Deloitte.

Оценка киберрисков в банках Казахстана

Июнь 2021 года

MAKING AN IMPACT THAT MATTERS
Since 1845

Введение

Компания «Делойт» в Казахстане при поддержке Агентства Республики Казахстан по регулированию и развитию финансового рынка провела свое первое комплексное исследование в области кибербезопасности, в ходе которого были проанализированы веб-ресурсы и мобильные приложения 24 казахстанских банков. В процессе работы мы использовали набор открытых онлайн-инструментов, таких как Google, Barracuda, Trusted Source, Haveibeenpwned и другие. Целью исследования было изучение различных аспектов обеспечения кибербезопасности банков, которые для удобства работы с ними мы разделили на десять направлений:

1. Доступность сайтов
2. Репутация домена
3. Заголовки HTTP
4. Защита трафика
5. Утечки адресов электронной почты
6. Открытые порты
7. Кибersквоттинг
8. Выполнение требований по защите персональных данных
9. Безопасность почтового сервера
10. Безопасность мобильного банкинга

Команда «Делойта» по кибербезопасности проверила и проанализировала данные, полученные по каждому направлению. Все наши наблюдения включены в отчет и сопровождаются кратким описанием и объяснением связанных с ними киберрисков. По каждому направлению составлены соответствующие заключения, в которых содержатся рекомендации по минимизации выявленных рисков.
Мы планируем проводить подобные обзоры на регулярной основе, чтобы определить, будут ли банки в будущем предпринимать меры и повышать безопасность своих веб-ресурсов и мобильных приложений.
Надеемся, что вы найдете настоящий отчет полезным. Если у вас возникли комментарии или вопросы по содержанию нашего отчета, вы всегда можете связаться с нами.

С наилучшими пожеланиями,

Владимир Ремыга
Директор Департамента управления рисками

Владимир Ремыга

Директор

Департамент управления рисками

Тел.: +994 12404 1210
Моб.: +994 51206 0123
+7 700 714 5505
vremyga@deloitte.com

1. Доступность сайтов
2. Репутация домена
3. Безопасность HTTP
4. Защита трафика
5. Утечки адресов электронной почты
6. Открытые порты
7. Кибersквоттинг
8. Выполнение требований по защите персональных данных
9. Безопасность почтового сервера
10. Безопасность мобильного банкинга

Резюме

Сегодня большинство руководителей банковского сектора Казахстана инвестируют значительные средства и ресурсы в цифровизацию финансовых услуг, считая этот процесс частью долгосрочной стратегии. Это означает, что все больше новых технологий интегрируются в нашу повседневную жизнь. Мобильный и интернет-банкинг, оплата по QR-коду, быстрые переводы, платежи и другие инструменты стали обыденным явлением в Казахстане.

Тем не менее наше исследование показало, что когда дело касается защиты и безопасности веб-серверов и мобильных приложений, далеко не все лидеры в области кибербезопасности в банковской сфере уделяют достаточно внимания этим весьма важным и актуальным вопросам. Так, многие банки пренебрегают базовыми рекомендациями по обеспечению безопасности при настройке своих веб-серверов. В результате даже не используя специализированное программное обеспечение, мы выявили серьезные недостатки в системах безопасности ряда банков. Более того, многие из этих проблем не являются чем-то новым либо уязвимостями нулевого дня. Наоборот, это давние и хорошо известные проблемы в области кибербезопасности. Часть выявленных недостатков может показаться незначительной. Однако следует напомнить, что в этой области нет «маленьких» уязвимостей. Любая из них может привести к более серьезным проблемам и стать в итоге причиной утечки конфиденциальных данных или прямого хищения средств.

В то же время в своей практике мы сталкивались с такой проблемой, как недостаточная осведомленность сотрудников банков в вопросах цифровой безопасности. Это показатель слабости существующих политик в области кибербезопасности и программ повышения осведомленности сотрудников в отношении защиты информационных активов. Фактически одно необдуманное действие сотрудника может поставить под угрозу данные всего банка и его клиентов.

Проблему усугубил кризис, вызванный эпидемией COVID-19, который оказал чрезвычайное экономическое давление на многие организации, в том числе на финансовые институты. Теперь им приходится приспосабливаться к «новой норме». В связи с тем, что значительное количество сотрудников по-прежнему работает из дома, руководители банков вынуждены любой ценой поддерживать их работоспособность. Однако если вопросу обеспечения кибербезопасности не будет уделено достаточного внимания в их тактических и стратегических планах, в краткосрочной перспективе такие банки могут оказаться скомпрометированными.

Участникам финансового рынка Казахстана необходимо принять реальность: кибербезопасность охватывает все аспекты бизнеса и общества. Ее необходимо рассматривать как связующую нить, способную объединить организацию, ее клиентов, поставщиков и профессиональные сообщества, и интегрировать во все аспекты деятельности и управленческие решения, которые руководство банков принимает каждый день.

1. Доступность сайтов
2. Репутация домена
3. Безопасность HTTP
4. Защита трафика
5. Утечки адресов электронной почты
6. Открытые порты
7. Киберсквоттинг
8. Выполнение требований по защите персональных данных
9. Безопасность почтового сервера
10. Безопасность мобильного банкинга

О «Делойте»

Как признанный лидер по консультированию в сфере кибербезопасности, «Делойт» помогает своим клиентам лучше согласовать стратегии и инвестиции в отношении киберрисков со стратегическими бизнес-приоритетами, повысить осведомленность об угрозах и прозрачности, а также укрепить способность компаний успешно справляться с киберинцидентами.

Используя экспертные знания, технологические инновации и комплексные цифровые решения, мы руководствуемся принципом - кибербезопасностью должна быть повсюду. Для этого наш портфель услуг в области кибербезопасности включает:

Стратегия кибербезопасности

Мы помогаем руководителям разработать программу киберрисков в соответствии со стратегическими целями и ее аппетитом к киберрискам.

- Киберстратегия, трансформация и оценка
- Управление киберрисками и соответствие нормативным требованиям
- Обучение, образование и повышение осведомленности в области кибербезопасности

Защита

Мы фокусируемся на создании эффективного контроля над наиболее чувствительными активами организации и баланса между необходимостью снижения риска, обеспечения производительности, ростом бизнеса и оптимизации затрат.

- Защита объектов инфраструктуры
- Управление уязвимостями
- Защита приложений
- Управление идентификацией и доступом
- Конфиденциальность и защита информации

Бдительность

Мы объединяем данные об угрозах, ИТ и бизнесе, чтобы снабдить команды безопасности интеллектуальными данными с богатым контекстом для выявления, предупреждения киберугроз и эффективного реагирования на инциденты.

- Подготовка к современным угрозам
- Аналитика киберрисков
- Операционный центр безопасности
- Киберразведка и анализ угроз

Устойчивость

Мы сочетаем проверенные процессы и технологии управления инцидентами для быстрой выявления и реагирования на киберугрозы, как со стороны внутренних, так и внешних сил.

- Реагирование на кибер-инциденты
- Кибербоевые учения

1. Доступность сайтов
2. Репутация домена
3. Безопасность HTTP
4. Защита трафика
5. Утечки адресов электронной почты
6. Открытые порты
7. Кибersквоттинг
8. Выполнение требований по защите персональных данных
9. Безопасность почтового сервера
10. Безопасность мобильного банкинга

«Делойт» в Казахстане

В Казахстане «Делойт» представлен компаниями ТОО «Делойт» и ТОО «Делойт ТСФ», являющимися частью «Делойт СНГ Холдингс Лимитед» («Делойт», СНГ), входящей в состав «Делойт Туш Томацу Лимитед» (ДТТЛ).

«Делойт» — признанный лидер на рынке консалтинга в области информационной безопасности. Наша деятельность получила высокую оценку отраслевых аналитиков, в том числе Gartner, Forrester и Kennedy.

За 20 лет присутствия в Казахстане «Делойт» реализовал сотни успешных проектов для финансовых институтов, государственных организаций, промышленных и торговых предприятий, сопровождая крупнейшие транснациональные проекты и являясь лидером в предоставлении услуг банковскому сектору. На сегодняшний день компания представлена четырьмя офисами в Алматы, Нур-Султане, Атырау и Актау, сотрудниками которых являются около 500 местных и зарубежных специалистов в области аудита, консалтинга, управления рисками, финансового консультирования, налогообложения и права.

Наши эксперты разрабатывают решения, полностью адаптируемые под потребности клиентов, стремясь удовлетворить растущий спрос на услуги в области кибербезопасности. В числе наших продуктов инструменты для расширенного мониторинга инцидентов, связанных с безопасностью, анализа данных по угрозам, управления киберугрозами и реагирования на инциденты, а также многие другие.

1. Доступность сайтов
2. Репутация домена
3. Безопасность HTTP
4. Защита трафика
5. Утечки адресов электронной почты
6. Открытые порты
7. Кибersквоттинг
8. Выполнение требований по защите персональных данных
9. Безопасность почтового сервера
10. Безопасность мобильного банкинга

Доступность сайтов

1. Доступность сайтов

01

Обеспечение высокой доступности веб-сайта — одна из приоритетных и жизненно важных задач для любого банка, поскольку помимо визитной карточки, веб-сайт, как правило, это еще и канал продаж, сервис самообслуживания и сопровождения клиентов.

Для целей исследования уровня доступности веб-сайтов банков Казахстана мы измерили и проанализировали следующие показатели:

1) первая отрисовка контента (FCP);
2) время отклика (RT);
3) задержка первоначально ввода (FID).

Первые два показателя основаны на времени обмена информацией между сервером и клиентом, а последний измеряет производительность веб-сайтов на стороне клиента.

1. Доступность сайтов

2. Репутация домена

3. Безопасность HTTP

4. Защита трафика

5. Утечки адресов электронной почты

6. Открытые порты

7. Кибersквоттинг

8. Выполнение требований по защите персональных данных

9. Безопасность почтового сервера

10. Безопасность мобильного банкинга

1. Доступность сайтов

1.1 Первая отрисовка контента (FCP)

Показатель FCP представлен компанией Google и измеряет время, необходимое для отображения содержимого веб-сайта в окне браузера в ответ на запрос пользователя. Данный показатель измеряется в секундах. Соответственно, чем меньше его значение, тем лучше результат.

В своем исследовании мы использовали веб-ресурс Google PageSpeed. Полученные при этом показатели времени были интерпретированы с использованием метрик, установленных официальным методом оценки производительности Google. Таким образом, согласно полученным результатам 9% банков получили оценку «хорошо», 73% — оценку «нуждается в улучшении» и оставшиеся 18% — оценку «плохо».

1. Доступность сайтов
2. Репутация домена
3. Безопасность HTTP
4. Защита трафика
5. Утечки адресов электронной почты
6. Открытые порты
7. Кибersквоттинг
8. Выполнение требований по защите персональных данных
9. Безопасность почтового сервера
10. Безопасность мобильного банкинга

Репутация домена

2. Репутация домена

02

Репутация домена играет решающую роль в доверительных отношениях между участниками киберпространства. С тех пор как провайдеры электронной почты и поисковые системы начали полагаться на информацию от провайдеров репутации доменов, значимость этого фактора возросла. Электронные письма, отправленные с доменов с низкими показателями репутации или внесенные в черные списки поставщиками услуг оценки сетевой репутации, могут быть промаркированы поставщиками сервисов электронной почты как спам, а их веб-ресурсы могут не отображаться в результатах поиска.

Ниже мы представили результаты нашего анализа репутации доменов казахстанских банков, который был проведен с использованием четырех провайдеров услуг оценки сетевой репутации: Talos Intelligence, TrustedSource, ReputationAuthority и Barracuda Reputation System.

1. Доступность сайтов

2. Репутация домена

3. Безопасность HTTP

4. Защита трафика

5. Утечки адресов электронной почты

6. Открытые порты

7. Кибersквоттинг

8. Выполнение требований по защите персональных данных

9. Безопасность почтового сервера

10. Безопасность мобильного банкинга

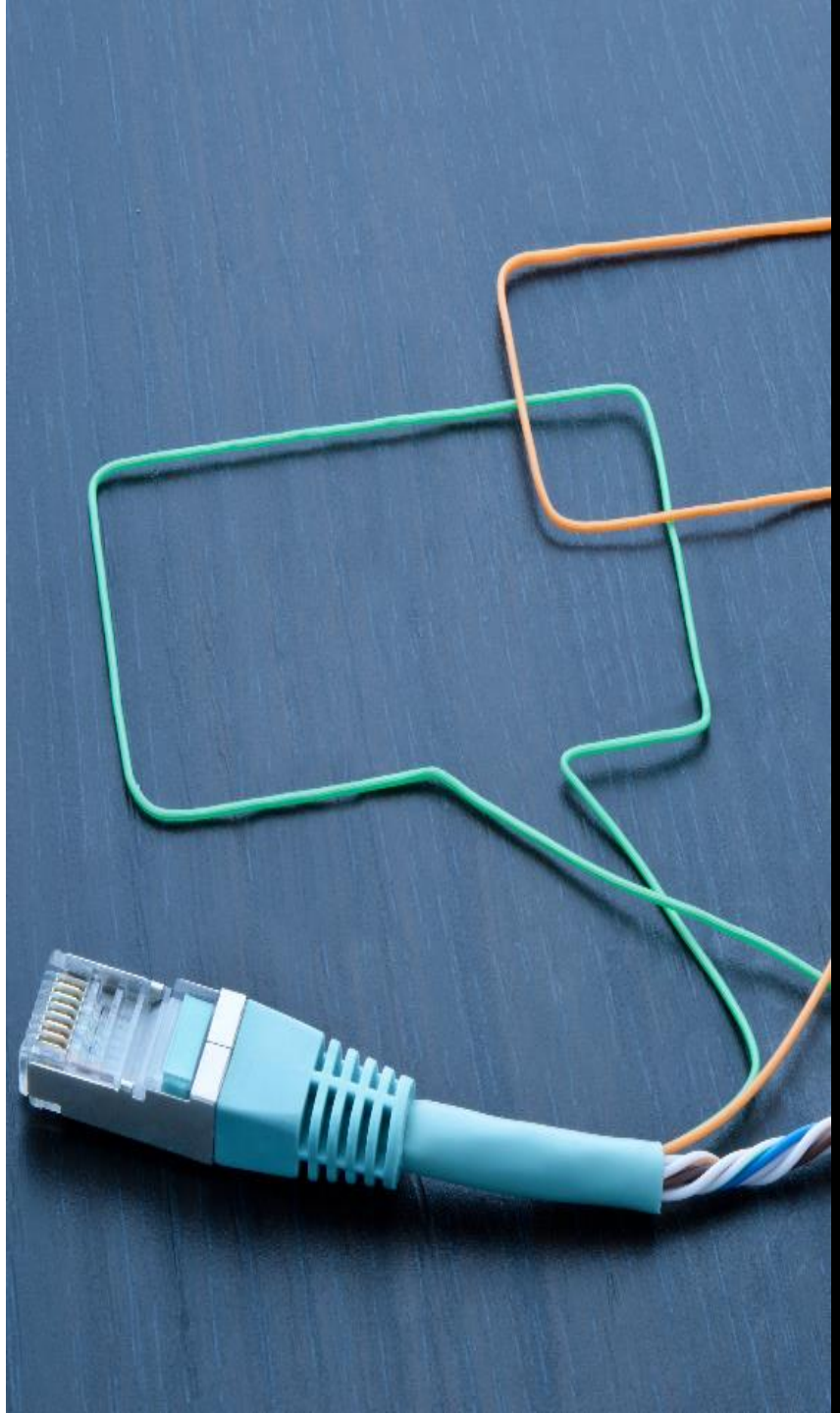
2. Репутация домена

2.1 Talosintelligence

Talos Intelligence предоставляет услуги оценки репутации домена на базе решений Cisco. Компания определяет и сопоставляет угрозы в режиме реального времени с использованием крупнейшей в мире сети обнаружения угроз, охватывающей электронные письма, веб-запросы, экземпляры вредоносных программ, наборы данных, анализа конечных точек и сетевых вторжений.

Решения Cisco полагаются на вердикты о репутации домена, предоставляемые Talosintelligence, в качестве первого фильтра для входящего трафика. Другие решения также могут работать на основе показателей репутации Talos Intelligence.

Talos делит репутацию доменов на четыре группы: доверенные, нейтральные, ненадежные и неизвестные. Прежде чем присвоить домену репутацию «доверенный», Talos собирает существенные положительные свидетельства об этом. Таким образом, не многие организации могут похвастаться наличием такого рейтинга. Тем приятнее отметить, что в Казахстане работает такой уникальный банк, с рейтингом «доверенный». Остальные домены местных банков имеют рейтинг «нейтральный».



