопасности информации организации.».

1.11. Дополнить Положение Приложением № 5 «Инструкция по организации парольной защиты» в следующей редакции:

«

Приложение № 5

Инструкция по организации парольной защиты

1. Данная инструкция регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей на автоматизированных рабочих местах (АРМ) сотрудников ГБПОУ АКТТ (далее – организация).

2. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей на компьютерах пользователей возлагается на специалиста организации.

3. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей на серверах возлагается на администраторов безопасности информации.

4. Личный пароль должен генерироваться и распределяться централизованно либо выбираться пользователем автоматизированной системы самостоятельно с учетом следующих требований:

— длина пароля должна быть не менее 6 символов;

— пароль не должен включать в себя легко вычисляемые сочетания символов, а также общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.);

5. При смене пароля новое значение должно отличаться от предыдущего не менее чем в 6 позициях;

6. Личный пароль пользователь не имеет права сообщать никому.

7. Владелец пароля должен быть ознакомлен под роспись с перечисленными выше требованиями и предупрежден об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение парольной информации.

8. В случае возникновении нештатных ситуаций, форс-мажорных обстоятельств и т.п. технологической необходимости использования имен и паролей сотрудника

(исполнителя) в его отсутствие, сотрудник обязан сразу же сменить свой пароль на новый.

9. Плановая смена паролей пользователя должна проводиться регулярно, не реже одного раза в 6 месяцев.

10. Внеплановая смена личного пароля или удаление учетной записи пользователя автоматизированной системы в случае прекращения его полномочий (увольнение, переход на другую работу внутри предприятия и т.п.) должна производиться немедленно после окончания последнего сеанса работы данного пользователя с системой администратором безопасности информации.

11. В случае компрометации личного пароля пользователя автоматизированной системы должны быть немедленно предприняты меры в соответствии с п.7 настоящей Инструкции в зависимости от полномочий владельца скомпрометированного пароля.

12. Пароли пользователей (вместе с именами соответствующих учетных записей) должны храниться в запечатанном конверте в сейфе администратора безопасности информации.

13. Хранение сотрудником (исполнителем) значений своих паролей на бумажном носителе допускается только в личном, опечатанном владельцем пароля сейфе.

14. Пользователю следует помнить, что при смене пароля на компьютере пользователя доступ к сетевым ресурсам под новым паролем без соответствующей смены пароля на сервере невозможен.».

1.12. Дополнить Положение Приложением № 6 «Порядок допуска лиц в помещения, в которых расположены элементы информационных систем персональных данных и ведется их обработка в рабочее и нерабочее время, а также в нештатных ситуациях» в следующей редакции:

«

Приложение № 6

Порядок допуска лиц в помещения, в которых расположены элементы информационных систем персональных данных и ведется их обработка в рабочее и нерабочее время, а также в нештатных ситуациях

1. Настоящий Порядок охраны и Порядок доступа лиц в помещения, в которых расположены элементы информационных систем персональных данных и ведется обработка персональных данных в рабочее и нерабочее время, а также нештатных ситуациях (далее - Порядок), устанавливает единые требования к доступу в служебные помещения в целях предотвращения нарушения прав субъектов персональных данных, обрабатываемых в ГБПОУ АКТТ (далее ОУ) и обеспечения соблюдения требований законодательства о персональных данных.

2. Настоящий Порядок обязателен для применения и исполнения всеми работниками ГБПОУ АКТТ.

3. Объектами охраны ОУ:

— помещения, в которых происходит обработка информации ограниченного доступа с использованием средств автоматизации или без использования данных средств;

— помещения, в которых установлены компьютеры, серверы и коммутационное оборудование, как защищенные, так и не защищенные средствами криптографической защиты (далее - СКЗИ), участвующие в обработке персональных данных в информационных системах.

— помещения, в которых хранятся ключевые документы СКЗИ.

4. Помещения, в которых ведется обработка персональных данных, должны обеспечивать сохранность информации и технических средств, исключать возможность бесконтрольного проникновения в помещение и их визуального просмотра посторонними лицами.

5. Бумажные носители персональных данных и электронные носители персональных данных (диски, флеш-накопители) хранятся в металлических шкафах, оборудованных опечатывающими устройствами.

6. Доступ в помещения

6.1. Доступ в помещения в рабочее время

В рабочее время доступ в помещения, в которых расположены элементы ИСПДн, разрешен только работникам, указанным в соответствующем утвержденном перечне лиц.

В рабочее время помещения, где расположены элементы ИСПДн, должны закрываться на замок и открываться только для санкционированного прохода,

Доступ обслуживающего персонала для уборки помещения допускается только в присутствии пользователей ИСПДн.

6.2. Доступ в помещения в нерабочее время

В нерабочее время доступ в помещения, в которых расположены элементы ИСПДн, разрешен только работникам, указанным в соответствующем перечне лиц при наличии служебной записки, подписанной руководителем подразделения и заверенной ответственным за обеспечение безопасности ПДн.

6.3. Доступ в помещения в нештатных ситуациях

Если перед вскрытием помещений обнаружено нарушение целостности замков, то помещения не вскрываются, составляется акт о случившемся и немедленно докладывается руководителю организации, администратору ИБ и службе безопасности, и принимаются меры по охране помещений до прибытия службы безопасности.

В дневное время суток сотрудник, обнаруживший нештатную ситуацию, должен поставить в известность непосредственного руководителя структурного подразделения — устно, администратора ИБ — устно, при необходимости — письменно.

