	Министерство науки и высшего образования Российской Федерации
	федеральное государственное бюджетное образовательное учреждение высшего образования
	«Владивостокский государственный университет экономики и сервиса»
	центр информационно-технического обеспечения

УТВЕРЖДАЮ
Ректор ВГУЭС
_____ Г.В. Гереньтьева
«___» _____ 2022

ИНСТРУКЦИЯ ПО ОРГАНИЗАЦИИ ПАРОЛЬНОЙ ЗАЩИТЫ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ФГБОУ ВО ВГУЭС

Центр информационно-технического обеспечения
СК-СТО-ИН-28-006-2022

РАЗРАБОТАНО
Ведущий инженер по защите информации центра информационно-технического обеспечения _____ А.И. Приймак
подпись, дата

СОГЛАСОВАНО
Проректор по учебно-воспитательной и научно - исследовательской работе _____ С.Ю. Голиков
подпись, дата

Руководитель центра информационно-технического обеспечения _____ Д.В. Гмарь
подпись, дата

Руководитель юридической службы _____ Д.В. Манежкин
подпись, дата

Руководитель службы документационного обеспечения управления _____ О.А. Зубкова
подпись, дата

Введено в действие приказом от «09» февраля 2022 № 81

Владивосток 2022

Перечень обозначений и сокращений

ВГУЭС, Университет	—	федеральное государственное бюджетное образовательное учреждение высшего образования «Владивостокский государственный университет экономики и сервиса»
Инструкция	—	инструкция по организации парольной защиты в информационных системах
ПДн	—	персональные данные
ИСПДн	—	информационная система персональных данных

1. Общие положения

1.1. Настоящая Инструкция по организации парольной защиты в информационных системах федерального государственного бюджетного образовательного учреждения высшего образования «Владивостокский государственный университет экономики и сервиса» разрешительной системы доступа определяет правила парольной защиты применяемых в информационных системах персональных данных федерального государственного бюджетного образовательного учреждения высшего образования «Владивостокский государственный университет экономики и сервиса».

1.2. Действие настоящей Инструкции распространяется на всех работников Университета, имеющих доступ к ресурсам информационных систем персональных данных для исполнения должностных (трудовых) обязанностей.

1.3. Пересмотр настоящей Инструкции осуществляется по мере необходимости, но не реже одного раза в три года.

2. Правила парольной защиты

2.1. Под паролем понимается идентификатор субъекта доступа, который является его (субъекта) секретом. Пользователь не должен сообщать никому личный пароль.

2.2. Различный уровень доступа пользователей к ресурсам ИСПДн Университета обеспечивается системой имён пользователей и паролей. Каждый пользователь имеет своё уникальное имя и известный только ему пароль.

2.3. Личные пароли должны генерироваться и распределяться централизованно либо выбираться пользователями самостоятельно с учётом следующих требований:

2.3.1. Длина пароля должна быть не менее восьми символов, длина ограничивается 32 символами.

2.3.2. Пароль является комбинацией цифр, букв и специальных символов («@», «#», «$», «&», «*», «%» и т. п.).

2.3.3. Пароль должен содержать по меньшей мере одну цифру, одну строчную букву, одну прописную букву, один специальный символ.

2.3.4. Пароль не должен обнаруживаться в словаре и включать в себя легко вычисляемые сочетания символов, например:

имя, отчество или фамилия;

день рождения и другие памятные даты (включая день, месяц, год);

другие данные, которые могут быть подобраны путём анализа информации о пользователе;

последовательности подряд идущих символов клавиатуры (например: «1234567» или «qwerty» и т. п.);

повторяющийся символ либо повторяющаяся комбинация из нескольких символов (например: «111111» или «w2w2w2» и т. п.);

использование одной цифры до или после слова (например, «Password1»);

замена букв на схожие по написанию цифры (например: «pa55w0rd»).

2.4. Полная плановая смена паролей пользователей должна проводиться регулярно, не реже одного раза в 90 дней. Повторное использование пароля недопустимо. При смене пароля новое значение должно отличаться от предыдущего не менее чем в 4 позициях. Пароли к используемым разным сервисам должны быть различными. Запрещается сообщать другим пользователям личный пароль.

2.5. Внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение, переход на другую должность внутри Университета и другие обстоятельства) администратора безопасности ИСПДн и других работников, которым по роду работы были предоставлены полномочия по управлению парольной защитой.

2.6. При возникновении нештатных ситуаций, форс-мажорных обстоятельств и т. п., приведших к технологической необходимости использования имён и паролей некоторых работников в их отсутствие (с разрешения непосредственного руководителя), такие работники могут сообщить свои пароли ответственному за обеспечение безопасности ПДн и обязаны при первой возможности сменить свои пароли на новые значения.

2.7. При подозрении на компрометацию данных учетной записи и пароля, пользователю необходимо изменить скомпрометированный пароль и немедленно об этом информировать непосредственного руководителя и администратора безопасности ИСПДн.

2.8. Хранение работником (исполнителем) значений своих паролей на бумажном носителе допускается только в личном сейфе, закрывающемся на ключ личном ящике стола, либо в сейфе у ответственного за обеспечение безопасности ПДн.

2.9. Покидая рабочее место, работник должен заблокировать рабочую станцию.

2.10. Повседневный контроль действий пользователей ИСПДн при работе с паролями, соблюдение порядка их смены, хранения и использования возлагается на администратора безопасности ИСПДн, периодический контроль возлагается на ответственного за обеспечение безопасности ПДн.

2.11. Все события, связанные с нарушением правил парольной защиты, должны регистрироваться и сообщаться ответственному за обеспечение безопасности ПДн.

2.12. Владельцы паролей должны быть ознакомлены с перечисленными выше требованиями и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение парольной информации.

2.13. Ответственность за обеспечение парольной политики в Университете возлагается на ответственного за обеспечение безопасности ПДн.

2.14. Ответственность за реализацию парольной политики в ИСПДн возлагается на администратора безопасности ИСПДн.