CYBER RISKS SCORING OF BANKS IN KAZAKHSTAN

WEBTOTEM.AI

Введение

Основной задачей данного исследования было выяснить, как банки Казахстана обеспечивают безопасность своих веб-ресурсов. В качестве эталона были выбраны лучшие мировые практики и рекомендации признанных разработчиков ПО и мировых сообществ. Подобный анализ Центр анализа и расследования кибер атак (Далее - ЦАРКА) подготовила с помощью своего продукта WebTotem AI. Проверка проводилась 28-го февраля 2020 года, в рамках подготовки к CFO Summit Kazakhstan.

В рамках исследования специалисты ЦАРКА не вмешивались в работу интернет-ресурсов банков: для проводимых проверок было достаточно отправить “легкие” HTTP и DNS-запросы и проанализировать ответы, которые приходят от сервера. Таким образом, все данные были собраны так, как это мог бы сделать обычный пользователь, посетивший ресурс.

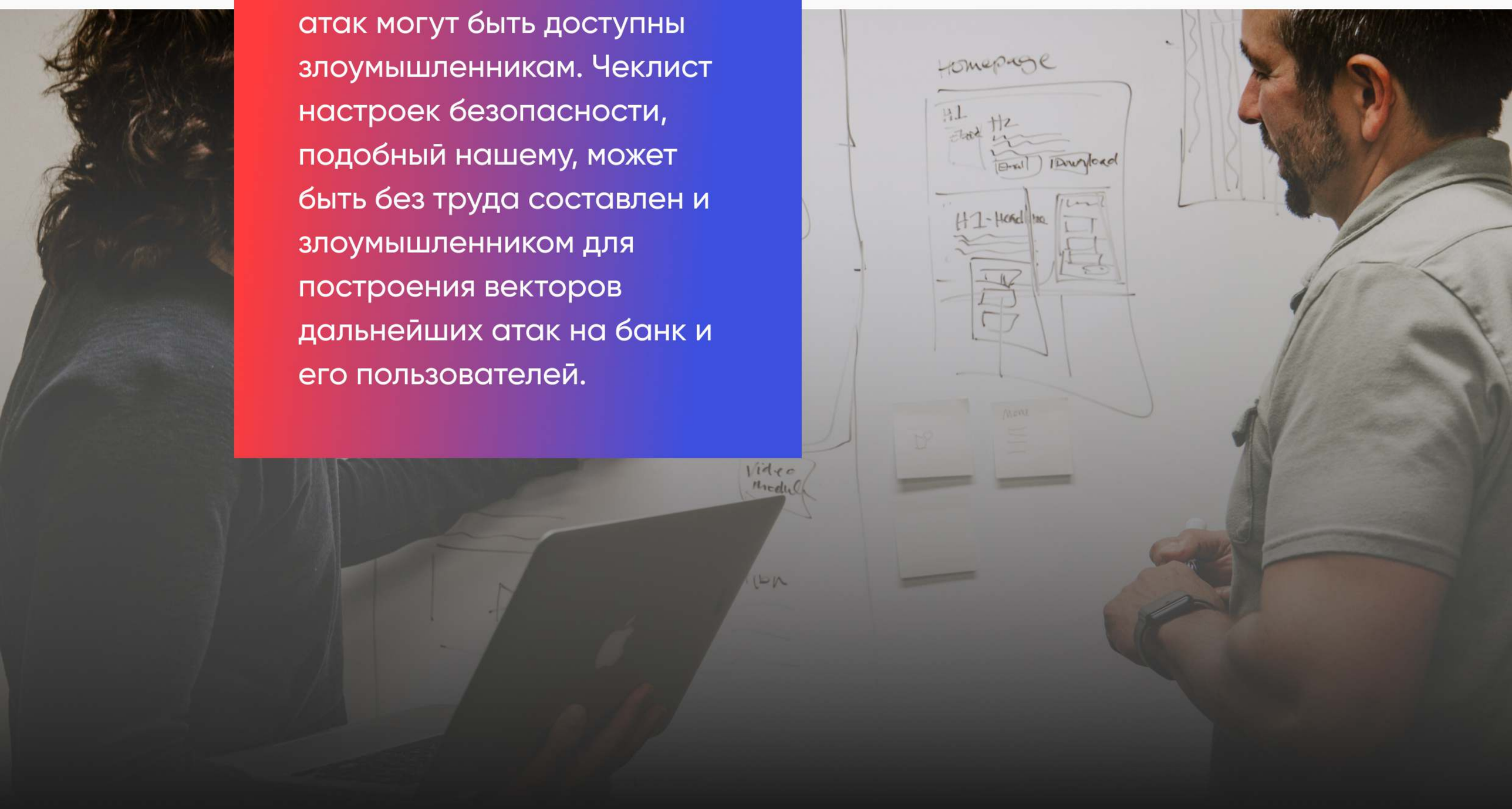
Данная работа не затрагивает атаки и уязвимости, защита от которых основана на фильтрации пользовательского ввода, а следовательно, не подразумевает проведение явных атак на ресурс. Она включает в себя анализ использования подходов по выполнению рекомендованных настроек для веб-серверов и связанных компонентов.

Мы надеемся, что приведенные в исследовании результаты помогут отделам информационной безопасности банков обратить внимание на недочеты, не позволяющие на сегодняшний день сказать, что уровень их защищенности полностью соответствует лучшим мировым практикам. Мы также рассчитываем, что этот анализ поспособствует проверке веб-ресурсов указанных банков внутренними службами и в дальнейшем они будут более ответственно подходить к их защите.

Цель исследования

Главной целью данного исследования является оценка уровня безопасности публично доступных банковских ресурсов (речь идет об официальном сайте банка) в соответствии с лучшими практиками **(GDPR ,OWASP Top-10, OWASP Application Security Verification Standard)**. Мы выбрали несколько пунктов, которые можно проверить, не вмешиваясь в работу веб-ресурса банка и исключая таким образом какой-либо технический ущерб. Важно отметить, что вся проанализированная нами информация находится в открытом доступе, и работа с ней не требует специальных навыков или недоступного обычному пользователю инструментария. Иными словами, мы хотели показать, что к подобным результатам может прийти любой заинтересованный пользователь с техническими навыками.

В ходе исследования мы попытались выяснить, какие потенциальные векторы атак могут быть доступны злоумышленникам. Чеклист настроек безопасности, подобный нашему, может быть без труда составлен и злоумышленником для построения векторов дальнейших атак на банк и его пользователей.



