МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ ТЫВА
Государственное бюджетное профессиональное образовательное учреждение
Республики Тыва
«Тувинский техникум информационных технологий»

ПРИКАЗ

«04» 12 2023 г. №1641

г. Кызыл

Об утверждении Политики информационной безопасности в ГБПОУ РТ «Тувинский техникум информационных технологий»

В соответствии с Федеральным законом от 27.07.2006 г. №152-ФЗ «О персональных данных», Федеральным законом от 27.07.2006 г. «Об информации, информационных технологиях и о защите информации»,

ПРИКАЗЫВАЮ:

1. Утвердить Политику информационной безопасности в ГБПОУ РТ «Тувинский техникум информационных технологий» согласно приложению.
2. Программисту (Хертек А.К.) разместить настоящее положение в официальном сайте ГБПОУ РТ «Тувинский техникум информационных технологий».
3. Контроль за исполнением настоящего приказа оставляю за собой.

Директор Ховалыг С-С.А.

	Министерство образования Республики Тыва
	Государственное бюджетное профессиональное образовательное учреждение Республики Тыва «Тувинский техникум информационных технологий»

УТВЕРЖДЕН
приказом № 1641
от 04.12.2023 г

Политика информационной безопасности в Государственном бюджетном профессиональном образовательном учреждении Республики Тыва «Тувинский техникум информационных технологий»

ЛНА-47
Версия 1.0

Принято на заседании
Педагогического совета
Протокол № 1
«25» 08 2023 г.

Ответственность	Должность	Фамилия/подпись	Дата
Разработал	Специалист по работе с общественностью	Лен-оол А.Ю.	05.12.2023
Согласовал	Заместитель директора по инновационно-цифровому образованию	Ооржак М-Н.М.	
Согласовал	Юрист-консульт	А.А. Дууза	
Согласовал	Председатель ССУ	Ч.Д. Куулар	
Согласовал	Председатель Родкомитета	У.Т. Ховалыг	

Кызыл, 2023 г.

Содержание

1.Общие положения

1.1. Целью настоящей политики является, обеспечение безопасности объектов, защиты ГБПОУ РТ «Тувинский техникум информационных технологий» (далее – ГБПОУ РТ «ТТИТ») от всех видов угроз, внешних и внутренних, умышленных и непреднамеренных, минимизация ущерба от возможной реализации угроз безопасности ПДн (УБПДн).

1.2. Требования настоящей Политики распространяются на всех сотрудников ГБПОУ РТ «ТТИТ» (штатных, временных, работающих по контракту и т.п.), а также всех прочих лиц (подрядчики, аудиторы и т.п.).

1.3. Положения и требования Политики распространяются на все подразделения ГБПОУ РТ «ТТИТ», основных разработчиков и исполнителей, которые участвуют в разработке, создании, развертывании, вводе в эксплуатацию информационной системы, в части их касающейся.

1.4. Безопасность персональных данных достигается путем исключения 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.

1.5. Информация и связанные с ней ресурсы должны быть доступны для авторизованных пользователей.

Должно осуществляться своевременное обнаружение и реагирование на УБПДн.

Должно осуществляться предотвращение преднамеренных или случайных, частичных или полных несанкционированных модификаций или уничтожения данных.

Состав объектов, подлежащих защите представлен в Перечень персональных данных, обрабатываемых в ИСПДн.

1.6. Нормативные ссылки:

Настоящая политика разработана на основании следующих документов:

- ISO/IEC IS 17799-2000. Information Technology. Code of practice for information se-curity management.
- BS 7799-2-2002. Information security management systems. Specification with guid-ance for use.
- COBIT Control Objectives for Information and related Technology, 3rd Edition, July 2000.
- Федеральный закон «О коммерческой тайне» № 98-ФЗ.
- Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».
- Нормативно-методические документы Федеральной службы по техническому и экспертному контролю Российской Федерации (далее - ФСТЭК России) по обеспечению безопасности ПДн при их обработке в ИСПДн:
- Приказа ФСТЭК России №21 от 18.02.2013 г. «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности

персональных данных при их обработке в информационных системах персональных данных».