1. Доступность сайтов
2. Репутация домена
3. Безопасность HTTP
4. Защита трафика
5. Утечки адресов электронной почты
6. Открытые порты
7. Киберсквоттинг
8. Выполнение требований по защите персональных данных
9. Безопасность почтового сервера
10. Безопасность мобильного банкинга

2. Репутация домена

2.2 Barracuda Reputation System (BRS)

BRS предоставляет информацию о репутации домена на базе Barracuda Central. Сервис ведет записи об IP-адресах известных спамеров и распространителей нежелательной корреспонденции. Эти данные собираются из спам-ловушек и других систем в Интернете. История отправки, связанная с IP-адресами всех почтовых серверов, анализируется с целью определить вероятность того, что сообщения с этих адресов являются безвредными.

Решения Barracuda Central в первую очередь полагаются на вердикты репутации домена, предоставляемые BRS, в качестве первого фильтра для возможной блокировки сетевых атак, отправляемых по электронной почте через Интернет и иные протоколы. Другие решения также могут полагаться на индикаторы репутации BRS.

BRS в режиме реального времени управляет двумя категориями IP-адресов и доменных имен. В первую попадают IP-адреса с репутацией «в черном списке/плохие», в другую «не в черном списке/хорошие».

Результаты нашего исследования указывают на то, что 100% местных банков имеют хорошую репутацию и в черном списке не значатся.

1. Доступность сайтов
2. Репутация домена
3. Безопасность HTTP
4. Защита трафика
5. Утечки адресов электронной почты
6. Открытые порты
7. Кибersквоттинг
8. Выполнение требований по защите персональных данных
9. Безопасность почтового сервера
10. Безопасность мобильного банкинга

2. Репутация домена

2.3 TrustedSource

TrustedSource предоставляет информацию о репутации домена на основе решения McAfee. Сервис оценивает данные о репутации и категории контента, а также шаблоны трафика электронной почты, Интернета и других сетей, выделяя IP-адреса, домены и URL-адреса. TrustedSource в режиме реального времени собирает с устройств безопасности McAfee упомянутые выше схемы трафика.

Решения McAfee полагаются на вердикты репутации домена, предоставляемые TrustedSource, в качестве основного фильтра для входящего трафика, блокировки сетевых атак, отправляемых по электронной почте через Интернет и другие протоколы, а также для уменьшения нежелательного сетевого трафика. Другие решения также могут полагаться на вердикты репутации TrustedSource.

Вердикт о репутации домена от TrustedSource оценивает риск как высокий, средний, минимальный или непроверенный. TrustedSource назначает вердикты о минимальном риске доменам, для которых во время тестирования не обнаружена подозрительная активность. Непроверенная репутация означает, что URL-адрес домена уже упоминался в веб-ссылке или ссылке электронной почты, но еще не был протестирован. По нашей оценке, основная часть доменов местных банков имеют репутацию с минимальным риском, и только один банк имеет непроверенную репутацию.

1. Доступность сайтов
2. Репутация домена
3. Безопасность HTTP
4. Защита трафика
5. Утечки адресов электронной почты
6. Открытые порты
7. Киберсквоттинг
8. Выполнение требований по защите персональных данных
9. Безопасность почтового сервера
10. Безопасность мобильного банкинга

2. Репутация домена

2.4 Заключение

Анализ доменной репутации казахстанских банков показывает, что в стране практически отсутствуют домены со слабой или отрицательной репутацией.

Это означает, что домены не использовались для рассылки спама, распространения вирусов или осуществления другой подозрительной деятельности либо, по крайней мере, они не попали в центр внимания на глобальном уровне и, следовательно, не подвергались оценке.

1. Доступность сайтов
2. Репутация домена
3. Безопасность HTTP
4. Защита трафика
5. Утечки адресов электронной почты
6. Открытые порты
7. Кибersквоттинг
8. Выполнение требований по защите персональных данных
9. Безопасность почтового сервера
10. Безопасность мобильного банкинга

Безопасность HTTP

3. Безопасность HTTP

03

Спектр средств защиты веб-сайтов весьма широк. Однако очень часто компрометация безопасности хотя бы одного такого компонента может привести к взлому всего сайта. При этом даже если злоумышленник всего лишь повредит содержимое главной страницы, не сумев получить конфиденциальную информацию или вывести какие-либо средства со счетов клиентов, потери, вызванные такой атакой, могут быть весьма существенными. Так, следствием подобной атаки может стать негативное влияние на репутацию и имидж финансовой организации. Именно по этой причине важно, чтобы банки выполняли все необходимые настройки и соблюдали все аспекты безопасности на своих интернет-ресурсах.

В этой части исследования мы сосредоточились на одном аспекте — настройке безопасности заголовков HTTP. Несмотря на то что это один из базовых компонентов, он также требует эффективного управления для обеспечения надлежащей защиты веб-ресурсов банка.

1. Доступность сайтов

2. Репутация домена

3. Безопасность HTTP

4. Защита трафика

5. Утечки адресов электронной почты

6. Открытые порты

7. Кибersквоттинг

8. Выполнение требований по защите персональных данных

9. Безопасность почтового сервера

10. Безопасность мобильного банкинга

3. Безопасность HTTP

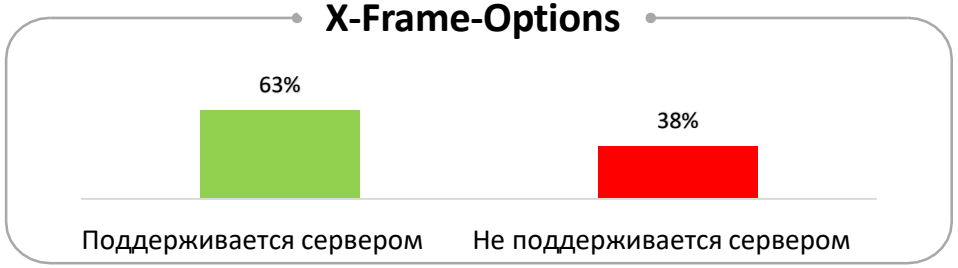
3.1 X-Frame-Options

Заголовок определяет, может ли браузер вывести страницу внутри тега <frame> или <iframe> на веб-странице в качестве HTTP-ответа. Неправильные настройки в заголовке могут быть использованы для атак типа «кликджекинг».

Логика данной атаки очень проста: пользователь сайта нажимает на один элемент страницы, но на самом деле взаимодействует с другим. Это может быть реализовано различными способами, но наиболее распространенный метод выглядит следующим образом: на страницу вставляется ссылка, которая выглядит безобидно. Поверх этой ссылки вредоносная страница размещает прозрачный <iframe> с src с сайта таким образом, чтобы кнопка находилась прямо над этой ссылкой. При попытке кликнуть на эту ссылку посетитель на самом деле нажимает на кнопку. В банковской отрасли это может привести к осуществлению быстрого платежа, который обычно не требует подтверждения. Организации могут узнать, уязвим ли их веб-сайт для кликджекинг-атак, добавив существующую ссылку на страницу iframe с простым HTML.

Этот пример демонстрирует важность защиты веб-сайтов от кликджекинг-атак. В свою очередь, X-Frame-Options является эффективной превентивной мерой защиты.

Заголовок X-Frame-Options может иметь три значения:
1) DENY: никогда не показывать страницу внутри фрейма;
2) SAMEORIGIN: разрешить открытие страницы внутри фрейма только в том случае, если родительский документ имеет тот же источник;
3) ALLOW-FROM URL: разрешить открытие страницы внутри фрейма только в том случае, если родительский документ находится на указанном в заголовке домене, например www.sample.com/frame-page.
Мы провели обзор и определили, используют ли местные банки данную превентивную меру. Результаты обзора показали, что 38% банков не используют X-Frame-Options.



1. Доступность сайтов
2. Репутация домена
3. Безопасность HTTP
4. Защита трафика
5. Утечки адресов электронной почты
6. Открытые порты
7. Кибersквоттинг
8. Выполнение требований по защите персональных данных
9. Безопасность почтового сервера
10. Безопасность мобильного банкинга

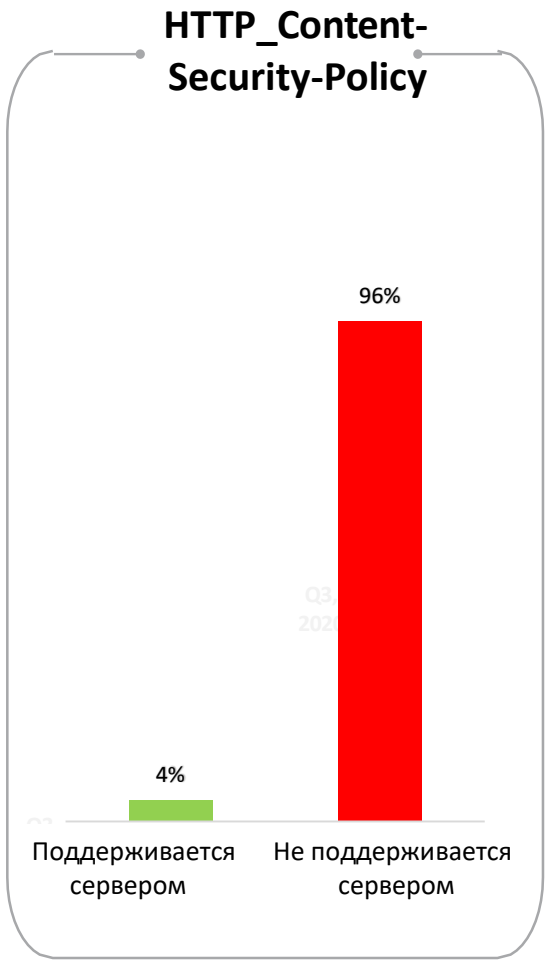
3. Безопасность HTTP

3.2 Content-Security-Policy (CSP)

CSP-заголовки позволяют разработчикам сайтов четко «объяснить» браузеру, в отношении каких адресов тот может выполнять межсайтовые запросы. CSP можно рассматривать как дополнительный уровень безопасности или стандарт безопасности браузера, который дает возможность создавать инструкции, описывающие, какие области, поддомены и типы ресурсов могут загружаться с определенной веб-страницы. CSP помогает загружать ресурсы JavaScript из определенной области, а также предотвращает запуск встроенного JavaScript на сайте. Это позволит обнаружить и предотвратить атаки XSS, Formjacking и SQL Injection.

Еще одним преимуществом использования CSP является возможность оперативно узнать о новых XSS-атаках. С позиции веб-разработчика правильно и грамотно развернуть CSP на своем ресурсе довольно проблематично, так как для каждой страницы необходимо устанавливать отдельную политику. В настройке CSP ему может помочь такая директива, как report-uri, с помощью которой разработчик может получать от браузера информацию обо всех нарушениях политики. Получая отчеты, веб-разработчик решает, какие источники нарушений нужно разрешить, и соответствующим образом обновляет политику — вручную либо с помощью специальных средств. Необходимо всего лишь перечислить ресурсы, которые будут включены в CSP. Помимо заголовков HTTP, правила CSP также могут быть добавлены в HTML-тег. Тем не менее администраторы веб-сайтов должны тщательно выполнять настройки правил CSP, поскольку неправильная конфигурация может привести к недоступности ресурсов и иллюзии защищенности.

По итогам нашего обзора веб-сайт только одного местного банка использует Content- Security-Policy, остальные банки не используют данный механизм защиты.



1. Доступность сайтов
2. Репутация домена
3. Безопасность HTTP
4. Защита трафика
5. Утечки адресов электронной почты
6. Открытые порты
7. Кибersквоттинг
8. Выполнение требований по защите персональных данных
9. Безопасность почтового сервера
10. Безопасность мобильного банкинга

3. Безопасность HTTP

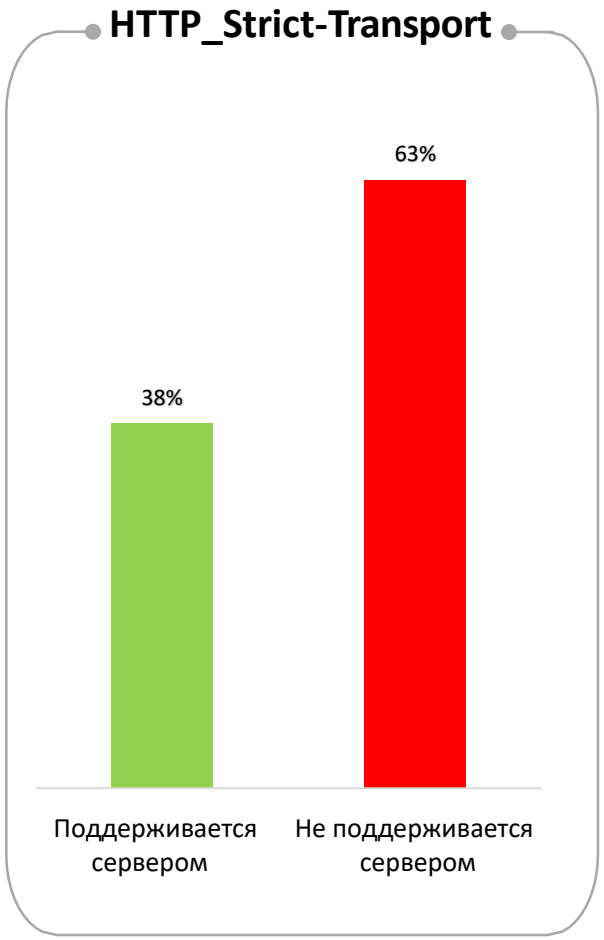
3.3 HTTP Strict Transport Security (HSTS)

Это механизм, принудительно активирующий защищенное соединение через протокол HTTPS. Данная политика безопасности позволяет сразу же устанавливать безопасное соединение вместо использования HTTP-протокола. Механизм использует особый заголовок Strict-Transport-Security для принудительного применения браузером протокола HTTPS даже в случае перехода по ссылкам с явным указанием протокола HTTP.

Представьте, что вы сидите в любимом кафе или в гостиничном номере и хотите воспользоваться бесплатным Wi-Fi. В таких местах пароли Wi-Fi часто печатаются на бумаге и никогда не меняются. Злоумышленники могут легко подключиться к общественной сети, что позволяет им просматривать данные любого, кто использует эту сеть, и манипулировать этими данными. Злоумышленники могут перехватить сетевой трафик любого веб-сайта через незащищенный HTTP, используя переадресацию 301 (301 redirect), чтобы перейти от HTTP к зашифрованному HTTPS. Этот способ позволяет злоумышленнику отключить SSL-шифрование и украсть личные данные или, что еще хуже, захватить данные для авторизации.

Таким образом, банковские сайты должны использовать только протокол HTTPS, а не HTTP. Даже если применяется сертификат SSL и трафик передается с HTTP на HTTPS с помощью переадресации 301, полная сетевая безопасность не гарантируется. Более высокий уровень безопасности обеспечивает HSTS.

Несмотря на то что HSTS-заголовки являются важным способом защиты пользователей от злоумышленников, их поддерживают только 38% банковских серверов в Казахстане, в то время как остальные 68% местных банков такие заголовки не применяют.



1. Доступность сайтов
2. Репутация домена
3. Безопасность HTTP
4. Защита трафика
5. Утечки адресов электронной почты
6. Открытые порты
7. Кибersквоттинг
8. Выполнение требований по защите персональных данных
9. Безопасность почтового сервера
10. Безопасность мобильного банкинга

3. Безопасность HTTP

3.4 X-Content-Type-Options

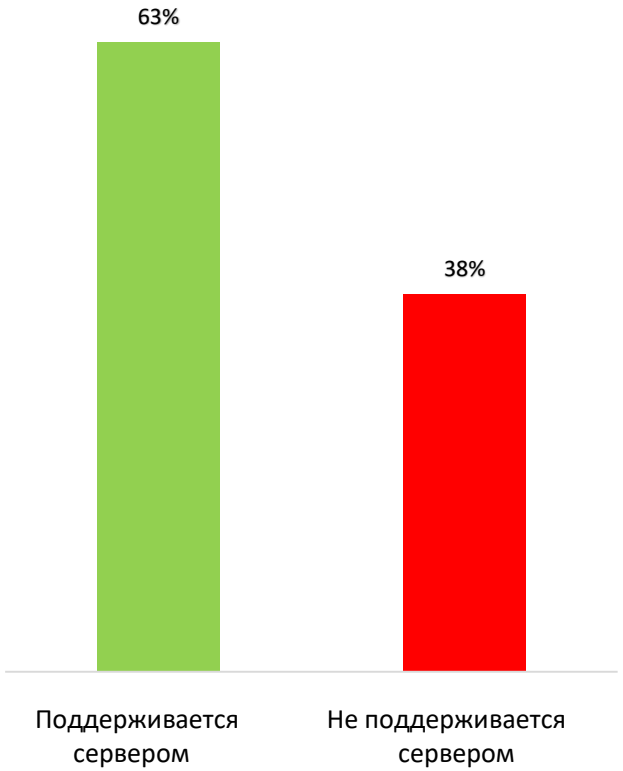
Любое содержимое HTTP заголовка должно включать метаданные о его типе, таким образом заголовок указывает браузеру не переопределять тип содержимого ответа. Например, если тип содержимого заголовка является изображением, браузер определит и отобразит его. В то время как если тип содержимого — HTML, отобразится разметка и запустится любой JavaScript-код.