Объект исследования

Для исследования мы взяли все банки второго уровня Казахстана. С полным списком можно ознакомиться по ссылке: egov.kz/cms/ru/articles/banks

Каждая проверка проводилась для официального сайта.

- Kaspi Bank
- Национальный Банк Пакистана
- Сбербанк
- Банк ЦентрКредит
- Altyn Bank
- Народный Банк Казахстана
- АТФ Банк
- КЗИ Банк
- Bank RBK
- Альфа Банк
- Евразийский Банк
- Банк Kassa Nova
- Citi Bank
- Исламский Банк "Al Hilal"
- ЖСС Банк Казахстана
- AsiaCredit Bank
- Capital Bank Kazakhstan
- First Heartland Jýsan Bank
- Хоум Кредит
- Заман Банк
- Tengri Bank
- Fortebank
- НурБанк
- Банк Китая в Казахстане
- Шинхан Банк Казахстан
- ВТБ

Cyber Risks Scoring Rating for Banks of Kazakhstan

	Bank	Software compositions	Website performance	IP/ Domain reputation	HTTP Security Headers and Content Security Policy Scoring	Traffic encryption	Information leak	Network security	Email security	Current state	GDPR compliance	
#1	Kaspi Bank	✗	73%	✓	99/100	✓	✓	✓	91%	✓	✗	-12
#2	Altyn Bank	✗	76%	✓	80/100	✓	✓	✓	85%	✓	✗	-17
#3	Bank RBK	✗	80%	✓	75/100	✓	✓	✓	85%	✓	✗	-17
#4	Citi Bank	✗	66%	✓	27/100	✓	✓	✓	91%	✓	✗	-17
#5	Capital Bank Kazakhstan	✗	69%	✓	42/100	✓	✓	✓	91%	✓	✗	-17
#6	Tengri Bank	✗	66%	✓	58/100	✓	✓	✓	79%	✓	✗	-19
#7	Банк Китая в Казахстане	✗	94%	✓	47/100	✓	✓	21,25	78%	✓	✗	-20
#8	Национальный Банк Пакистана	✓	99%	✓	77/100	✗	✓	✓	78%	✓	✗	-22
#9	Народный Банк Казахстана	✓	84%	✓	100/100	✓	38	✓	86%	✓	✗	-25
#10	Альфа Банк	✗	73%	✓	88/100	✓	✓	5432	85%	✓	✗	-27
#11	Исламский Банк "Al Hilal"	✗	90%	✓	57/100	✓	✓	✓	67%	✓	✗	-27
#12	First Heartland Jýsan Bank	✗	77%	✓	70/100	✓	✓	21,25	60%	✓	✗	-29
#13	Fortebank	✗	79%	✓	52/100	✓	✓	25	53%	✓	✗	-29
#14	Шинхан Банк Казахстан	✗	91%	✓	50/100	✗	✓	✓	78%	✓	✗	-32
#15	Сбербанк	✗	63%	✓	51/100	✓	85	25	63%	✓	✗	-34
#16	АТФ Банк	✗	93%	✓	100/100	✓	155	✓	72%	✓	✗	-35
#17	Евразийский Банк	✗	44%	✓	64/100	✓	13	✓	91%	✓	✗	-37
#18	ЖСС Банк Казахстана	✗	69%	✓	46/100	✓	22	✓	91%	✓	✗	-37
#19	Хоум Кредит	✗	83%	✓	88/100	✓	20	25	66%	✓	✗	-45
#20	НурБанк	✗	71%	✓	67/100	✓	18	✓	41%	✓	✗	-49
#21	ВТБ	✗	82%	✓	32/100	✓	1	✓	66%	✓	✗	-50
#22	Банк ЦентрКредит	✗	27%	✓	74/100	✓	2	✓	67%	✓	✗	-52
#23	КЗИ Банк	✓	91%	✓	73/100	✗	6	✓	62%	✓	✗	-52
#24	Банк Kassa Nova	✗	75%	Forcepoint ThreatSeeker malicious site	51/100	✗	19	✓	91%	✓	✗	-59
#25	AsiaCredit Bank	✗	85%	✓	77/100	✗	3	25,21	61%	✓	✗	-62
#26	Заман Банк	✗	84%	✓	57/100	✗	4	25,21	56%	✓	✗	-62

В таблице выше представлена краткая информация, которую удалось выявить в результате анализа данных из открытых источников.

Software composition

В данном разделе описаны результаты, которые могут охарактеризовать риск эксплуатации веб-уязвимостей, таких как SQL Injection, Cross Site Scripting, Broken Authentication and Session Management, Insecure Direct Object References, Cross Site Request Forgery, Security Misconfiguration, Insecure Cryptographic Storage, Failure to restrict URL Access, Insufficient Transport Layer Protection, Unvalidated Redirects and Forwards. Подробнее можно ознакомиться по ссылке: https://www.owasp.org/

Факторы риска: Если не обновлена CMS или ее компоненты, то с высокой вероятностью существует эксплоит, который позволяет проэксплуатировать уязвимости старых версий.

Отсутствие обновлений означает:

1. Устаревшая версия, которая с высокой вероятностью уже не поддерживается разработчиком.
2. Версия подвержена потенциальным угрозам безопасности.

Из 26 доменов данный пункт проходят только 3 домена.

Kaspi Bank ✗	Национальный Банк Пакистана ✓	Сбербанк ✗	Банк ЦентрКредит ✗
Altyn Bank ✗	Народный Банк Казахстана ✓	АТФ Банк ✗	КЗИ Банк ✓
Bank RBK ✗	Альфа Банк ✗	Евразийский Банк ✗	Банк Kassa Nova ✗
Citi Bank ✗	Исламский Банк "Al Hilal" ✗	ЖСС Банк Казахстана ✗	AsiaCredit Bank ✗
Capital Bank Kazakhstan ✗	First Heartland Jýsan Bank ✗	Хоум Кредит ✗	Заман Банк ✗
Tengri Bank ✗	Fortebank ✗	НурБанк ✗	
Банк Китая в Казахстане ✗	Шинхан Банк Казахстан ✗	ВТБ ✗	

Website performance

Оценка скорости загрузки основана на данных FCP и FID, полученных методом имитации загрузки сайта. Тестирование наилучшей практики производительности выполняется для анализа устойчивости сайта к нагрузкам.

Факторы риска: Низкая производительность позволит злоумышленникам перегружать веб-ресурс, делая его недоступным для пользователей.

В целом у 46% доменов наблюдается высокая скорость загрузки, у следующих 46% – средняя, а у последних 8% – низкая.

