ЧАСТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
«СТАВРОПОЛЬСКИЙ КООПЕРАТИВНЫЙ ТЕХНИКУМ»

СОГЛАСОВАНО
Протокол заседания
Студенческого совета
от «30» августа 2023 г. № 1
Председатель Совета
_____

УТВЕРЖДАЮ
Директор Частного профессионального
образовательного учреждения
«Ставропольский кооперативный техникум»
_____ А.А. Намитоков
от «30» августа 2023 г. Приказ № 112

ПОЛОЖЕНИЕ О РАЗРЕШИТЕЛЬНОЙ СИСТЕМЕ ДОПУСКА
к ресурсам информационной системы персональных данных
«Автоматизированное рабочее место оператора УОП»
частного профессионального образовательного учреждения
«Ставропольский кооперативный техникум»

1 Общие положения

1.1 Настоящее Положение разработано с целью обеспечения обоснованного и правомерного доступа к информационным ресурсам информационной системы персональных данных «Автоматизированное рабочее место оператора УОП» (далее по тексту - ИСПДн).

- Настоящее Положение разработано в соответствии с Федерального закона от 29 декабря 2012 года № 273-ФЗ «Об образовании в Российской Федерации»;
- Федерального закона от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (ред. 31.07.2023);
- Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» (ред. 06.02.2023);
- и другими нормативными правовыми актами по вопросам обеспечения защиты персональных данных.

1.2 Разрешительная система допуска к ресурсам ИСПДн представляет собой совокупность процедур оформления права субъектов на доступ к информационным ресурсам ИСПДн и ответственных лиц, осуществляющих реализацию этих процедур.

1.3 Подлежащие защите информационные ресурсы ИСПДн включаются в «Перечень информационных ресурсов, подлежащих защите в ИСПДн» (Приложение 1).

1.4 Объектами доступа являются: информационные ресурсы в ИСПДн.

1.5 Субъектами доступа являются:

- уполномоченные сотрудники Учреждения.

1.6 Субъекты доступа несут персональную ответственность за соблюдение ими установленного в ИСПДн порядка обеспечения защиты информационных ресурсов.

1.7 Ответственными лицами, осуществляющими реализацию процедур оформления прав субъектов на доступ к информационным ресурсам ИСПДн, является Администратор безопасности ИСПДн.

2 Допуск к информационным ресурсам сотрудников организации

2.1 Сотрудники Учреждения допускаются к работе в ИСПДн на основании утвержденного «Перечня лиц, доступ которых к персональным данным, обрабатываемым в информационной системе персональных данных «Автоматизированное рабочее место оператора УОП», необходим для выполнения служебных (трудовых) обязанностей».

2.2. Допуск сотрудников к информации, содержащей персональные данные, осуществляется в объеме, необходимом для выполнения ими должностных обязанностей. Права доступа сотрудников к защищаемой информации и выполняемые роли определяются в Матрице доступа (Приложение 2).

2.3. С целью соблюдения принципа персональной ответственности каждому сотруднику Учреждения, допущенному к работе в ИСПДн должно быть сопоставлено персональное уникальное имя (учетная запись пользователя), под которым он будет регистрироваться и работать в системе.

2.4. Использование несколькими сотрудниками при самостоятельной работе в ИСПДн одного и того же имени пользователя («группового имени») **ЗАПРЕЩЕНО.**

2.5 Процедура регистрации (создания учетной записи) пользователя и предоставления (или изменения) ему прав доступа к ресурсам ИСПДн осуществляется с использованием сертифицированных средств защиты информации от несанкционированного доступа.

2.6 Для загрузки компьютера и регистрации в системе в ИСПДн предусмотрены три типа учетных записей:

- учетная запись администратора безопасности позволяет производить настройку программного обеспечения, средств защиты информации и добавлять/удалять пользователей в систему;
- учетная запись пользователя наделена ограниченными правами.

2.7 Учетная запись представляет собой комбинацию Логин/Пароль.

Логин - представляет собой имя учетной записи, созданной для входа в систему.

Пароль - это секретное слово или набор символов, предназначенный для подтверждения личности и полномочий пользователя системы ИСПДн. Требования к паролю регламентируется организационно-распорядительными документами

2.8 После определения роли пользователя и в соответствии с обозначенными для него в матрице доступа правами Администратор безопасности ИСПДн в соответствии с документацией на средства защиты производит необходимые действия по созданию (изменению, удалению) учетной записи пользователя, присвоению ему начального значения пароля и заявленных прав доступа к ресурсам ИСПДн, включению его в соответствующие группы пользователей и другие необходимые действия.

