Министерство общего и профессионального образования
Свердловской области
Государственное автономное профессиональное образовательное учреждение
Свердловской области
«Нижнетагильский техникум металлообрабатывающих производств и сервиса»

СИСТЕМА МЕНЕДЖМЕНТА КАЧЕСТВА

СТАНДАРТ ТЕХНИКУМА

Утверждаю:
Директор ГАПОУ СО «НТТМПС»
_____ / Залманов Я.П. /
«___» _____ 20___ г.

Код 11.10.1 № 10.1.29
Год 20 19

Номер регистрации _____

Ввести в действие с 19.06.2019
Приказ № 207-л от 19.06.2019

ПОЛИТИКА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ГАПОУ СО «Нижнетагильский техникум
металлообрабатывающих производств и сервиса»

Нижний Тагил, 2019

РАССМОТРЕНО
Протокол Совета автономного учреждения
_____ О.В. Шаймарданова
председатель совета
Протокол от 19.06.2019 № 5

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Политика обеспечения информационной безопасности государственного автономного профессионального образовательного учреждения «Нижнетагильский техникум металлообрабатывающих производств и сервиса», (далее – НТТМПС, техникум) представляет собой совокупность документированных правил, процедур, практических приемов или руководящих принципов в области безопасности информации, которыми руководствуется организация в своей деятельности.

1.2. Разработка и реализация Политики осуществляется путем выработки четкой позиции в решении вопросов информационной безопасности. Политика должна быть доведена до всех работников и обучающихся техникума и быть доступной в установленном порядке для заинтересованных сторон.

1.3. Политика является методологической основой для:

- формирования и проведения единой политики в области обеспечения безопасности информации в техникуме;
- принятия управленческих решений и разработке практических мер по воплощению политики обеспечения информационной безопасности и выработки комплекса мер, направленных на выявление, отражение и ликвидацию последствий реализации различных видов угроз безопасности информации;
- разработки предложений по совершенствованию правового, нормативного, технического и организационного обеспечения информационной безопасности в техникуме.

1.4. Использование Политики в качестве основы для построения комплексной системы обеспечения информационной безопасности позволит оптимизировать затраты на ее построение. При разработке Политики необходимо учитывать основные принципы создания комплексных систем обеспечения информационной безопасности, характеристики и возможности организационно-технических методов и аппаратно-программных средств защиты информации и противодействия угрозам безопасности информации.

1.5. Действие разрабатываемой Политики не распространяется на отношения, возникающие при обработке информации ограниченного доступа, содержащей сведения, составляющие государственную тайну. Защита информации, содержащей сведения, составляющие государственную тайну, осуществляется в соответствии с законодательством Российской Федерации о государственной тайне.

2. Перечень нормативных правовых актов РФ, действующих в области обеспечения информационной безопасности

2.1. Политика разрабатывается с учетом требований нормативных правовых актов Российской Федерации, нормативных и методических документов, а также национальных стандартов, действующих в области обеспечения информационной безопасности:

- Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;
- Федеральный закон "О защите детей от информации, причиняющей вред их здоровью и развитию" от 29.12.2010 № 436-ФЗ;
- Доктрина информационной безопасности Российской Федерации, утвержденная Указом Президента Российской Федерации от 05.12.2016 № 646;

- Требования к защите персональных данных при их обработке в информационных системах персональных данных, утвержденные Постановлением Правительства Российской Федерации от 01.11.2012 № 1119;
- Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утвержденное Постановлением Правительства Российской Федерации от 15.09.2008 № 687;
- Требования к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем, и дальнейшего хранения содержащейся в их базах данных информации, утвержденные Постановление Правительства Российской Федерации от 06.07.2015 № 676;
- Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденные приказом ФСТЭК России от 18.02.2013 № 21;
- Состав и содержание 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, утвержденные приказом ФСБ России от 10.07.2014 № 378.

3. Цели и задачи обеспечения информационной безопасности

3.1. Основной целью, на достижение которой должны быть направлены положения разрабатываемой Политики, является защита информации, содержащейся в информационных системах техникума от наиболее распространенных угроз информационной безопасности, вызванных неэффективностью процедур контроля, технологических сбоев, несанкционированных действий сотрудников или иных форм незаконного вмешательства в информационные ресурсы и информационные системы.

Указанная цель достигается посредством обеспечения и постоянного поддержания конфиденциальности, целостности и доступности информации.

