	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
_____ Т.Ю. Терентьева
«___» _____ 2022

РЕГЛАМЕНТ ОРГАНИЗАЦИИ ДВУХФАКТОРНОЙ АУТЕНТИФИКАЦИИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ УНИВЕРСИТЕТА

Центр информационно-технического обеспечения
СК-СТО-РГ-23-001-2022

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

СОГЛАСОВАНО
Проректор по цифровому развитию _____ В.В. Крюков
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

ТОТР	—	алгоритм создания одноразовых паролей для защищенной аутентификации, генерация пароля на основе времени, время является параметром. Используется не точное указание времени, а текущий интервал с установленными заранее границами (Time-based One-Time Password Algorithm, RFC 6238)
VDI	—	инфраструктура виртуальных рабочих столов (Virtual Desktop Infrastructure)
ПДн	—	персональные данные
ИСПДн	—	информационная система персональных данных
СЭО	—	система электронного образования

1. Общие положения

1.1. Настоящий Регламент организации двухфакторной аутентификации (далее - Регламент) разработан на основании Федерального закона от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации», с учетом положений приказа ФСТЭК России от 11 февраля 2013 года № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», Методического документа «Меры защиты информации в государственных информационных системах» (утв. ФСТЭК России 11 февраля 2014 года) в целях реализации требований к защите информации в государственных информационных системах Университета

1.2. Настоящий регламент устанавливает требования к организации двухфакторной аутентификации в информационных системах федерального государственного бюджетного образовательного учреждения высшего образования «Владивостокский государственный университет экономики и сервиса» далее (Университет).

1.3. Целью организации двухфакторной аутентификации в информационных системах Университета является обеспечение защиты информационных систем от несанкционированного доступа.

1.4. Двухфакторная аутентификация — это метод идентификации пользователя в информационной системе или сервисе при помощи запроса аутентификационных данных двух разных типов, что обеспечивает двухслойную, а, следовательно, более эффективную защиту учетной записи от компрометации.

1.5. Двухфакторная аутентификация должна применятся в ИСПДн, ЭИОС и VDI, при получении доступа из внешней сети.

1.6. Двухфакторная аутентификация обеспечивает защиту учетной записи пользователя при удаленном подключении к автоматизированному рабочему месту (АРМ) из внешней сети, а также защиту от несанкционированного проникновения в информационную систему Университета через учетную запись пользователя.

1.7. Действие настоящего Регламента распространяется на всех пользователей, сотрудников, учащихся, имеющих доступ к ресурсам информационных систем Университета, в которых применяется двухфакторная аутентификация.

2. Правила организации двухфакторной аутентификации

2.1. Для двухфакторной аутентификации в университете применяется одноразовый пароль защищенной аутентификации, основанный на службе времени (TOTP, RFC 6238), период действия одноразового пароля 30 секунд.

2.2. Для генерации одноразовых паролей (второго фактора) пользователю требуется смартфон на базе ОС IOS или Android с установленным специальным приложением Яндекс.Ключ или «Google Authenticator». Скачивать специальное приложение разрешено только из официального магазина приложений (App Store, Google Play).

2.3. Для первоначальной настройки приложения и получения секретного ключа пользователи, которым необходимо использовать двухфакторную аутентификацию, могут самостоятельно получить его на сайте по ссылке https://api.vvsu.ru/services/settwofactor. Так же пользователь может самостоятельно сменить код (второй фактор) в случае подозрения на компрометацию через ввод текущего кода. Если код (второй фактор) у пользователя привязан, но он его утратил, то смена возможна только через обращение в техническую поддержку ЦИТО.

2.4. После настройки приложения одноразовый пароль генерируется автоматически, при этом специальное приложение работает автономно (не требуется наличия доступа к ресурсам сети Интернет или услугам сотовой связи).

2.5. Доступ к смартфону с установленным специальным приложением должен быть органичен для третьих лиц и защищен графическим ключем, пин-кодом, паролем или средствами биометрической аутентификации. При утрате смартфона пользователь обязан незамедлительно информировать службу технической поддержки ЦИТО для блокировки доступа к информационным системам.

2.6. При получении доступа в информационные системы, требующие двухфакторную аутентификацию, пользователю требуется ввести имя учетной записи, одноразовый пароль и личный пароль, при этом аутентификация может быть разбита на два этапа. В связи с тем, что генерация одноразового пароля осуществляется на основании интервала времени, пользователю в редких случаях потребуется ввести одноразовый пароль два раза.

2.7. Наличие у пользователя второго фактора аутентификации не отменяет соблюдения требований «Инструкции по организации парольной защиты в информационных системах ФГБОУ ВО ВГУЭС» размещенной на по адресу: https://e-campus.vvsu.ru/instructions/porta_services/

3. Ответственность за выполнение требований Регламента

3.1. Пользователь несет ответственность за выполнение настоящего Регламента и соблюдение мер информационной безопасности, препятствующих компрометации пароля, а также за разглашение парольной информации.

3.2. Все события, связанные с нарушением правил парольной защиты, должны регистрироваться и сообщаться администратору безопасности ИСПДн в ЦИТО.

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