DIGITAL RESILIENCE ASSOCIATION

Результаты анализа защищенности интернет-ресурсов государственных органов Кыргызской Республики

2025

WEBTOTEM

tsarka group

Глоссарий

DIGITAL RESILIENCE ASSOCIATION

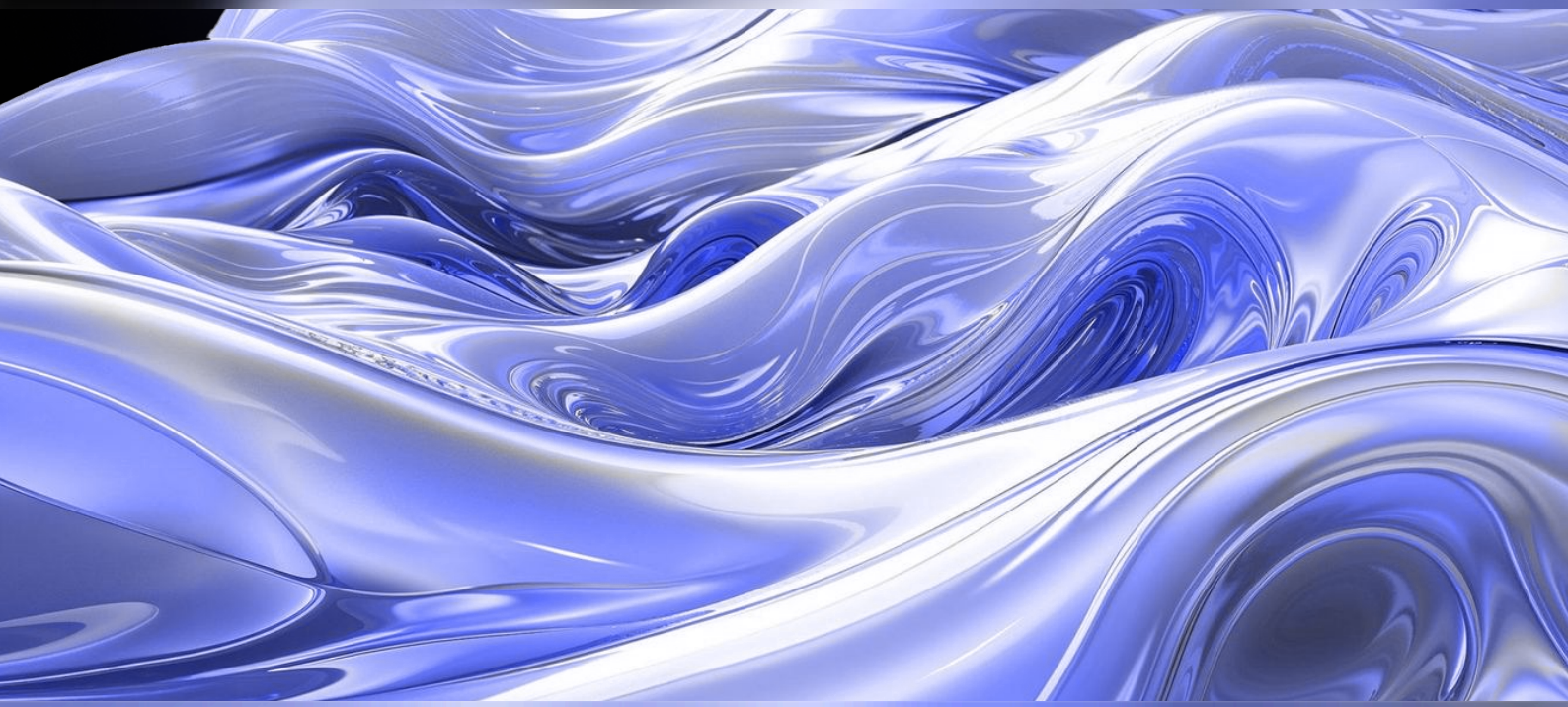
Информационная безопасность – это состояние информационной системы при котором она способна обеспечить конфиденциальность, целостность и доступность хранимых данных.

