ОБЛАСТНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ «СТАРООСКОЛЬСКИЙ ТЕХНИКУМ ТЕХНОЛОГИЙ И ДИЗАЙНА»

РАССМОТРЕНО
На заседании Педагогического совета
ОГАПОУ «Старооскольский техникум технологий и дизайна»
Протокол № 1 от 31.08.2022 года

УТВЕРЖДЕНО
Приказом директора ОГАПОУ «Старооскольский техникум технологий и дизайна»
от 01.09.2022 года № 469
_____ С.В.Ткалич

ПОЛОЖЕНИЕ ОБ ИНФОРМАЦИОННОЙ БЕЗОПАСТНОСТИ В ОГАПОУ СТАРООСКОЛЬСКИЙ ТЕХНИКУМ ТЕХНОЛОГИЙ И ДИЗАЙНА

1. Общие положения

1.1. Настоящее Положение разработано на основе:

- Федерального закона Российской Федерации от 27.07.2006г. №152-ФЗ «О персональных данных», с последующими изменениями.
- Федерального закона Российской Федерации от 27.07.2006г. №149-ФЗ «Об информации, информационных технологиях и о защите информации», с последующими изменениями.
- Постановления Правительства Российской Федерации от 01.11.2012г. №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
- Приказа ФСТЭК Российской Федерации от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».
- Устава ОГАПОУ «Старооскольский техникум технологий и дизайна».

1.2. Положение регламентирует политику ОГАПОУ «Старооскольский техникум технологий и дизайна», (далее техникум) по защите информации, безопасности информационных и коммуникационных ресурсов и технологий, порядке обращения с документами, содержащими служебную информацию ограниченного распространения и устанавливает:

- объекты защиты информации и субъекты доступа к информации информационных систем и ресурсов;
- основные угрозы информационной безопасности в техникуме;
- основные принципы построения системы защиты информации техникума;
- меры, методы и средства обеспечения информационной безопасности.[1]

[1] **Продолжение документа находится в электронной версии на официальном сайте ОГАПОУ «Старооскольский техникум технологий и дизайна», по адресу: sttd31@mail.ru**

2. . Объекты, подлежащие защите

2.1. В техникуме обрабатывается информация, содержащая сведения ограниченного распространения (служебная информация, персональные данные), и открытые сведения.

2.2. Основные объекты, подлежащие защите:

- информационные системы персональных данных (далее – ИСПД), а также открытая (общедоступная) информация, необходимая для работы техникума, независимо от формы и вида ее представления;
- процессы обработки информации в информационных системах техникума, информационные технологии, регламенты и процедуры сбора, обработки, хранения и передачи информации;
- информационная инфраструктура, включающая системы обработки и анализа информации, технические и программные средства её обработки, передачи и отображения, в том числе каналы информационного обмена и телекоммуникации, системы и средства защиты информации.

2.3. Особенности объектов, подлежащих защите:

- объединение в единую систему большого количества технических средств обработки и
- необходимость обеспечения непрерывности функционирования техникума;
- высокая интенсивность информационных потоков;
- разнообразие категорий пользователей.

3. Цели и задачи системы обеспечения информационной безопасности

3.1. Субъектами доступа к информации при обеспечении информационной безопасности техникума являются:

- работники техникума, участвующие в информационном обмене в соответствии с возложенными на них должностными обязанностями;
- физические лица, сведения о которых накапливаются, хранятся и обрабатываются в информационных системах техникума.
- сотрудники внешних организаций, занимающихся разработкой, поставкой, ремонтом и обслуживанием оборудования или информационных систем.

3.2. Перечисленным субъектам необходимо обеспечить:

- своевременность доступа к необходимой им информации (ее доступность);
- достоверность (полноту, точность, актуальность, целостность) информации;
- конфиденциальность (сохранение в тайне) определенной части информации, защиту от навязывания ложной (недостоверной, искаженной) информации;
- возможность осуществления контроля и управления процессами обработки и передачи информации;
- защиту информации от незаконного распространения.

3.3. Целью обеспечения информационной безопасности в Организации, на достижение которой направлено настоящее Положение, является защита от возможного нанесения субъектам доступа к информации материального, физического, морального или иного ущерба посредством случайного или преднамеренного воздействия на информацию, ее носители, процессы обработки и передачи.

3.4. Основные задачи системы обеспечения информационной безопасности.