1.7. Список терминов и определений

Владелец информационного актива - подразделение ГБПОУ РТ «ТТИТ», реализующее полномочия владения, пользования и распоряжения информацией в соответствии со своими функциями и задачами. Владелец информационного актива определяется на этапе создания соответствующих массивов данных.

Данные – различные виды информации, представленные в электронной форме.

Доступность – обеспечение того, что авторизованные пользователи имеют доступ к информационному активу всегда, когда это необходимо.

Идентификация риска – процесс выявления и классификации рисков.

Информационный актив – различные виды информации (платежной, финансово-аналитической, медицинской, служебной, управляющей, справочной и пр.) на всех этапах ее жизненного цикла, обеспечивающей основную деятельность ГБПОУ РТ «ТТИТ» и представляющей ценность с точки зрения достижения поставленных целей.

Информационная безопасность – состояние и режим эксплуатации средств хранения, доставки и автоматизированной обработки, при котором обеспечивается уровень защиты информационных активов, достаточный для минимизации ущерба, вызванного возможными нарушениями безопасности.

Информационная система персональных данных – 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.

Инцидент информационной безопасности – действительное, предпринимаемое или вероятное нарушение информационной безопасности. Нарушение может быть вызвано ошибками персонала, неправильным функционированием технических средств, природными факторами, преднамеренными злоумышленными действиями, приводящими к нарушению доступности, целостности, конфиденциальности информации.

Конфиденциальность – обеспечение доступности информации только ограниченному кругу лиц, имеющих соответствующие полномочия.

Критичный информационный актив (критичная информация) – информация, создание, модификация и обработка которой связаны с повышенным риском информационной безопасности.

Критичные операции – операции, связанные с повышенными рисками информационной безопасности.

Критичные процессы/системы – процессы/системы, связанные с использованием критичных информационных активов.

Критичные уязвимости – недостатки и ошибки системного и прикладного программного обеспечения на всех уровнях архитектуры автоматизированных систем, создающие повышенные риски информационной безопасности критичным информационным активам.

Межсетевой экран – локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в информационную систему персональных данных и (или) выходящей из информационной системы.

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

Обезличивание персональных данных – действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных.

Оценка риска – оценка вероятности реализации риска и величины возможных потерь при реализации конкретного вида риска и/или совокупных рисков, принимаемых на себя ГБПОУ РТ «ТТИТ».

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

Программное (программно-математическое) воздействие – несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ.

Риск – возможность возникновения у ГБПОУ РТ «ТТИТ» финансовых потерь (убытков), незапланированных расходов или возможность снижения планируемых доходов, возможность потери репутации.

Операционный риск – риск, возникающий в результате недостатков в организации деятельности ГБПОУ РТ «ТТИТ», используемых технологиях, функционировании информационных систем, неадекватных действий или ошибок сотрудников, а также в результате внешних событий.

Информационный риск (ИТ-риск, риск автоматизации процессов) – риск, связанный с использованием информационных технологий, неудовлетворительным состоянием автоматизированных систем ГБПОУ РТ «ТТИТ».

Риск информационной безопасности – риск, являющийся составной частью ИТ-риска, возникающий вследствие наличия угроз безопасности информационным активам ГБПОУ РТ «ТТИТ».

Руководство – директор, заместители директора, начальники структурных подразделений.

Система обеспечения информационной безопасности – часть общей системы менеджмента ГБПОУ РТ «ТТИТ», предназначенная для создания,

реализации, эксплуатации, мониторинга, анализа, поддержки и повышения информационной безопасности ГБПОУ РТ «ТТИТ». Включает структуру, политики, совокупность мероприятий, методов и средств, обеспечивающих требуемый уровень безопасности информационных активов участниками соответствующих процессов.

Угроза информационной безопасности – внешний или внутренний фактор, создающий риск информационной безопасности.