Уязвимость – недостаток или недоработка информационной системы, которая может быть использована с целью несанкционированного доступа к данным, их изменению или удалению.

Риск – потенциальный ущерб, который может быть нанесен организации в случае использования уязвимостей системы в преступных целях.

Кибер-атака – использование технологий с целью несанкционированного доступа в систему и получения контроля над ней.

Интернет-ресурс – веб-сайт, электронный информационный ресурс, функционирующий и доступен в сети Интернет.



Введение

В последние годы вопросы кибербезопасности приобрели особую значимость, особенно в государственном секторе, где защищённость цифровых ресурсов напрямую влияет на национальную безопасность и доверие граждан к электронным услугам. Государственные интернет-ресурсы служат важными точками взаимодействия между органами власти и населением, однако они также являются привлекательными целями для кибератак.

Данное исследование направлено на оценку защищённости веб-ресурсов государственных органов Кыргызской Республики. В рамках анализа были изучены основные аспекты безопасности, включая конфигурацию протоколов шифрования, защиту веб-приложений, корректность настроек почтовых серверов и используемого программного обеспечения. Проверки проводились неинвазивными методами, что позволило получить объективную картину состояния кибербезопасности без вмешательства в работу исследуемых систем.

Результаты исследования позволят выявить потенциальные уязвимости, определить распространённые ошибки в настройках и предложить рекомендации для повышения уровня защиты государственных интернет-ресурсов. **Цель данного отчёта — не только обозначить текущие риски**, но и способствовать укреплению цифровой безопасности в государственном секторе.

TSARKA искренне надеется, что проделанная работа поможет отделам информационной безопасности обратить внимание на выявленные уязвимости, которые потенциально могут быть использованы злоумышленниками, а также будет способствовать повышению уровня защиты в соответствии с лучшими мировыми практиками.

Информация об исследовании

Цель исследования

Основной целью данного исследования было провести комплексную оценку уровня кибербезопасности интернет-ресурсов государственных органов Кыргызской Республики, выявить существующие уязвимости и сформировать практические рекомендации по их устранению. Результаты помогут укрепить информационную защиту в государственном секторе, повысить доверие граждан к цифровым услугам и создать базу для дальнейшего совершенствования мер кибербезопасности.

Такой подход даёт как специалистам, так и широкому кругу читателей общее представление о текущих рисках и путях их минимизации.

Метод исследования

Эксперты TSARKA использовали неинвазивные методы анализа, изучая основной домен государственного органа, его главную страницу и почтовый сервер. Тестирование проводилось без воздействия на работоспособность веб-ресурсов, с применением «лёгких» HTTP- и DNS-запросов, а также анализа ответов сервера.

Исследование включало оценку соответствия конфигурации веб-серверов и связанных компонентов рекомендованным настройкам безопасности. Для проверки были выбраны ключевые контрольные точки, доступные без вмешательства в работу веб-ресурсов, что исключает возможность нанесения технического ущерба.

Периметр аудита

В рамках исследования были проанализированы веб-ресурсы государственных органов Кыргызской Республики. Оценка проводилась по ключевым критериям, позволяющим объективно определить уровень их защищённости и выявить потенциальные уязвимости.

- Использование уязвимых или устаревших технологий
- Шифрование трафика и утечки информации
- Безопасность почтовых серверов
- Конфигурация веб-сервера
- Безопасность контента и передачи данных
- Соответствие стандартам

75

веб-ресурсов были проверены на предмет наличия уязвимостей

Полный перечень интернет-ресурсов, которые вошли в периметр анализа защищенности:

Веб-сайт med.kg	Веб-сайт edu.gov.kg	Веб-сайт mineconom.gov.kg	Веб-сайт mvd.gov.kg	Веб-сайт mfa.gov.kg	Веб-сайт minjust.gov.kg	Веб-сайт agro.gov.kg	Веб-сайт mtd.gov.kg
Веб-сайт minenergo.gov.kg	Веб-сайт minfin.kg	Веб-сайт minculture.gov.kg	Веб-сайт mlsp.gov.kg	Веб-сайт mchs.gov.kg	Веб-сайт sti.gov.kg	Веб-сайт gknb.gov.kg	Веб-сайт e.srs.kg
Веб-сайт infocom.kg	Веб-сайт stat.kg	Веб-сайт bishkek.gov.kg	Веб-сайт oshcity.gov.kg	Веб-сайт nesk.kg	Веб-сайт tulpar-card.kg	Веб-сайт meria.tokmokcity.kg	Веб-сайт naryn-raiadmin.gov.kg
Веб-сайт batken.gov.kg	Веб-сайт talas.gov.kg	Веб-сайт cci.kg	Веб-сайт kse.kg	Веб-сайт gov.kg	Веб-сайт gik.kg	Веб-сайт fiu.gov.kg	Веб-сайт customs.gov.kg
Веб-сайт esep.kg	Веб-сайт president.kg	Веб-сайт kenesh.kg	Веб-сайт zakupki.gov.kg	Веб-сайт portal.tunduk.kg	Веб-сайт koomtalkuu.gov.kg	Веб-сайт elicense.gov.kg	Веб-сайт ombudsman.kg
Веб-сайт digital.gov.kg	Веб-сайт patent.gov.kg	Веб-сайт gosreg.gov.kg	Веб-сайт forest.gov.kg	Веб-сайт naskr.gov.kg	Веб-сайт archive.kg	Веб-сайт nism.gov.kg	Веб-сайт ik.kg
Веб-сайт jalal-abad.gov.kg	Веб-сайт data.gov.kg	Веб-сайт invest.gov.kg	Веб-сайт sot.kg	Веб-сайт religion.gov.kg	Веб-сайт mkk.gov.kg	Веб-сайт nbkr.kg	Веб-сайт gosstroy.gov.kg
Веб-сайт darek.kg	Веб-сайт sf.gov.kg	Веб-сайт zakupki.okmot.kg	Веб-сайт shailoo.gov.kg	Веб-сайт kyrgyztest.gov.kg	Веб-сайт guobdd.kg	Веб-сайт olympic.kg	Веб-сайт knu.kg
Веб-сайт main.teksher.kg	Веб-сайт nisi.kg	Веб-сайт railway.kg	Веб-сайт mammulk.gov.kg	Веб-сайт prokuror.kg	Веб-сайт fsa.gov.kg	Веб-сайт antimonopolia.gov.kg	Веб-сайт kca.gov.kg
Веб-сайт mil.gov.kg	Веб-сайт cadastre.kg	Веб-сайт salyk.kg	Веб-сайт stat.gov.kg	Веб-сайт ik.gov.kg			

Результаты оценки защищенности

В рамках исследования был проведен анализ конфигурации SSL/TLS, использование шифров, корректность настроек веб-серверов, защиту веб-приложений, а также безопасность почтовых сервисов.

В частности, тестировалась поддержка устаревших протоколов, наличие критических уязвимостей, правильность реализации механизмов аутентификации и защиты данных.

По результатам исследования средний показатель защищённости государственных интернет-ресурсов составил 66%.

Это указывает на хороший уровень безопасности в большинстве случаев, однако выявленные уязвимости и ошибки конфигурации свидетельствуют о необходимости дальнейшего совершенствования мер киберзащиты.

Обзор результатов сканирования

Веб-сайт	Безопасность	Оценка
sot.kg	High	81 %
gknb.gov.kg	High	80 %
sot.kg	High	79 %
gknb.gov.kg	High	79 %
sot.kg	High	79 %
gknb.gov.kg	High	79 %

Методология расчета

Шифрование трафика

Описание критерия

Проведён автоматизированный анализ веб-ресурсов государственных органов с целью выявления уязвимостей в шифровании трафика, конфигурации веб-серверов, защите веб-приложений, почтовых сервисов и используемых программных компонентов. Проверки выполнялись неинвазивными методами, включая отправку HTTP- и DNS-запросов, анализ заголовков, сертификатов, доступных эндпоинтов и версий программного обеспечения. Данные были сопоставлены с известными базами уязвимостей (CVE, NVD).