Однако определение типа содержимого является необязательной процедурой, и веб-разработчики не всегда используют ее. Это означает, что браузеры должны самостоятельно идентифицировать тип просматриваемого контента. По этой причине для определения типа содержимого они вынуждены применять методы сниффинга, когда заголовки типа содержимого не передаются.

Это привело к возникновению серьезной угрозы безопасности. Избежать ее можно, добавив X-Content-Type-Option nosniff в заголовок HTTP, чтобы браузеры, поддерживающие определение типа MIME, использовали предоставленный сервером Content-Type и не интерпретировали содержимое как другой тип контента. Добавление этой строки также обеспечивает защиту Cross-Origin Read Blocking (CORB) для файлов HTML, TXT, JSON и XML (за исключением SVG image/svg+xml).

63% веб-ресурсов местных банков используют X-Content-Type-Options — nosniff-заголовок. Остальные 38% банков данный механизм защиты не применяют.

HTTP_X-Content-Type



1. Доступность сайтов
2. Репутация домена
3. Безопасность HTTP
4. Защита трафика
5. Утечки адресов электронной почты
6. Открытые порты
7. Кибersквоттинг
8. Выполнение требований по защите персональных данных
9. Безопасность почтового сервера
10. Безопасность мобильного банкинга

3. Безопасность HTTP

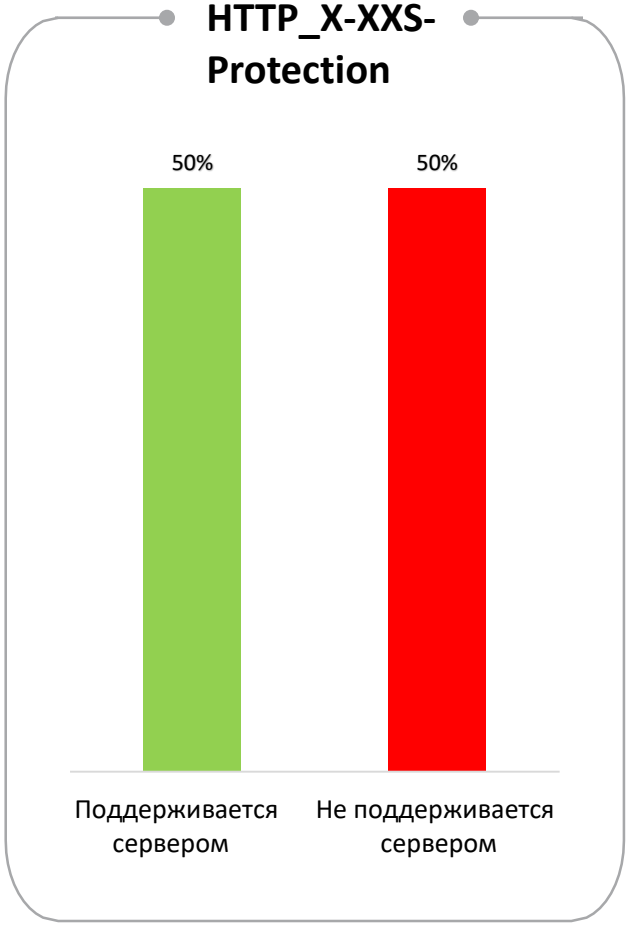
3.5 X-XSS-Protection

Этот заголовок защищает пользователей веб-сайта от атак типа Cross Site Scripting (XSS) путем фильтрации содержимого сайта на стороне клиента.

В большинстве случаев эта мера защиты для современных браузеров (Internet Explorer 8, Chrome, Edge, Opera и Safari) не требуется, если сайты внедряют сильную политику безопасности контента Content-Security-Policy.

Тем не менее задача по устранению уязвимости XSS на стороне пользователя должна являться приоритетной при разработке веб-сайтов. После обеспечения безопасности на уровне кода заголовок XSS Protection должен быть активирован в интернет-браузерах для повышения уровня их безопасности.

Согласно нашему обзору 50% местных банков имеют заголовок X-XSS-Protection в ответе сервера, тогда как оставшиеся 50% эту меру защиты не используют.



1. Доступность сайтов
2. Репутация домена
3. Безопасность HTTP
4. Защита трафика
5. Утечки адресов электронной почты
6. Открытые порты
7. Кибersквоттинг
8. Выполнение требований по защите персональных данных
9. Безопасность почтового сервера
10. Безопасность мобильного банкинга

3. Безопасность HTTP

3.6 Set-cookie security flags

Веб-приложения следят за сеансами пользователей через идентификатор сеанса. Это значение передается пользователю с информацией о заголовке HTTP Set-Cookie. Интернет-браузеры хранят данное значение и автоматически добавляют его в каждый HTTP-запрос, который создается до тех пор, пока сохраненные cookie-файлы остаются действительными.

Файлы cookie также могут использоваться для других целей, например для сохранения ссылки на последнее выбранное изображение в галерее. Таким образом, трафик HTTP может быть уменьшен и веб-сервер может решить некоторые задачи с помощью интернет-браузера пользователя.

Хотя эта опция весьма полезна, организациям все еще необходимо определить, какие значения файлов cookie важны для обеспечения безопасности, а именно значение, которое содержит идентификационный номер пользователя (идентификатор сеанса). Это значение должно передаваться только в безопасном запросе HTTPS. Исключением являются экстренные случаи.

Информация о файлах cookie может быть украдена по средством JavaScript с помощью таких атак, как XSS. Для них в качестве защиты могут быть использованы HttpOnly- и Secure-флаги. Это помогает предотвратить кражу информации о файлах cookie и свести к минимуму потенциальный вред.

Флаг HttpOnly является высокоэффективным методом защиты файлов cookie, который предотвращает их чтение при помощи JavaScript.

Если флаг HttpOnly установлен в ответе HTTP, файл cookie не бывает доступен на стороне клиента.

В результате браузер не показывает файлы cookie третьим лицам, даже если существует уязвимость Cross-Site Scripting (XSS) и пользователь случайно использует вредоносную ссылку, которая эксплуатирует данную уязвимость.

Еще один случай, в котором файлы cookie должны быть защищены во время передачи данных между клиентом и сервером, — это возможность доступа к странице веб-сервера банка как по http-, так и https-протоколам. В отличие от протокола http трафик https зашифрован. Для защиты информации сеанса из файла cookie следует использовать только защищенный протокол https. Этого можно добиться, добавив Secure-флаг в заголовок set-cookie.

Результаты нашего обзора свидетельствуют о том, что 42% местных банков используют защищенные флаги, а 58% не используют.

1. Доступность сайтов
2. Репутация домена
3. Безопасность HTTP
4. Защита трафика
5. Утечки адресов электронной почты
6. Открытые порты
7. Кибersквоттинг
8. Выполнение требований по защите персональных данных
9. Безопасность почтового сервера
10. Безопасность мобильного банкинга

3. Безопасность HTTP

3.7 Public-Key-Pins

Данный заголовок ответа позволяет прикрепить публичные ключи веб-сервера в браузере, тем самым исключив возможность для браузера принимать сертификаты с другими общедоступными ключами от данного сервера. Эта мера может предотвратить атаки клиентов веб-сервиса с поддельными сертификатами.

Для того чтобы понять логику закрепления общедоступных ключей, необходимо знать, что предлагают безопасные соединения и как они работают. Когда пользователи хотят получить безопасный доступ к веб-сайту, сервер отправляет свой собственный общедоступный ключ, который затем используется для шифрования входящего трафика на сервер от пользователей. Этот сертификат содержит следующую информацию: название сайта, срок действия сертификата и количество используемых битов криптографических ключей.

При отправке клиенту общедоступного ключа браузер должен убедиться в подлинности сертификата, для этого он сверяется с Центром Сертификации (CA), который подписывает сертификаты веб-серверов. Эта информация также содержится в сертификате. Основываясь на информации из CA, браузеры могут подтвердить подлинность сертификата веб-серверов. Если проблем не обнаружено, браузеры продолжают безопасно работать с веб-сервером.

К сожалению, вредоносная деятельность распространена в киберпространстве. Основываясь на своем опыте и последних событиях, киберспециалисты знают, что CA может подписать сертификат от имени другого веб-сайта. В основном это происходит в результате хакерских атак на CA.
HTTP Public Key Pinning (HPKP) был создан для предотвращения атак с подписанными поддельными сертификатами. Используя эту функцию, веб-сайты могут сообщать значения хэша своих сертификатов браузерам с заголовком Public-Key-Pins.

Если веб-сайт утверждает, что владеет сертификатом, отличающимся от указанного, браузер откажется устанавливать безопасное соединение или даже сообщит об этом на указанный URL-адрес.

Функция HPKP защищает пользователей и веб-сайты в тех случаях, когда CA был скомпрометирован или взломан для подписания поддельных сертификатов.

Заголовок ответа Expect-CT сообщает браузерам, что сервер получил сертификат через общедоступный CA (журнал прозрачности сертификата). Это относительно новый заголовок, который предназначен для замены HTTP Public Key Pinning (HPKP). Его цель — защита пользователей веб-сайта от атак с поддельными сертификатами.

В апреле 2018 года компания Google впервые приняла технологию прозрачности сертификатов (CT) как обязательную. По данным на 23 ноября 2020 года, в журналы CT, мониторингом которых занимается Google, было сделано 11 266 751 018 записей. Технология CT зависит от трех нижеследующих операций.

- Для каждого сертификата, подписанного в апреле 2018 года, CT должны быть добавлены записи в общедоступный журнал прозрачности сертификатов.
- Владельцы веб-сайтов должны заниматься мониторингом и надзором. Они несут ответственность за добавление заголовка Expect-CT в ответ сервера. После того, как сканирование и системы уведомления были введены в действие, через систему CT-журнала можно узнать, был ли сертификат веб-сайта подписан CA.
- Используя информацию в журнале CT, браузеры должны также проверять, отвечают ли требованиям сертификаты, которые они получают от веб-сайтов.

Согласно нашему обзору 100% местных банков имеют заголовок Expect-CT в ответе от сервера.

1. Доступность сайтов
2. Репутация домена
3. Безопасность HTTP
4. Защита трафика
5. Утечки адресов электронной почты
6. Открытые порты
7. Кибersквоттинг
8. Выполнение требований по защите персональных данных
9. Безопасность почтового сервера
10. Безопасность мобильного банкинга

3. Безопасность HTTP

3.8

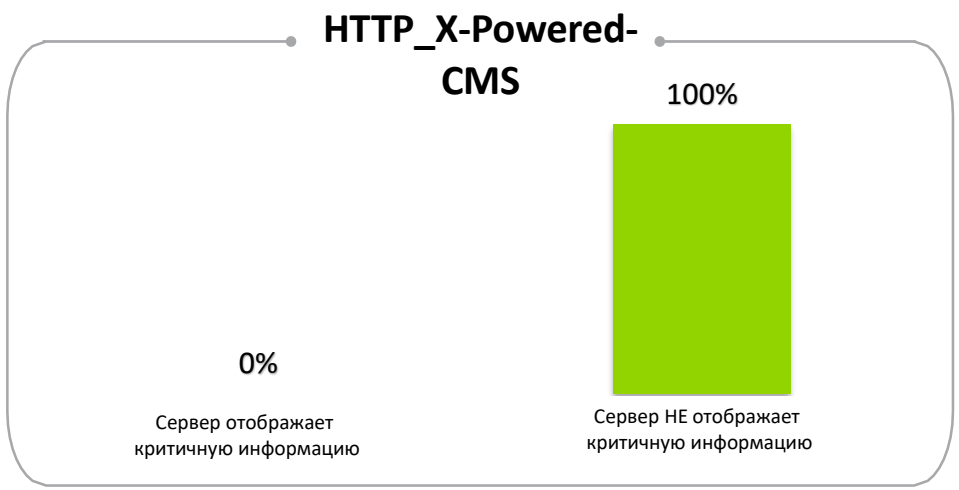
X-Powered-CMS и X-Powered-By

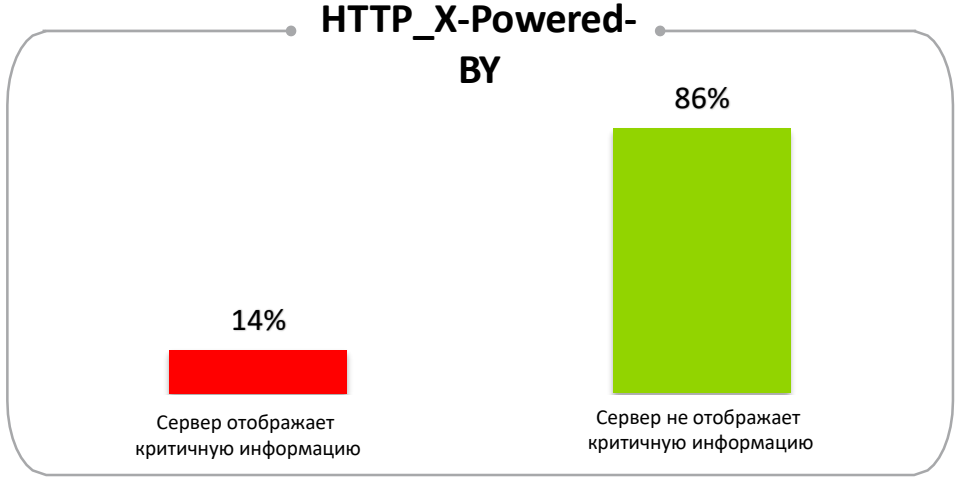
Заголовок X-Powered-CMS предоставляет название и версию системы управления контентом (CMS), которая генерирует ответ сервера, например Bitrix или Express. Этот заголовок также предоставляет информацию о технологиях, на основе которых создан веб-сайт. Он часто добавляется по умолчанию в ответы сервера, построенные с использованием определенных технологий, таких как ASP.NET или PHP.

Раскрытие этой информации не представляет серьезного риска, если программное обеспечение веб-сайта регулярно обновляется. Однако если это возможно, разумным решением будет скрыть имена и версии технологий от посторонних глаз, так как это может сократить время, необходимое злоумышленникам для сбора информации и определения последующих векторов атаки.

В ходе обзора мы определили, что 100% веб-сайтов удалили или изменили заголовок X-Powered-CMS.

Между тем 14% местных банков имели дефолтные значения для заголовка X-Powered-By, в то время как 86% удалили или изменили его. К сожалению, из анализа были исключены два банка, так как их целевые сайты не отвечали на наши запросы.