Целостность – обеспечение точности и полноты информации и методов ее обработки.

1.8. Сокращения и обозначения

В настоящем положении используются следующие сокращения:

АС - аавтоматизированная система;

АВС - аантивирусные средства;

АРМ - аавтоматизированное рабочее место;

БД - база данных;

ВрП - ввредоносная программа;

ГМД - гибкий магнитный диск;

ИТ (IT) - иинформационные технологии;

ИСПДн - иинформационная система персональных данных;

ГБПОУ РТ «ТТИТ» (Учреждение) – Государственное бюджетное профессиональное образовательное учреждение Республики Тыва «Тувинский техникум информационных технологий»;

ПДн - пперсональные данные;

НДПДн - ннесанкционированный доступ к персональным данным;

МЭ - ммежсетевой экран;

ЛВС - ллокальная вычислительная сеть;

НСД - ннесанкционированный доступ;

ПО - программное обеспечение;

СЗИ - средства защиты информации;

СЗПДн - система (подсистема) защиты персональных данных;

СОВ - система обнаружения вторжений;

СУБД - система управления базами данных;

УБПДн - угрозы безопасности персональных данных;

ЭЦП - электронноцифровая подпись.

2. Система защиты персональных данных

2.1. Система защиты персональных данных (СЗПДн), строится на основании:

- перечня персональных данных, подлежащих защите;
- модели угроз безопасности персональных данных;
- руководящих документов ФСТЭК и ФСБ России.

На основании этих документов определяется необходимый уровень защищенности ПДн каждой ИСПДн Учреждения. На основании анализа

актуальных угроз безопасности ПДн описанного в Модели угроз делается заключение о необходимости использования технических средств и организационных мероприятий для обеспечения безопасности ПДн. Выбранные необходимые мероприятия отражаются в Плане мероприятий по обеспечению защиты ПДн.

2.2. Для каждой ИСПДн должен быть составлен список используемых технических средств защиты, а так же программного обеспечения участвующего в обработке ПДн, на всех элементах ИСПДн:

- АРМ пользователей;
- сервера приложений;
- СУБД;
- граница ЛВС;
- каналов передачи в сети общего пользования и (или) международного обмена, если по ним передаются ПДн.

2.3. В зависимости от уровня защищенности ИСПДн и актуальных угроз, СЗПДн может включать следующие технические средства:

- антивирусные средства для рабочих станций пользователей и серверов;
- средства межсетевого экранирования;
- средства криптографической защиты информации, при передаче защищаемой информации по каналам связи.

Так же в список должны быть включены функции защиты, обеспечиваемые штатными средствами обработки ПДн операционными системами (ОС), прикладным ПО и специальными комплексами, реализующими средства защиты. Список функций защиты может включать:

- управление и разграничение доступа пользователей;
- регистрация и учет действий с информацией;
- обеспечение целостности данных;
- мониторинг обнаружения вторжений.

Список используемых технических средств отражается в Плане мероприятий по обеспечению защиты персональных данных. Список используемых средств должен поддерживаться в актуальном состоянии. При изменении состава технических средств защиты или элементов ИСПДн, соответствующие изменения должны быть внесены в Список и утверждены руководителем Учреждения или лицом, ответственным за обеспечение защиты ПДн.

3. Требования к подсистемам СЗПДН

3.1. СЗПДн включает в себя следующие подсистемы:

- управления доступом, регистрации и учета;
- обеспечения целостности и доступности;
- антивирусной защиты;
- межсетевого экранирования;
- анализа защищенности;

- обнаружения вторжений;
- криптографической защиты.

3.2. Подсистемы управления доступом, регистрации и учета.

Подсистема управления доступом, регистрации и учета предназначена для реализации следующих функций:

- идентификации и проверка подлинности субъектов доступа при входе в ИСПДн;
- идентификации терминалов, узлов сети, каналов связи, внешних устройств по логическим именам;
- идентификации программ, томов, каталогов, файлов, записей, полей записей по именам;
- регистрации входа (выхода) субъектов доступа в систему (из системы), либо регистрация загрузки и инициализации операционной системы и ее останова.
- регистрации попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам;
- регистрации попыток доступа программных средств к терминалам, каналам связи, программам, томам, каталогам, файлам, записям, полям записей.