Высокая скорость: 80-100% Средняя скорость: 50-79% Низкая скорость: 0-49%

Kaspi Bank	Национальный Банк Пакистана	Сбербанк	Банк ЦентрКредит
Altyn Bank	Народный Банк Казахстана	АТФ Банк	КЗИ Банк
Bank RBK	Альфа Банк	Евразийский Банк	Банк Kassa Nova
Citi Bank	Исламский Банк "Al Hilal"	ЖСС Банк Казахстана	AsiaCredit Bank
Capital Bank Kazakhstan	First Heartland Jýsan Bank	Хоум Кредит	Заман Банк
Tengri Bank	Fortebank	НурБанк	
Банк Китая в Казахстане	Шинхан Банк Казахстан	ВТБ	

IP - domain reputation

Хорошая репутация означает, что веб-ресурс безопасен, в то время как статус «черный список» антивирусов предупреждает посетителей о возможных угрозах безопасности.

Факторы риска: Если веб-ресурс занесен в черный список одной из баз репутации, он может быть заблокирован от посещения браузерами и даже может исчезнуть из результатов поисковых систем. Это в первую очередь приводит к потере трафика, доверия клиентов и, следовательно, денег.

Проверка репутации домена в различных базах антивирусных ПО.

В целом 96% сайтов считаются “чистыми”, только 4% (1 домен) был выявлен Forcepoint ThreatSeeker это может означать, попал в черный список этой системы как “потенциально вредоносный”.

Kaspi Bank	Национальный Банк Пакистана	Сбербанк	Банк ЦентрКредит
Altyn Bank	Народный Банк Казахстана	АТФ Банк	КЗИ Банк
Bank RBK	Альфа Банк	Евразийский Банк	Банк Kassa Nova
Citi Bank	Исламский Банк "Al Hilal"	ЖСС Банк Казахстана	AsiaCredit Bank
Capital Bank Kazakhstan	First Heartland Jýsan Bank	Хоум Кредит	Заман Банк
Tengri Bank	Fortebank	НурБанк	
Банк Китая в Казахстане	Шинхан Банк Казахстан	ВТБ	

HTTP Security Headers and Content Security Policy Scoring

Всякий раз, когда браузер запрашивает страницу с веб-сервера, сервер отвечает содержимым вместе с заголовками ответа HTTP . Некоторые из этих заголовков содержат мета - данные , такие как Content-Encoding, Cache-Control, коды статуса и т.д. Наряду с этим есть также заголовки безопасности HTTP, которые сообщают вашему браузеру, как вести себя при работе с контентом вашего сайта. Например, с помощью Strict-Transport-Security вы можете заставить браузер взаимодействовать исключительно по HTTPS. Ниже мы рассмотрим шесть различных заголовков безопасности HTTP (в произвольном порядке), о которых вам следует знать, и мы рекомендуем использовать их, если это возможно.

Content-Security-Policy (“Политика защиты контента”, CSP) - Заголовок обеспечивает дополнительный уровень безопасности. Эта политика помогает предотвратить такие атаки, как межсайтовый скриптинг (XSS) и другие атаки с использованием кода, путем определения утвержденных источников контента и, таким образом, позволяющих браузеру загружать их.

Все основные браузеры в настоящее время предлагают полную или частичную поддержку политики безопасности контента . И это не нарушит доставку контента, если он действительно будет доставлен в более старый браузер, он просто не будет выполнен.

X-XSS-Protection - Заголовок предназначен для включения фильтра межсайтового скриптинга (XSS filter), встроенного в современные веб-браузеры. Он останавливает загрузку страницы при обнаружении атаки (XSS). Обычно он включен по умолчанию, но использование данного заголовка активирует работу XSS-фильтра. Заголовок поддерживается веб-браузерами Internet Explorer 8+, Chrome и Safari.

HTTP Strict Transport Security (HSTS) - Заголовок Strict-Transport-Security представляет собой усиление безопасности, путем ограничения обращения веб-браузеров к веб-серверам только по протоколу HTTPS. Это гарантирует, что соединение не может быть установлено, используя небезопасное соединение HTTP, которое может быть подвержено атакам. На сегодняшний день большая часть популярных веб-браузеров, кроме Opera Mini и старых версий Internet Explorer, поддерживают HTTP Strict Transport Security.

X-Frame-Options - Заголовок обеспечивает защиту от атаки Clickjacking, запрещая загрузку плавающих фреймов (iframes) на вашем сайте. Поддерживается веб-браузерами Internet Explorer 8+, Chrome 4.1+, Firefox 3.6.9+, Opera 10.5+, Safari 4+.

Expect CT- Заголовок предотвращает использование ошибочно выданных сертификатов, позволяя веб-сайтам создавать отчеты и дополнительно обеспечивать соблюдение требований прозрачности сертификатов. Когда данный заголовок включен, веб-сайт отправляет браузеру запрос, проверить появляется ли сертификат в публичных логах CT.

X-Content-Type-Options - Заголовок X-Content-Type предлагает контрмеры против прослушивания MIME. Он инструктирует браузер следовать типам MIME, указанным в заголовке. Используемый как функция для обнаружения формата загружаемого файла, сниффинг MIME может также использоваться для выполнения атак с использованием межсайтовых сценариев.

Feature Policy - Заголовок предоставляет возможность разрешать или запрещать функции браузера, как в его собственном фрейме, так и в содержимом внутри встроенного фрейма (<iframe>).

HTTP Security Headers and Content Security Policy Scoring

Content-Security-Policy (“Политика защиты контента”, CSP) – это один из основных способов снижения рисков, возникающих при эксплуатации XSS-атак. С помощью CSP администратор сайта может определять атрибуты, разрешенные к использованию на страницах — шрифты, стили, изображения, скрипты JS, SWF и так далее.

Фактор риска: Недостаток в безопасности заголовков может привести к атакам, нацеленным на посетителей, таким как инъекция вредоносного кода, XSS и изменение контента веб- ресурса на вредоносный.

В целом у **23%** доменов наблюдается высокая оценка, у следующих **58%** – средняя, а у последних **19%** – низкая.