Для достижения основной цели защиты и обеспечения указанных свойств информации система информационной безопасности должна обеспечивать решение следующих задач:

- своевременное выявление, оценку и прогнозирование источников угроз информационной безопасности, причин и условий, способствующих нанесению ущерба субъектам информационных отношений, нарушению нормального функционирования систем;
- создание механизма оперативного реагирования на угрозы безопасности информации;
- создание условий для минимизации и локализации наносимого ущерба неправомерными действиями физических и юридических лиц, ослабление негативного

влияния и ликвидация последствий нарушения безопасности информации;

- защиту от вмешательства в процесс функционирования систем техникума посторонних лиц (доступ к информационным ресурсам должны иметь только зарегистрированные в установленном порядке пользователи);
- разграничение доступа пользователей к информационным, программным и иным ресурсам – обеспечение доступа только к тем ресурсам, которые необходимы конкретным пользователям для выполнения своих служебных обязанностей;
- защиту от несанкционированных программ, включая компьютерные вирусы;
- защиту информации от утечки по техническим каналам при ее обработке, хранении и передаче по каналам связи.

3.5. Основные пути решения задач системы информационной безопасности техникума.

Основные цели обеспечения информационной безопасности и решение перечисленных выше задач достигаются:

- учётом всех подлежащих защите информационных систем Организации;
- учётом действий персонала, осуществляющего обслуживание программных и технических средств информационной системы;
- подготовкой должностных лиц (работников), ответственных за организацию и осуществление практических мероприятий по обеспечению информационной безопасности;
- персональной ответственностью за свои действия каждого работника, в рамках своих функциональных обязанностей имеющего доступ к информационным ресурсам техникума;
- непрерывным поддержанием необходимого уровня защищенности элементов информационных систем техникума;
- эффективным контролем над соблюдением пользователями информационных ресурсов техникума требований по обеспечению информационной безопасности.

4. Основные угрозы информационной безопасности техникума

4.1. Существует два вида угроз информационной безопасности:

- искусственные – угрозы, вызванные деятельностью человека;
- естественные – угрозы, вызванные воздействиями на информационную систему и ее элементы объективных физических процессов техногенного характера или стихийных природных явлений, не зависящих от человека.

4.2. Наиболее значимыми угрозами информационной безопасности являются:

- нарушение функциональности компонентов информационных систем Организации, блокирование информации, нарушение технологических процессов, срыв своевременного решения задач;
- нарушение целостности (искажение, подмена, уничтожение) информационных ресурсов техникума, а также фальсификация (подделка) документов;
- нарушение конфиденциальности (разглашение, утечка) персональных данных.

4.3. Основные источники угроз информационной безопасности техникума:

- непреднамеренные (ошибочные, случайные, без злого умысла и корыстных целей) нарушения сбора, обработки и передачи информации, приводящие к разглашению сведений ограниченного распространения, потере ценной информации или нарушению работоспособности элементов информационных систем;
- преднамеренные (в корыстных целях, по принуждению третьими лицами, со злым умыслом и т.п.) действия легально допущенных к информационным ресурсам техникума пользователей, которые приводят к разглашению сведений ограниченного распространения, потере ценной информации или нарушению работоспособности элементов информационных систем техникума;
- удаленное несанкционированное вмешательство посторонних лиц из внешних сетей общего назначения (прежде всего через сеть Интернет), через легальные и несанкционированные каналы подключения к таким сетям, используя недостатки

протоколов обмена, средств защиты и разграничения удаленного доступа к информационным ресурсам;

- технические сбои элементов информационных систем.

4.4. Пути реализации угроз информационной безопасности техникума.

4.4.1. Пути реализации непреднамеренных искусственных угроз информационной безопасности техникума.

Работники техникума, являющиеся авторизованными субъектами доступа информационных систем, а также работники, обслуживающие отдельные элементы информационных систем, являются внутренними источниками случайных воздействий. Основные пути реализации непреднамеренных искусственных (субъективных) угроз информационной безопасности техникума (действия, совершаемые людьми случайно, по незнанию, невнимательности или халатности, из любопытства, но без злого умысла):

- неосторожные действия, приводящие к частичному или полному нарушению функциональности элементов информационных систем Организации;

- неосторожные действия, приводящие к разглашению информации ограниченного распространения или делающие ее общедоступной;

- разглашение, передача или утрата атрибутов разграничения доступа (ключей (логинов), паролей, ключевых носителей и т. п.);

- игнорирование установленных правил при работе с информационными ресурсами;

- неосторожная порча носителей информации;

- неосторожное повреждение каналов связи;

- заражение компьютеров вирусами;

- некомпетентное использование, настройка или неправомерное отключение средств защиты.

4.4.2. Пути реализации преднамеренных искусственных (субъективных) угроз информационной безопасности.

