КАЗАНСКИЙ (ПРИВОЛЖСКИЙ) ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ

СЕТЕВАЯ БЕЗОПАСНОСТЬ В ЭЛЕКТРОННОМ ОБУЧЕНИИ

Валитов Рамиль Аделевич
Зам. директора,
Департамент развития
образовательных ресурсов

Томск, 2014

СИСТЕМА ЭЛЕКТРОННОГО ОБУЧЕНИЯ КФУ

Некоторые факты….

Портал электронного обучения https://e.kfu.ru – ключевой элемент системы

MOODLE – система управления обучением, опыт использования с 2008 года

По данным веб-метрики ~ 2000 уникальных посетителей в день

Используется в ВПО (для поддержку очного, заочного обучения) и в ДПО

ЧТО МОЖЕТ СДЕЛАТЬ ХАКЕР В СЛУЧАЕ УСПЕШНОЙ АТАКИ?

1. Доступ к персональным данным учащихся
2. Изменение содержимого курса
3. Просмотр тестов и ответов
4. Изменение оценок
5. Использование серверов для различных вредоносных действий (спам-рассылка, рассылка вирусов, …)
6. Уничтожение данных (удаление курса, оценок, пользователей, базы данных, файлов, всей системы управления обучением)

…

…

КАК ДЕЙСТВУЕТ ХАКЕР?

(MITM-атака)

КАК ДЕЙСТВУЕТ ХАКЕР?

1. **Места подключения**
2. Способы подключения
3. Устройства:
    1. Микрокомпьютеры
    2. Роутеры
4. Работа с трафиком

Серверная

Домашняя сеть

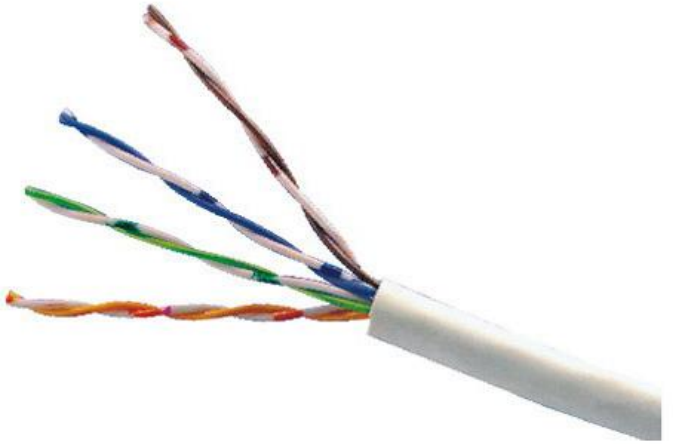
Общественные места

(Интернет-кафе, городские зоны бесплатного W-iFi, гостиницы и т.д.)

Сеть университета

КАК ДЕЙСТВУЕТ ХАКЕР?

1. Места подключения
2. **Способы подключения**
3. Устройства:
    1. Микрокомпьютеры
    2. Роутеры
4. Работа с трафиком



Беспроводное подключение по Wi-Fi

(при наличии у пользователя Wi-Fi сети)

Проводное подключение к локальной сети

(например, с помощью зажимов-крокодилов)

КАК ДЕЙСТВУЕТ ХАКЕР?

1. Места подключения
2. Способы подключения
3. Устройства:
    1. **Микрокомпьютеры**
    2. Роутеры
4. Работа с трафиком

Raspberry Pi

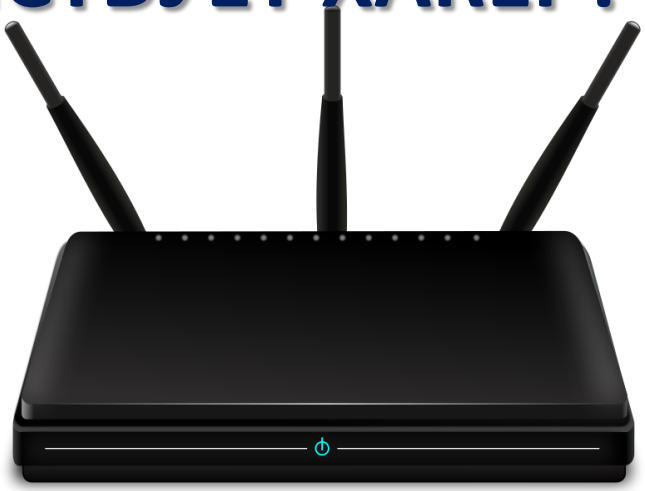
(абсолютно бесшумный, без кулера)