3.2. Обеспечение цели информационной безопасности осуществляется через решение следующих задач, таких как:

- оценка состояния информационной безопасности, прогнозирование и обнаружение угроз безопасности информации, определение приоритетных направлений их предотвращения и ликвидации последствий их проявления;
- обеспечение соблюдения требований законодательства Российской Федерации в области информационной безопасности;
- возложение ответственности за обеспечение безопасности информации в информационных системах на каждого сотрудника техникума в пределах его полномочий;
- обеспечение эффективной работы механизмов оперативного реагирования на компьютерные инциденты информационной безопасности;
- разграничение доступа пользователей к информационным, аппаратным, программным и иным ресурсам, защита информации от несанкционированного доступа;
- обеспечение работоспособности криптографических средств защиты информации;
- постоянный контроль выполнения требований законодательства Российской Федерации в области обеспечения информационной безопасности.

4. Основные направления деятельности по обеспечению информационной безопасности

4.1. Деятельность по обеспечению информационной безопасности призвана способствовать снижению рисков от угроз в информационной сфере, повышению эффективности и устойчивости в управлении информационными ресурсами и системами.

4.2. К основным направлениям обеспечения информационной безопасности относятся:

- правовое обеспечение информационной безопасности – деятельность направлена на создание и поддержание в актуальном состоянии системы локальных нормативных актов, регламентирующих деятельность по обеспечению информационной безопасности;
- обеспечение информационной безопасности при управлении информационными ресурсами деятельность направлена на идентификацию, классификацию информационных систем и ресурсов, а также их владельцев, формирование и поддержание необходимого уровня информационной безопасности информационных ресурсов;
- обеспечение информационной безопасности, связанное с сотрудниками – деятельность направлена на минимизацию рисков, вызванных действиями сотрудников в отношении информационных ресурсов, путем создания системы непрерывного обучения, тренировки и проверки осведомленности всех сотрудников по вопросам обеспечения информационной безопасности;
- физическая безопасность информационных ресурсов – деятельность направлена на минимизацию и предотвращение ущерба, вызванного физическим воздействием на информационные системы и ресурсы;
- управление доступом к информационным ресурсам – деятельность направлена на создание порядка доступа к информационным ресурсам, контроль и мониторинг доступа;
- управление инцидентами информационной безопасности деятельность направлена на проведение мероприятий по своевременному выявлению и реагированию на инциденты информационной безопасности;
- соответствие обязательным требованиям деятельность направлена на соответствие требованиям законодательства Российской Федерации, локальных нормативных актов по обеспечению информационной безопасности.

5. Принципы формирования системы обеспечения информационной безопасности

5.1. Построение системы обеспечения информационной безопасности в техникуме и ее функционирование осуществляется в соответствии с основными принципами формирования системы обеспечения информационной безопасности.

5.2. К основным принципам формирования системы обеспечения информационной безопасности в техникуме относятся:

законность – предполагает разработку системы обеспечения информационной безопасности в соответствии с действующим законодательством Российской Федерации в данной области с применением всех дозволенных методов обнаружения и пресечения правонарушений при работе с информацией. Все пользователи информационных систем должны иметь представление об ответственности за правонарушения в области обеспечения информационной безопасности;

системность – предполагает учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, имеющих существенное значение для понимания и решения проблемы обеспечения информационной безопасности.

При создании системы защиты должны учитываться все слабые и наиболее уязвимые места информационных систем, а также характер, возможные объекты и направления атак на них со стороны нарушителей, пути проникновения в информационные системы и несанкционированного доступа к информации;

персональная ответственность предполагает возложение персональной ответственности на каждого сотрудника в пределах его должностных полномочий за несоблюдение регламентирующих документов в области обеспечения информационной безопасности;

минимизация полномочий – предполагает предоставление прав доступа сотрудникам к информационным ресурсам в том случае и объеме, необходимом для качественного выполнения своих служебных (трудовых) обязанностей;

своевременность – предполагает своевременность выявления проблем, связанных с обеспечением информационной безопасности, и обнаружение угроз безопасности информации, потенциально способных нанести ущерб;

комплексный подход – предполагает всестороннее обеспечение информационной безопасности и предусматривает использование взаимоувязанных программно-технических, организационных, правовых мер обеспечения информационной безопасности на единой концептуальной основе.