В ночное время суток при возникновении нештатной ситуации, должна быть оповещена служба безопасности (охрана), событие в обязательном порядке регистрируется в журнале дежурств, с указанием точного времени инцидента, краткого описания событий, с указанием ФИО оповещенных лиц, описанием действий, направленных на устранение нештатной ситуации. Если создается угроза уничтожения ПДн, то дежурный по организации вместе с подразделением охраны имеет право вскрыть помещения и принять меры к спасению технических средств и документов,

При этом также составляется служебная записка о случившемся и немедленно докладывается лицу, ответственному за обеспечение безопасности ПДн.

7. Вскрытие и закрытие (опечатывание) помещений, в которых ведется обработка персональных данных, производится работниками, имеющими право доступа в данные помещения.

8. Перед закрытием помещений, в которых ведется обработка персональных данных, по окончании рабочего времени работники, имеющие право доступа в помещения, обязаны:

— убрать бумажные носители персональных данных и электронные носители персональных данных (диски, флеш-карты) в шкафы, закрыть и опечатать шкафы;

— отключить технические средства (кроме постоянно действующей техники) и электроприборы от сети;

— выключить освещение;

— закрыть окна;

— подключить охранную сигнализацию либо опечатать помещение.

9. Перед открытием помещений, в которых ведется обработка персональных данных, работники, имеющие право доступа в помещения, обязаны:

— провести внешний осмотр с целью установления целостности двери и замка;

— открыть дверь и осмотреть помещение, проверить наличие и целостность печатей на шкафах.

10. При обнаружении неисправности двери и запирающих устройств работники обязаны:

— не вскрывая помещение, в котором ведется обработка персональных данных, доложить непосредственному руководителю и специалисту по защите информации;

— в присутствии не менее двух иных работников, включая непосредственного руководителя, вскрыть помещение и осмотреть его;

— составить акт о выявленных нарушениях и передать его руководителю ОУ для организации служебного расследования.

11. Право самостоятельного входа в помещения, где обрабатываются персональные данные, имеют только работники, непосредственно работающие в данном помещении.

Иные работники имеют право пребывать в помещениях, где обрабатываются персональные данные, только в присутствии работников, непосредственно работающих в данных помещениях.

12. При работе с информацией, содержащей персональные данные, двери помещений должны быть всегда закрыты.

Присутствие иных лиц, не имеющих права доступа к персональным данным, должно быть исключено.

При невозможности обеспечения отсутствия иных лиц в помещении при обработке персональных данных, необходимо развернуть монитор (при обработке ПДн на АРМ) таким образом, чтобы исключить подсматривание.

13. Техническое обслуживание компьютерной и организационной техники, сопровождение программных средств, уборка помещения, в котором ведется обработка

персональных данных, а также проведение других работ осуществляются в присутствии работника, работающего в данном помещении или лица, ответственного за данное помещение.

14. Ответственность за соблюдение порядка доступа в помещения, в которых ведется обработка персональных данных, возлагается на Руководителей отделов, обрабатывающих персональные данные.».

2. Настоящие изменения вступают в силу со дня подписания и распространяются на правоотношения, возникшие с 1 сентября 2025 г.

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

№ изменения	Краткое содержание изменения, отметка о ревизии	Номер листа				Всего листов	ФИО, должность лица, внесшего изменения	Дата внесения изменения
		измененного	замененного	нового	изъятого			

ЛИСТ СОГЛАСОВАНИЯ

СОГЛАСОВАНО:

№ п/п	Должность	ФИО	Подпись	Дата
1.	Заместитель директора по УПРиЭД	А.Н. Ушанков		3 09 25
2.	Заместитель директора по ВР	С.Ю. Полякова		3.09.25
3.	Заместитель директора по УиНМР	Н.В. Слюдова		3.09.25
4.	Заместитель директора по ОВ	А.А. Домахин		03.09.2025
5.	Заместитель директора по БиАХЧ	П.В. Лашенков		3.09.25
6.	Председатель ППО в ГБПОУ АКТТ	Г.А. Перелыгина		03.09.25
7.	Начальник отдела ИТ	Е.Г. Зайцев		3.09.25
8.	Юрисконсульт	Т.В. Гринина		03.09.25

СОГЛАСОВАНО
ППО в ГБПОУ АКТТ
Протокол от «27» августа 2025 г. № 50

ЛИСТ РАССЫЛКИ ДОКУМЕНТА

Фамилия, инициалы	Должность	№ экз.	Форма рассылки	Дата получения	Подпись в получении
А.Н. Ушанков	Заместитель директора по УПРиЭД	*1*	*электронная*	3 09 25	
С.Ю. Полякова	Заместитель директора по ВР	*1*	*электронная*	3.09.25	
Н.В. Слюдова	Заместитель директора по УиНМР	*1*	*электронная*	3.09.25	
А.А. Домахин	Заместитель директора по ОВ	*1*	*электронная*	03.09.2025	
П.В. Лашенков	Заместитель директора по БиАХЧ	*1*	*электронная*	3.09.25	
Г.А. Перелыгина	Председатель ППО в ГБПОУ АКТТ	*1*	*электронная*	03.09.25	
Е.Г. Зайцев	Начальник отдела ИТ	*1*	*электронная*	03.09.25	
Т.В. Гринина	Юрисконсульт	*1*	*электронная*	03.09.25	