Score :	0-49	50-79	80-100

Kaspi Bank 99	Национальный Банк Пакистана 77	Сбербанк 51	Банк ЦентрКредит 74
Altyn Bank 80	Народный Банк Казахстана 100	АТФ Банк 100	КЗИ Банк 73
Bank RBK 75	Альфа Банк 88	Евразийский Банк 64	Банк Kassa Nova 51
Citi Bank 27	Исламский Банк "Al Hilal" 57	ЖСС Банк Казахстана 46	AsiaCredit Bank 77
Capital Bank Kazakhstan 42	First Heartland Jýsan Bank 70	Хоум Кредит 88	Заман Банк 57
Tengri Bank 58	Fortebank 52	НурБанк 67	
Банк Китая в Казахстане 47	Шинхан Банк Казахстан 50	ВТБ 32	

Traffic encryption

Одной из самых важных является проверка настроек SSL/TLS, поскольку сегодня эти криптографические протоколы являются самым популярным методом обеспечения защищенного обмена данными через Интернет. В 2019 году создатели браузеров FireFox, Safari, Edge и Chrome сообщили, что в 2020 году, начиная с марта месяца, браузеры перестанут поддерживать TLS 1.0 и 1.1. Рекомендуется перейти на TLS 1.2, а еще лучше TLS 1.3, иначе браузеры будут отображать ошибку.

Факторы риска: Перехват данных — это только один из нескольких различных видов атак, объединенных под общим названием «человек посередине». Каждая атака типа «человек посередине» или MITM, подразумевает наличие посредника (человека или устройства), который имеет возможность перехватывать и модифицировать данные, пересылаемые между двумя абонентами системы связи, которые, как правило, даже не подозревают о вмешательстве злоумышленников в обмен информацией между ними.

Суть атаки заключается в том, что злоумышленник «пропускает» веб-трафик жертвы (возможно, путем изменения параметров DNS-сервера или файла hosts на машине жертвы) «через себя». В то время пока жертва считает, что обращается напрямую к веб-сайту своего банка, трафик проходит через промежуточный узел злоумышленника, который таким образом получает все отправляемые пользователем данные (логин, пароль, ПИН-код и т. п.).

Traffic encryption

Мы выбрали следующие проверки SSL/TLS:

Заголовок	Описание
Рейтинг	Общий рейтинг настройки SSL, согласно ресурсу SSL Labs. Он зависит от многих факторов: корректности сертификата, настройки сервера, поддерживаемых сервером алгоритмов и др. Градация от A+ до F.
Поддержка слабых параметров алгоритма Диффи – Хеллмана	Для обмена ключами по протоколу Диффи – Хеллмана могут быть использованы слабые параметры, что снижает безопасность ресурса.
Уязвимость POODLE	Позволяет расшифровать данные пользователя.
Уязвимость FREAK	Злоумышленник может заставить пользователя и сервер при установлении соединения и обмена данными применять “экспортные” ключи, длина которых сильно ограничена.
Подверженность атаке Logjam	Как и FREAK, Logjam основана на понижении уровня шифрования до экспортного уровня, где длина ключа составляет 512 бит. Отличие состоит в том, что Logjam атакует алгоритм Диффи – Хеллмана.
Уязвимость DROWN	Позволяет дешифровать TLS-трафик клиента, если на серверной стороне не отключена поддержка протокола SSL 2.0 во всех серверах, оперирующих одним и тем же приватным ключом.
Уязвимость ROBOT	Полностью нарушает конфиденциальность TLS при использовании RSA для получения сессионного ключа.
Уязвимость Beast	Злоумышленник может расшифровать данные, которыми обмениваются две стороны, использующие TLS 1.0, SSL 3.0 и ниже.
Уязвимость CVE-2016-2107	Удаленный злоумышленник может использовать эту уязвимость для извлечения текста из зашифрованных пакетов, используя технику Padding Oracle.
Уязвимость Heartbleed	Получение доступа к данным, которые хранятся в памяти клиента или сервера.
Уязвимость Ticketbleed	Удаленный злоумышленник может извлекать фрагменты содержимого памяти сервера посредством поля Session ID протокола TLS.
SSL Renegotiation	Безопасное пересогласование SSL позволяет уменьшить риск DoS или MITM-атаки.
Поддержка RC4	Исследователи обнаружили, что можно за короткое время расшифровать данные, которые были скрыты при помощи шифра RC4.
Поддержка Forward Secrecy	Свойство определенных протоколов согласования ключей, которое гарантирует, что сеансовые ключи не будут скомпрометированы, даже если скомпрометирован закрытый ключ сервера.
Версия TLS	Протокол TLS шифрует интернет-трафик всех видов, делая безопасным обмен данными в интернете.
Поддержка SSL 2.0 и SSL 3.0	Оба протокола считаются устаревшими и имеют множество уязвимостей, поэтому рекомендуются к отключению на стороне сервера.
Поддержка NPN и ALPN	Позволяет указать, какой протокол использовать после установления безопасного соединения SSL/TLS между клиентом и сервером.

Traffic encryption

Список банков, где были выявлены проблемы с SSL/TLS:

Kaspi Bank ✓	Национальный Банк Пакистана ✗	Сбербанк ✓	Банк ЦентрКредит
Altyn Bank ✓	Народный Банк Казахстана ✓	АТФ Банк ✓	КЗИ Банк ✗
Bank RBK ✓	Альфа Банк ✓	Евразийский Банк ✓	Банк Kassa Nova ✗
Citi Bank ✓	Исламский Банк "Al Hilal" ✓	ЖСС Банк Казахстана ✓	AsiaCredit Bank ✗
Capital Bank Kazakhstan ✓	First Heartland Jýsan Bank ✓	Хоум Кредит ✓	Заман Банк ✗
Tengri Bank ✓	Fortebank ✓	НурБанк ✓	
Банк Китая в Казахстане ✓	Шинхан Банк Казахстан ✗	ВТБ ✓	

Information leak

Любая утечка информации несет в себе те или иные негативные экономические и репутационные последствия для компании.
Так как сотрудники банков могут использовать корпоративные e-mail-адреса для регистрации на различных сервисах, в результате взлома данных сервисов адреса электронной почты, пароли и иная персональная информация утекают в сеть. Злоумышленники могут воспользоваться чувствительной информацией для осуществления атаки на информационные системы Банка, так как зачастую, в 90% случаев пароли учетных записей пользователей на различных сервисах совпадают. Получив доступ к корпоративной почте, злоумышленник получает доступ к рабочей переписке и переданным по e-mail рабочим документам, что в свою очередь несет в себе репутационную и финансовую угрозу для Банка.