1. Доступность сайтов
2. Репутация домена
3. Безопасность HTTP
4. Защита трафика
5. Утечки адресов электронной почты
6. Открытые порты
7. Кибersквоттинг
8. Выполнение требований по защите персональных данных
9. Безопасность почтового сервера
10. Безопасность мобильного банкинга

3. Безопасность HTTP

3.9

X-Powered-CMS и X-Powered-By

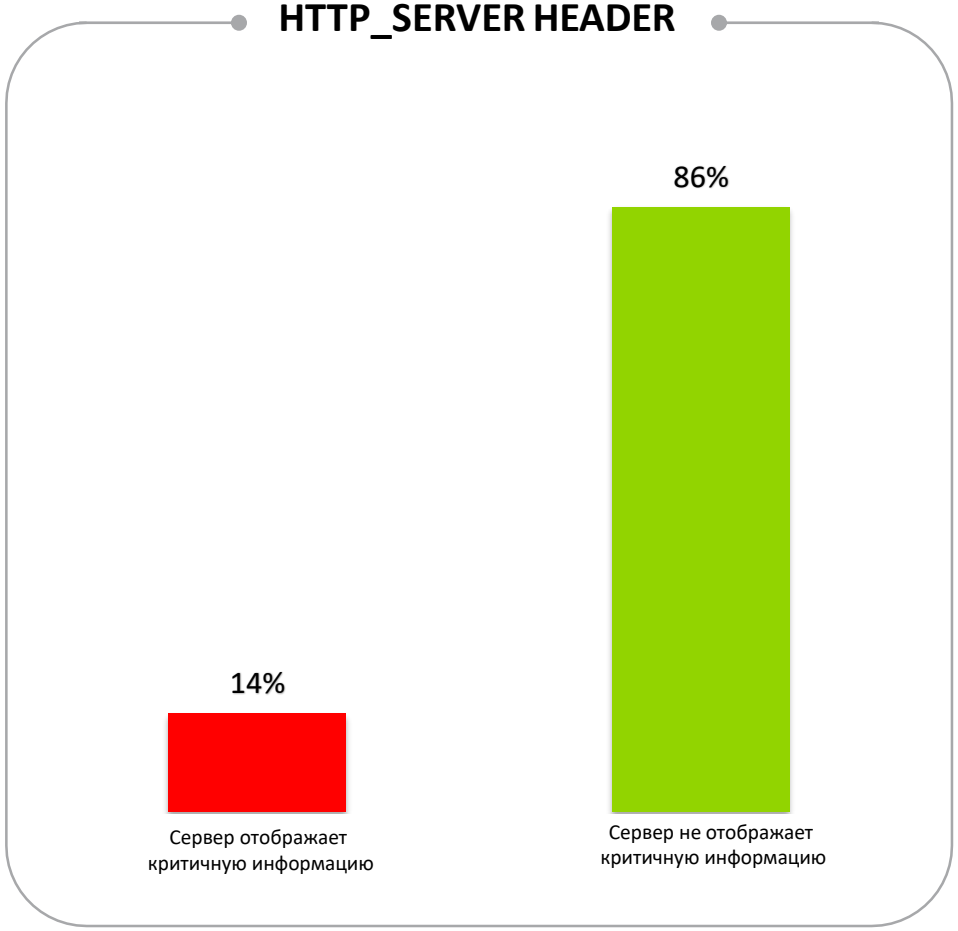
Заголовок ответа от сервера предоставляет информацию о программном обеспечении, используемом сервером для обработки запросов.

Распространенные значения включают nginx/x.x.x, Apache/x.x.x и Microsoft-IIS/x.x.

Раскрытие этой информации не представляет прямой угрозы, но может сократить время, необходимое злоумышленникам для сбора информации и определения последующих векторов атаки.

Наш обзор ответов от анализируемых веб-серверов показал, что 14% местных банков отображают информацию о программном обеспечении, которое они используют, в то время как 86% удалили или изменили значение заголовка.

HTTP_SERVER HEADER



1. Доступность сайтов
2. Репутация домена
3. Безопасность HTTP
4. Защита трафика
5. Утечки адресов электронной почты
6. Открытые порты
7. Кибersквоттинг
8. Выполнение требований по защите персональных данных
9. Безопасность почтового сервера
10. Безопасность мобильного банкинга

3. Безопасность HTTP

3.10

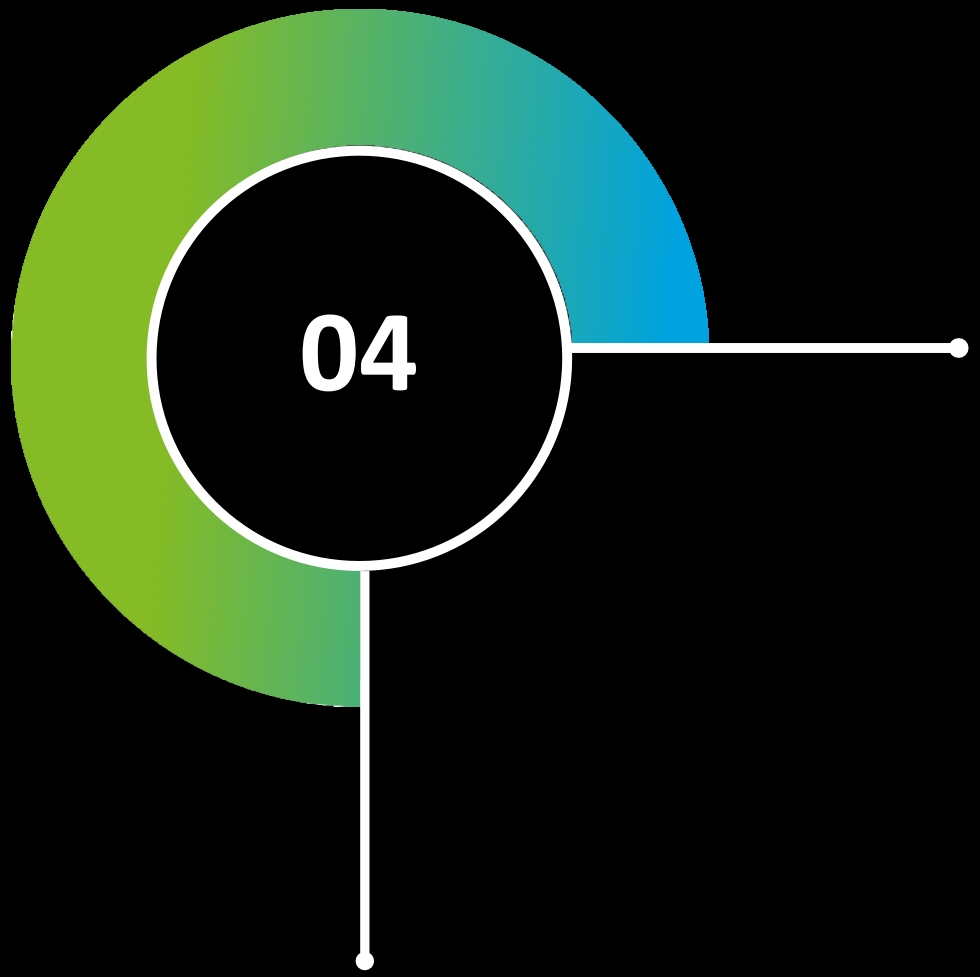
Заключение

Настройка и поддержание безопасности веб-сайта является сложной задачей, которая включает в себя ряд областей. Нарушение целостности в любой из них может стать фатальным для всего приложения и его данных. По этой причине нельзя игнорировать безопасность заголовков HTTP.

Наш анализ показал, что большинство казахстанских банков рассматривают заголовки HTTP как незначительный фактор. Это означает, что связанные с ними риски безопасности не компенсируются.

Безопасные HTTP-заголовки служат хорошей отправной точкой для обеспечения надежной защиты веб-сайтов, так как большинство из них легко поддается настройке. Следование лучшим практикам в области HTTP-безопасности позволит использовать заголовки как дополнительный уровень защиты любых веб-активов.

1. Доступность сайтов
2. Репутация домена
3. Безопасность HTTP
4. Защита трафика
5. Утечки адресов электронной почты
6. Открытые порты
7. Кибersквоттинг
8. Выполнение требований по защите персональных данных
9. Безопасность почтового сервера
10. Безопасность мобильного банкинга



TLS и SSL

4. Защита трафика

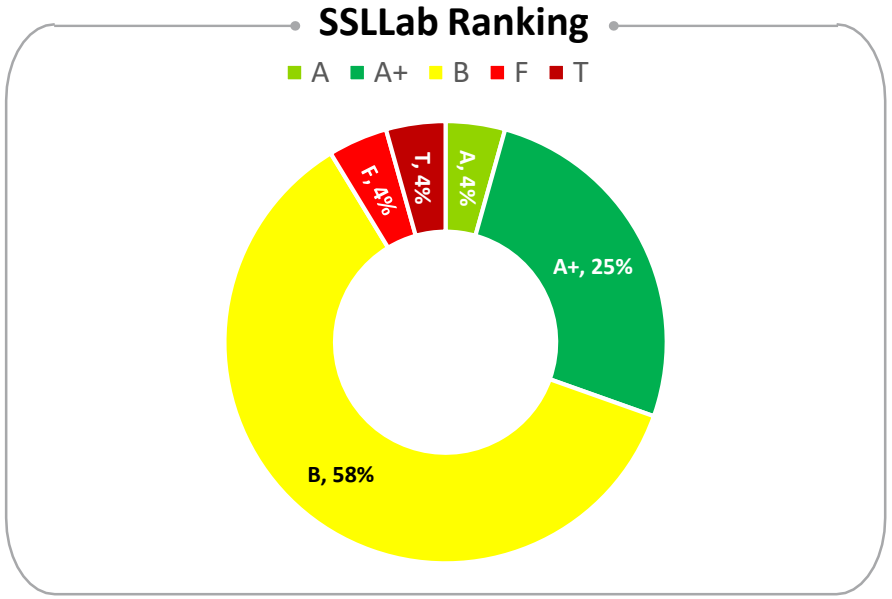
4.1 SSL Labs

Сегодня компании выбирают услуги и партнеров на основе HTTPS, этот протокол является безопасной версией общего протокола HTTP для доступа к веб-ресурсам. В HTTPS данные шифруются с помощью Transport Layer Security (TLS) или Secure Sockets Layer (SSL). На сегодняшний день эти криптографические протоколы считаются наиболее популярными методами обеспечения безопасной связи через Интернет.
Для подключения к SSL/TLS сервер должен иметь установленный цифровой сертификат, подтверждающий подлинность домена и владельца сайта. Это необходимо для того, чтобы пользователи посетили исходный ресурс, а не фальшивую страницу, созданную злоумышленником.

Однако наличие сертификата SSL не означает, что данные пользователей сайта полностью защищены. SSL/TLS имеет большое количество настроек и функций, которые могут по-разному влиять на безопасность соединения и его клиентов. Неправильные настройки могут позволить злоумышленникам перехватывать данные передаваемыми между сервером и клиентом, и манипулировать ими.

Предупреждения и ограничения, встроенные в браузеры, упростили возможность определения надежности шифрования сайта. Для оценки этих параметров мы использовали ресурс Qualys SSL Labs, который оценивает настройки веб-ресурсов SSL/TLS по шкале от A+ (лучший) до F (худший) на основе многочисленных параметров. Более подробная информация по ссылке: https://github.com/ssllabs/research/wiki/SSL-Server-Rating-Guide.

Наш обзор параметров SSL/TLS местных банков с использованием ресурса SSL Labs показал, что 25% из них имеют оценку A+, 4% — оценку A, 58% — оценку B, 4% — оценку F и 4% — оценку T. Рейтинг T свидетельствует о том, что сертификат безопасности данного банка не является надежным. Результаты нашего обзора показывают, что домены большинства рассматриваемых банков настроены в соответствии с требованиями безопасности и пользователи могут доверять исходному ресурсу.



1. Доступность сайтов
2. Репутация домена
3. Безопасность HTTP
4. Защита трафика
5. Утечки адресов электронной почты
6. Открытые порты
7. Кибersквоттинг
8. Выполнение требований по защите персональных данных
9. Безопасность почтового сервера
10. Безопасность мобильного банкинга

4. Защита трафика

4.2 Поддержка SSL 2.0 и SSL 3.0

SSL и TSL являются протоколами шифрования и авторизации. С помощью этих протоколов осуществляется безопасная передача данных с сервера на сервер или с сервера к клиенту. TSL — улучшенная версия SSL. Тем не менее некоторые общедоступные веб-ресурсы по-прежнему поддерживают SSL для шифрования.

В 1995 году протокол SSL был впервые опубликован компанией Netscape как SSL 2.0 (протокол SSL 1.0, первая версия SSL, никогда не был доступен всем пользователям). SSL 2.0, присутствовавший на рынке некоторое время, имел серьезную уязвимость, что привело к его замене в 1996 году на более новую версию, SSL 3.0. Начиная с 90-х годов в SSL 2.0 и 3.0 был обнаружен ряд уязвимостей, некоторые из которых были подтверждены IETF в 2011 и 2015 годах. Многие из этих уязвимостей больше не представляют угрозы, но на практике SSL не так надежен, как должен быть.

Интернет-браузеры, которым необходимо было бороться с уязвимостью в системе безопасности, начали предупреждать пользователей, отмечая веб-сайты, которые использовали сертификаты SSL, как небезопасные. Эти SSL недостатки дают TLS много преимуществ. Чтобы перейти на протокол TLS, SSL 2.0 и SSL 3.0 должны быть отключены в настройках сервера.

Наш обзор веб-сайтов местных банков показал, что ни один из них не поддерживает протокол SSL.

1. Доступность сайтов
2. Репутация домена
3. Безопасность HTTP
4. Защита трафика
5. Утечки адресов электронной почты
6. Открытые порты
7. Кибersквоттинг
8. Выполнение требований по защите персональных данных
9. Безопасность почтового сервера
10. Безопасность мобильного банкинга

4. Защита трафика

4.3 Поддержка RC4

Алгоритм шифрования RC4 — также известный как ARC4 или ARCFOUR — широко используется в компьютерных сетях различных систем информационной безопасности (таких как протоколы SSL и TLS, алгоритмы беспроводной безопасности WEP и WPA). Принцип работы RC4, как и любого шифра потока, основан на применении генератора псевдослучайных битов. Ключ записан на вход генератора, а псевдослучайные биты считываются на выходе. Длина ключа может составлять от 40 до 2048 битов.

В настоящее время алгоритм RC4 больше не считается безопасным, и вопрос о его использовании следует рассмотреть самым тщательным образом. Часть зашифрованного RC4 трафика HTTPS (например, идентификатор сеанса, передаваемый в cookies) веб-сайтов, работающих на его основе, возможно расшифровать за десятки часов. Также его применение позволяет реализовать атаку MitM, «подслушивая» и сохраняя зашифрованный трафик, и выполнять запросы от имени жертвы.

Наш обзор веб-сайтов местных банков показал, что ни один из них не использует алгоритм RC4 для шифрования.

1. Доступность сайтов
2. Репутация домена
3. Безопасность HTTP
4. Защита трафика
5. Утечки адресов электронной почты
6. Открытые порты
7. Киберсквоттинг
8. Выполнение требований по защите персональных данных
9. Безопасность почтового сервера
10. Безопасность мобильного банкинга

4. Защита трафика

4.4 Устаревшие версии TLS

Протокол Transport Layer Security (TLS) предоставляет зашифрованную связь для обеспечения безопасности и конфиденциальности информации. Версия TLS 1.0 применяется с 1999 года и является эволюцией старого протокола шифрования SSL. Существует также более современный протокол TLS 1.2, который появился в августе 2008 года, и самый последний TLS 1.3, вышедший в августе 2018 года.

В 2011 году была обнаружена уязвимость в протоколе TLS 1.0, которая позволяет расшифровать файлы cookie, используемые для проверки подлинности пользователей. Кроме того, в TLS 1.0 и 1.1 используются ненадежные алгоритмы хэширования MD5 и SHA-1. В 2020 году все основные браузеры прекратили поддержку TLS 1.0 и TLS 1.1. Отключение этих протоколов также рекомендуется на стороне сервера.

Мы обнаружили, что 50% банковских сайтов по-прежнему поддерживают уязвимые версии TLS — 1.0 и 1.1. Остальные 50% используют только защищенные версии 1.2 и 1.3 протокола TLS.

1. Доступность сайтов
2. Репутация домена
3. Безопасность HTTP
4. Защита трафика
5. Утечки адресов электронной почты
6. Открытые порты
7. Кибersквоттинг
8. Выполнение требований по защите персональных данных
9. Безопасность почтового сервера
10. Безопасность мобильного банкинга

4. Защита трафика

4.5

SSL Renegotiation (повторное обращение)

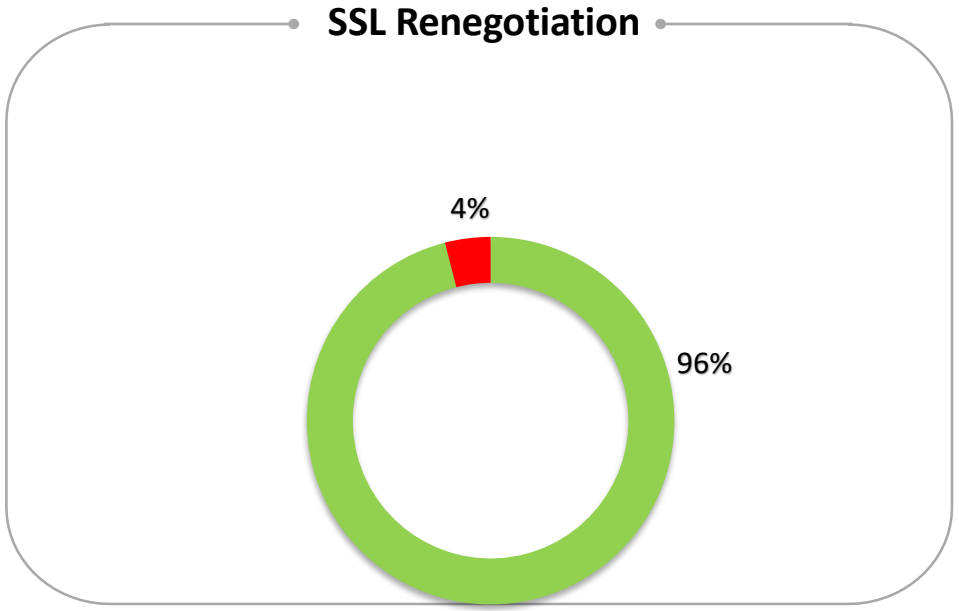
Повторное обращение SSL удобно, когда уже установлена регулярная сессия SSL и требуется проверка подлинности клиента. Например, предположим, что вы просматриваете сайт онлайн-магазина, который использует SSL и имеет подключение HTTPS. Изначально вы просматриваете сайт анонимно, добавляя продукты в корзину. Но когда вы решите сделать покупку, вам будет предложено пройти в личный кабинет и авторизоваться, используя соединение SSL. Любая информация, собранная до этой проверки подлинности (например, продукты добавленные в корзину), должна сохраниться даже после прохождения авторизации. Таким образом, вновь созданный сеанс SSL использует существующее соединение. Обратите внимание, что повторное обращение может быть запрошено в любое время клиентом или сервером.