Подсистема управления доступом может быть реализована с помощью штатных средств обработки ПДн (операционных систем, приложений и СУБД). Так же может быть внедрено специальное техническое средство или их комплекс осуществляющие дополнительные меры по аутентификации и контролю. Например, применение единых хранилищ учетных записей пользователей и регистрационной информации, использование биометрических и технических (с помощью электронных пропусков) мер аутентификации и других.

3.3. Подсистема обеспечения целостности и доступности.

Подсистема обеспечения целостности и доступности предназначена для обеспечения целостности и доступности ПДн, программных и аппаратных средств ИСПДн Учреждения, а также средств защиты, при случайной или намеренной модификации.

Подсистема реализуется с помощью организации резервного копирования обрабатываемых данных, а также резервированием ключевых элементов ИСПДн.

3.4 Подсистема антивирусной защиты.

Подсистема антивирусной защиты предназначена для обеспечения антивирусной защиты серверов и АРМ пользователей ИСПДн Учреждения.

Средства антивирусной защиты предназначены для реализации следующих функций:

- резидентный антивирусный мониторинг;
- антивирусное сканирование;
- скрипт-блокирование;

- централизованную/удаленную установку/деинсталляцию антивирусного продукта, настройку, администрирование, просмотр отчетов и статистической информации по работе продукта;

- автоматизированное обновление антивирусных баз;

- ограничение прав пользователя на остановку исполняемых задач и изменения настроек антивирусного программного обеспечения;

- автоматический запуск сразу после загрузки операционной системы.

Подсистема реализуется путем внедрения специального антивирусного программного обеспечения на все элементы ИСПДн.

3.5 Подсистема межсетевого экранирования

Подсистема межсетевого экранирования предназначена для реализации следующих функций:

- фильтрации открытого и зашифрованного (закрытого) IP-трафика по следующим параметрам;

- фиксации во внутренних журналах информации о проходящем открытом и закрытом IP-трафике;

- идентификации и аутентификацию администратора межсетевого экрана при его локальных запросах на доступ;

- регистрации входа (выхода) администратора межсетевого экрана в систему (из системы) либо загрузки и инициализации системы и ее программного останова;

- контроля целостности своей программной и информационной части;

- фильтрации пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств;

- фильтрации с учетом входного и выходного сетевого интерфейса как средство проверки подлинности сетевых адресов;

- регистрации и учета запрашиваемых сервисов прикладного уровня;

- блокирования доступа не идентифицированного объекта или субъекта, подлинность которого при аутентификации не подтвердилась, методами, устойчивыми к перехвату;

- контроля за сетевой активностью приложений и обнаружения сетевых атак.

Подсистема реализуется внедрением программно-аппаратных комплексов межсетевого экранирования на границе ЛСВ, классом не ниже 4.

3.6 Подсистема анализа защищенности

Подсистема анализа защищенности, должна обеспечивать выявления уязвимостей, связанных с ошибками в конфигурации ПО ИСПДн, которые могут быть использованы нарушителем для реализации атаки на систему.

Функционал подсистемы может быть реализован программными и программно-аппаратными средствами.

3.7 Подсистема обнаружения вторжений

Подсистема обнаружения вторжений, должна обеспечивать выявление сетевых атак на элементы ИСПДн подключенные к сетям общего пользования и (или) международного обмена.

Функционал подсистемы может быть реализован программными и программно-аппаратными средствами.

3.8 Подсистема криптографической защиты

Подсистема криптографической защиты предназначена для исключения НСД к защищаемой информации в ИСПДн Учреждения, при ее передаче по каналам связи сетей общего пользования и (или) международного обмена.

Подсистема реализуется внедрения криптографических программно-аппаратных комплексов.