Основные возможные пути умышленной дезорганизации работы, вывода элементов информационных систем из строя, несанкционированного доступа к информации, с корыстными целями:

- умышленные действия, приводящие к частичному или полному нарушению функциональности элементов информационных систем техникума;

- действия по дезорганизации функционирования информационных систем техникума, хищение электронных документов и носителей информации; несанкционированное копирование электронных документов и носителей информации;

- умышленное искажение информации, ввод неверных данных;

- перехват данных, передаваемых по каналам связи и их анализ;

- незаконное получение атрибутов разграничения доступа (используя халатность пользователей, путем подделки, подбора пароля);

- хищение или вскрытие шифров защиты информации;

- применение подслушивающих устройств, фото и видео съемка для несанкционированного съема информации.

4.5. Пути реализации основных естественных угроз информационной безопасности:

- выход из строя оборудования информационных систем и оборудования обеспечения его функционирования;

- выход из строя или невозможность использования линий связи;

- пожары и стихийные бедствия.

4.6. Утечка информации по техническим каналам.

5. Основные принципы построения системы обеспечения информационной безопасности

Построение системы обеспечения информационной безопасности техникума должны осуществляться в соответствии со следующими основными принципами:

5.1. Законность. Предполагает осуществление защитных мероприятий и разработку системы защиты информации в соответствии с действующим законодательством в области информации, информатизации и защиты информации, а также других нормативных актов по информационной безопасности, утвержденных органами государственной власти. Принятые меры информационной безопасности не должны препятствовать доступу правоохранительных органов в предусмотренных законодательством случаях к ресурсам конкретных информационных систем. Все пользователи информационных систем техникума должны иметь представление об ответственности за правонарушения в области информации.

5.2. Системность. Системный подход к построению системы обеспечения информационной безопасности предполагает учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, значимых для понимания и решения проблемы обеспечения информационной безопасности техникума.

При создании системы защиты учитываются все слабые и наиболее уязвимые места информационных систем, а также характер, возможные объекты и направления атак на неё со стороны нарушителей, пути несанкционированного доступа к информации. Система защиты должна строиться с учетом возможности появления принципиально новых путей реализации угроз безопасности.

5.3. Комплексность. Комплексное использование методов и средств защиты информационных систем предполагает согласованное применение программных и технических средств при построении целостной системы защиты, перекрывающей все значимые каналы реализации угроз.

5.4. Непрерывность защиты. Для обеспечения этого принципа необходима постоянная организационная (административная) поддержка (своевременная смена и обеспечение правильного хранения и применения имен, паролей, ключей шифрования, перераспределение полномочий).

5.5. Своевременность. Предполагается упреждающий характер мер обеспечения информационной безопасности, то есть постановка задач по комплексной защите информации и реализация мер обеспечения безопасности информации на ранних стадиях разработки информационных систем. Разработка системы защиты ведется параллельно с разработкой и развитием самой подлежащей защите информационной системы.

5.6. Преемственность и совершенствование. Предполагает постоянное совершенствование мер и средств защиты информации на основе преемственности организационных и технических решений, кадрового состава, анализа функционирования информационных систем техникума и систем информационной защиты с учетом изменений в методах и средствах перехвата информации, нормативных требований по защите, достигнутого отечественного и опыта в этой области.

5.7. Персональная ответственность. Предполагает возложение ответственности за обеспечение информационной безопасности на каждого работника техникума в пределах его полномочий. В соответствии с этим принципом распределение прав и обязанностей работников строится таким образом, чтобы в случае любого нарушения круг виновников был четко известен или сведен к минимуму.

5.8. Предполагает предоставление пользователям минимальных прав доступа в соответствии со служебной необходимостью. Доступ к информации должен предоставляться только в том случае и объёме, если это необходимо работнику для выполнения его должностных обязанностей.

5.9. Гибкость системы информационной безопасности.

Предполагает способность системы информационной безопасности реагировать на изменения внешней среды и условий осуществления техникума своей деятельности. В число таких изменений входят:

- изменение существующих или внедрение принципиально новых информационных систем;
- ввод в эксплуатацию новых технических средств.

5.10. Простота применения средств защиты.

Механизмы и методы системы защиты информации должны быть понятны и просты в использовании. Применение средств и методов защиты не связано со знанием специальных языков или с выполнением действий, требующих значительных дополнительных трудозатрат при обычной работе зарегистрированных пользователей, а также не требует от пользователя выполнения малопонятных ему операций.

5.11. Обоснованность и техническая реализуемость.

Предполагает, что информационные технологии, технические и программные средства, средства и меры защиты информации реализуются на современном техническом уровне и обоснованы для достижения заданного уровня безопасности информации и экономической целесообразности, а также соответствуют установленным нормам и требованиям по безопасности информации.

5.12. Специализация и профессионализм.

