Digital Compliance

197198, г. Санкт-Петербург,
ул. Красного Курсанта, д. 25, лит Ж
тел.: +7 (812) 703 15 47, +7 (495) 223-07-86

Экспертное заключение по результатам анализа защищенности веб-ресурсов selectel.ru и my.selectel.ru компании ООО «Селектел»

Даты проведения работ:
04.10.2021-05.11.2021
24.01.2022-25.01.2022

Технические менеджеры проекта:
Н. В. Келесис
Д. Ю. Морозов

Директор департамента аудита:
Г. С. Чербов

Резюме

В данном экспертном заключении представлены результаты анализа защищенности веб-ресурсов *selectel.ru* и *my.selectel.ru*, принадлежащих компании ООО «Селектел».

Работы проводились в соответствии с договором ДК-КУ-2021/25 от 30.08.2021 специалистами компании Digital Compliance в периоды с 04.10.2021 по 05.11.2021 и с 24.01.2022 по 25.01.2022. Тестирование проводилось по модели Black Box. Специалисты не имели исходный код приложений или какую-либо дополнительную документацию, кроме публичной. В веб-приложении *my.selectel.ru* на аккаунты специалистов были начислены средства для тестирования функциональности.

В ходе работ не было выявлено ни одной уязвимости, позволяющей получить доступ непосредственно к серверам Системы, а также не было выявлено уязвимостей с высоким уровнем риска.

Приложение 1. Анализ уровня защищенности. Справочная информация

Анализ уровня защищенности

Для анализа уровня защищенности необходимо оценить критичность и вероятность реализации выявленных в ходе аудита уязвимостей. Вероятность реализации определяется доступностью и простотой реализации уязвимости.

Критичность реализации уязвимости

Свойство «критичность реализации» некоторой уязвимости характеризует возможные последствия реализации данной уязвимости с точки зрения угроз нарушения конфиденциальности, целостности и доступности информации, обрабатываемой на уязвимом ресурсе. Описание уровней критичности реализации уязвимостей приведено в Таблице А–1.

Таблица А–1. Уровни критичности уязвимостей

Значение	Нарушение конфиденциальности	Нарушение целостности	Нарушение доступности
Отсутствует	Не происходит	Не происходит	Не происходит
Низкий	Получение нарушителем доступа к некритичной информации в результате эскалации привилегий	Нарушение целостности некритичной информации с правами обычного пользователя	Кратковременный отказ в обслуживании критичного приложения
Средний	Нарушение конфиденциальности критичной информации с правами обычного пользователя	Нарушение целостности критичной информации с правами обычного пользователя	Долгосрочный отказ в обслуживании критичного приложения или кратковременный отказ в обслуживании ОС
Высокий	Нарушение конфиденциальности критичной информации с правами администратора	Нарушение целостности критичной информации с правами администратора	Долгосрочный отказ в обслуживании ОС

Риск уязвимости

Уязвимость имеет высокий уровень риска в случае, если один из показателей (критичность или вероятность) для данной уязвимости имеет уровень «Высокий», а второй имеет уровень не ниже, чем «Средний».