4.Пользователи ИСПДН

4.1. В Концепции информационной безопасности определены основные категории пользователей. На основании этих категории должна быть произведена типизация пользователей ИСПДн, определен их уровень доступа и возможности.

4.2. В ИСПДн Учреждения можно выделить следующие группы пользователей, участвующих в обработке и хранении ПДн:

- администратора ИСПДн;
- оператора АРМ;
- технического специалиста по обслуживанию периферийного оборудования.

Данные о группах пользователях, уровне их доступа и информированности должен быть отражен в Положение о разграничении прав доступа к обрабатываемым персональным данным.

4.3. Администратор ИСПДн

Администратор ИСПДн, сотрудник Учреждения, ответственный за настройку, внедрение и сопровождение ИСПДн. Обеспечивает функционирование подсистемы управления доступом ИСПДн и уполномочен осуществлять предоставление и разграничение доступа конечного пользователя (Оператора АРМ) к элементам хранящим персональные данные.

Администратор ИСПДн обладает следующим уровнем доступа и знаний:

- обладает полной информацией о системном и прикладном программном обеспечении ИСПДн;
- обладает полной информацией о технических средствах и конфигурации ИСПДн;
- имеет доступ ко всем техническим средствам обработки информации и данным ИСПДн;
- обладает правами конфигурирования и административной настройки технических средств ИСПДн.

4.4. Оператор АРМ

Оператор АРМ, сотрудник Учреждения, осуществляющий обработку ПДн. Обработка ПДн включает: возможность просмотра ПДн, ручной ввод ПДн в систему ИСПДн, формирование справок и отчетов по информации, полученной

из ИСПД. Оператор не имеет полномочий для управления подсистемами обработки данных и СЗПДн.

4.5. Технический специалист по обслуживанию периферийного оборудования

Технический специалист по обслуживанию, сотрудник Учреждения, осуществляет обслуживание и настройку периферийного оборудования ИСПДн. Технический специалист по обслуживанию не имеет доступа к ПДн, не имеет полномочий для управления подсистемами обработки данных и безопасности.

Технический специалист по обслуживанию обладает следующим уровнем доступа и знаний:

- обладает частью информации о системном и прикладном программном обеспечении ИСПДн;
- обладает частью информации о технических средствах и конфигурации ИСПДн;
- знает, по меньшей мере, одно легальное имя доступа.

4.9 Требования к персоналу по обеспечению защиты ПДн

Все сотрудники ГБПОУ РТ «ТТИТ», являющиеся пользователями ИСПДн, должны четко знать и строго выполнять установленные правила и обязанности по доступу к защищаемым объектам и соблюдению принятого режима безопасности ПДн.

При вступлении в должность нового сотрудника, обязан организовать его ознакомление с должностной инструкцией и необходимыми документами, регламентирующими требования по защите ПДн, а также обучение навыкам выполнения процедур, необходимых для санкционированного использования ИСПДн.

Сотрудник должен быть ознакомлен со сведениями настоящей Политики, принятых процедур работы с элементами ИСПДн и СЗПДн.

Сотрудники ГБПОУ РТ «ТТИТ», использующие технические средства аутентификации, должны обеспечивать сохранность идентификаторов (электронных ключей) и не допускать НСД к ним, а также возможность их утери или использования третьими лицами. Пользователи несут персональную ответственность за сохранность идентификаторов.

Сотрудники ГБПОУ РТ «ТТИТ» должны следовать установленным процедурам поддержания режима безопасности ПДн при выборе и использовании паролей (если не используются технические средства аутентификации).

Сотрудники ГБПОУ РТ «ТТИТ» должны обеспечивать надлежащую защиту оборудования, оставляемого без присмотра, особенно в тех случаях, когда в помещение имеют доступ посторонние лица. Все пользователи должны знать требования по безопасности ПДн и процедуры защиты оборудования, оставленного без присмотра, а также свои обязанности по обеспечению такой защиты.

