

**ОБЛАСТНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ
ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
«СТАРООСКОЛЬСКИЙ ТЕХНИКУМ ТЕХНОЛОГИЙ И ДИЗАЙНА»
(«ОГАПОУ «Старооскольский техникум технологий и дизайна»)**

РАССМОТREНО

На заседании Общего собрания работников
ОГАПОУ «Старооскольский техникум
технологий и дизайна»

Протокол № 1 от «24» марта 2023 г.

УТВЕРЖДАЮ

Директор ОГАПОУ «Старооскольский
техникум технологий и дизайна»

С.В. Ткалич

Приказ от «24» марта 2023 г. № 250



**ПОЛИТИКА
ОГАПОУ «СТАРООСКОЛЬСКИЙ ТЕХНИКУМ ТЕХНОЛОГИЙ И ДИЗАЙНА»
В ОТНОШЕНИИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ**

I. Общие положения

1.1. Настоящее Положение о Политике в отношении обработки персональных данных (далее – Положение) ОГАПОУ «Старооскольский техникум технологий и дизайна» (далее – техникум) 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.
- Федерального закона Российской Федерации от 29.12.2012г. №273-ФЗ «Об образовании в Российской Федерации», 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».
- Устава ОГАПОУ «Старооскольский техникум технологий и дизайна».

1.2. Политика разработана в соответствии с целями, задачами и принципами обеспечения безопасности персональных данных, изложенных в Концепции информационной безопасности информационной системы персональных данных (далее – ИСПД).

1.3. В Политике определены требования к персоналу, задействованному в работе с ИСПД техникума, степень ответственности персонала, структура и необходимый уровень защищенности, статус и должностные обязанности сотрудников, ответственных за обеспечение безопасности персональных данных в ИСПД.

1.4. Целью настоящей Политики является, обеспечение безопасности объектов защиты техникума от всех видов угроз, внешних и внутренних, умышленных и непреднамеренных, минимизация ущерба от возможной реализации угроз безопасности персональных данных (далее - УБПД).

1.5. 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.

1.6. Информация и связанные с ней ресурсы должны быть доступны для авторизованных пользователей. Должно осуществляться своевременное обнаружение и реагирование на УБПД. Должно осуществляться предотвращение преднамеренных или случайных, частичных или полных несанкционированных модификаций или уничтожения данных.

II. Термины и определения:

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

2.2. Информационная система персональных данных (ИСПД) - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

2.3. 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.

2.4. Оператор персональных данных (оператор) – юридическое лицо, самостоятельно организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

2.5. Распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

2.6. Уничтожение персональных данных - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

2.7. Автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники.

2.8. Предоставление персональных данных – действия, направленные на раскрытие

персональных данных определенному лицу или определенному кругу лиц.

2.9. Блокирование персональных данных – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

2.10. Обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

III. Область действия

3.1. Требования настоящей Политики распространяются на всех сотрудников техникума (штатных, временных, работающих по контракту и т.п.), а также всех прочих лиц – представителей организаций, которые находятся в договорных отношениях с техникумом (подрядчики и т.п.).

IV. Согласие субъекта персональных данных на обработку его персональных данных

4.1. Субъект персональных данных принимает решение о предоставлении его персональных данных и дает согласие на их обработку свободно, своей волей и в своем интересе. Согласие на обработку персональных данных является конкретным, предметным, информированным, сознательным и однозначным.

4.2. В случае получения согласия на обработку персональных данных от представителя субъекта персональных данных полномочия данного представителя на дачу согласия от имени субъекта персональных данных проверяются Учреждением.

4.3. В случаях, предусмотренных федеральным законом, обработка персональных данных осуществляется только с согласия в письменной форме субъекта персональных данных.

4.4. В случае недееспособности субъекта персональных данных согласие на обработку его персональных данных дает законный представитель субъекта персональных данных.

V. Система защиты персональных данных

5.1. Система защиты персональных данных (далее - СЗПД) строится на основании:

- перечня защищаемой информации;
- модели угроз безопасности персональных данных;
- Положении об обеспечении безопасности персональных данных ОГАПОУ «Старооскольский техникум технологий и дизайна».

5.2. Список функций защиты:

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

Список используемых средств должен поддерживаться в актуальном состоянии. При изменении состава технических средств защиты или элементов ИСПД, соответствующие изменения должны быть внесены в Список.

VI. Требования к СЗПД

6.1. СЗПД включает в себя следующие подсистемы:

- управления доступом, регистрации и учета;
- обеспечения целостности и доступности;
- антивирусная защита.

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

- идентификации и проверки подлинности субъектов доступа при входе в ИСПД;
- 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 регистрации загрузки и инициализации операционной системы.

6.3. Подсистема управления доступом может быть реализована с помощью штатных средств обработки персональных данных, (далее – ПД) операционных систем, приложений.