SSL Renegotiation может иметь известные уязвимости, если настроено небезопасно. В этой связи некоторые разработчики предпочитают отключать его на стороне сервера.

Однако проблемы возникают и в том случае, когда серверы отключают SSL Renegotiation и не дают никаких указаний о статусе безопасности.

Это создает неудобства для пользователей и вынуждает их настраивать свой уровень защиты вручную. По этой причине очень важно, чтобы сервер пропускал только безопасное повторное обращение SSL и ограничивал количество SSL-подключений.

Наш обзор веб-сайтов казахстанских банков показал, что 4% из них имеют небезопасные механизмы SSL Renegotiation или совсем отключили их, в то время как остальные 96% обеспечили требуемую защиту.



1. Доступность сайтов
2. Репутация домена
3. Безопасность HTTP
4. Защита трафика
5. Утечки адресов электронной почты
6. Открытые порты
7. Кибersквоттинг
8. Выполнение требований по защите персональных данных
9. Безопасность почтового сервера
10. Безопасность мобильного банкинга

4. Защита трафика

4.6

Уязвимость BEAST

Версии протокола TLS до 2006 года были уязвимы для атак BEAST. Злоумышленники могут расшифровать данные, которыми обмениваются обе стороны, используя протоколы TLS 1.0, SSL 3.0 и ниже. Для этого метода атаки злоумышленник и жертва должны находиться в одной сети.
С помощью метода BEAST пароли можно разделить на небольшие пакеты и расшифровать. Хакеры, которые расшифровывают один байт данных за две секунды, могут получить доступ к учетным данным с помощью системы аутентификации 1000–2000 символов за полчаса. Используя современный метод, можно сократить это время до 10 минут. В этом методе для обхода аналогичной политики (SOP) применяется программный компонент Java-апплет.
В 2011 году исследователи в области безопасности обнаружили более практичные способы использования уязвимости BEAST. Данные, зашифрованные с использованием режима CBC с цепочкой IV, позволяют выполнять атаки MitM для получения незашифрованных HTTP-заголовков с помощью блочных атак с выбранной границей в сеансе HTTPS вместе с кодом JavaScript, который использует атаку BEAST.

Лучший способ защитить пользователей от атак BEAST — отключить SSL и TLS версии ниже 1.2 на стороне сервера. Наш обзор веб-сайтов банков показал, что 27% финансовых институтов Казахстана потенциально уязвимы к BEAST-атаке из-за поддержки старых версий TLS, в то время как остальные 73% используют версии TLS 1.2 и выше или устраняют данную уязвимость на стороне сервера.

1. Доступность сайтов
2. Репутация домена
3. Безопасность HTTP
4. Защита трафика
5. Утечки адресов электронной почты
6. Открытые порты
7. Кибersквоттинг
8. Выполнение требований по защите персональных данных
9. Безопасность почтового сервера
10. Безопасность мобильного банкинга

4. Защита трафика

4.7

Уязвимость CVE-2016-2107

В первой половине 2016 года большинство зашифрованных сайтов находились под угрозой из-за уязвимости CVE-2016-2107, о которой стало известно в 2013 году в результате исправления уязвимости Lucky 13. Эта уязвимость позволяет осуществлять MitM-атаки и получать конфиденциальную информацию в незашифрованном виде в результате атак на сеансы AES CBC.

Несмотря на то что уязвимость была устранена новым патчем для криптографической библиотеки OpenSSL, некоторые веб-сайты по-прежнему используют устаревшие версии OpenSSL.

Наша проверка веб-сайтов местных банков показала, что 4% (один веб-сайт) были уязвимы для CVE-2016-2107, в то время как остальные 96% имеют новые версии OpenSSL и устойчивы к данной уязвимости.

1. Доступность сайтов
2. Репутация домена
3. Безопасность HTTP
4. Защита трафика
5. Утечки адресов электронной почты
6. Открытые порты
7. Кибersквоттинг
8. Выполнение требований по защите персональных данных
9. Безопасность почтового сервера
10. Безопасность мобильного банкинга

4. Защита трафика

4.8

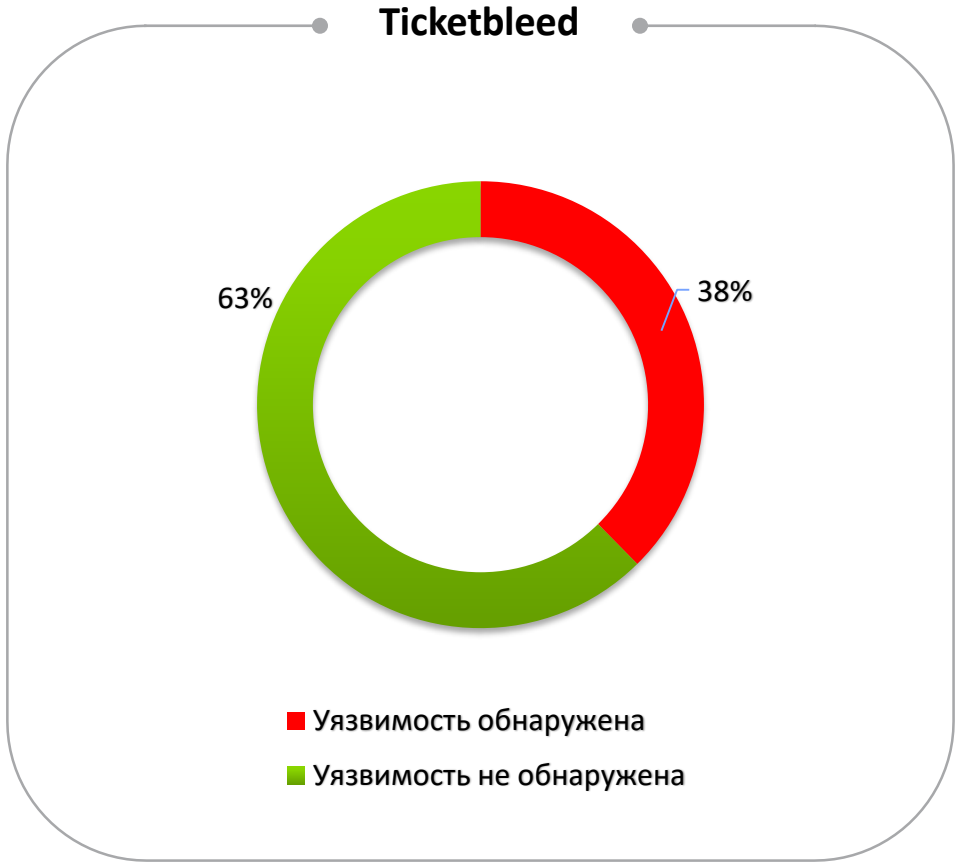
Уязвимость Ticketbleed

В этой части нашего обзора мы установили, что треть банков имеют дополнительную уязвимость.

В начале 2017 года стало известно об уязвимости, наносящей вред именно продуктам компании F5 Networks. Ticketbleed — это программная уязвимость, которая позволяет злоумышленнику удаленно извлекать до 31 байта неинициализированной памяти одновременно в стеке устройств F5 BIG-IP TLS/SSL. В этой памяти может храниться потенциально важная информация или конфиденциальные учетные данные, сохранившиеся после других подключений.

Для того чтобы устранить эту уязвимость, требуется только обновление версии TMOS.

Наша проверка веб-сайтов местных банков показала, что 38% из них уязвимы к Ticketbleed, в то время как остальные 63% обеспечили устойчивую защиту.



1. Доступность сайтов
2. Репутация домена
3. Безопасность HTTP
4. Защита трафика
5. Утечки адресов электронной почты
6. Открытые порты
7. Кибersквоттинг
8. Выполнение требований по защите персональных данных
9. Безопасность почтового сервера
10. Безопасность мобильного банкинга

4. Защита трафика

4.9

Другие уязвимости

В дополнение к вышеуказанным наблюдениям мы проверили каждый веб-ресурс в рамках этого отчета на следующие уязвимости: Weak Diffie-Hellman parameters, ROBOT, GOLDENDOODLE, POODLE, FREAK, DROWN и Heartbleed. Наша проверка показала, что ни один из сайтов местных банков не подвергался подобным атакам.

1. Доступность сайтов

2. Репутация домена

3. Безопасность HTTP

4. Защита трафика

5. Утечки адресов электронной почты

6. Открытые порты

7. Кибersквоттинг

8. Выполнение требований по защите персональных данных

9. Безопасность почтового сервера

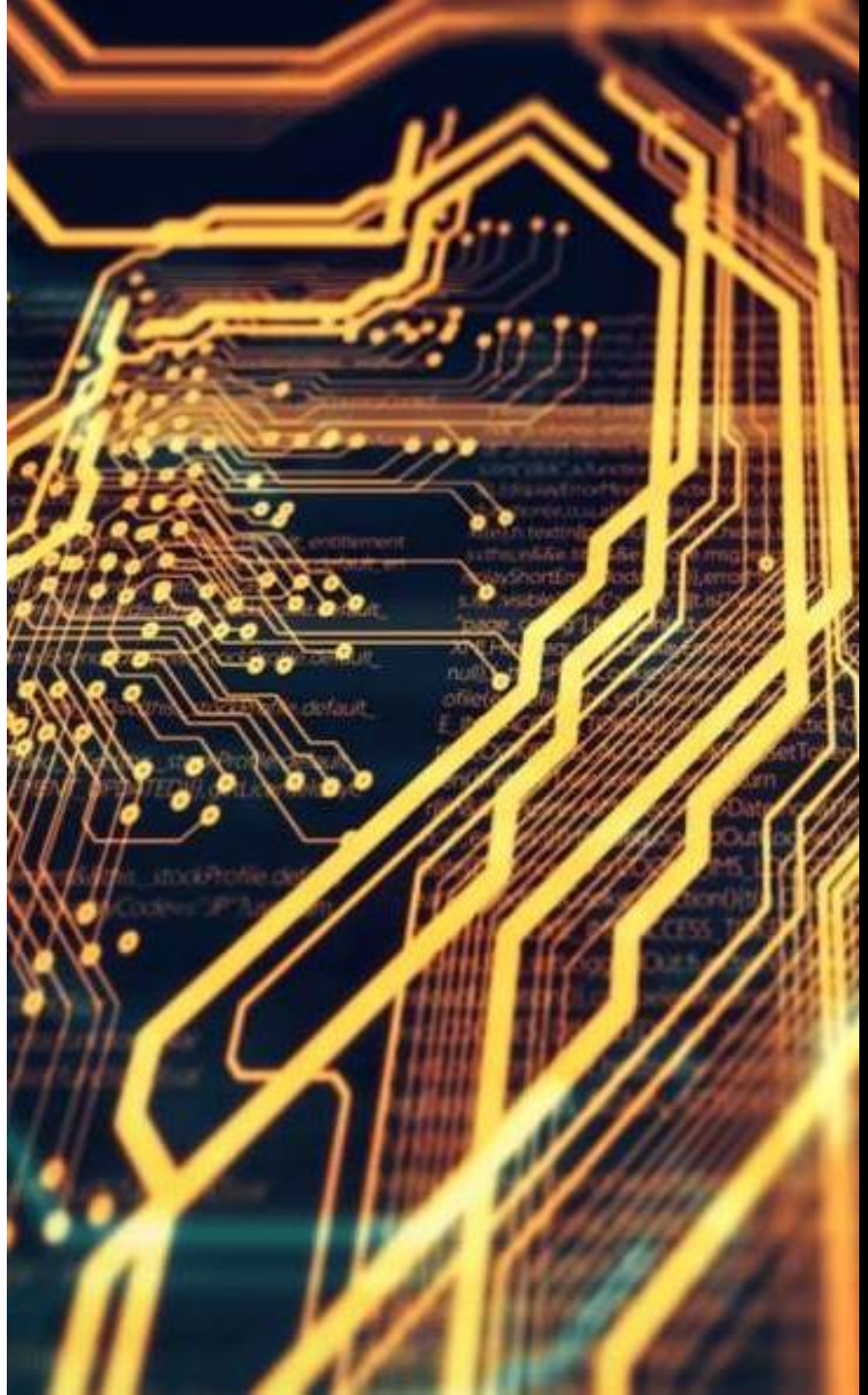
10. Безопасность мобильного банкинга

4. Защита трафика

4.10

Заключение

Внедрение протокола TLS имеет жизненно важное значение для обеспечения безопасности банков и их клиентов в интернет-пространстве. Однако неправильно настроенные веб-серверы могут подвергать данные угрозе вместо того, чтобы защищать их. Наш анализ показал, что на сайтах большинства казахстанских банков настройки SSL/TLS выполнены должным образом. Тем не менее некоторые банки по-прежнему поддерживают устаревшие версии протоколов, что делает их уязвимыми к потенциальным атакам.



1. Доступность сайтов

2. Репутация домена

3. Безопасность HTTP

4. Защита трафика

5. Утечки адресов электронной почты

6. Открытые порты

7. Киберсквоттинг

8. Выполнение требований по защите персональных данных

9. Безопасность почтового сервера

10. Безопасность мобильного банкинга

Утечки адресов электронной почты

5. Утечки адресов электронной почты

05

Утечки данных происходят довольно часто, что является одним из недостатков глобальной цифровизации. Даже в тех случаях, когда организация ответственно подходит к защите своих веб-ресурсов и информационных активов, человеческий фактор по-прежнему подвергает их риску. Сотрудники, не имеющие достаточного уровня цифровой грамотности, часто используют корпоративные электронные адреса для регистрации на сторонних веб-ресурсах. Даже организации, которые уделяют особое внимание вопросам безопасности, подвергаются риску утечки данных, поскольку киберпространство становится все более уязвимым для изощренных кибератак. Веб-ресурс Information is Beautiful опубликовал впечатляющую статистику утечки данных, которая демонстрирует, что многие ведущие организации по всему миру испытывают проблемы с утечками данных, что позволяет злоумышленникам создавать базы данных имен пользователей и паролей путем сбора информации. Некоторые недобросовестные лица пытаются расширить эти базы данных с помощью информации, которую они получают от каждой новой утечки и продают на черном рынке.

Организации должны быть готовы справляться с ситуациями, когда учетные данные сотрудников подвергаются утечке на веб-сайте, где сотрудник зарегистрировался с использованием корпоративной электронной почты. Технически неосведомленные пользователи могут использовать одинаковые или похожие варианты учетных данных в нескольких веб-приложениях, а попавший в общий доступ пароль и пароль от корпоративной электронной почты могут совпадать или отличаться лишь незначительно.

Взломанные корпоративные электронные адреса могут быть использованы злоумышленниками для получения конфиденциальной информации и проведения фишинговых атак. Также существует опасность публикации компрометирующей информации от имени организации. Все эти ситуации подвергают компании риску потерять финансы, доверие клиентов и репутацию.

Существуют ресурсы, которые помогают организациям определить, были ли какие-либо из их учетных записей скомпрометированы во время утечки данных. Любой человек может воспользоваться ресурсом haveibeenpwned.com, чтобы узнать, подвергался ли конкретный адрес электронной почты утечке. Если это произошло, веб-сайт предоставит подробную информацию об инциденте.