2.9 После создания учетной записи, пользователь должен авторизоваться в системе.

2.10 Администратор безопасности ИСПДн обязан проверить наличие записей о входе пользователя в систему в журнале регистрации событий средств зашиты информации от несанкционированного доступа.

2.11 Для всех пользователей ИСПДн устанавливается режим принудительного запроса смены пароля не реже одного раза в 90 дней, максимальное количество неуспешных попыток аутентификации (ввода неправильного пароля) до блокировки - 5 попыток, блокировка программно-технического средства или учетной записи пользователя в случае достижения установленного максимального количества неуспешных попыток аутентификации - 15 минут.

2.12 В случае производственной необходимости пользователю ИСПДн могут быть сопоставлены несколько уникальных имен (учетных записей).

2.13 При изменении должностных обязанностей сотрудника, связанных с переводом в другое подразделение, переводом на другую должность и т.п., учетная запись пользователя подлежит изменению (корректировке), при этом старые полномочия аннулируются.

2.14 После внесения изменений в Матрицу доступа Администратор безопасности ИСПДн производит настройку средств защиты рабочих станций (автоматизированных

рабочих мест).

2.15 На время отпуска пользователей ИСПДн Администратором безопасности осуществляется блокирование их учетных записей.

3 Допуск к информационным ресурсам сторонних организаций, деятельность которых не связана с исполнением функций Учреждения

3.1 К организациям, деятельность которых не связана с исполнением функций Учреждения, могут относиться:

- правоохранительные органы;
- судебные органы;
- органы статистики;
- органы исполнительной и законодательной власти субъектов Российской Федерации;
- средства массовой информации и пр.

3.2 Допуск к информационным ресурсам сторонних организаций, деятельность которых не связана с исполнением функций Учреждения, регламентируется законодательством Российской Федерации, договорами и соглашениями об информационном обмене и другими нормативными актами.

4 Допуск к информационным ресурсам ИСПДн сторонних организаций, выполняющих работы в Учреждении на договорной основе

4.1 К организациям, выполняющим работы на договорной основе, могут относиться:

- организации, осуществляющие монтаж и настройку технических средств ИСПДн, сопровождение прикладного программного обеспечения;
- организации, оказывающие услуги в области защиты информации (проведение специальных проверок и исследований, монтаж и настройка средств защиты информации, контроль эффективности системы защиты информации, аттестация объектов информатизации и т.п.);
- организации, осуществляющие поставку товаров для обеспечения повседневной деятельности (мебели, канцтоваров, оргтехники, расходных материалов и т.п.).

4.2 Порядок допуска определяется в договоре на выполнение работ (оказание услуг). Кроме того, лицам, привлекаемым на договорной основе для обеспечения функционирования информационной системы (ремонт, гарантийное обслуживание, регламентные и иные работы) в соответствии с организационно-распорядительными документами оператора, на срок действия договора, должны быть присвоены учетные записи.

4.3 Решением о допуске является подписанный в установленном порядке договор на выполнение работ или оказание услуг.

4.4 В договор на оказание услуг включается условие о неразглашении сведений, составляющих персональные данные, а также служебной информации, ставшей известной в ходе выполнения работ, если для их выполнения предусмотрено использование таких сведений. Со всех работников сторонней организации, участвующих в выполнении работ, в этом случае берется подписка о неразглашении таких сведений.

5 Контроль функционирования разрешительной системы допуска к информационным ресурсам организации

5.1 Контроль функционирования разрешительной системы допуска к информационным ресурсам организуется в соответствии с:

- планом основных мероприятий по защите информации на текущий год;
- функциональными обязанностями должностных лиц;
- приказами руководителя Учреждении.

5.2 Контроль функционирования разрешительной системы допуска к информационным ресурсам ИСПДн осуществляется ответственными лицами. Организация контроля возлагается на Администратора безопасности.

6. Порядок внесения изменений и дополнений

6.1. Изменения и дополнения в настоящее Положение вносятся по мере необходимости.

6.2. Предложения об изменениях и дополнениях в настоящее Положение рассматриваются на заседании Студенческого совета, Совета техникума, и в случае их одобрения Положение утверждается приказом директора Техникума в новой редакции.

СОГЛАСОВАНО
Протокол заседания
Совета техникума
от «30» августа 2023 г. № 1
Председатель Совета
_____А.А. Намитоков