Список банков, где были выявлены утечки информации:

Kaspi Bank ✓	Национальный Банк Пакистана ✓	Сбербанк 85	Банк ЦентрКредит 2
Altyn Bank ✓	Народный Банк Казахстана 38	АТФ Банк 155	КЗИ Банк 6
Bank RBK ✓	Альфа Банк ✓	Евразийский Банк 13	Банк Kassa Nova 19
Citi Bank ✓	Исламский Банк "Al Hilal" ✓	ЖСС Банк Казахстана 22	AsiaCredit Bank 3
Capital Bank Kazakhstan ✓	First Heartland Jýsan Bank ✓	Хоум Кредит 20	Заман Банк 4
Tengri Bank ✓	Fortebank ✓	НурБанк 18	
Банк Китая в Казахстане ✓	Шинхан Банк Казахстан ✓	ВТБ 1	

Всего найдено
386 утечек

Network security

Был проведен анализ портов, которые не используются напрямую самим веб-сервером (**порты 80 и 443**). Отметим, что просто наличие открытых портов не является уязвимостью, однако с точки зрения лучших практик безопасности, веб-сервер не должен иметь открытых портов кроме тех, которые подразумевают работу с веб-сервисами.

Список банков с открытыми портами:

Kaspi Bank ✓	Национальный Банк Пакистана ✓	Сбербанк 25	Банк ЦентрКредит ✓
Altyn Bank ✓	Народный Банк Казахстана ✓	АТФ Банк ✓	КЗИ Банк ✓
Bank RBK ✓	Альфа Банк 5432	Евразийский Банк ✓	Банк Kassa Nova ✓
Citi Bank ✓	Исламский Банк "Al Hilal" ✓	ЖСС Банк Казахстана ✓	AsiaCredit Bank 25,21
Capital Bank Kazakhstan ✓	First Heartland Jýsan Bank 21,25	Хоум Кредит 25	Заман Банк 25,21
Tengri Bank ✓	Fortebank 25	НурБанк ✓	
Банк Китая в Казахстане 21,25	Шинхан Банк Казахстан ✓	ВТБ ✓	

Email security

Более 90% почтового трафика содержит спам, фишинг, вредоносные программы и другие электронные угрозы. Электронная почта является основным вектором заражения для вымогателей и вредоносных программ. Данный пункт проверяет, правильно ли настроен почтовый сервер веб-ресурса для предотвращения этих распространенных угроз.

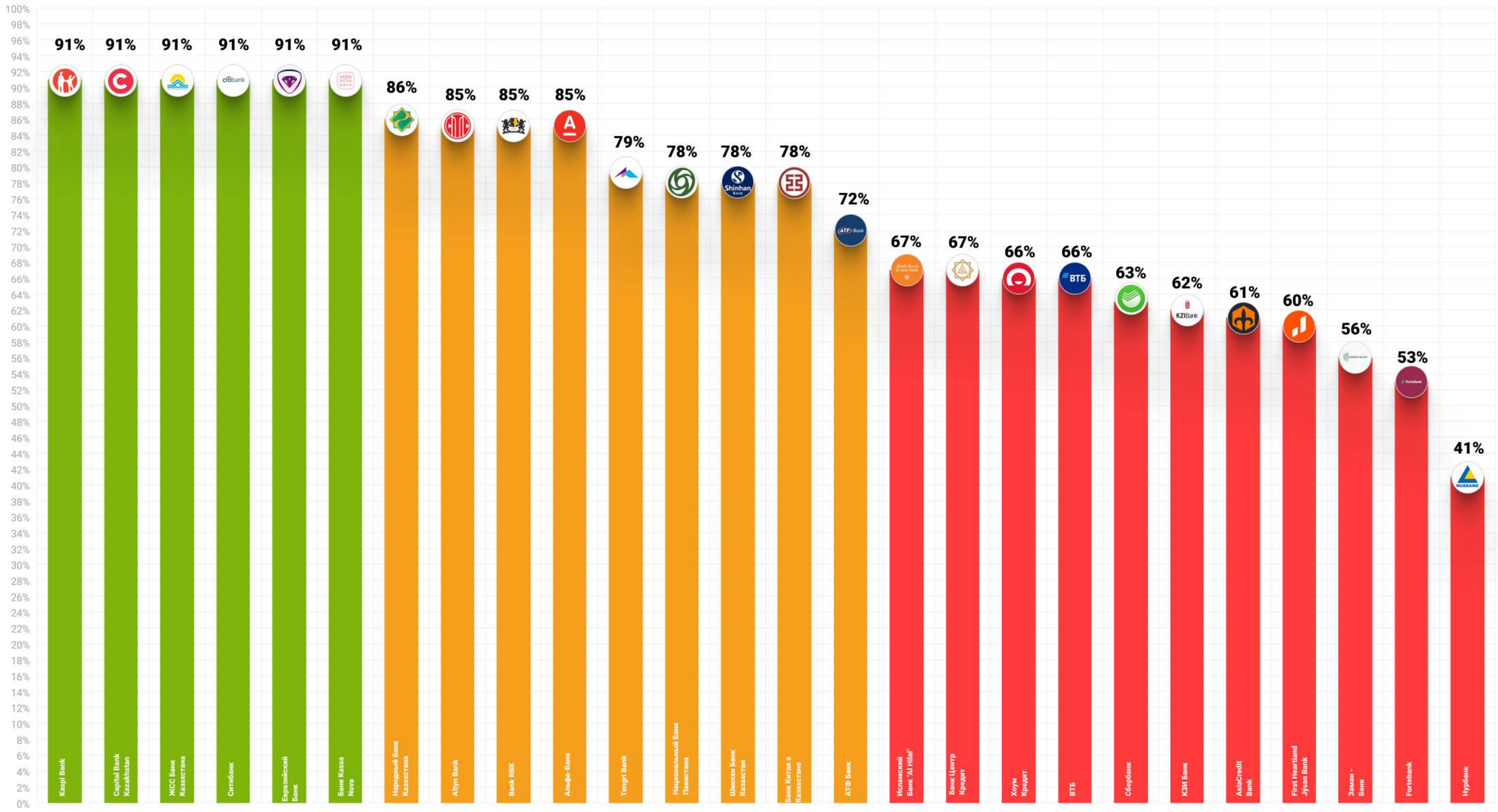
Мы выбрали следующие проверки Email security:

Название проверки	Описание
MX Connection Test	Если порт 25 заблокирован от внешнего доступа на самом сервере MX, сервер не сможет получать входящие сообщения (сервера-отправители никогда не будут искать альтернативный порт). Порт должен быть хотя бы доступен через прокси-сервер или маршрутизатор. Если 3 порта открыты (25, 465 и 587). Ваша система требует аутентификации (AUTH) на порту 587, прежде чем будет выдана команда MAIL FROM если соединение с портом 25 или 465 не удастся, оценка снижается.
Reverse DNS Test	Многие почтовые серверы проводят обратный поиск для проверки подлинности домена отправителя. Если тест не пройден, связь с сервером-отправителем может быть заблокирована. Различные службы репутации могут также дать вашей системе более низкий балл, если обратная запись отсутствует. Чтобы правильно отправлять и получать электронную почту, действующий домен должен иметь в DNS соответствующую MX-запись, которая содержит 3 части информации: доменное имя, имя хоста (например, servername.domain.com) и IP. Запрос имени хоста для преобразования адреса в его IP называется прямым поиском. Обратный поиск — это обратный процесс: преобразование IP в его имя хоста. Многие почтовые серверы проводят обратный поиск для проверки подлинности домена отправителя. В случае неудачи теста связь с сервером отправителя может быть заблокирована. Различные службы репутации также могут дать вашей системе более низкий балл, если обратная запись отсутствует.
DNSBL Verification Test	Если какой-либо IP, принадлежащий вашей сети, занесен в черный список, почтовые серверы, которые подписываются на DNSBL, блокируют связь с вашим сервером. Черный список на основе DNS проверяет IP-адреса, связанные с рассылкой спама и другими вредоносными программами.
SPF Server Test	Сегодня почти все оскорбительные сообщения в электронной почте содержат поддельные адреса отправителей. Жертвы, адреса которых подвергаются насилию, часто страдают от последствий, потому что их репутация снижается, и им приходится снимать с себя ответственность за злоупотребления или тратить свое время на сортировку ошибочно перенаправленных сообщений о сбое (Источник: OpenSpf.org). Этот тест проверяет, подтверждаете ли вы свои местные адреса отправителей. Обычная практика рассылки спама включает в себя спуфинг (подделку) адреса электронной почты, используемого в поле FROM. Sender Policy Framework (SPF) — это метод, используемый для предотвращения такого типа подделки: вы создаете SPF запись на вашем DNS сервере для указания и ограничения того, каким адресам хостов разрешено отправлять электронную почту, используя ваше доменное имя.
SPF Client Test	Если ваш сервер не поддерживает проверку SPF, возникающие проблемы могут быть двоякими: 1) Вы рискуете принимать и обрабатывать большее количество спама, что увеличивает нагрузку на системные ресурсы. 2) Вы рискуете обрабатывать большее количество недопустимых сбоев и отказов доставки, известных как обратное рассеяние.

Email security

Название проверки	Описание
Open Relay and Email Format Test	Если сервер разрешает отправку сообщений на нелокальные адреса (не прошедшими проверку подлинности отправителями или не доверенными IP-адресами), он считается открытым ретранслятором. Таким образом, сервер может быть использован спамерами и, следовательно, занесен в черный список.
SMTP Plain Text Authentication Test	Спамеры могут взломать учетные записи пользователей, собирая пароли, которые передаются на сервер в виде открытого текста с помощью механизмов PLAIN или AUTH LOGIN. Этот тест пытается подключиться к почтовому серверу через порты 25 и 465. Для каждого подключения он проверяет список доступных методов аутентификации. Сервер получит наименьшее количество баллов, если на порту 25 поддерживаются PLAIN или AUTH LOGIN. Наибольший балл присуждается, если включен протокол SMTP SSL, а механизмы PLAIN и AUTH LOGIN на порте 25 недоступны. Обратите внимание, что если AUTH не поддерживается, ваш MX проходит тест поскольку пароли в виде простого текста не могут быть прослушаны.
POP3 Connection Test	Если в соединении POP3 используется стандартный порт 110, соединение небезопасно и может быть взломано, что может привести к потере сообщений и конфиденциальности. Проверяет какой порт использует POP3. Если POP3-соединение использует стандартный порт 110, соединение не является безопасным и может быть нарушено, что приводит к потенциальной потере сообщений и конфиденциальности.
IMAP Connection and Authentication Test	IMAP изначально поддерживает зашифрованные механизмы входа в систему, но эту защиту можно обойти, если используется вход в систему в виде простого текста через порт 143. Поэтому содержание сообщения уязвимо для воздействия и потери конфиденциальности. Проверяет порт используемый для IMAP. Стандартный ненадежный порт для IMAP-соединений - 143. Защищенный, зашифрованный порт - 993.

Сводная таблица



Current state

Осуществляет проверку на предмет взлома ресурса, по внешним признакам:

- Наличие на сайте вредоносных скриптов
- Наличие на сайте скрытых сетевых майнеров - криптоджекинг
- Проверка скорости работы сайта
- Жалобы от пользователей на наличие вирусов на сайте, которые обнаружило их антивирусное ПО
- Внесение сайта в «черный список» репутационных баз поисковых систем

Факторы риска: Сетевой криптоджекинг (также известный, как крипто-майнинг) наиболее распространенная форма крипто-майнинговых вредоносных программ. Как правило, это вредоносное действие выполняется с помощью скриптов, запущенных на веб-сайте, что позволяет браузеру жертвы автоматически майнить криптовалюту во время посещения. Такие сетевые майнеры скрыто реализуются на разных веб-сайтах, независимо от их популярности или категории.

Kaspi Bank ✓	Национальный Банк Пакистана ✓	Сбербанк ✓	Банк ЦентрКредит ✓
Altyn Bank ✓	Народный Банк Казахстана ✓	АТФ Банк ✓	КЗИ Банк ✓
Bank RBK ✓	Альфа Банк ✓	Евразийский Банк ✓	Банк Kassa Nova ✓
Citi Bank ✓	Исламский Банк "Al Hilal" ✓	ЖСС Банк Казахстана ✓	AsiaCredit Bank ✓
Capital Bank Kazakhstan ✓	First Heartland Jýsan Bank ✓	Хоум Кредит ✓	Заман Банк ✓
Tengri Bank ✓	Fortebank ✓	НурБанк ✓	
Банк Китая в Казахстане ✓	Шинхан Банк Казахстан ✓	ВТБ ✓	

GDPR compliance

Персональные данные должны обрабатываться таким образом, чтобы обеспечить им надлежащую безопасность, включая защиту от несанкционированной или незаконной обработки и от случайной потери, уничтожения или повреждения, с использованием соответствующих технических или организационных мер (« целостность и конфиденциальность »).

Факторы риска: Согласно требованиям GDPR (General Data Protection Regulation) и Директивы о конфиденциальности и электронных средствах связи (ePrivacy Directive) веб-сайты обязаны предоставлять пользователям информацию о том, как обрабатываются их персональные данные, файлы cookie и как выполняется передача пользовательских данных. Файлы cookie могут хранить множество данных достаточных для идентификации пользователя без его ведома и согласия. В большинстве случаев пользователи веб-сайта должны согласиться с правилами хранения и обработки их персональных данных.