1. Доступность сайтов
2. Репутация домена
3. Безопасность HTTP
4. Защита трафика
5. Утечки адресов электронной почты
6. Открытые порты
7. Кибersквоттинг
8. Выполнение требований по защите персональных данных
9. Безопасность почтового сервера
10. Безопасность мобильного банкинга

5. Утечки адресов электронной почты

5.1 Наш поход к оценке

Для целей настоящего отчета мы составили список сотрудников всех местных банков на основе общедоступной информации из социальных сетей (например, LinkedIn). После чего мы использовали автоматизированный инструмент сбора информации и сформировали шаблон электронной почты каждого банка с помощью Hunter.io. Это позволило нам определить список потенциальных корпоративных адресов электронной почты на основе имен и фамилий идентифицированных сотрудников. Мы проверили, была ли электронная почта подвержена утечке с помощью Haveibeenpwned.

Каждый банк был помещен в одну из следующих категорий на основе количества корпоративных адресов электронной почты, которые просочились в Интернет:

1) 5 и менее адресов электронной почты;
2) 6–50 адресов электронной почты;
3) 51–100 адресов электронной почты;
4) более 100 адресов электронной почты.

1. Доступность сайтов
2. Репутация домена
3. Безопасность HTTP
4. Защита трафика
5. Утечки адресов электронной почты
6. Открытые порты
7. Кибersквоттинг
8. Выполнение требований по защите персональных данных
9. Безопасность почтового сервера
10. Безопасность мобильного банкинга

5. Утечки адресов электронной почты

5.2 Результаты

Для того чтобы избежать утечки информации, банкам следует принимать во внимание все риски, должным образом обучать своих сотрудников и повышать их осведомленность в вопросах кибербезопасности.

Данные мероприятия должны проводиться на регулярной основе.

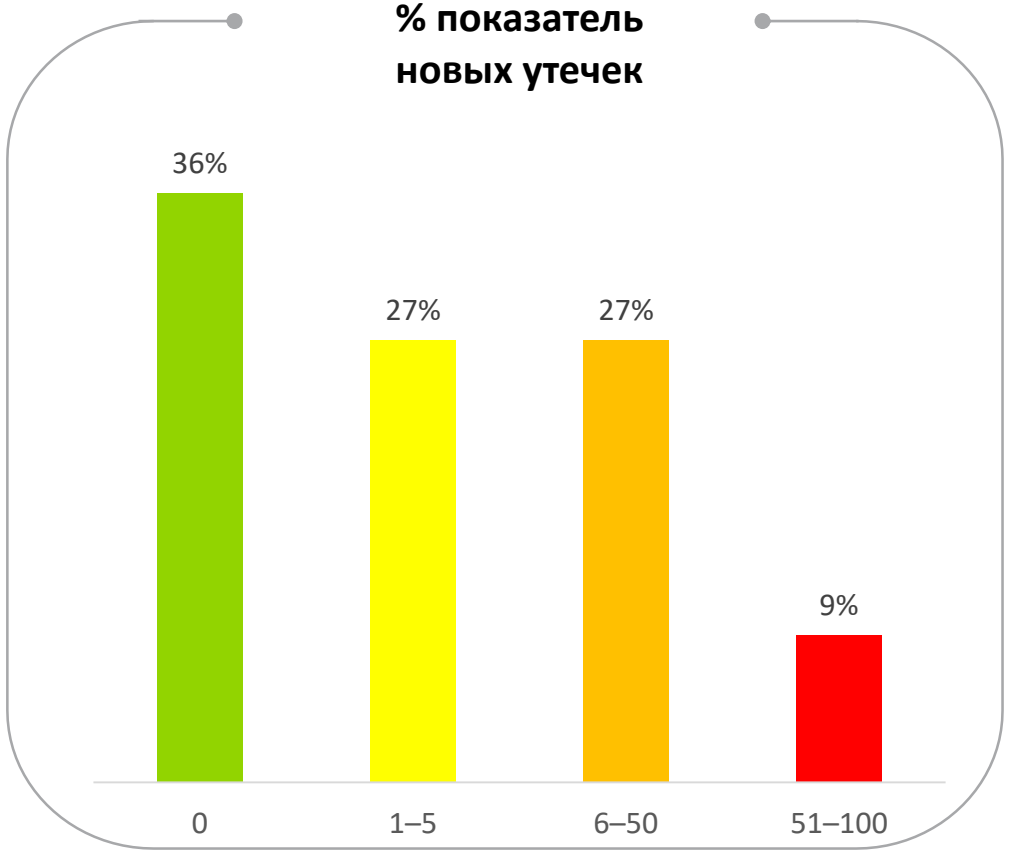
Программы повышения осведомленности по вопросам безопасности должны включать следующие мероприятия:

1) фишинг-тест: оценка текущего уровня информированности сотрудников и областей риска идентификации;

2) интерактивные семинары: повышение осведомленности в сфере информационной безопасности;

3) программы обучения и оценки персонала в различных предметных областях, обеспечивающие им необходимые компетенции в области кибербезопасности;

4) мероприятия по поддержанию культуры безопасности: мониторинг ландшафта и угроз кибербезопасности, поддержка программы в актуальном состоянии.



1. Доступность сайтов
2. Репутация домена
3. Безопасность HTTP
4. Защита трафика
5. Утечки адресов электронной почты
6. Открытые порты
7. Киберсквоттинг
8. Выполнение требований по защите персональных данных
9. Безопасность почтового сервера
10. Безопасность мобильного банкинга

Открытые порты

6. Открытые порты

06

Мы проанализировали внешние доступные порты, которые не являются необходимыми для функционирования веб-сайта. Наличие ненужных открытых портов не обязательно является признаком уязвимости. Однако согласно передовой практике порты и службы, которые не являются обязательными для работы веб-сайта, должны быть закрыты или отфильтрованы с помощью устройства безопасности или программного обеспечения. Веб-сайты требуют, чтобы порты 80 (HTTP) и 443 (HTTPS) функционировали и были доступны.

Для определения состояния портов мы использовали инструмент сканирования Nmap с параметрами легкого сканирования. Для целей данного отчета мы проанализировали только 100 самых распространенных портов.

Результаты нашего теста показали, что из 24 банков у 15 были открыты только необходимые порты, а на остальных девяти веб-серверах также были открыты порты (помимо 80 и 443), которые не обязательны для нормального функционирования веб-сайта.

1. Доступность сайтов
2. Репутация домена
3. Безопасность HTTP
4. Защита трафика
5. Утечки адресов электронной почты
6. Открытые порты
7. Кибersквоттинг
8. Выполнение требований по защите персональных данных
9. Безопасность почтового сервера
10. Безопасность мобильного банкинга

6. Открытые порты

6.1

Заключение

Повышение безопасности веб-серверов за счет сокращения векторов атак должно являться ключевой задачей администраторов. Этого можно достичь, установив и сохранив только необходимые сервисы (порты), которые предоставляют доступ к внутренним и внешним клиентам.

Некоторые администраторы впадают в другую крайность, разрешая использование только порта 443 на своих веб-серверах и блокируя порт 80. Однако открытие порта 80 не повышает вероятности атаки на веб-серверы, поскольку поступающие через него запросы обычно обслуживаются тем же программным обеспечением, которое обеспечивают работу порта 443.

1. Доступность сайтов

2. Репутация домена

3. Безопасность HTTP

4. Защита трафика

5. Утечки адресов электронной почты

6. Открытые порты

7. Кибersквоттинг

8. Выполнение требований по защите персональных данных

9. Безопасность почтового сервера

10. Безопасность мобильного банкинга

Киберсквоттинг

7. Кибersквоттинг

07

Кибersквоттинг — это регистрация доменов, которые копируют названия известных брендов с целью последующей перепродажи, фишинговых атак или незаконного использования для предложения конкурирующих товаров и услуг. Сайты, зарегистрированные кибersквоттерами, могут вводить в заблуждение существующих пользователей, тем самым нанося ущерб репутации организаций.

Многие методы кибersквоттинга могут нанести большой урон банкам. Создание веб-сайта с названием, аналогичным официальному веб-сайту финансовой организации, который содержит публикуемые от ее имени фейковые объявления или новости, может поставить такую организацию и ее бренд в очень сложную ситуацию. Обезопасить себя от подобных рисков компании могут, тщательно анализируя этот метод атаки и практикуя защиту от кибersквоттинга.

Для того чтобы защититься от кибersквоттера, необходимо стать законным владельцем множества доменов, которые звучат как оригинальный товарный знак. Такая мера позволит перенаправить потенциальных посетителей на основной домен и уберечь правообладателей от несанкционированных действий других кибersквоттеров.

Мы проанализировали защитную практику в сфере кибersквоттинга всех 24 местных банков. Контрольный список содержит доменные имена, состоящие из гомоглифов и двухбуквенных вариаций.

Гомоглифы — это знаки, которые графически идентичны или похожи, но имеют разные значения, такие как буква «O» и цифра «0». Гомоглифы также могут возникать в результате использования разных алфавитов. Во время проверки мы использовали следующую таблицу:

l	**1**
o	**0**
l	**j**
m	**rn**
q	**g**
d	**b**

Так, с ее помощью мы построили следующий домен имени сайта «randomsite.kz»:

1) **rand0msite.kz;**
2) **randornsite.kz;**
3) **randomsjte.kz.**

Удвоение букв в доменных именах — еще один эффективный метод кибersквоттинга. Таким образом, доменное имя randomsite.kz может быть изменено на randomsiite.kz, что является незначительным изменением, которое может легко остаться незамеченным. Наша проверка показала, что защитный кибersквоттинг с регистрацией гомоглифических и двухбуквенных вариаций своих доменных имен практикует меньшая часть казахстанских банков. Мы рекомендуем на регулярной основе проводить мониторинг на наличие доменов, компрометирующих безопасность и репутацию банка или угрожающих им.

1. Доступность сайтов
2. Репутация домена
3. Безопасность HTTP
4. Защита трафика
5. Утечки адресов электронной почты
6. Открытые порты
7. Кибersквоттинг
8. Выполнение требований по защите персональных данных
9. Безопасность почтового сервера
10. Безопасность мобильного банкинга

7. Кибersквоттинг

7.1 Заключение

Кибersквоттинг стал прибыльной практикой в Интернете, которая может негативно сказаться на репутации коммерческих брендов. Владельцы таких брендов или товарных знаков могут столкнуться с юридическими проблемами при попытке бороться с кибersквоттингом, поскольку бывает сложно установить, являются ли такие действия незаконными, так как это явление сочетает в себе как законную, так и незаконную деятельность.

Хотя споры о доменных именах, возникающие в результате кибersквоттинга и связанных с ним практик, могут быть разрешены с помощью процедур Uniform Domain Name Resolution Policy, превентивные меры позволяют их владельцам избежать финансовых затрат, необходимых для инициирования этого процесса. Владельцы товарных знаков могут заранее позаботиться о регистрации доменных имен, похожих на их товарные знаки, тем самым предупредив действия кибersквоттеров. Однако наш анализ показывает, что такая практика не распространена среди местных банков и не является частью их стратегии кибербезопасности, что может привести к реализации широкого спектра киберрисков.

1. Доступность сайтов
2. Репутация домена
3. Безопасность HTTP
4. Защита трафика
5. Утечки адресов электронной почты
6. Открытые порты
7. Кибersквоттинг
8. Выполнение требований по защите персональных данных
9. Безопасность почтового сервера
10. Безопасность мобильного банкинга

Выполнение требований по защите персональных данных

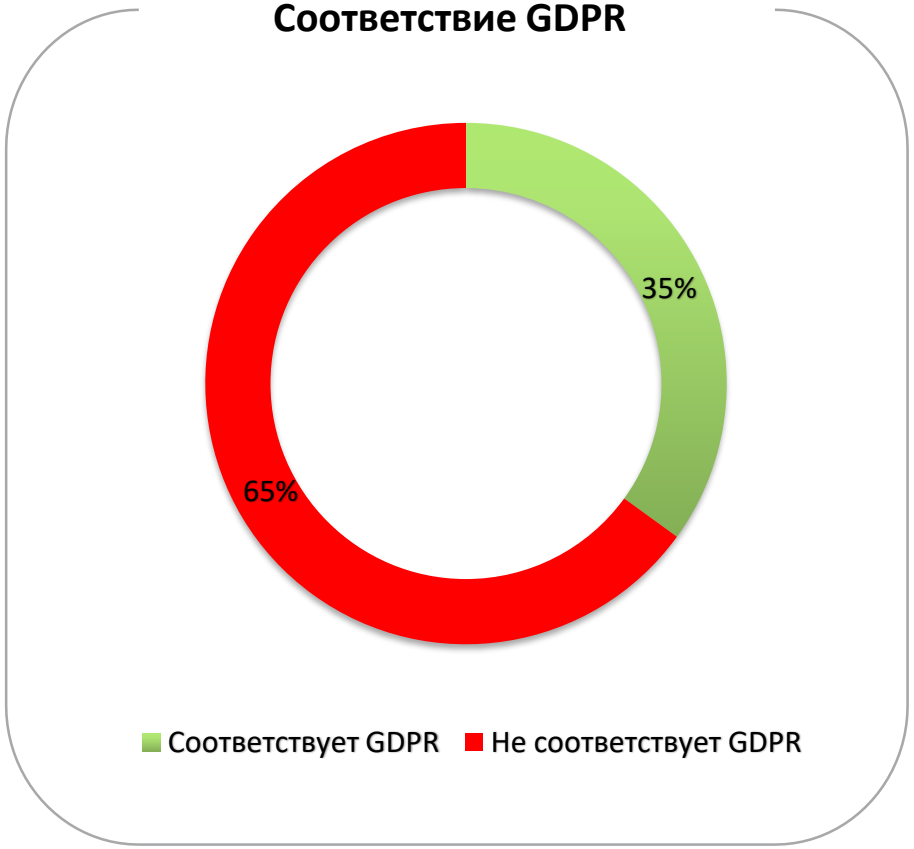
8. Выполнение требований по защите персональных данных

08

GDPR, или Общее положение о защите персональных данных, — это постановление ЕС о защите данных и конфиденциальности, которое распространяется на всех лиц, находящихся на территории Европейского союза. GDPR касается любых работ и услуг, связанных со сбором и обработкой персональных данных людей, проживающих на территории ЕС.

Согласно регламенту Европейской комиссии к персональным данным относится любая информация о человеке, независимо от того, связана ли она с его частной, профессиональной или общественной жизнью. К такой информации относится, например, имя, домашний адрес, фотография, адреса электронной почты, банковская информация, сообщения в социальных сетях, медицинская информация или IP-адрес. Это означает, что веб-сайты не должны собирать статистические данные и личную информацию или хранить ненужные файлы cookie для технической работы сайта без предварительного согласия со стороны пользователя.

Наш обзор веб-сайтов 24 банков показал, что 35% из них были приведены в соответствие с требованиями GDPR. Остальные 65% не соответствуют данным требования.



1. Доступность сайтов
2. Репутация домена
3. Безопасность HTTP
4. Защита трафика
5. Утечки адресов электронной почты
6. Открытые порты
7. Кибersквоттинг
8. Выполнение требований по защите персональных данных
9. Безопасность почтового сервера
10. Безопасность мобильного банкинга

8. Выполнение требований по защите персональных данных

8.1 Заключение

Законодательство Республики Казахстан не обязывает юридические лица, предоставляющие финансовые услуги, соблюдать требования GDPR. Однако в пункте 2 статьи 3 GDPR, который касается территориального охвата, говорится, что даже компании, созданные за пределами ЕС, подпадают под действие требований GDPR, если они предлагают товары или услуги реальным лицам (субъектам данных), проживающим в ЕС, или отслеживают поведение таких лиц, независимо от того, требуется ли оплата от субъекта данных. Другими словами, если какой-либо банк хранит данные хотя бы одного клиента из Европы, он автоматически попадает под действие GDPR.

Более того, соответствие требованиям GDRP может стать решающим фактором для потенциальных клиентов (особенно если они из ЕС), которые ищут поставщика финансовых услуг в Казахстане.