ODROID

(размером с кредитную карту)

КАК ДЕЙСТВУЕТ ХАКЕР?

1. Места подключения
2. Способы подключения
3. Устройства:
    1. Микрокомпьютеры
    2. **Роутеры**
4. Работа с трафиком



Wi-Fi роутер с USB разъемом
(незаметно крепится над фальшпотолком)

+ USB Flash для загрузки специальной прошивки и ПО

OpenWrt
Wireless Freedom

+ специальная прошивка и ПО

КАК ДЕЙСТВУЕТ ХАКЕР?

1. Места подключения
2. Способы подключения
3. Устройства:
    1. Микрокомпьютеры
    2. Роутеры
4. **Работа с трафиком**

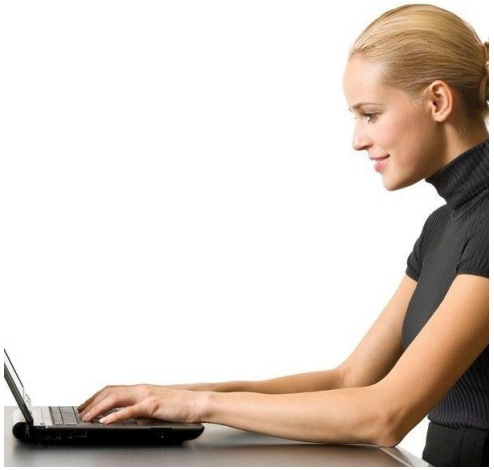
Анализ трафика для кражи пароля
(при незащищенном соединении)

Перенаправление пользователя на созданный сайт-клон для сбора логина/пароля
(при защищенном соединении)

КАК ДЕЙСТВУЕТ ХАКЕР?

1. Места подключения
2. Способы подключения
3. Устройства:
    1. Микрокомпьютеры
    2. Роутеры
4. **Работа с трафиком**

Студенты



Преподаватели

Администраторы

ПАРОЛИ МОГУТ БЫТЬ УКРАДЕНЫ У ПОЛЬЗОВАТЕЛЕЙ С ЛЮБОЙ РОЛЬЮ В СИСТЕМЕ!

КАК ДЕЙСТВУЕТ ХАКЕР?

1. ~~Места подключения~~
2. Способы подключения
3. Устройства:
    1. Микрокомпьютеры
    2. Роутеры
4. ~~Работа с трафиком~~

Для защиты мы используем меры, направленные на подавление возможности реализации пунктов 1 и 4.

БЕЗОПАСНОСТЬ СИСТЕМЫ ЭЛЕКТРОННОГО ОБУЧЕНИЯ КФУ

БЕЗОПАСНОСТЬ В КФУ

1. **Дата-центр**
2. HTTPS, SSL
3. Браузеры
4. OCSP stapling
5. HSTS
6. SPDY
7. PCI, FIPS
8. Анализ

Сервера размещены в дата-центре ИТ-парка – один из лучших дата-центров РФ

Высокий уровень физической безопасности серверов

Международный уровень надежности Tier 3, все системы зарезервированы по схеме N+1

БЕЗОПАСНОСТЬ В КФУ

1. Дата-центр
2. **HTTPS, SSL**
3. Браузеры
4. OCSP stapling
5. HSTS
6. SPDY
7. PCI, FIPS
8. Анализ

SSL-сертификат

Все данные шифруются с помощью специального SSL-сертификата, который подтверждает валидность наших серверов