Описание потенциальной атаки

Злоумышленники могут перехватывать данные при слабом шифровании, внедрять вредоносный код, обходить аутентификацию и использовать уязвимости серверов. Ошибки конфигурации и отсутствие базовых мер безопасности позволяют получить несанкционированный доступ или подделывать официальные ресурсы.

Негативные последствия

Атаки могут привести к утечке персональных данных, компрометации систем и снижению доверия к госуслугам. Возможны распространение вредоносного ПО, финансовые потери и угрозы национальной безопасности.

8

критичных из 75 интернет-ресурсов без сертификата безопасности

Детальный анализ и перечень проверок, которые проводились относительно шифрования трафика приведены далее:

- Недостатки в конфигурировании алгоритма Диффи – Хеллмана
- Уязвимость POODLE
- Уязвимость FREAK
- Возможность проведения атаки Logjam
- Уязвимость ROBOT
- Уязвимость Beast
- CVE-2019-5096, CVE-2019-5097
- CVE-2016-2107, CVE-2013-2566
- Уязвимость Heartbleed
- Используемые шифры и их стойкость, поддержка RC4
- Поддержка Forward Secrecy
- Версия TLS
- Поддержка устаревших версий TLS (1.0, 1.1) и SSL (2.0, 3.0)

Ресурсы без сертификата безопасности

- Forest.Gov.Kg
- Zakupki.Gov.Kg
- Archive.Kg
- Darek.Kg
- Meria.Tokmokcity.Kg
- Religion.Gov.Kg
- Energy.Gov.Kg
- Okmot.Kg

Веб-ресурсы, с наиболее защищенными портами

- cadastre.kg
- cci.kg
- fsa.gov.kg
- gik.kg
- www.gov.kg
- gosreg.gov.kg
- ik.gov.kg
- kenesh.kg
- koomtalkuu.gov.kg
- minculture.gov.kg
- minfin.kg
- med.kg
- railway.kg
- gknb.gov.kg
- mtd.gov.kg
- naryn-raiadmin.gov.kg
- naskr.gov.kg
- salyk.kg
- president.kg
- mkk.gov.kg
- sti.gov.kg

Методология расчета

Репутация домена

Описание критерия

Проверка репутации домена проводится с целью выявления его присутствия в чёрных списках (blacklists), антивирусных базах, базах фишинговых сайтов и спам-листах. Анализ осуществляется с использованием открытых сервисов (VirusTotal, Google Safe Browsing, Spamhaus, OpenPhish и др) и автоматизированных инструментов, позволяющих определить, был ли домен замечен в вредоносной активности или используется для распространения фишинга, спама или атак.

Описание потенциальной атаки

Если домен организации попадает в чёрные списки, злоумышленники могут использовать это в атаках на пользователей, подделывая или компрометируя оригинальный сайт. Также домен может быть скомпрометирован для распространения вредоносного ПО или включён в ботнет-сети. Попадание в базы фишинга может свидетельствовать о том, что сайт уже используется в мошеннических схемах или атакующие имитируют официальный ресурс.

Негативные последствия

Низкая репутация домена приводит к блокировке сайта антивирусными системами и браузерами, снижению доверия пользователей, потере органического трафика и возможным правовым последствиям. В результате граждане могут подвергнуться фишинговым атакам, а организация потеряет контроль над своей цифровой репутацией. Если домен будет использован в распространении спама или вредоносного контента, он может быть заблокирован поисковыми системами и почтовыми провайдерами.

0

из 75 веб-ресурсов имеют отрицательную репутацию

Методология расчета

Открытые пути

Описание критерия

Анализ веб-ресурсов на наличие критичных открытых путей включает проверку доступности директорий, файлов конфигурации, резервных копий и административных панелей. Используются автоматизированные инструменты WebTotem, который перебирает известные пути и файлы (например, /admin, /backup, /config.php). Это помогает выявить потенциальные точки утечки информации или незащищённые интерфейсы.