1. Доступность сайтов
2. Репутация домена
3. Безопасность HTTP
4. Защита трафика
5. Утечки адресов электронной почты
6. Открытые порты
7. Киберсквоттинг
8. Выполнение требований по защите персональных данных
9. Безопасность почтового сервера
10. Безопасность мобильного банкинга

Безопасность почтового сервера

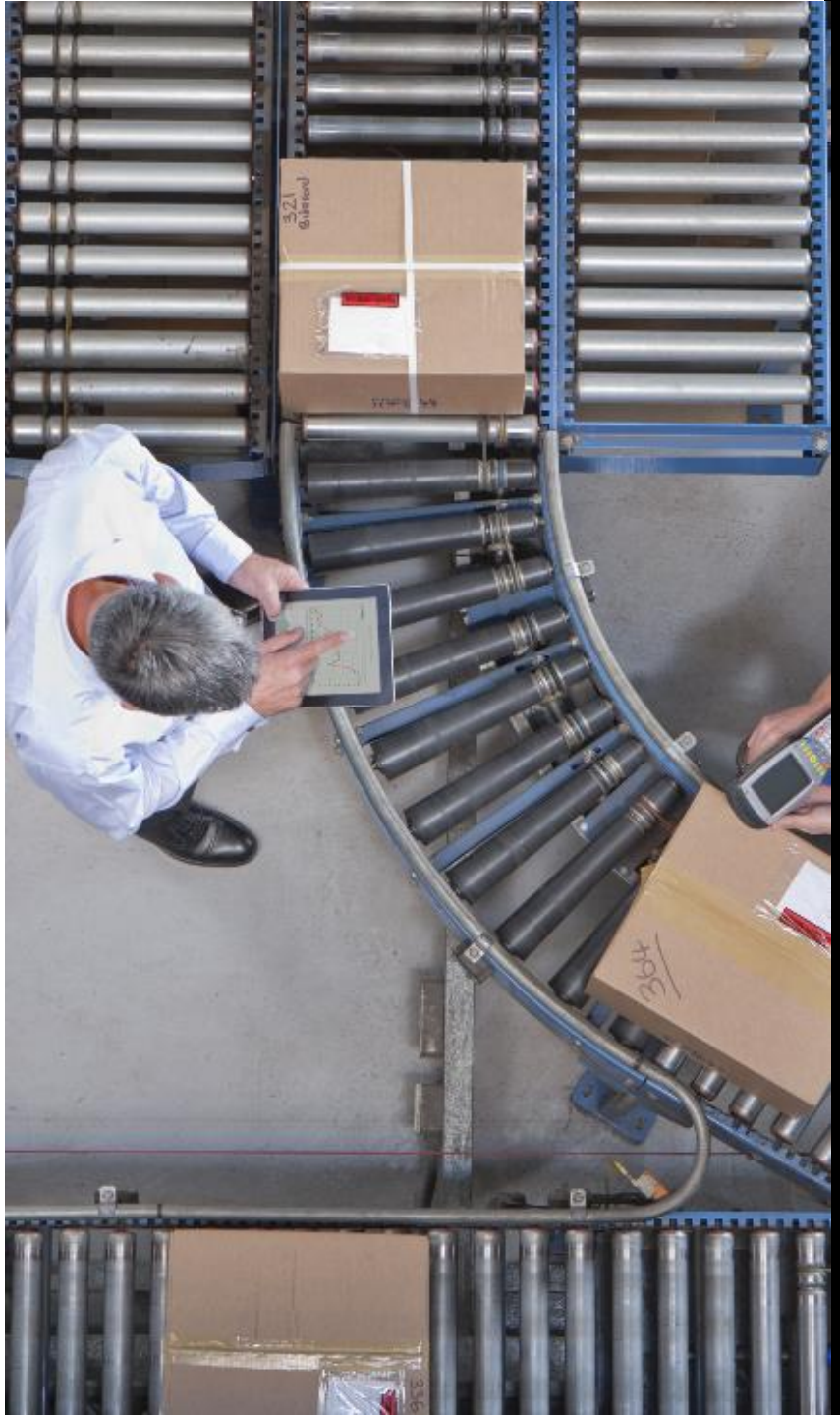
9. Безопасность почтового сервера

09

Распространенной точкой входа для злоумышленников, стремящихся закрепиться в корпоративной сети и получить ценные банковские данные, является электронная почта. Основная проблема при использовании электронной почты — ее небезопасность. Уязвимости, связанные с электронной почтой, развязывают руки злоумышленникам в причинении неудобств и различного рода проблем, компрометирующих компанию, будь то спам-сообщения, вредоносные программы, фишинговые атаки, изощренные целевые атаки или утечка корпоративных адресов электронной почты в общий доступ. Поскольку большинство организаций используют электронную почту для ведения бизнеса, один из приоритетных векторов атак хакеров часто направлен именно на нее.

Прежде чем прибегать к комплексным методам защиты, важно убедиться, что применяются базовые параметры обеспечения безопасности сотрудников компании и общего повышения репутации электронной почты. Так, в большинстве случаев фильтры спама будут игнорировать письма, отправленные с домена банка, не воспринимая их, как вредоносные.

Для анализа основных настроек безопасности почтовых серверов мы составили список почтовых (MX) серверов по доменному имени каждого банка (с помощью MX Lookup). Следующим нашим шагом стала проверка настройки безопасности каждого сервера с помощью инструмента диагностики SMTP с сайта mxtoolbox.com.



1. Доступность сайтов

2. Репутация домена

3. Безопасность HTTP

4. Защита трафика

5. Утечки адресов электронной почты

6. Открытые порты

7. Кибersквоттинг

8. Выполнение требований по защите персональных данных

9. Безопасность почтового сервера

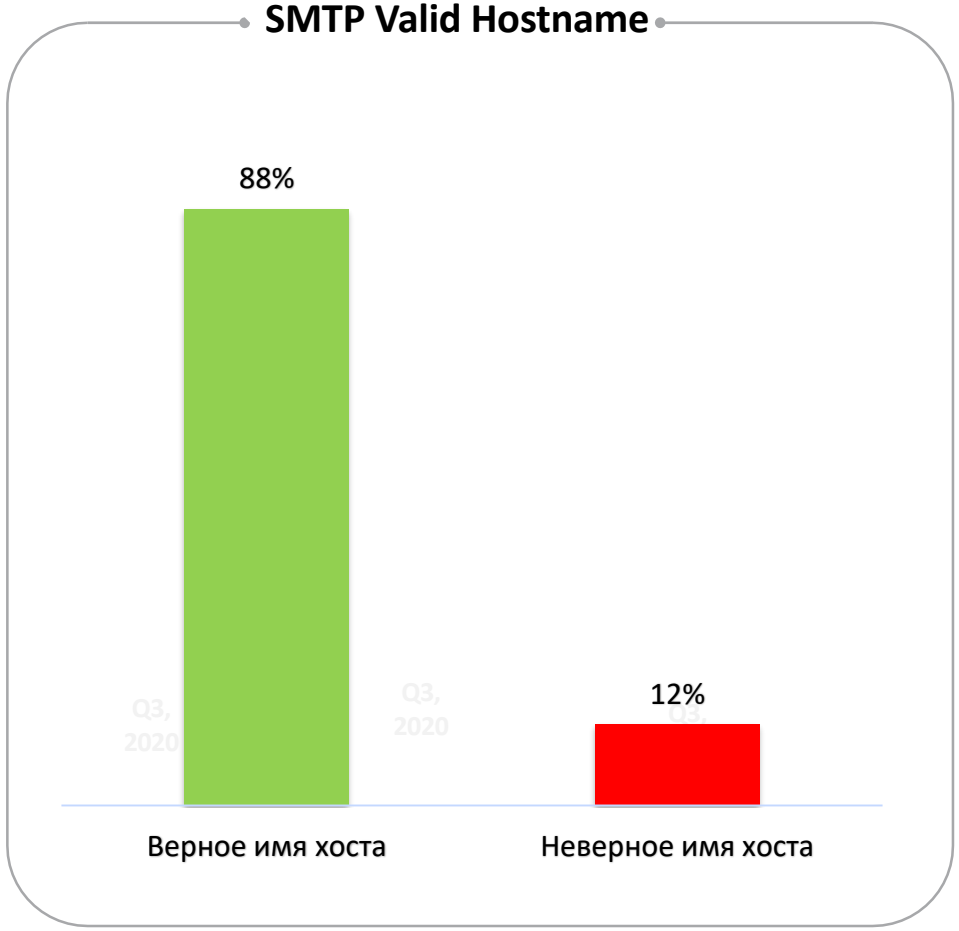
10. Безопасность мобильного банкинга

9. Безопасность почтового сервера

9.1 SMTP-проверка имени хоста

Тест позволяет проверить, является ли обратная запись DNS (PTR) допустимым именем хоста. Согласно лучшим практикам отправки электронной почты запись PTR должна быть действительным именем хоста. Если запись PTR не является действительным именем хоста, существует вероятность возникновения проблем при доставке электронной почты посредством служб защиты от спама.

Согласно результатам нашего тестирования 88% банков получили рейтинг «верное имя хоста», и 12% — рейтинг «неверное имя хоста».



1. Доступность сайтов
2. Репутация домена
3. Безопасность HTTP
4. Защита трафика
5. Утечки адресов электронной почты
6. Открытые порты
7. Кибersквоттинг
8. Выполнение требований по защите персональных данных
9. Безопасность почтового сервера
10. Безопасность мобильного банкинга

9. Безопасность почтового сервера

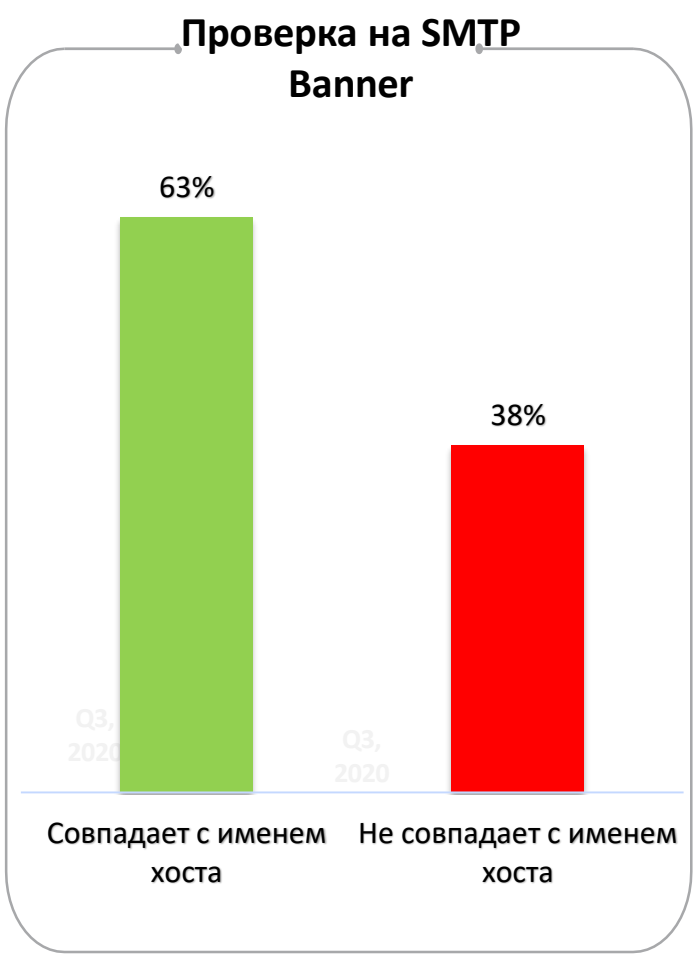
9.2 Проверка на SMTP Banner

Серверы электронной почты отвечают на соединения через порт 25 с помощью строки текста, который называется SMTP-баннер. Основная цель — объявить сервер и любую информацию, которую администратор хотел бы передать во вне. Лучше всего указать имя вашего сервера в баннере SMTP, чтобы любой, кто подключается через ваш IP-адрес, имел представление о том, к кому он обращается. Вы получите предупреждение, если имя, под которым вы себя представляете, находится не в том же домене, что и имя хоста, которое мы получаем.

Некоторое время назад многие серверы «маскировали» свои баннеры SMTP, заменяя символы звездочками для всех, кто находится за пределами их сети. Логика, лежащая в основе этого, заключалась в том, что владельцы не хотели транслировать какую-либо информацию о своей сети пользователям извне из-за страха предоставить им данные, которые могли бы помочь при атаке на сервер. Выгоды от этого минимальны, и многие серверы выполняют проверку баннеров как часть защиты от спама, поэтому такая практика сопряжена с отрицательными затратами.

Некоторые почтовые серверы могут использовать несоответствующий или замаскированный баннер как индикатор возможного источника спама в системе подсчета очков, но большинство не будет отклонять входящую почту исключительно на этом основании. Если у вас нет записи PTR или ваша запись не совпадает с вашим именем хоста, мы рекомендуем вам связаться с интернет-провайдером и попросить настроить обратную (PTR) запись, которая соответствует имени хоста вашего почтового сервера.

Согласно результатам нашего тестирования, 63% имен хостов банков совпадают с обратной записью (PTR), а 38% — не совпадают.



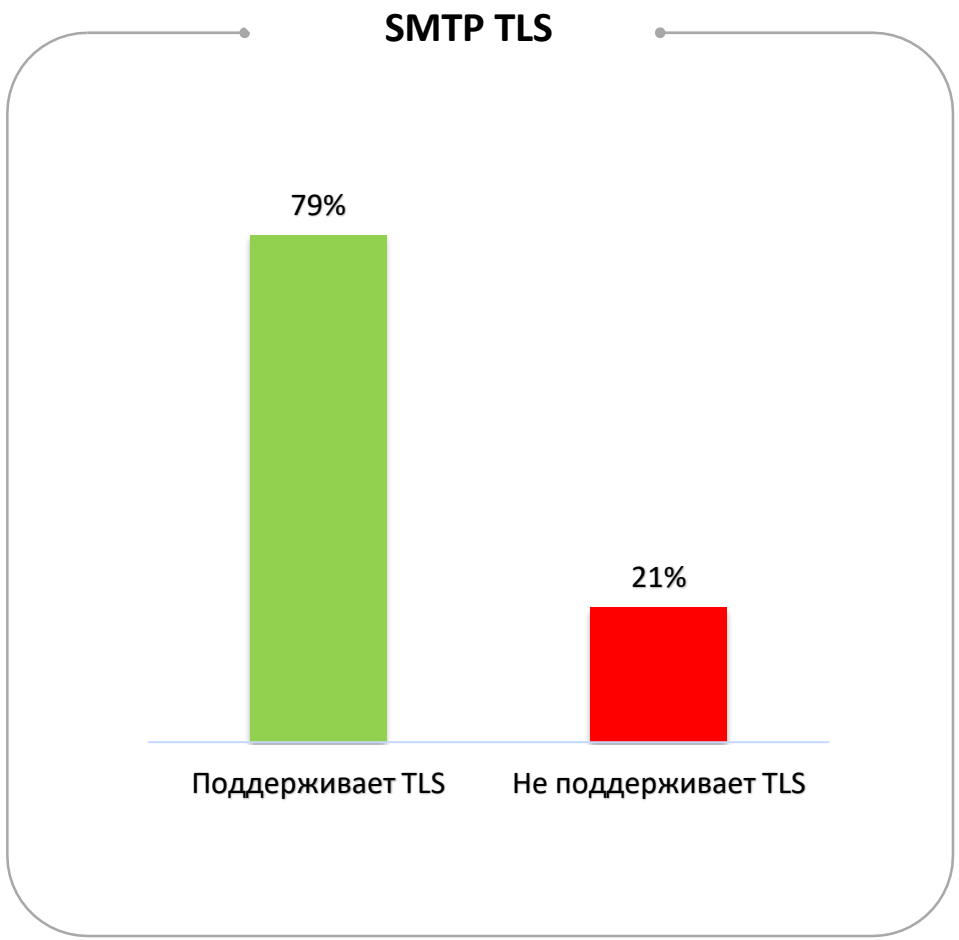
1. Доступность сайтов
2. Репутация домена
3. Безопасность HTTP
4. Защита трафика
5. Утечки адресов электронной почты
6. Открытые порты
7. Киберсквоттинг
8. Выполнение требований по защите персональных данных
9. Безопасность почтового сервера
10. Безопасность мобильного банкинга

9. Безопасность почтового сервера

9.3 SMTP TLS

Протокол TLS расшифровывается как Transport Layer Security и позволяет почтовым серверам обмениваться электронными письмами через зашифрованное соединение с использованием того же механизма, что и HTTPS, для защиты веб-трафика. Во всех случаях, кроме нескольких, вы все равно сможете отправлять и получать электронную почту, но ваши сообщения будут передаваться в виде обычного текста без шифрования TLS.

По результатам нашего исследования 79% банков поддерживают протокол TLS. Однако 21% заявили об отсутствии его поддержки. Это означает, что после подключения к такому почтовому серверу и запроса с помощью команды EHLO для определения того, какие команды и протоколы он поддерживает, в его ответе на ваш запрос будет отсутствовать строка «250-STARTTLS», указывающая на поддержку сервером протокола TLS.