Список банков, где были выявлены проблемы GDPR:

- Kaspi Bank
- Национальный Банк Пакистана
- Сбербанк
- Банк ЦентрКредит
- Altyn Bank
- Народный Банк Казахстана
- АТФ Банк
- КЗИ Банк
- Bank RBK
- Альфа Банк
- Евразийский Банк
- Банк Kassa Nova
- Citi Bank
- Исламский Банк "Al Hilal"
- ЖСС Банк Казахстана
- AsiaCredit Bank
- Capital Bank Kazakhstan
- First Heartland Jýsan Bank
- Хоум Кредит
- Заман Банк
- Tengri Bank
- Fortebank
- НурБанк
- Банк Китая в Казахстане
- Шинхан Банк Казахстан
- ВТБ

Заключение

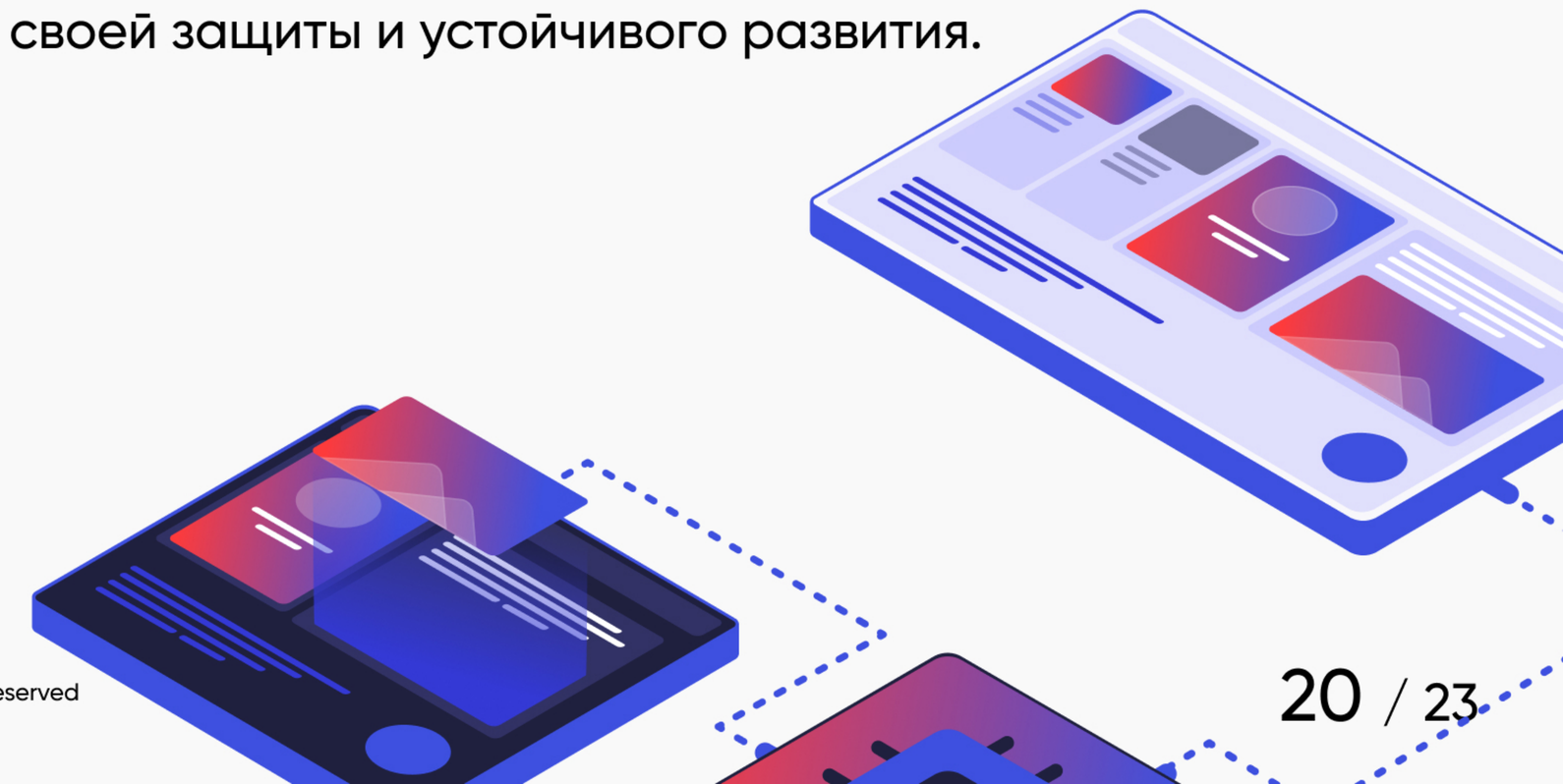
В процессе исследования безопасности веб-ресурсов банков в Казахстане, мы собрали статистику выполнения общедоступных рекомендаций по настройке веб-серверов и взаимосвязанных компонентов.

Получив общее представление о защищенности веб-ресурсов банков, мы пришли к главному выводу: многие банки пренебрегают даже самыми распространенными и простыми в реализации советами по повышению безопасности своих веб-ресурсов.

Рассмотрев веб-ресурсы казахстанских банков с разных сторон, мы выяснили, что достаточно известные уязвимости и проблемы безопасности до сих пор присутствуют на них. Данный факт позволяет злоумышленникам рассчитывать на успешную реализацию атак на эти финансовые организации.

Проведенное исследование продуктом WebTotem AI указало на ряд слабых и уязвимых мест казахстанских банков, которые при кажущейся только на первый взгляд малозначимости и трудности в реализации злоумышленниками, могут в дальнейшем привести к существенным денежным потерям и даже необратимому репутационному краху.

В настоящее время, в эпоху скоростного обмена информации, быстро меняющимся цифровом мире сознание пользователей информационных услуг растет ежедневно, и все больше приоритетом при выборе выступает гарантия в обеспечении конфиденциальности и целостности своих данных.
Хорошая новость в том, что у банков сегодня есть все шансы и готовые инструменты для налаживания системы управления информационной безопасности, внедрению своевременных мероприятий и целесообразных продуктов для обеспечения своей защиты и устойчивого развития.



О компании

WebTotem - это инструмент для мониторинга безопасности веб-сайтов, защищающий компании от вторжений и постоянно развивающихся киберугроз.