Описание потенциальной атаки

Злоумышленники могут использовать открытые пути для получения конфиденциальных данных, таких как резервные копии, файлы конфигурации с логинами и паролями или исходный код веб-приложения. Доступность директорий администрирования без защиты позволяет атакующему попробовать подбор паролей (Brute Force) или эксплуатировать известные уязвимости.

Негативные последствия

Если на сервере обнаружены открытые пути к критически важным файлам, это может привести к утечке данных, компрометации учетных записей или полному захвату веб-ресурса. Злоумышленники могут загрузить вредоносный код, изменить содержимое сайта или использовать доступ к серверу для дальнейших атак. Это создаёт серьёзные риски как для безопасности организации, так и для её репутации.

29

из 75 веб-ресурсов имеют минимум 2 критичных открытых путей

Пути входа в админ-панели и панели управления

/admin/login

/wp-admin

/dashboard

/admin/login

/user/login, /member/login

Открытый доступ к серверным файлам и логам

/server-status

/phpinfo.php

/error_log, /log, /logs

Конфиденциальные файлы, которые не должны быть доступны

.git, .svn, .hg

.env

config.php, config.bak

Файлы баз данных и бэкапы

/dump.sql, /database.sql, /export.sql, /db_backup.zip,

/backup.tar.gz

config.php, config.bak

/backup, /backups

Открытые API

/api, /api/v1, /api/v2

Веб-ресурсы с наилучшими показателями по сканированию открытых путей

med.kg

mineconom.gov.kg

agro.gov.kg

edu.gov.kg

gknb.gov.kg

president.kg

Методология расчета

Открытые порты

Описание критерия

Анализ выполнялся для выявления нестандартных (не дефолтных) открытых портов, которые могут представлять угрозу. Проверялись доступные извне сетевые сервисы, их версии и потенциальные уязвимости, исключая стандартные порты (80, 443 и др.), необходимые для работы веб-ресурса.

Описание потенциальной атаки

Злоумышленники могут использовать открытые порты для обнаружения сервисов, атак на устаревшее ПО или перебора паролей. Неавторизованный доступ к FTP, RDP, MySQL или другим сервисам позволяет захватить контроль над сервером или провести дальнейшую атаку.

Негативные последствия

Открытые нестандартные порты увеличивают риск утечки данных, взлома серверов и проникновения в сеть организации. Уязвимые сервисы могут быть использованы для удалённого доступа, внедрения вредоносного кода или включения серверов в ботнет.

34

Веб-ресурсов из 75 имеют критичные открытые порты

Открытые порты

80 443 110 143 22 53 21 25 554 3000
8000 106 465 587 993 995 8443 111 5666
8080 3306 8081 1025 1110 3389 5432 23 135
445 3128 1720 2000 5060 9100 179 81 514
1723 113

Рекомендации

Закрыть все критические порты в интернет-доступе.

Оставить только необходимые сервисы, например, HTTPS (443), DNS (53) и защищённую почту.

Если порт должен быть открыт – ограничить доступ по IP или VPN.

Веб-ресурсы, с наиболее защищенными портами

bishkek.gov.kg forest.gov.kg med.kg mfa.gov.kg minjust.gov.kg
agro.gov.kg e.srs.kg infocom.kg www.gov.kg zakupki.gov.kg
koomtalkuu.gov.kg digital.gov.kg data.gov.kg invest.gov.kg sot.kg
gosstroy.gov.kg zakupki.okmot.kg shailoo.gov.kg olympic.kg
main.teksher.kg railway.kg mammulk.gov.kg prokuror.kg cadastre.kg
sf.gov.kg

Software composition

Описание потенциальной атаки

Различные виды атак направленные основным образом на получение данных

Описание критерия

в данном разделе описана подверженность главной страницы веб-ресурса атакам и списка OWASP Top 10.

Негативные последствия

неправомерный доступ к данным.

