УДК 004.056:378

Шкуренков Егор Сергеевич, студент
Шишов Олег Алексеевич, ассистент кафедры безопасности информационных технологий
(РГУ нефти и газа (НИУ) имени И.М. Губкина, г. Москва)
Egor S. Shkurenkov, student
Oleg A. Shishov, assistant lecturer, Department of Information Technology Security
(Gubkin University, Moscow)

ЗАЩИЩЁННОСТЬ САЙТОВ И ПОЧТЫ УНИВЕРСИТЕТОВ КАК УСЛОВИЕ ПОДГОТОВКИ ИНЖЕНЕРНЫХ КАДРОВ В ЦИФРОВОЙ ОБРАЗОВАТЕЛЬНОЙ СРЕДЕ

SECURITY OF UNIVERSITY WEBSITES AND E-MAIL AS A CONDITION FOR TRAINING ENGINEERS IN THE DIGITAL EDUCATIONAL ENVIRONMENT

Аннотация. Обследованы сайты 166 российских университетов: защитные HTTP-заголовки, сертификаты, записи SPF и DMARC. Вузы защищают почту не хуже крупных сайтов, но вдвое чаще раскрывают версии серверного ПО. Предложены меры, не требующие затрат.

Abstract. Websites of 166 Russian universities were surveyed: security HTTP headers, certificates, SPF and DMARC records. Universities protect e-mail as well as major sites but disclose server software versions twice as often. Zero-cost measures are proposed.

Подготовка инженерно-технических кадров сегодня идёт в цифровой среде: сайт университета, личный кабинет, корпоративная почта и системы дистанционного обучения сопровождают студента ежедневно. Если эта среда сама устроена небезопасно — сайт доступен без шифрования, письма от имени вуза легко подделать, — то любые знания о фишинге [1], которые даёт курс информационной безопасности, обесцениваются: студент не может отличить настоящую рассылку деканата от поддельной, потому что настоящая выглядит так же подозрительно. Методы защиты веб-приложений систематизированы в [2], защищённая передача данных рассмотрена в [3]; однако состояние защищённости сайтов именно образовательных организаций, которые обрабатывают персональные данные десятков тысяч обучающихся, в литературе количественно не описано, хотя навыки обследования и настройки таких систем входят в требования работодателей к выпускникам технических направлений [4].

Цель работы — оценить защищённость официальных сайтов и почтовых доменов российских университетов по проверяемым извне признакам и сопоставить её с уровнем популярных российских сайтов, чтобы определить, какие меры должны стать частью цифровой образовательной среды технического вуза.

Выборка: 166 официальных доменов российских университетов, присутствующих в рейтинге популярности доменов Tranco [5]. 8 октября 2026 г. для каждого домена выполнены: запрос главной страницы с фиксацией перехода на HTTPS и шести защитных HTTP-заголовков (HSTS, Content-Security-Policy, X-Frame-Options, X-Content-Type-Options, Referrer-Policy, Permissions-Policy) и раскрытия версии серверного ПО; соединение TLS с чтением издателя сертификата; запросы DNS-записей SPF и DMARC, защищающих от подделки отправителя почты. Ответ получен от 149 сайтов; почту принимают 165 доменов. Метод представляет собой активное обследование конфигурации, подобное инструментальному аудиту систем [6]. Для сравнения взяты показатели 500 наиболее посещаемых сайтов зоны .ru, полученные той же методикой (таблица 1).

Таблица 1 – Защищённость сайтов университетов и популярных сайтов .ru, % доменов

Показатель	Университеты	Топ-500 .ru
Переход на HTTPS	93,3	89,8
Заголовок HSTS (запрет незащищённого соединения)	29,5	39,7
Content-Security-Policy	22,1	27,0
X-Frame-Options (защита от встраивания страницы)	41,6	37,5
Ни одного защитного заголовка	33,6	36,2
Средний индекс защищённости (из 6)	1,53	1,61
Раскрытие версии серверного ПО	46,3	20,3
Сертификат Let's Encrypt	52,4	39,8
Запись SPF (домены с почтой)	98,8	94,5
Запись DMARC	84,2	81,9
DMARC со строгой политикой	58,2	63,7
Нет ни SPF, ни DMARC	0,6	5,5

Университеты не уступают крупным сайтам по базовым мерам: HTTPS включён у 93,3 % сайтов, записи SPF есть у 98,8 % почтовых доменов, DMARC — у 84,2 %, без какой-либо почтовой защиты остаётся менее одного процента доменов. Однако две группы показателей обнаруживают систематическое отставание. Во-первых, защитные заголовки: HSTS выставляют 29,5 % вузов против 39,7 % популярных сайтов, Content-Security-Policy — 22,1 против 27,0 %, а треть сайтов не выставляет ни одного заголовка. Во-вторых, раскрытие версии серверного программного обеспечения: 46,3 % сайтов университетов сообщают её в заголовках ответа — в 2,3 раза чаще, чем популярные сайты, — что облегчает нарушителю подбор известных уязвимостей. Строгая политика DMARC, при которой поддель-

ные письма от имени вуза отклоняются, действует лишь у 58,2 % доменов; у 26,1 % политика «только наблюдение», то есть письмо «от деканата» с чужого сервера будет доставлено студенту.