Клиент **WebTotem** может:

• Предотвращать взломы с помощью пошаговых рекомендаций по обеспечению безопасности
• Получать проактивную защиту от новых киберугроз
• Оценивать и управлять рисками кибербезопасности

Кибербезопасность все еще стоит дорого, и достаточно сложно найти инженера безопасности в штат компании. Миссия **WebTotem** заключается в том, чтобы донести революционный продукт, построенный на основе искусственного интеллекта, до людей из нетехнической сферы, чтобы они имели возможность защитить свой бизнес в один клик.

Мы поднимаем стандарты в области безопасности бизнес-сайтов по всему миру.

В рамках реализации концепции «Киберщит Казахстана», Система **WebTotem** уже второй год используется Министерством цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан для осуществления мониторинга и защиты всей доменной зоны .kz, что составляет около 160 000 доменов.

С 2019 года, по запросу заинтересованных организаций в Польше, WebTotem осуществляет мониторинг 1 148 036 сайтов доменной зоны .pl.

WebTotem признан лучшим SaaS решением для бизнеса (B2B, SaaS and Enterprise Solutions) на Echelon Asia Summit 2018 в Сингапуре. Также WebTotem является региональным **победителем** Seedstars Kazakhstan.

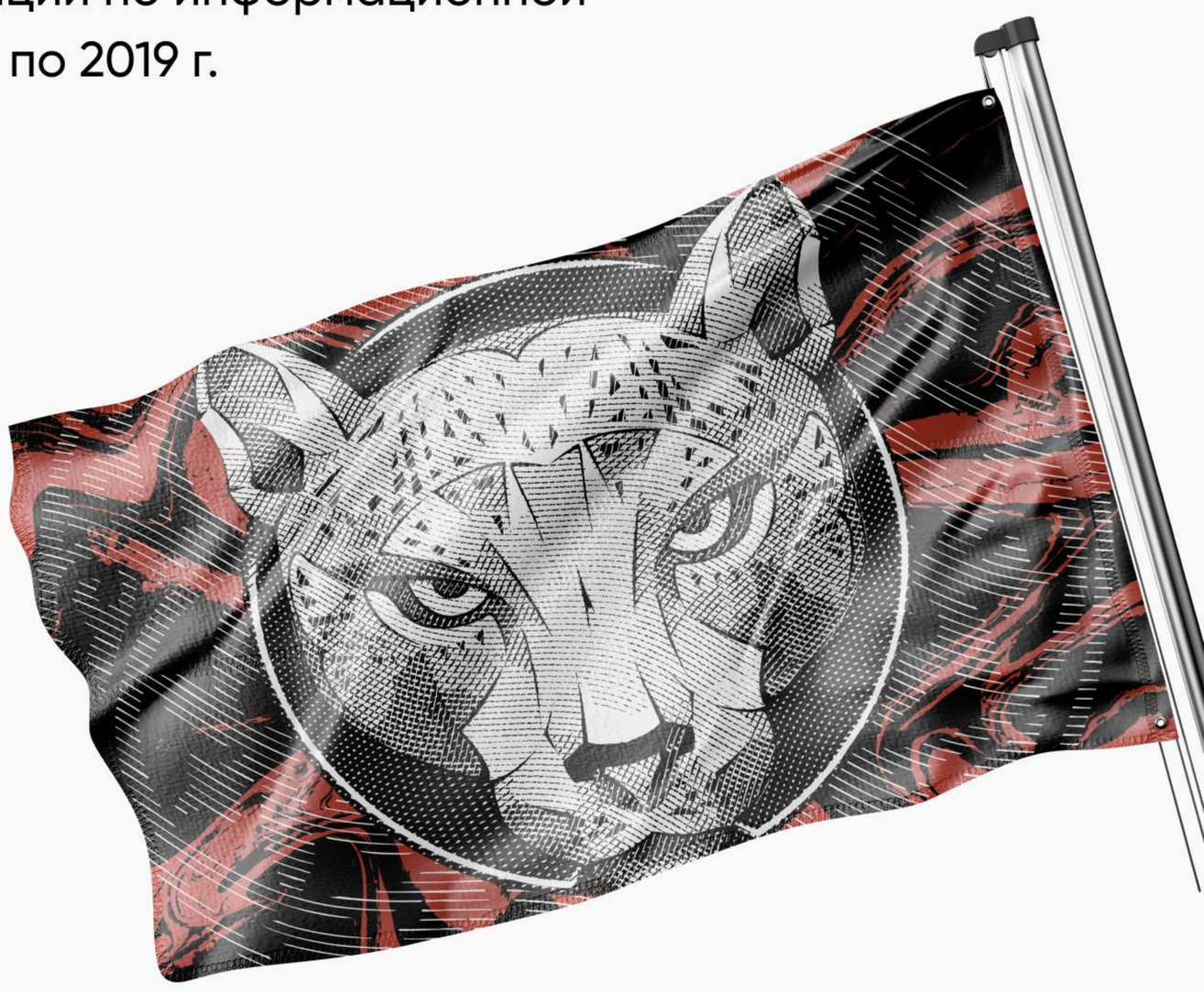
В 2019 году **WebTotem** был выбран для прохождения программы CyberNorth в лучшем европейском акселлераторе StartupWiseGuys в Эстонии и бизнес программы GIST (Global Innovation through Science and Technology) при поддержке правительства США.

О компании

ЦАРКА – одна из ведущих организаций в области информационной безопасности в Центральной Азии. Организация была образована в 2015 году и за время своего существования завоевала признание специалистов по информационной безопасности по всему миру. Первый частный CERT в Казахстане.

Организация предоставляет широкий спектр услуг в области оценки защищенности, в том числе проведение аудитов ИБ и тестирований на проникновение, анализ защищенности банковских систем и бизнес приложений, веб приложений, информационных инфраструктур.

Более 50 экспертов. Эксперты **ЦАРКА** обладают сертификатами OSCP, OSWP, CHFI, CISA, CCNA Security, ISO/IEC 27001-2015, OSCE и CEH и регулярно принимают участие в международных конференциях, таких как PHDays, ZeroNights, Инфофорум, КодИБ. Эксперты организации являются авторами публикаций на таких ресурсах как журнал Xakep, HabraHabr, DigitalReport, ProfIT.kz и др.
Команда **ЦАРКА** занимала 1 и 2 места в соревновании The Standoff на международной конференции по информационной безопасности PositiveHackDays с 2017 по 2019 г.



Контакты

info@wtotem.com

г.Нур-Султан, проспект Мангилик ел 19/2, 93кв