Сотрудникам запрещается устанавливать постороннее программное обеспечение, подключать личные мобильные устройства и носители информации, а также записывать на них защищаемую информацию.

Сотрудникам запрещается разглашать защищаемую информацию, которая стала им известна при работе с информационными системами ГБПОУ РТ «ТТИТ», третьим лицам.

При работе с ПДн в ИСПДн сотрудники Учреждения обязаны обеспечить отсутствие возможности просмотра ПДн третьими лицами с мониторов АРМ или терминалов.

При завершении работы с ИСПДн сотрудники обязаны защитить АРМ или терминалы с помощью блокировки ключом или эквивалентного средства контроля, например, доступом по паролю, если не используются более сильные средства защиты.

Сотрудники ГБПОУ РТ «ТТИТ» должны быть проинформированы об угрозах нарушения режима безопасности ПДн и ответственности за его нарушение. Они должны быть ознакомлены с утвержденной формальной процедурой наложения дисциплинарных взысканий на сотрудников, которые нарушили принятые политику и процедуры безопасности ПДн.

Сотрудники обязаны без промедления сообщать обо всех наблюдаемых или подозрительных случаях работы ИСПДн, могущих повлечь за собой угрозы безопасности ПДн, а также о выявленных ими событиях, затрагивающих безопасность ПДн, руководству подразделения и лицу, отвечающему за немедленное реагирование на угрозы безопасности ПДн.

5. Ответственность сотрудников ИСПДн ГБПОУ РТ «ТТИТ»

5.1. В соответствии со ст. 24 Федерального закона Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных» лица, виновные в нарушении требований данного Федерального закона, несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

5.2. Действующее законодательство РФ позволяет предъявлять требования по обеспечению безопасной работы с защищаемой информацией и предусматривает ответственность за нарушение установленных правил эксплуатации ЭВМ и систем, неправомерный доступ к информации, если эти действия привели к уничтожению, блокированию, модификации информации или нарушению работы ЭВМ или сетей (статьи 272,273 и 274 УК РФ).

5.3. Администратор ИСПДн и администратор безопасности несут ответственность за все действия, совершенные от имени их учетных записей или системных учетных записей, если не доказан факт несанкционированного использования учетных записей.

5.4. При нарушениях сотрудниками Учреждения – пользователей ИСПДн правил, связанных с безопасностью ПДн, они несут ответственность, установленную действующим законодательством Российской Федерации.

5.5. Приведенные выше требования нормативных документов по защите информации должны быть отражены в Положениях о подразделениях, и должностных инструкциях сотрудников Учреждения.

5.6. Необходимо внести в Положения о подразделениях Учреждения, осуществляющих обработку ПДн в ИСПДн сведения об ответственности их руководителей и сотрудников за разглашение и несанкционированную модификацию (искажение, фальсификацию) ПДн, а также за неправомерное вмешательство в процессы их автоматизированной обработки.

6. Организация системы обеспечения информационной безопасности

6.1. Общее руководство системой обеспечения информационной безопасности в ГБПОУ РТ «ТТИТ» осуществляет директор.

6.2. Директор:

- утверждает и пересматривает политику информационной безопасности ГБПОУ РТ «ТТИТ»;
- организует процесс управления информационной безопасностью в ГБПОУ РТ «ТТИТ», включая определение подразделений, ответственных за управление отдельными процессами обеспечения информационной безопасности, утверждение положений о них;
- обеспечивает условия и утверждает бюджет для эффективной реализации политики информационной безопасности;
- рассматривает информацию и отчеты о состоянии информационной безопасности ГБПОУ РТ «ТТИТ».

Все подразделения ГБПОУ РТ «ТТИТ» и их руководители отвечают за реализацию политики информационной безопасности и управление процессами ее обеспечения в рамках своей компетенции.