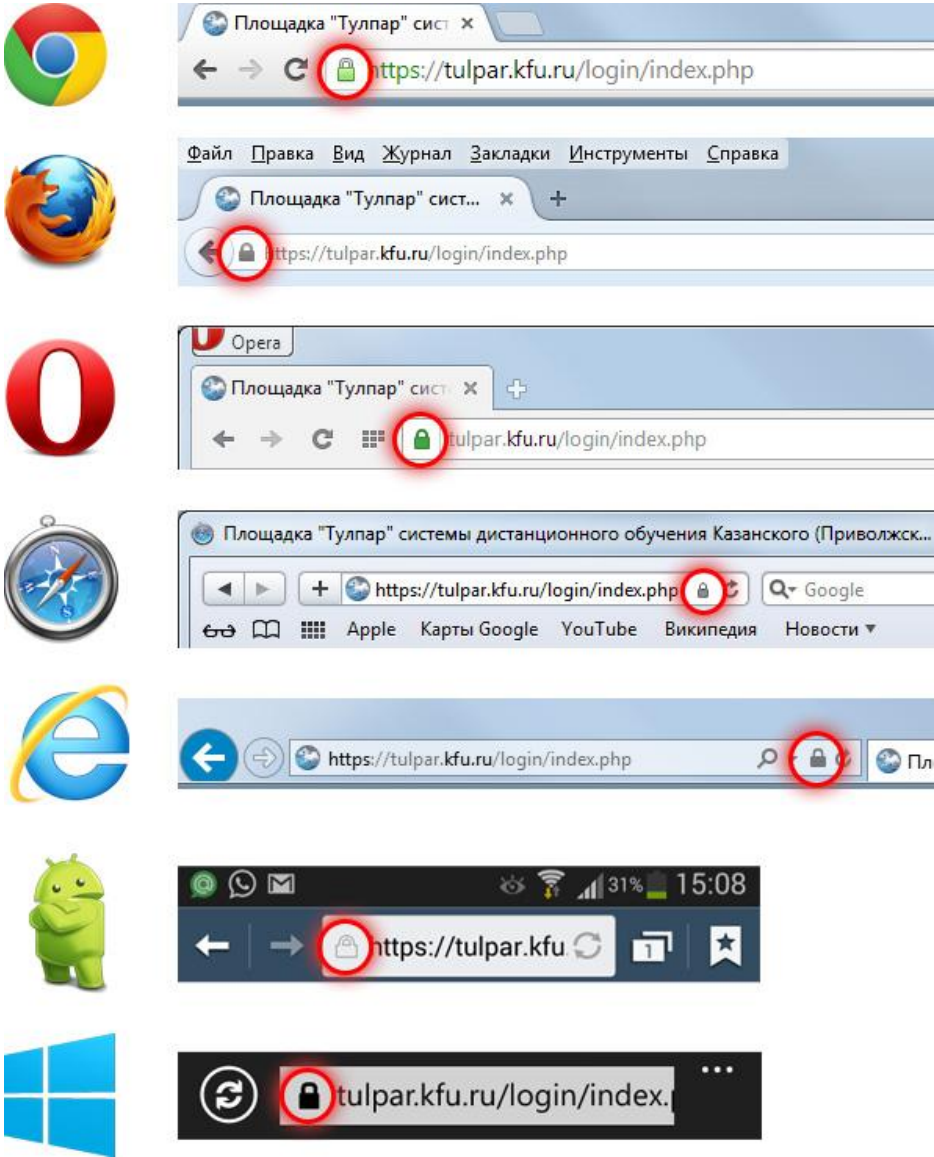
Сервера поддерживают все современные актуальные криптографические протоколы **TLS 1.0, TLS 1.1, TLS 1.2.**

Внедрено использование защищенного Интернет-соединения с шифрованием при передаче важных уязвимых данных (например, пароль пользователя)