обоснованность и техническая реализуемость – информационные технологии, технические и программные средства, средства и меры защиты информации должны быть реализованы на современном уровне развития науки и техники, обоснованы с точки зрения достижения заданного уровня безопасности информации и экономической целесообразности, а также должны соответствовать установленным нормам и требованиям по информационной безопасности;

обязательность контроля – предполагает обязательность и своевременность выявления и пресечения попыток нарушения установленных правил обеспечения информационной безопасности. Выявленные недостатки системы обеспечения информационной безопасности должны немедленно доводиться до сведения руководителя организации, а также оперативно устраняться.

6. Основные организационные, технические и правовые меры обеспечения безопасности информации

Для организации и внедрения системы защиты информации в техникуме важное значение имеет анализ технических, структурных, эксплуатационных и иных особенностей информационных систем, используемых технологий и архитектурных решений.

В данном разделе целесообразно указать меры защиты информации, включающие в себя правовые (законодательные), организационные, технические и физические, а также применение криптографических методов и средств защиты информации, необходимых для обеспечения информационной безопасности.

6.1. *Правовые (законодательные) меры обеспечения безопасности информационных систем*

К правовым (законодательным) мерам обеспечения безопасности информационных систем относятся действующие в Российской Федерации правовые акты, регламентирующие правила обращения с информацией, закрепляющие права и обязанности участников

информационных отношений в процессе ее обработки и использования, а также устанавливающие ответственность за нарушения принятых в них правил.

Следует учитывать, что лица, виновные в нарушении обязательных требований по обеспечению информационной безопасности несут дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации.

Правовые меры защиты носят в основном упреждающий, профилактический характер и требуют постоянной разъяснительной работы с пользователями и обслуживающим персоналом информационной системы.

6.2. *Организационные меры обеспечения безопасности информационных систем* – меры организационного характера, регламентирующие процессы функционирования информационных систем, использование их ресурсов, деятельность обслуживающего персонала, а также порядок обращения пользователей информации с информационными системами таким образом, чтобы в наибольшей степени затруднить либо исключить возможность реализации угроз информационной безопасности, снизить размер потерь в случае реализации угроз.

6.3. *Технические меры обеспечения безопасности информационных систем* должны быть основаны на использовании единых программных и технических средств, входящих в состав информационных систем и выполняющих самостоятельно или в комплексе с другими средствами функции защиты.

Технические меры обеспечения безопасности информационных систем реализуются, в том числе посредством применения средств защиты информации, прошедших оценку соответствия в форме обязательной сертификации на соответствие требованиям по безопасности информации. Данный перечень размещен на официальном сайте ФСТЭК России (www.fstec.ru).

Применение организационных и технических мер защиты информации, реализуемых в информационных системах в рамках их систем защиты информации, в зависимости от угроз безопасности информации, используемых информационных технологий и структурно-функциональных характеристик информационных систем должны обеспечивать:

- идентификацию и аутентификацию субъектов доступа и объектов доступа;
- управление доступом субъектов доступа к объектам доступа;
- ограничение программной среды;
- защиту машинных носителей информации;
- регистрацию событий безопасности;
- антивирусную защиту; обнаружение вторжений;
- контроль (анализ) защищенности информации;
- обеспечение целостности информационной системы и информации;
- защиту технических средств;
- защиту информационной системы, ее средств, систем связи и передачи данных, в том числе, посредством применения активных и пассивных средств защиты информации, обрабатываемой техническими средствами информационных систем и циркулирующей в помещениях объекта от утечки по техническим каналам.

Организационные и технические меры защиты информации, реализуемые в рамках системы защиты информации информационной системы, в зависимости от информации, содержащейся в информационной системе, целей создания информационной системы и

задач, решаемых этой информационной системой, должны быть направлены на обеспечение конфиденциальности, целостности и доступности информации.

6.4. *Криптографические методы и средства защиты (далее — СКЗИ)* используются для обеспечения информационной безопасности.

Использование СКЗИ для обеспечения безопасности информации необходимо в случаях, если:

- информация подлежит криптографической защите в соответствии с законодательством Российской Федерации;
- в информационной системе существуют угрозы, которые могут быть нейтрализованы только с помощью данных средств (передача информации по каналам связи, не защищенным от перехвата нарушителем передаваемой по ним информации или от несанкционированных воздействий на эту информацию (например, при передаче информации, содержащей сведения конфиденциального характера, по информационно-телекоммуникационным сетям общего пользования;
- хранение информации на носителях, несанкционированный доступ к которым со стороны нарушителя не может быть исключен с помощью некриптографических методов и способов).