6.3. Заместитель директора по инновационно-цифровому образованию:

- проводит первичные и внеплановые инструктажи по информационной безопасности;
- разрабатывает нормативные, инструктивные и методические документы ГБПОУ РТ «ТТИТ» по обеспечению информационной безопасности;
- разрабатывает требования по защите информационных активов в аспектах целостности и конфиденциальности на основе анализа рисков информационной безопасности;
- осуществляет контроль соответствия требованиям на всех стадиях жизненного цикла автоматизированных систем, от проектирования до снятия с эксплуатации;
- обеспечивает управление ключевыми системами средств криптографической защиты;
- организует проведение единой антивирусной политики в ГБПОУ РТ «ТТИТ»;
- проводит аудит подразделений по выполнению данной политики;

- проводит расследования инцидентов и фактов нарушений информационной безопасности и информирует руководство ГБПОУ РТ «ТТИТ» о результатах проведенного расследования;
- организует обучение персонала ГБПОУ РТ «ТТИТ» по вопросам информационной безопасности;
- осуществляет инструментальный контроль и мониторинг текущего состояния информационной безопасности, информирует руководство ГБПОУ РТ «ТТИТ» об инцидентах информационной безопасности;
- осуществляет регистрацию инцидентов, имеющих отношение к информационной безопасности;
- регулярно (не реже одного раза в полгода) информирует руководство ГБПОУ РТ «ТТИТ» о состоянии информационной безопасности в Учреждении, в том числе, в составе сводных отчетов;
- обеспечивает взаимодействие с уполномоченными государственными органами по вопросам лицензирования и сертификации;
- взаимодействует с удостоверяющими центрами сторонних организаций;
- осуществляет анализ, оценку и прогноз риска, связанного с нарушением информационной безопасности ГБПОУ РТ «ТТИТ» и составляет совместно с заместителем директора по инновационно-цифровому образованию список мер по уменьшению этих рисков.

6.4 Программисты:

- обеспечивает выполнение требований информационной безопасности при подключении и администрировании коммуникационного оборудования, операционных систем, СУБД и систем доставки;
- проводит обновление системного ПО, связанное с устранением критичных уязвимостей;
- обеспечивает доступность информационных активов в условиях отказов и других неблагоприятных событий в части коммуникационного оборудования, операционных систем, СУБД и систем доставки.
- обеспечивает выполнение требований информационной безопасности при администрировании автоматизированных систем;
- ведет Фонд программ и документации ГБПОУ РТ «ТТИТ»;
- обеспечивает доступность информационных активов в условиях отказов и других неблагоприятных событий в части автоматизированных систем.
- обеспечивает реализацию требований информационной безопасности в разрабатываемых и находящихся на сопровождении АС.
- разрабатывает требования в области информационных технологий, участвует в формировании решений, связанных с организацией технологических процессов, разрабатывает предложения по использованию современных информационных технологий с учетом требований по обеспечению информационной безопасности.

7. Общие требования по обеспечению информационной безопасности ГБПОУ РТ «ТТИТ»

В основе процессов управления информационной безопасностью ГБПОУ РТ «ТТИТ» лежат следующие общие требования:

7.1 Назначение и распределение ролей и обеспечение доверия к персоналу

«Ролевое» управление является основным механизмом управления полномочиями пользователей и администраторов в автоматизированных системах.

Роли формируются с учетом принципа минимальности полномочий.

7.1.1 Роли пользователю назначаются администратором ИСПДн в момент создания ему логина и пароля.

7.1.2 Ни одна роль не должна позволять пользователю проводить единолично критичные операции.

7.1.3 Критичные технологические процессы должны быть защищены от ошибочных и несанкционированных действий администраторов. Штатные процедуры администрирования, диагностики и восстановления должны выполняться через специальные роли в автоматизированных системах без непосредственного доступа к данным.

7.1.4 В критичных системах по решению владельца информационного актива может вводиться роль администратора информационной безопасности АС, в функции которого входит подтверждение прав и полномочий пользователей, заведенных в системе ее администратором.

7.1.5 Приказы и распоряжения, актуальная информация по вопросам обеспечения информационной безопасности, в том числе по выявленным нарушениям, доводятся до всех сотрудников ГБПОУ РТ «ТТИТ» под роспись.