БЕЗОПАСНОСТЬ В КФУ

1. Дата-центр
2. HTTPS, SSL
3. **Браузеры**
4. OCSP stapling
5. HSTS
6. SPDY
7. PCI, FIPS
8. Анализ

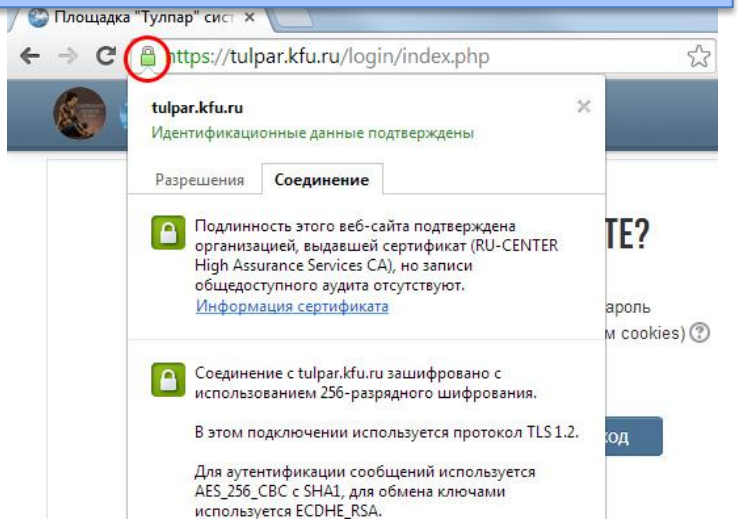
Индикация надежного защищенного соединения во всех браузерах и платформах (Windows, Linux, Android, iOS)



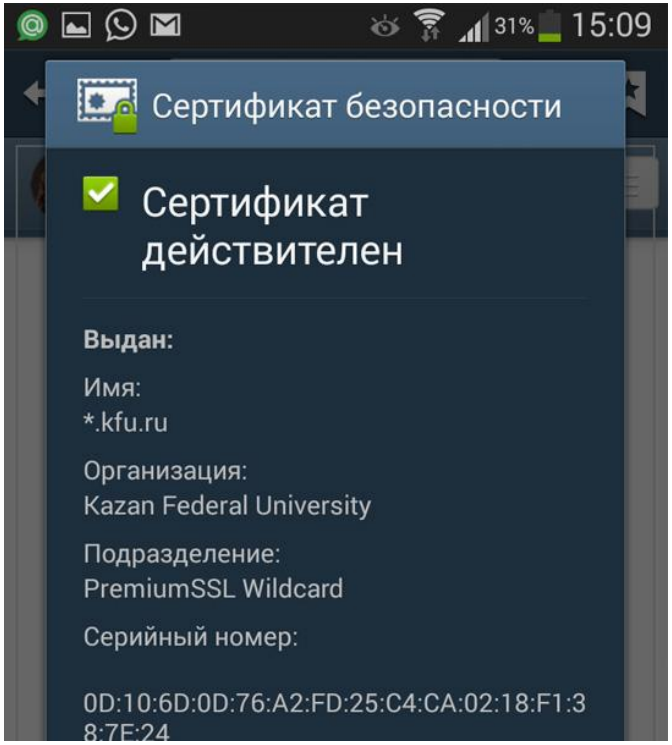
БЕЗОПАСНОСТЬ В КФУ

1. Дата-центр
2. HTTPS, SSL
3. **Браузеры**
4. OCSP stapling
5. HSTS
6. SPDY
7. PCI, FIPS
8. Анализ

Подробные сведения о корректном защищенном соединении, сертификате безопасности



Google Chrome (Windows 7)



Android

БЕЗОПАСНОСТЬ В КФУ

1. Дата-центр
2. HTTPS, SSL
3. Браузеры
4. **OCSP stapling**
5. HSTS
6. SPDY
7. PCI, FIPS
8. Анализ

Для подтверждения валидности сертификата сервера настроены на предоставление всей необходимой цепочки сертификатов вплоть до корневого центра сертификации.