Предполагает привлечение к разработке средств и реализации мер защиты информации специализированных организаций, наиболее подготовленных к конкретному виду деятельности по обеспечению безопасности информационных ресурсов, имеющих опыт практической работы и государственную лицензию на право оказания услуг в этой области. Реализация административных мер и эксплуатация средств защиты осуществляется профессионально подготовленными специалистами защиты информации техникума.

5.13. Обязательность контроля.

Предполагает обязательность и своевременность выявления и пресечения попыток нарушения установленных правил обеспечения безопасности информации. Контроль за деятельностью любого пользователя, каждого средства защиты и в отношении любого объекта защиты осуществляется на основе применения средств оперативного контроля и регистрации и охватывает санкционированные и несанкционированные действия пользователей. Выявленные работниками техникума недостатки системы защиты информации доводятся до сведения непосредственного руководителя

6. Меры обеспечения информационной безопасности

6.1. К законодательным (правовым) мерам обеспечения информационной безопасности относятся действующие в Российской Федерации законодательные и иные нормативные 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 этих правил. Правовые меры обеспечения информационной безопасности носят упреждающий, профилактический характер и требуют постоянной разъяснительной работы с пользователями и обслуживающим персоналом информационных систем техникума.

6.2. К технологическим мерам обеспечения информационной безопасности относятся технологические решения и приемы, направленные на уменьшение возможности совершения работниками техникума ошибок и нарушений в рамках предоставленных им прав и полномочий.

6.3. Организационные (административные) меры обеспечения информационной безопасности – это меры организационного характера, регламентирующие процессы функционирования системы обработки данных, использование её ресурсов, деятельность обслуживающего персонала, а также порядок взаимодействия пользователей с системой таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности или снизить размер потерь в случае их реализации. Организационными (административными) мерами обеспечения информационной безопасности являются:

- регламентация доступа в здание техникума;
- регламентация допуска работников к использованию информационных ресурсов;
- анализ требований к элементам системы на основе заявок пользователей на обслуживание и модификацию аппаратных и программных ресурсов;

- обеспечение и контроль физической целостности (неизменности конфигурации) средств вычислительной техники;

- деятельность по обеспечению информационной безопасности;

- условия обработки информационных ресурсов конфиденциального характера, ответственность за нарушения установленного порядка пользования информационными ресурсами техникума.

6.4. Физические меры обеспечения информационной безопасности основаны на применении механических, электронных или электронно-механических устройств, специально предназначенных для создания физических препятствий на возможных путях проникновения и доступа потенциальных нарушителей к элементам информационных систем и защищаемой информации.

6.5. Технические меры обеспечения информационной безопасности основаны на использовании электронных устройств и специальных программ выполняющих (самостоятельно или в комплексе с другими средствами) функции защиты информации.

7. Права и обязанности работников техникума по обеспечению информационной безопасности

7.1. Директор техникума организует работу по построению системы обеспечения информационной безопасности. В частности:

- назначает ответственного за организацию информационной безопасности из числа работников техникума;

- утверждает круг лиц, имеющих доступ к защищаемой информации и порядок их работы;

- утверждает комплект документов, определяющих политику в отношении информационной безопасности и защиты информации в техникуме, а также локальные акты, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства РФ.

7.2. Ответственный за организацию информационной безопасности:

- обеспечивает защиту информации, циркулирующей на объектах информатизации;

- проводит систематический контроль работы систем защиты информации, применяемых в информационной системе;

- проводит инструктаж пользователей информационной системы;

- контролирует обеспечение функционирования систем защиты информации (настройка и сопровождение подсистемы управления доступом пользователя к защищаемым информационным ресурсам информационной системы, антивирусная защита, резервное копирование данных и т.д.);

- участвует в работах по внесению изменений в программную конфигурацию информационной системы;

- определяет порядок и осуществляет контроль ремонта средств вычислительной техники, входящих в состав информационной системы;

- принимает меры по оперативному изменению паролей при увольнении или перемещении сотрудников, имевших допуск к информационной системе;

- устраняет выявленные нарушения и недостатки, дает обязательные для исполнения указания по вопросам обеспечения положений инструкций по защите информации;

- в случае выявления попыток несанкционированного доступа к информации или попыток хищения, копирования, изменения, незамедлительно принимает меры пресечения и докладывает директору техникума;

7.3. Несоответствие применяемых в мер установленным требованиям или нормам по обеспечению информационной безопасности и защите информации, является нарушением и влечёт административное наказание в соответствии с законодательством РФ.

8. Заключительные положения

8.1. Положение вступает в силу с момента его утверждения.

8.2. Положение является локальным актом техникума. Внесение изменений и дополнений в Положение осуществляется в порядке его принятия.

8.3. Настоящее Положение может быть изменено (дополнено) локальным актом техникума.