Также может быть внедрено специальное техническое средство или их комплекс, осуществляющий 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.

6.4. Подсистема обеспечения целостности и доступности, предназначена для обеспечения целостности и доступности ПД, программных и аппаратных средств ИСПД, а также средств защиты при случайной или намеренной модификации. Подсистема реализуется с помощью организации резервного копирования обрабатываемых данных, а также резервированием ключевых элементов ИСПД.

6.5. Подсистема антивирусной защиты, предназначена для обеспечения антивирусной защиты серверов и автоматизированного рабочего места (далее – АРМ) пользователей ИСПД.

6.6. Средства антивирусной защиты предназначены для реализации следующих функций:

- резидентный антивирусный мониторинг;
- антивирусное сканирование;
- централизованная/удаленная установка/деинсталляция антивирусного продукта, настройка, администрирование, просмотр отчетов и статистической информации по работе продукта;
- автоматизированное обновление антивирусных баз;
- автоматический запуск сразу после загрузки операционной системы.

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

VII. Основные принципы построения системы защиты

7.1. Построение системы обеспечения безопасности ПД в ИСПД и ее функционирование должны осуществляться в соответствии со следующими основными

принципами: законность, системность, комплексность, непрерывность, своевременность, преемственность и непрерывность совершенствования, персональная ответственность, минимизация полномочий, взаимодействие и сотрудничество, простота применения средств защиты, обязательность контроля.

7.2. Законность, предполагает осуществление защитных мероприятий и разработку СЗПД в соответствии с действующим законодательством в области защиты ПД и других нормативных актов по безопасности информации, утвержденных органами государственной власти и управления в пределах их компетенции. Пользователи и обслуживающий персонал ПД в ИСПД должны быть осведомлены о порядке работы с защищаемой информацией и об ответственности за нарушение защиты ПД

7.3. Системность, предполагает системный подход к построению СЗПД а также учет всех взаимосвязанных, взаимодействующих и изменяющихся условий и факторов, существенно значимых для понимания и решения проблемы обеспечения безопасности ПД в ИСПД.

7.4. Комплексность, комплексное использование методов и средств защиты предполагает согласованное применение разнородных средств при построении целостной системы защиты, перекрывающей все существенные (значимые) каналы реализации угроз и не содержащей слабых мест на стыках отдельных ее компонентов.

7.5. Непрерывность, непрерывный целенаправленный процесс, предполагающий принятие соответствующих мер на всех этапах жизненного цикла ИСПД. ИСПД должны находиться в защищенном состоянии на протяжении всего времени их функционирования. В соответствии с этим принципом должны приниматься меры по недопущению перехода ИСПД в незащищенное состояние.

7.6. Своевременность, предполагает упреждающий характер мер обеспечения безопасности ПД, то есть постановку задач по комплексной защите ИСПД и реализацию мер обеспечения безопасности ПД на ранних стадиях разработки ИСПД в целом и ее системы защиты информации в частности.

7.7. Преемственность и совершенствование, предполагают постоянное совершенствование мер и средств защиты информации на основе преемственности организационных и технических решений, кадрового состава, анализа функционирования ИСПД и ее системы защиты с учетом изменений в методах и средствах перехвата информации, нормативных требований по защите, достигнутого отечественного и зарубежного опыта в этой области.

7.8. Персональная ответственность, предполагает возложение ответственности за обеспечение безопасности ПД и системы их обработки на каждого сотрудника в пределах его полномочий.

7.9. Принцип минимизации полномочий, доступ к ПД должен предоставляться только в том случае и объеме, если это необходимо сотруднику для выполнения его должностных обязанностей.

7.10. Взаимодействие и сотрудничество, предполагает создание благоприятной атмосферы в коллективах подразделений, обеспечивающих функционирование ИСПД, для снижения вероятности возникновения негативных действий связанных с человеческим фактором.

7.11. Простота применения средств защиты. Механизмы защиты должны быть интуитивно понятны и просты в использовании. Применение средств защиты не должно быть связано со знанием специальных языков или с выполнением действий, требующих

значительных дополнительных трудозатрат при обычной работе зарегистрированных установленным порядком пользователей, а также не должно требовать от пользователя выполнения рутинных малопонятных ему операций (ввод нескольких паролей и имен и т.д.).

7.12. Обязательность контроля, предполагает обязательность и своевременность выявления и пресечения попыток нарушения установленных правил обеспечения безопасности ПД.

VIII. Пользователи ИСПД

8.1. В ИСПД можно выделить следующие группы пользователей, участвующих в обработке и хранении ПД:

Ответственный за организацию работы по обработке персональных данных:

- обеспечивает функционирование подсистемы управления доступом ИСПД и уполномочен осуществлять предоставление и разграничение доступа конечного пользователя (оператора АРМ) к элементам, хранящим персональные данные.