СКЗИ обеспечивают защиту информации при условии соблюдения требований эксплуатационно-технической документации на СКЗИ и требований, действующих нормативных правовых документов в области реализации и эксплуатации СКЗИ; для обеспечения безопасности информации при их обработке в информационных системах должны использоваться СКЗИ, прошедшие в установленном порядке процедуру оценки соответствия.

Перечень СКЗИ, сертифицированных ФСБ России, опубликован на официальном сайте Центра по лицензированию, сертификации и защите государственной тайны ФСБ России (www.clsz.fsb.ru).

6.5. *Физические меры защиты* основаны на применении разного рода механических, электронных или электронно-механических устройств и сооружений, специально предназначенных для создания физических препятствий на возможных путях проникновения и доступа потенциальных нарушителей к компонентам системы и защищаемой информации, а также технических средств визуального наблюдения, связи и охранной сигнализации.

Физическая защита зданий, помещений, объектов и средств информатизации должна осуществляться путем установления соответствующих постов охраны, с помощью технических средств охраны или любыми другими способами, предотвращающими или существенно затрудняющими проникновение в них посторонних лиц, хищение документов и носителей информации, самих средств информатизации, а также исключающими нахождение внутри контролируемой (охраняемой) зоны технических средств съема информации.

7. Обучение сотрудников и повышение осведомленности в вопросах обеспечения информационной безопасности

7.1. Все пользователи информационной системы должны быть ознакомлены с организационно- распорядительными документами по обеспечению информационной безопасности, в части, их касающейся, должны знать и неукоснительно выполнять инструкции и знать общие обязанности по обеспечению безопасности информации. Доведение требований

указанных документов до лиц, допущенных к обработке защищаемой информации, осуществляется под подпись.

7.2. Пользователи информационной системы, а также руководящий и обслуживающий персонал должны быть ознакомлены со своим уровнем полномочий, а также организационно-распорядительной, нормативной, технической и эксплуатационной документацией, определяющей требования и порядок обработки конфиденциальной информации.

7.3. Целью обучения сотрудников является, снижение потерь (материальных, финансовых, ущерб репутации и т.д.) от угроз, связанных с незнанием или непониманием основных положений законодательства Российской Федерации в области обеспечения информационной безопасности и правил по защите информации.

7.4. Задачи повышения осведомленности сотрудников в вопросах информационной безопасности:

- информирование сотрудников о существующих угрозах и проблемах информационной безопасности, которые могут возникнуть при автоматизированной обработке информации;
- выработка у сотрудников умения оценивать возможные последствия своих действий (адекватно оценивать связанные с ними риски информационной безопасности);
- выработка у сотрудников привычек, способствующих поддержанию высокого уровня информационной безопасности;
- доведение до сотрудников их обязанностей в области обеспечения информационной безопасности и степени их ответственности в случае утечки конфиденциальной информации; оценка эффективности, развитие и совершенствование проводимых мероприятий по информационной безопасности в целом.

7.5. Формы и методы повышения осведомленности сотрудников в области информационной безопасности:

- инструктаж при приеме на работу; повышение квалификации (курсы, семинары);
- изучение подраздела «Информационная безопасность» официального сайта техникума http://nttmps.ru/page/201

8. Ответственность работников за несоблюдение требований Политики обеспечения информационной безопасности

8.1. Работники, независимо от занимаемой должности, несут ответственность, предусмотренную действующим законодательством Российской Федерации, за несоблюдение принципов и требований настоящей Политики обеспечения информационной безопасности техникума.

8.2. Лица, виновные в нарушении требований Политики обеспечения информационной безопасности, могут быть привлечены к дисциплинарной, административной, гражданско-правовой и уголовной ответственности.

9. Порядок пересмотра и внесения изменений в Политику обеспечения информационной безопасности

9.1. Пересмотр принятой Политики может меняться и дорабатываться с учетом изменений законодательства Российской Федерации в области обеспечения информационной безопасности и особенностей информационной инфраструктуры в техникуме.

Система менеджмента качества

Политика обеспечения информационной безопасности ГАПОУ СО «Нижнетагильский техникум металлообрабатывающих производств и сервиса»

Локальный акт разработан:
Белоусова Н.В., зам. директора по СПР _____ 17.06.2019.
(дата, подпись)

С кем согласовано ФИО/должность	Дата согласования	Подпись
Щербина Е.В., методист		
Дубинин О.А., программист		
Камолова С.М., преподаватель	17.06.19	