Состав инфраструктуры доверия у вузов однороден: сертификаты выпущены либо бесплатным центром Let's Encrypt (52,4 % сайтов), либо коммерческим GlobalSign (47,6 %); отечественный удостоверяющий центр и зарубежные сети доставки контента не используются вовсе. Подпись зоны DNSSEC есть у 3,6 % доменов, запись CAA, ограничивающая выпуск сертификатов, — у 6,0 % (у популярных сайтов — 13,4 %). Иначе говоря, университеты обеспечили минимально необходимое шифрование, но не перешли к мерам, которые требуют осознанного управления доверием: без записи CAA сертификат для домена вуза может выпустить любой центр, а без DNSSEC получатель не может проверить подлинность самой записи, хотя обе меры также не требуют затрат.

Для цифровой образовательной среды это означает конкретный перечень мер, каждая из которых реализуется настройкой и не требует закупок: перевод DMARC в строгую политику с получением отчётов, включение HSTS и запрета встраивания страницы, сокрытие версии серверного ПО, регулярное внешнее обследование по приведённой методике. Раскрытие версии серверного ПО стоит в одном ряду с другими непреднамеренными утечками сведений, которыми пользуется нарушитель: метаданными публикуемых на сайте изображений [7] и открытыми страницами вуза в социальных сетях [8]. Отдельная задача ближайших лет — переход инфраструктуры сертификатов на постквантовые алгоритмы в связи с развитием квантовых вычислений [9]: он потребует автоматизированного перевыпуска, к которому сегодня готовы лишь вузы, использующие Let's Encrypt. Важно и образовательное следствие: защищённо настроенный сайт и почта вуза становятся эталоном, на котором студенты инженерных направлений учатся отличать подлинные ресурсы, а открытые результаты обследования — учебным материалом для курсов информационной безопасности, построенным на реальных, а не учебных данных.

Ограничения работы: обследование выполнено однократно и только по внешним признакам; выборка ограничена вузами, попавшими в рейтинг Tranco, то есть наиболее посещаемыми; внутренние сервисы (личные кабинеты, системы дистанционного обучения) не проверялись; сравнение с коммерческими сайтами корректно лишь по внешним признакам. Тем не менее полученные значения задают базовый уровень 2026 г. и могут использоваться для оценки эффекта мер по защите цифровой образовательной среды. Повторное обследование по той же методике через год покажет, меняется ли состояние защищённости вузов быстрее, чем у коммерческих сайтов, и может быть выполнено силами студенческой исследовательской группы в рамках учебного курса — как практикум, формирую-

щий навыки обследования, анализа данных и настройки защиты, востребованные работодателями.

Список литературы

1. Мельников, В. А. Классификация технологий применения фишинга в качестве метода социальной инженерии / В. А. Мельников, А. А. Першина // Новые технологии в газовой промышленности (газ, нефть, энергетика) : Тезисы докладов, Москва, 23–27 октября 2023 года. – Москва: Российский государственный университет нефти и газа (национальный исследовательский университет) им. И.М. Губкина, 2023. – С. 307-308. – EDN VVHDRR.
2. Боровков, В. Е. Методы защиты веб-приложений от злоумышленников / В. Е. Боровков, П. Г. Ключарев // Вопросы кибербезопасности. – 2023. – № 5 (57). – С. 89-99. – DOI 10.21681/2311-3456-2023-5-89-99.
3. Мельников, В. А. Исследование существующих методов и технологий обеспечения защищенной передачи информации / В. А. Мельников // Цифровое общество: образование, экономика, технологии : Материалы III Международной научно-практической конференции, Новокузнецк, 18–19 марта 2025 года. – Москва: ООО "Актуальность.РФ", 2025. – С. 299-304. – EDN OYPKNT.
4. Свидетельство о государственной регистрации программы для ЭВМ № 2026662602 Российская Федерация. Интеллектуальный анализатор цифровых компетенций вакансий : заявл. 17.04.2026 : опубл. 29.04.2026 / В. А. Мельников, А. А. Мельникова. – EDN XUTTOK.
5. Tranco: A Research-Oriented Top Sites Ranking Hardened Against Manipulation / V. Le Pochat, T. Van Goethem, S. Tajalizadehkhoob [et al.] // Proceedings 2019 Network and Distributed System Security Symposium. – 2019. – DOI 10.14722/ndss.2019.23386.
6. Мельников, В. А. Инструменты для аудита безопасности на ALT Linux на примере Lynis / В. А. Мельников, А. А. Першина // Глобальные научные тренды: междисциплинарные исследования : Сборник статей II Международной научно-практической конференции, Саратов, 25 марта 2025 года. Часть 1. – Саратов: ООО Издательство "Кубик", 2025. – С. 90-102. – EDN DBAKYT.
7. Свидетельство о государственной регистрации программы для ЭВМ № 2024689825 Российская Федерация. Интеллектуальный анализатор метаданных изображений : № 2024689342 : заявл. 28.11.2024 : опубл. 11.12.2024 / А. А. Першина, В. А. Мельников. – EDN NSFRGS.
8. Свидетельство о государственной регистрации программы для ЭВМ № 2024687883 Российская Федерация. Программа для пассивного мониторинга компании в социальных сетях : № 2024684563 : заявл. 14.10.2024 : опубл. 22.11.2024 / А. А. Першина, В. А. Мельников. – EDN HMCRRK.
9. Казанцев, И. С. Перспективы развития квантовых вычислений / И. С. Казанцев, В. А. Мельников, А. А. Першина // Интеллектуальные техноло-

гии в эргодизайне и когнитивных науках : сборник материалов всероссийской научно-практической онлайн-конференции с международным участием, Брянск, 10–11 июня 2025 года. – Брянск: Брянский государственный технический университет, 2025. – С. 122-130. – EDN QVDUSI.