При этом реализуется «классическая» проверка по **CLR**(Certificate Revocation List), а также сервера обеспечивают поддержку технологии OCSP stapling. **OCSP** (Online Certificate Status Protocol) – протокол, проверяющий, был ли отозван SSL-сертификат. Он был создан в качестве альтернативы CRL, с целью уменьшить время SSL-переговоров.

БЕЗОПАСНОСТЬ В КФУ

1. Дата-центр
2. HTTPS, SSL
3. Браузеры
4. OCSP stapling
5. **HSTS**
6. SPDY
7. PCI, FIPS
8. Анализ

С целью уменьшения вероятности атаки SSL strippling (когда атакующий производит «прозрачную» подмену HTTPS-сессии на HTTP) на сервере реализована поддержка **Strict Transport Security (HSTS)** для форсированной активации исключительно HTTPS соединений на стороне клиента.

Google

Внедрение HTTPS повышает общий поисковый рейтинг сайта для Google

https://e.kfu.ru

Для Портала используется HSTS

Для MOODLE используется гибридный подход

БЕЗОПАСНОСТЬ В КФУ

1. Дата-центр
2. HTTPS, SSL
3. Браузеры
4. OCSP stapling
5. HSTS
6. **SPDY**
7. PCI, FIPS
8. Анализ

Для повышения скорости работы по HTTPS, сервер настроен на использование (в дополнение к **HTTP 1.1**) протокола **SPDY** (на текущий момент серверами поддерживается версия 3.1), разработанного компанией Google для снижения времени загрузки веб-страниц и их элементов.

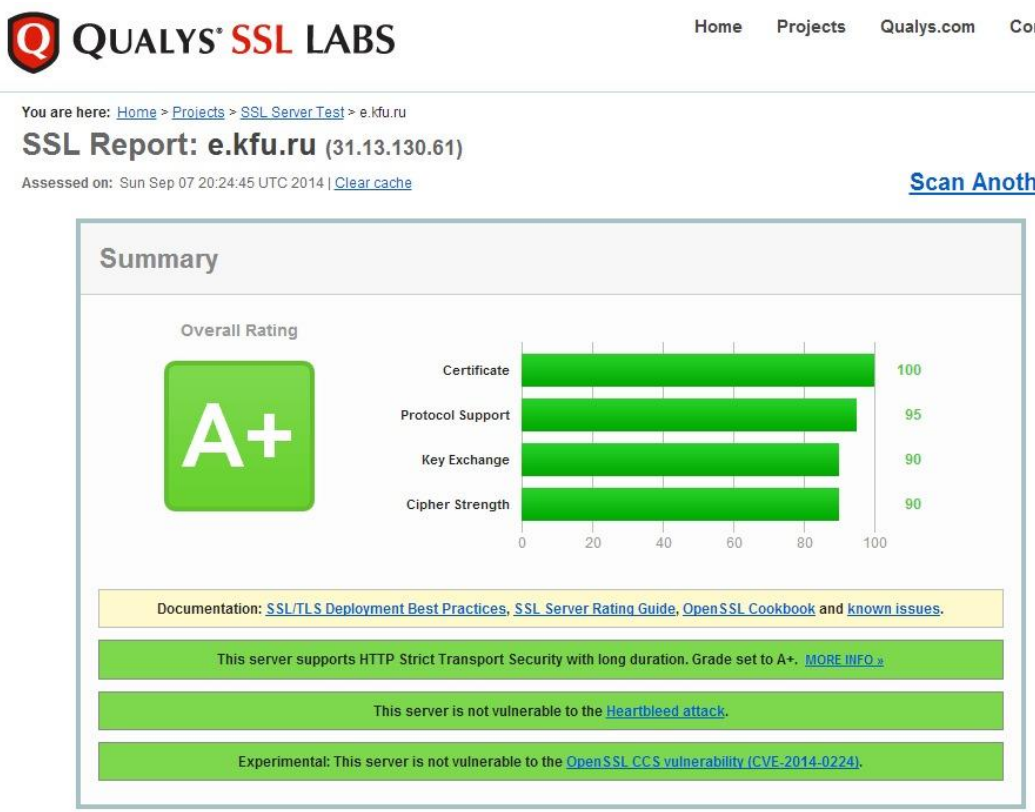
БЕЗОПАСНОСТЬ В КФУ

1. Дата-центр
2. HTTPS, SSL
3. Браузеры
4. OCSP stapling
5. HSTS
6. SPDY
7. **PCI, FIPS**
8. Анализ