30
интернет-ресурсов подвержены атакам OWASP Top 10

111
найдено CVE на 42 интернет-ресурсах

9 Количество уязвимых технологий

Apache, WordPress, PHP, Drupal, Bootstrap, Elementor, IIS, jQuery, Nginx

Наиболее часто встречающиеся CVE

CVE-2024-0660, CVE-2024-6526, CVE-2022-31630

Веб-сайты с лучшими результатами по CVE

antimonopolia.gov.kg, archive.kg, bishkek.gov.kg, cadastre.kg, e.srs.kg, edu.gov.kg, fiu.gov.kg, forest.gov.kg, gknb.gov.kg, gosstroy.gov.kg, kenesh.kg, med.kg, mfa.gov.kg, minenergo.gov.kg, minjust.gov.kg, mvd.gov.kg, nesk.kg, olympic.kg, portal.tunduk.kg, president.kg, prokuror.kg, railway.kg, salyk.kg, sf.gov.kg, shailoo.gov.kg, sti.gov.kg

Субдомены

Описание критерия

Анализ инфраструктуры государственных веб-ресурсов выявил 555 субдоменов, принадлежащих 75 государственным сайтам. Это говорит о разветвленной цифровой экосистеме, в которой различные сервисы и системы разнесены по отдельным поддоменам.

Субдомены используются для:

- Разделения функционала (например, portal.gov.kg, mail.gov.kg).
- Внутренних административных ресурсов (admin.example.gov.kg).
- Тестовых и архивных версий (test.example.gov.kg, old.example.gov.kg).
- API-сервисов и интеграций (api.example.gov.kg).

Большое количество субдоменов может представлять потенциальный риск, так как неактуальные, устаревшие или неправильно настроенные субдомены становятся уязвимыми для атак (например, Subdomain Takeover).

Тестовые субдомены часто плохо защищены и могут содержать конфиденциальные данные.

Субдомены могут указывать на старые версии ПО с известными уязвимостями.

22	11	11	20	555
Количество доменов **test.***.kg	Количество доменов **admin.***.kg	Количество доменов **dev.***.kg	Количество доменов **old.***.kg	Количество обнаруженных субдоменов

Веб-ресурсы, с лучшими результатами проверки субдоменов

meria.tokmokcity.kg, batken.gov.kg, www.gov.kg, portal.tunduk.kg, religion.gov.kg, sf.gov.kg, zakupki.okmot.kg, www.knu.kg, main.teksher.kg, minenergo.gov.kg, e.srs.kg, bishkek.gov.kg, naryn-raiadmin.gov.kg, ik.gov.kg, jalal-abad.gov.kg, talas.gov.kg, elicense.gov.kg, patent.gov.kg, nism.gov.kg, data.gov.kg, invest.gov.kg, nisi.kg, mineconom.gov.kg, stat.gov.kg, gosreg.gov.kg, cadastre.kg, mineconom.gov.kg, stat.gov.kg, gosreg.gov.kg, mineconom.gov.kg, gosreg.gov.kg, mineconom.gov.kg, gosreg.gov.kg, kca.gov.kg, mtd.gov.kg, gknb.gov.kg

HTTP Security заголовки

Описание критерия

Анализ HTTP-заголовков безопасности проводился с целью проверки их наличия и корректности настройки. при передачи данных от веб-сервера к клиенту, могут передаваться мета – данные, которые могут быть использованы при атаке. В процессе анализа проверялись такие заголовки как: Strict-Transport-Security, Content-Security-Policy, X-XSS-Protection, HTTP Strict Transport Security, X-Frame-Options, Expect-CT

Описание потенциальной атаки

При отсутствии или неправильной настройке HTTP-заголовков злоумышленники могут выполнить внедрение вредоносного кода (XSS), подменить контент, украсть пользовательские данные или использовать сайт в мошеннических схемах. Отсутствие Content Security Policy (CSP) позволяет загружать сторонние скрипты, а отсутствие X-Frame-Options делает сайт уязвимым для атак Clickjacking.

Негативные последствия

Компрометация пользовательских сессий, подмене контента, краже учетных данных и использованию веб-ресурса для атак на посетителей.