7.1.6 Реализуются программы обучения персонала ГБПОУ РТ «ТТИТ» и информирования в вопросах обеспечения информационной безопасности. Периодически проверяется и оценивается уровень компетентности персонала в этих вопросах.

7.2 Управление доступом к информационным активам и регистрация.

7.2.1 Все информационные активы идентифицируются, категорируются и имеют своих владельцев.

7.2.2 Не предоставляется доступ к информационной сети ГБПОУ РТ «ТТИТ» электронно вычислительных устройствам не прошедших сетевую идентификацию.

7.2.3 Пользователям ИСПДн запрещается самостоятельно подключать сетевое оборудование (WI-Fi роутеры, планшеты, сотовые телефоны и т.д.) Не корпоротивное сетевое оборудование не будет иметь доступа к информационной сети ГБПОУ РТ «ТТИТ».

7.2.4 Доступ ко всем информационным активам ГБПОУ РТ «ТТИТ» осуществляется только после авторизации пользователя. Средством авторизации (аутентификации является) является доменная учетная запись.

7.2.5 Блокировка учетной записи пользователя производится:

- при увольнении сотрудника в момент отметки обходного листа;

- по распоряжению директора ГБПОУ РТ «ТТИТ»;
- при возникновении угрозы НДПДн из-под данной учетной записи.

7.2.6 Правила сетевого файлообмена в ГБПОУ РТ «ТТИТ» регулируется на основании Положения хранения файлов на сервере.

7.2.7 Проводится периодический (для наиболее критичных систем - не реже одного раза в год) формальный контроль соответствия согласованных и реальных прав доступа к информационным активам текущему статусу пользователя.

7.3 Антивирусная защита

7.3.1 Каждый сотрудник ГБПОУ РТ «ТТИТ» обязан выполнять правила эксплуатации антивирусного ПО и требования антивирусной безопасности в отношении внешних источников и носителей информации, а также сети Интернет, немедленно прекращать работу и информировать службы автоматизации и безопасности при подозрениях на вирусное заражение.

7.3.2 Для снижения влияния человеческого фактора, исключения возможности отключения или не обновления антивирусных средств, контроль и управление антивирусным программным обеспечением, а также устранение выявленных уязвимостей в системном программном обеспечении производится централизованно в автоматизированном режиме. При этом обеспечивается минимально возможный период обновления с учетом обязательного предварительного тестирования на совместимость с системным и прикладным ПО.

7.4 Использование ресурсов Интернет

7.4.1 Использование ресурсов Интернет в подразделениях ГБПОУ РТ «ТТИТ» разрешается исключительно в производственных целях.

7.4.2 Доступ к сайтам информационной сети интернет, посещение которых может угрожать безопасности информационной сети ГБПОУ РТ «ТТИТ» запрещен.

7.4.4 Прямое подключение к рабочим станциям ЛВС ГБПОУ РТ «ТТИТ» мобильных телефонов, беспроводных (радио) интерфейсов, модемов и прочего оборудования, позволяющего выходить в Интернет, запрещается.

7.4.5 Порядок публикации информации в сети Интернет определяется отдельными регламентами.

7.4.6 Запрещается передача необезличенных ПДн через сеть интернет.

7.4.7 На узлах доступа в сеть Интернет принимаются необходимые меры для противодействия хакерским атакам и распространению спама.

7.4.8 Непрерывность критичных рабочих процессов при наступлении отказов и сбоев обеспечивается резервированием оборудования, каналов связи, резервным копированием информации, регулярной проверкой их работоспособности и адекватности. Процедуры восстановления после сбоев документируются в соответствующих регламентах и планах.

7.4.9 Правила резервного копирования определены в Положении резервного копирования информационных систем».

Лист ознакомления

№ п/п	Должность	Ф.И.О.	Подпись	Дата

№ п/п	Должность	Ф.И.О.	Подпись	Дата