Методы шифрования и настройки сервера обеспечивают поддержку совместимости стандартам PCI (Payment Card Industry, что является необходимым условием для проведения безопасных онлайн платежей) и FIPS 140-2 (стандарт безопасности правительства США для криптографических модулей)

БЕЗОПАСНОСТЬ В КФУ

1. Дата-центр
2. HTTPS, SSL
3. Браузеры
4. OCSP stapling
5. HSTS
6. SPDY
7. PCI, FIPS
8. **Анализ**



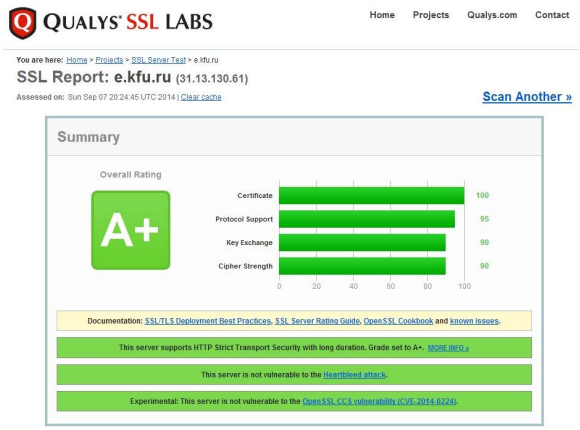
hackstacks.com

QUALYS®
ON DEMAND SECURITY

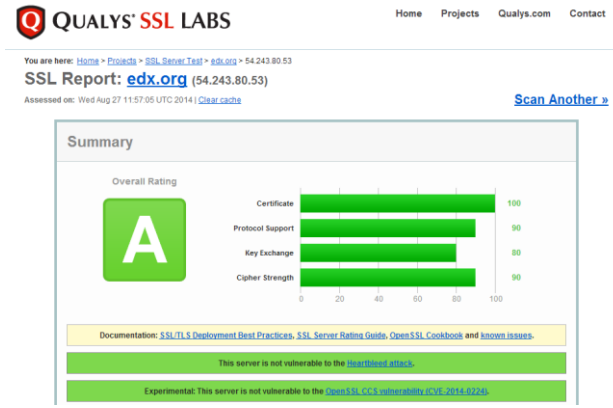
Для анализа конфигурации и уровня безопасности серверов использовался сервис от Qualys SSL Labs.