24 интернет ресурсов имеют низкие показатели по HTTP Security

Веб-ресурсы, с наилучшим показателями по Security Headers

- gknb.gov.kg
- antimonopolia.gov.kg
- gosstroy.gov.kg
- president.kg
- batken.gov.kg
- tulpar-card.kg
- esep.kg
- naryn-raiadmin.gov.kg
- tulpar-card.kg

Анализ DNS

Описание критерия

Проводился для выявления потенциальных уязвимостей, связанных с защитой домена, почтовых серверов и веб-приложений. Проверка включала конфигурацию DNSSEC, корректность записей CNAME, MX, безопасность электронной почты (SPF, DKIM, DMARC) и наличие Web Application Firewall (WAF). Также анализировалась доступность SMTP-портов, которые могут быть использованы для атак на почтовые сервисы.

Анализ 75 государственных интернет-ресурсов показал серьёзные недостатки в настройке DNS-безопасности, особенно в защите почтовых сервисов и механизмов предотвращения атак.

16
Доменов не настроили MX-записи, что делает невозможной официальную работу почтовых сервисов.

20
Доменов имеют слабые или отсутствующие SPF-записи, что позволяет злоумышленникам подделывать e-mail с этих доменов.

49
Доменов не используют DMARC, увеличивая вероятность фишинговых атак и мошенничества.

8
Доменов не имеют TXT-записей, что может указывать на нехватку базовой конфигурации безопасности.

Проблемы защиты веб-ресурсов:

Только 12 сайтов (16%) используют WAF, оставляя более 80% государственных сайтов без защиты от веб-атак.

Ни один сайт не использует DNSSEC, что делает все домены уязвимыми для атак подмены DNS (DNS Spoofing, Cache Poisoning).

Положительные аспекты:

Все 75 сайта настроили CAA-записи, что ограничивает выпуск SSL-сертификатов только доверенными центрами и предотвращает возможную компрометацию сертификатов.

Рекомендации

- Настроить SPF и DMARC на всех доменах для защиты от подделки e-mail.
- Включить WAF на всех критически важных веб-ресурсах
- Внедрить DNSSEC для предотвращения атак подмены DNS

Веб-ресурсы, с наилучшими показателями по сканированию DNS

fiu.gov.kg, gknb.gov.kg, sot.kg, railway.kg, shailoo.gov.kg, med.kg, nism.gov.kg, prokuror.kg, sti.gov.kg, customs.gov.kg, edu.gov.kg, infocom.kg, minfin.kg, salyk.kg, mvd.gov.kg, mfa.gov.kg, gik.kg, patent.gov.kg, kca.gov.kg, minculture.gov.kg, digital.gov.kg, ik.gov.kg, nisi.kg, mkk.gov.kg, mlsp.gov.kg, president.kg

Заключение

Результаты анализа защищенности веб-ресурсов Кыргызской Республики показали наличие тенденции к увеличению уровня информационной безопасности, однако в ряде веб-ресурсов были выявлены серьезные уязвимости, которые нуждаются в исправлении в кратчайшие сроки.

Основные уязвимости касаются неправильной настройки DNS, отсутствия базовой защиты от фишинга и спуфинга, наличия открытых портов и директорий, а также устаревших технологий с известными уязвимостями

Некоторые интернет-ресурсы находятся на минимальном уровне защищенности, несмотря на публичную значимость и потенциальные риски утечки данных или компрометации

Рекомендации

- Провести централизованный аудит и стандартизацию конфигураций
- Назначить ответственных за кибербезопасность в каждом ведомстве
- Исключить доступ к критически важным административным и резервным путям
- Обновить устаревшие компоненты веб-приложений и внедрить системы мониторинга уязвимостей.
- Обязать использование базовых мер защиты электронной почты (SPF, DKIM, DMARC).
- Внедрить систему регулярного автоматического сканирования и оценки уровня безопасности всех сайтов.

DIGITAL RESILIENCE ASSOCIATION

Контакты:

info@.....

site

телефон