Администратор информационных систем персональных данных (программист):

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

Оператор АРМ (пользователь ИСПД)

Оператор АРМ - сотрудник техникума, осуществляющий обработку ПД. Обработка ПД включает: возможность просмотра ПД, ручной ввод ПД в систему ИСПД, формирование справок и отчетов по информации, полученной из ИСПД. Оператор не имеет полномочий для управления подсистемами обработки данных и СЗПД.

IX. Требования к персоналу по обеспечению защиты ПД

9.1. Все сотрудники техникума, являющиеся пользователями ИСПД, должны четко знать и строго выполнять установленные правила режима безопасности ПД.

9.2. При вступлении в должность нового сотрудника непосредственный начальник подразделения, в которое поступает сотрудник, обязан организовать его ознакомление с должностной инструкцией и необходимыми документами, регламентирующими требования по защите ПД, а также обучение навыкам выполнения процедур, необходимых для санкционированного использования ИСПД.

9.3. Сотрудник должен быть ознакомлен со сведениями настоящей Политики, принятых процедур работы с элементами ИСПД и СЗПД.

9.4. Сотрудники техникума 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 ПД и процедуры защиты оборудования, оставленного без присмотра, а также свои обязанности по обеспечению такой защиты.

9.5. Сотрудникам запрещается устанавливать постороннее программное обеспечение, подключать личные мобильные устройства и носители информации, а так

же записывать на них защищаемую информацию.

X. Ответственность сотрудников ИСПД

10.1. В соответствии со ст. 24 Федерального закона Российской Федерации от 27.07.2006г. №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.

10.2. При нарушениях сотрудниками - пользователями ИСПД правил, связанных с безопасностью ПД, они несут ответственность, установленную действующим законодательством Российской Федерации.

XI. Заключительные положения

11.1. Настоящее Положение о должностных инструкциях является локальным нормативным актом Техникума, принимается на Общем собрании работников и утверждается приказом директора Техникума.

11.2. Все изменения и дополнения, вносимые в настоящее Положение, оформляются в письменной форме в соответствии действующим законодательством Российской Федерации.

11.3. Настоящее Положение вступает в силу с момента его подписания и действует до утверждения новой редакции Положения.

СОГЛАСОВАНО:

Юрисконсульт



Д.В. Касимовский

Приложение 1.

**Перечень документов по соблюдению
«Политики ОГАПОУ «Старооскольский техникум технологий и дизайна»
в отношении персональных данных»**

1. Акт внутреннего аудита соответствия обработки ПДн требованиям к защите ПДн
2. Акт об уничтожении персональных данных
3. Дополнительное соглашение с работником, допущенным к обработке персональных данных
4. Инструкция сотрудника, ответственного за обеспечение безопасности ПДн
5. Инструкция сотрудника, ответственного за организацию обработки ПДн
6. Обязательство о неразглашении информации, содержащей персональные данные
7. Отзыв работника своего согласия на обработку персональных данных
8. Перечень должностей, замещение которых предусматривает осуществление обработки ПДн
9. Перечень сведений конфиденциального характера
10. Положение о внутреннем аудите соответствия обработки ПДн установленным требованиям
11. Положение о разграничении прав доступа к обрабатываемым ПДн
12. Положение об обработке и защите ПДн работников
13. Положение об обработке и защите ПДн обучающихся и их родителей
14. Правила, устанавливающие процедуры, направленные на выявление и предотвращение нарушений законодательства РФ в сфере ПДн
15. Приказ о внесении изменений в Политику оператора в отношении обработки ПДн и ЛНА, регламентирующие вопросы обработки и защиты ПДн
16. Приказ о назначении должностного лица, представляющего интересы организации при проведении проверки
17. Приказ о назначении ответственного за обеспечение безопасности ПДн
18. Приказ о назначении ответственного за организацию обработки ПДн
19. Приказ о назначении ответственного за техническую защиту ПДн
20. Приказ о создании комиссии по уничтожению документов, содержащих ПДн
21. Приказ об утверждении перечня должностей работников, замещение которых предусматривает осуществление обработки ПДн
22. План внутреннего контроля соответствия обработки ПДн требованиям защиты ПДн
23. Регламент допуска работников к обработке ПДн
24. Регламент по проведению контрольных мероприятий и реагированию на инциденты
25. Сведения о реализуемых требованиях к защите ПДн
26. Согласие законного представителя обучающегося (воспитанника) на обработку ПДн обучающегося (воспитанника)
27. Согласие на обработку ПДн, разрешенных субъектом ПДн для распространения

28. Согласие обучающегося на обработку своих ПДн
29. Согласие работника на обработку ПДн
30. Согласие сотрудника на хранение копии личных документов в личном деле
31. Требование о прекращении передачи (распространения, предоставления, доступа) ПДн, разрешенных субъектом ПДн для распространения