Порталу электронного обучения КФУ была присвоена максимальная оценка A+

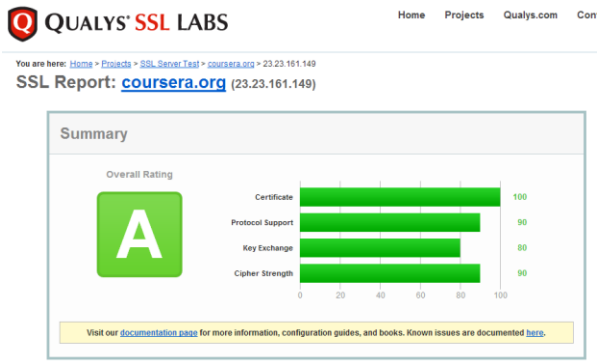
СРАВНЕНИЕ



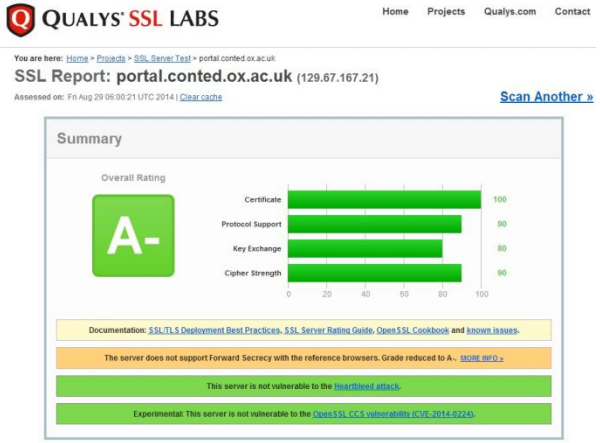
Портал электронного обучения КФУ - оценка A+



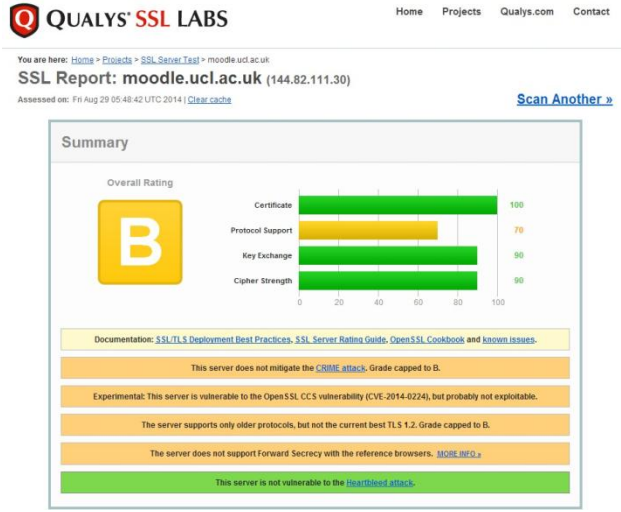
edX - оценка A



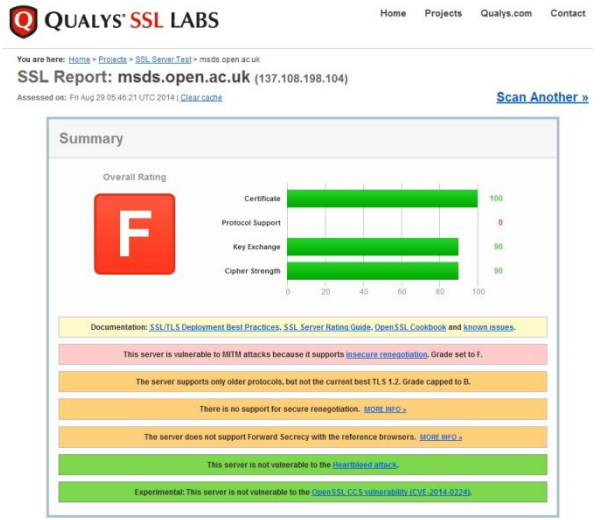
Coursera - оценка A



The University of Oxford (MOODLE) - оценка A-



University College London (MOODLE) - оценка B



The Open University (MOODLE) - оценка F

ЗАКЛЮЧЕНИЕ

1. Использование защищенных соединений позволяет не только обеспечить сохранность данных пользователя, но и общую безопасность и надежность системы электронного обучения, т.к. препятствует атакам, ориентированным на кражу пароля пользователя, в т.ч. с высоким уровнем доступа (преподаватель, администратор).

2. Внедрение HTTPS повышает общий поисковый рейтинг сайта для Google.

3. Использование HTTPS также необходимо в случае сетевого взаимодействия федеральных университетов в области электронного обучения, когда планируется по принципу единого входа предоставлять онлайн-доступ к ресурсам любого из университетов-партнеров. В этом случае учащемуся достаточно авторизоваться только на портале «родного» университета для получения авторизованного доступа к ресурсам университетов-партнеров. Для реализации такой схемы «доверия», необходимо, чтобы у каждого университета была безопасная онлайн-авторизация.

СПАСИБО!

Валитов Рамиль Аделевич

E-mail: ramil.valitov@kpfu.ru