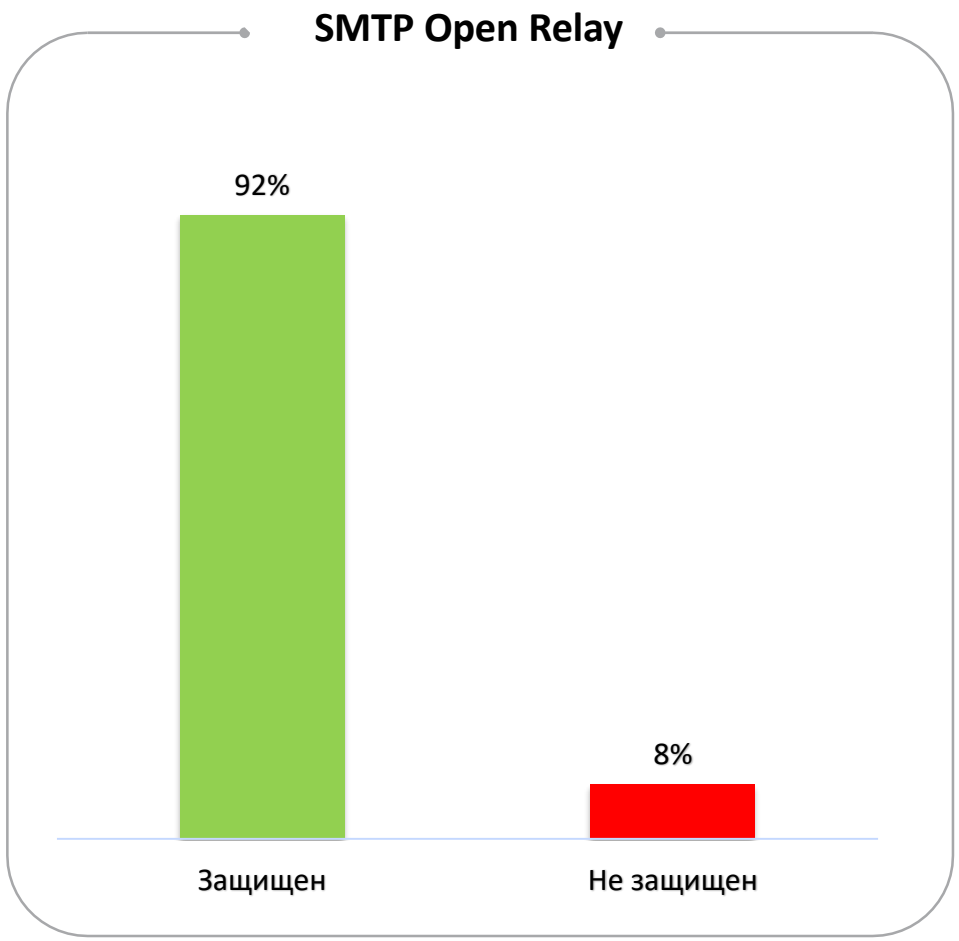
1. Доступность сайтов
2. Репутация домена
3. Безопасность HTTP
4. Защита трафика
5. Утечки адресов электронной почты
6. Открытые порты
7. Киберсквоттинг
8. Выполнение требований по защите персональных данных
9. Безопасность почтового сервера
10. Безопасность мобильного банкинга

9. Безопасность почтового сервера

9.4 SMTP Open Relay

Многие почтовые серверы сегодня имитируют прием неправильно адресованных писем, но затем отклоняют такие сообщения, не пересылая отправителю ответ на них. Этот метод используется для предотвращения директори-атак по сбору информации. При данной атаке злоумышленник отправляет вам тысячи автоматически сгенерированных сообщений электронной почты на адреса из вашего домена в попытках найти действительные. Если ваш сервер ответит с ошибкой (5xx), злоумышленник поймет, что это не настоящий адрес электронной почты. Если ваш сервер примет сообщение (2xx), злоумышленник поймет, что этот адрес настоящий.

В ходе анализа мы имитировали отправку сообщения на поддельный адрес электронной почты test@example.kz. Далее на основании полученных ответов мы определяли, является ли сервер открытым ретранслятором. В случае положительного ответа это означало бы, что он принимает почту в домены, за которые не несет ответственности, а затем передает ее соответствующему серверу. Если сервер ответил кодом 200 на нашу команду RCPT TO, это не означает, что он работает с SMTP Open Relay (сервером без авторизации), это означает только то, что он можете быть открытым ретранслятором.
По результатам нашего тестирования, 92% банков получили рейтинг «защищен», 8% — «не защищен».



1. Доступность сайтов
2. Репутация домена
3. Безопасность HTTP
4. Защита трафика
5. Утечки адресов электронной почты
6. Открытые порты
7. Кибersквоттинг
8. Выполнение требований по защите персональных данных
9. Безопасность почтового сервера
10. Безопасность мобильного банкинга

9. Безопасность почтового сервера

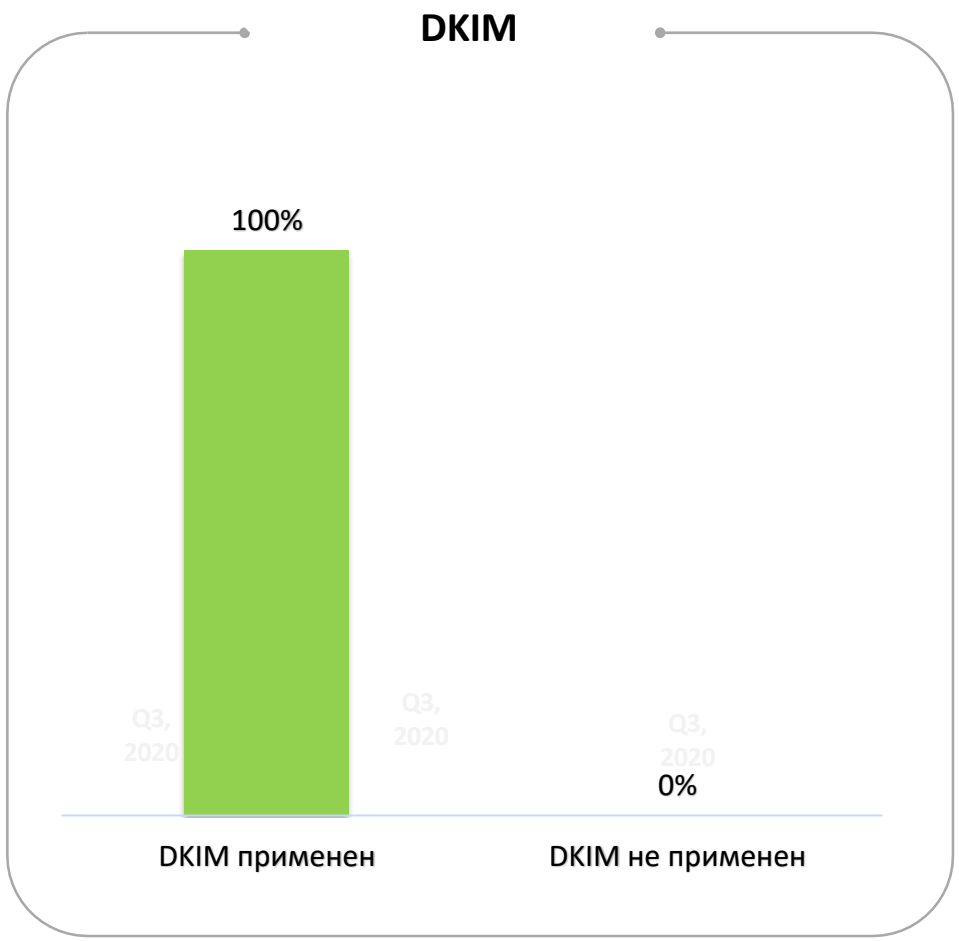
9.5

DomainKeys Identified Mail

Технология DKIM используется для предотвращения спуфинга при отправке писем из вашего домена.

Спуфингом называется разновидность сетевой атаки с использованием электронной почты, при которой злоумышленник выдает себя за другое лицо. Для того чтобы предотвратить спуфинг, некоторые серверы электронной почты требуют подтверждения подлинности отправителя с помощью ключа DKIM.

Технология DKIM позволяет добавлять в заголовки всех исходящих сообщений зашифрованную подпись. Серверы электронной почты расшифровывают заголовки входящих сообщений и проверяют, не менялось ли сообщение после отправки.
Подписи DKIM повышают уровень безопасности электронной почты и помогают предотвращать спуфинг. Согласно результатам нашего обзора во всех банках используется собственный ключ DKIM для всех исходящих сообщений.



1. Доступность сайтов
2. Репутация домена
3. Безопасность HTTP
4. Защита трафика
5. Утечки адресов электронной почты
6. Открытые порты
7. Кибersквоттинг
8. Выполнение требований по защите персональных данных
9. Безопасность почтового сервера
10. Безопасность мобильного банкинга

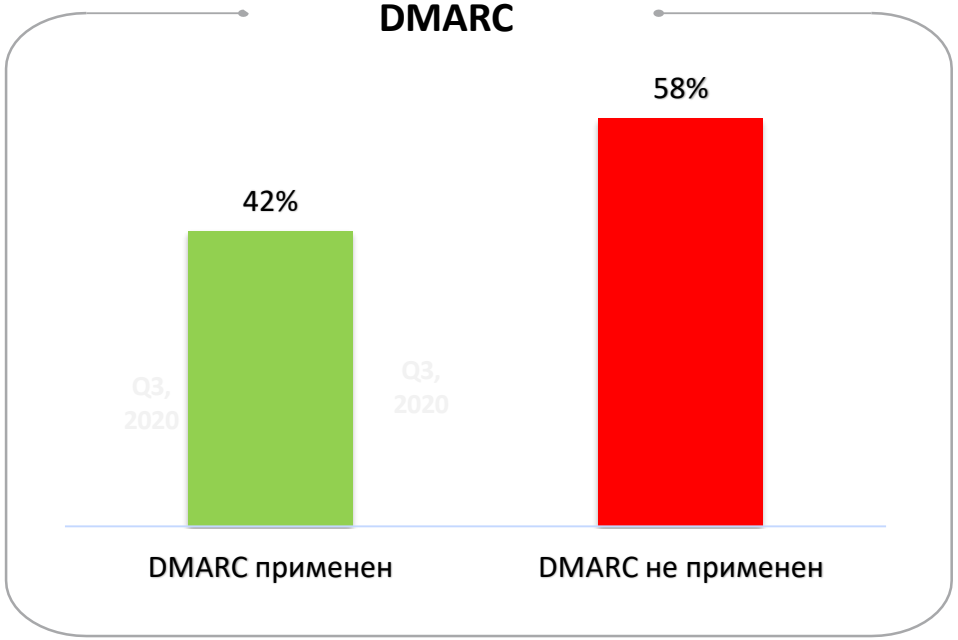
9. Безопасность почтового сервера

9.6 Механизм Domain-based Message Authentication Reporting and Conformance

DMARC — один из механизмов защиты компании от фишинга с использованием имени ее домена. Смысл фишинговой атаки заключается в отправке мошеннического письма якобы от лица известной компании. Фактически же на устройство пользователя загружается вирус, и происходит кража личных данных — логинов и паролей, данных кредитных карт, номеров телефона и т. п. Сами письма маскируются под легальные рассылки, и важную роль тут играет использование основного домена атакуемого банка.
Проверяется, соответствует ли домен электронного адреса в строке «От:» идентификаторам проверки SPF и подписи DKIM. Если совпадение полное, письмо отправляется во входящие получателя. Если же есть сомнения, оно обрабатывается согласно выбранной политике DMARC:

- «none» — письмо попадает во входящие получателя. Владельцу домена приходит отчет с информацией об отправке сообщения для анализа, кто отправляет письма от данного имени и разрешено ли им это делать;
- «quarantine» — почтовый сервер получателя отправляет письмо в папку «Спам», владельцы домена продолжают анализировать данные;
- «reject» — письма, не прошедшие проверку DMARC, отклоняются и не попадают ни в одну папку почтового ящика получателя. Устанавливая данный тип политики, убедитесь, что третьи лица, которым разрешено отправлять сообщения от вашего имени, добавлены в белый список, иначе их письма также будут отклонены. Это относится и к CRM-системам, и к сервисам почтовых рассылок.

Для того чтобы проверить, применяются ли мониторинговые инструменты для домена, мы использовали ресурс dmarcian.com. Результат обзора показал, что большая часть местных банков не использует данный механизм защиты (58%).



1. Доступность сайтов
2. Репутация домена
3. Безопасность HTTP
4. Защита трафика
5. Утечки адресов электронной почты
6. Открытые порты
7. Кибersквоттинг
8. Выполнение требований по защите персональных данных
9. Безопасность почтового сервера
10. Безопасность мобильного банкинга

9. Безопасность почтового сервера

9.7 Заключение

Согласно результатам нашего исследования высокие показатели в каждой из тестируемых категорий дают основание полагать, что подавляющее большинство рассмотренных банков понимают важность защиты своей электронной почты.

Слабым местом для четверти участников национального финансового сектора оказалось неразглашение имени своего сервера, как попытка скрыть конфиденциальную информацию. Подобная практика некоторое время назад могла считаться обоснованной. Однако сейчас объявление организацией имени своего сервера оказывает положительное влияние на безопасность, поскольку в данном случае все стороны, участвующие в пересылке писем и непосредственной переписке, могут быть уверены в том, что общаются с представителями компании, а не со злоумышленниками.

Также мы рекомендуем банкам уделить внимание развитию функций выявления почтовым сервером реального отправителя письма.

1. Доступность сайтов

2. Репутация домена

3. Безопасность HTTP

4. Защита трафика

5. Утечки адресов электронной почты

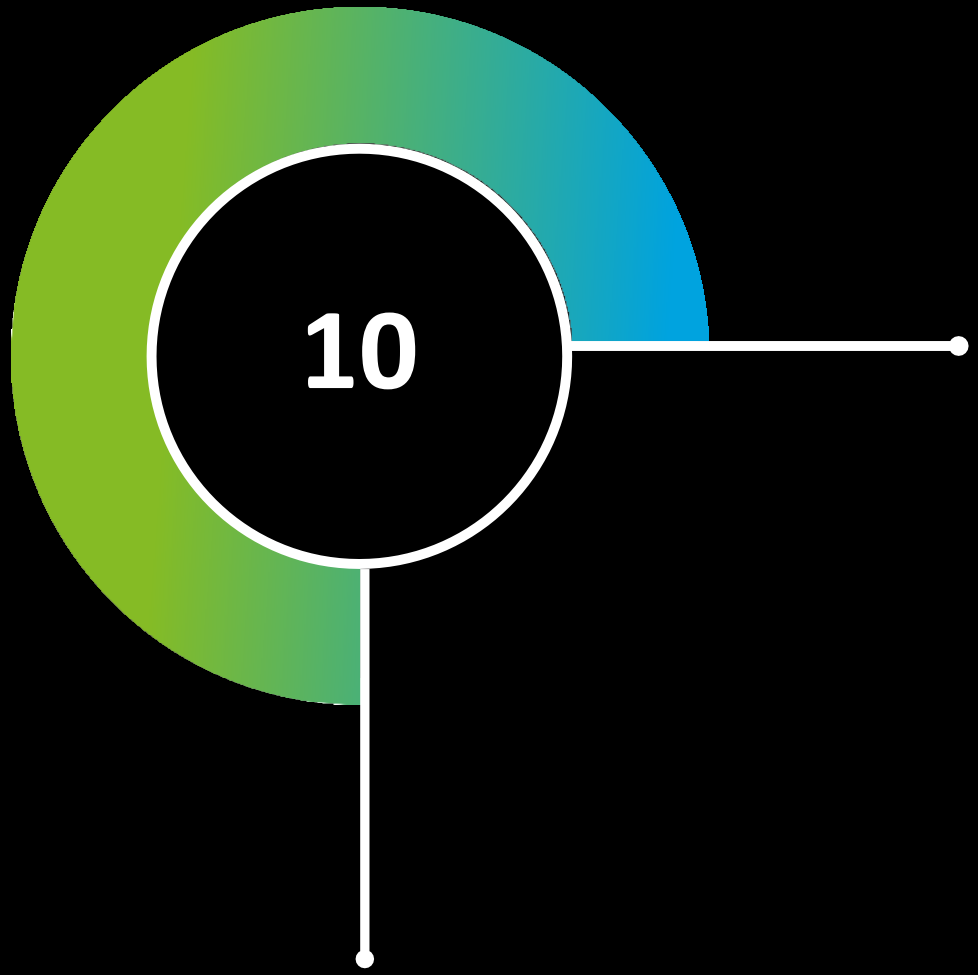
6. Открытые порты

7. Кибersквоттинг

8. Выполнение требований по защите персональных данных

9. Безопасность почтового сервера

10. Безопасность мобильного банкинга



Безопасность мобильного банкинга

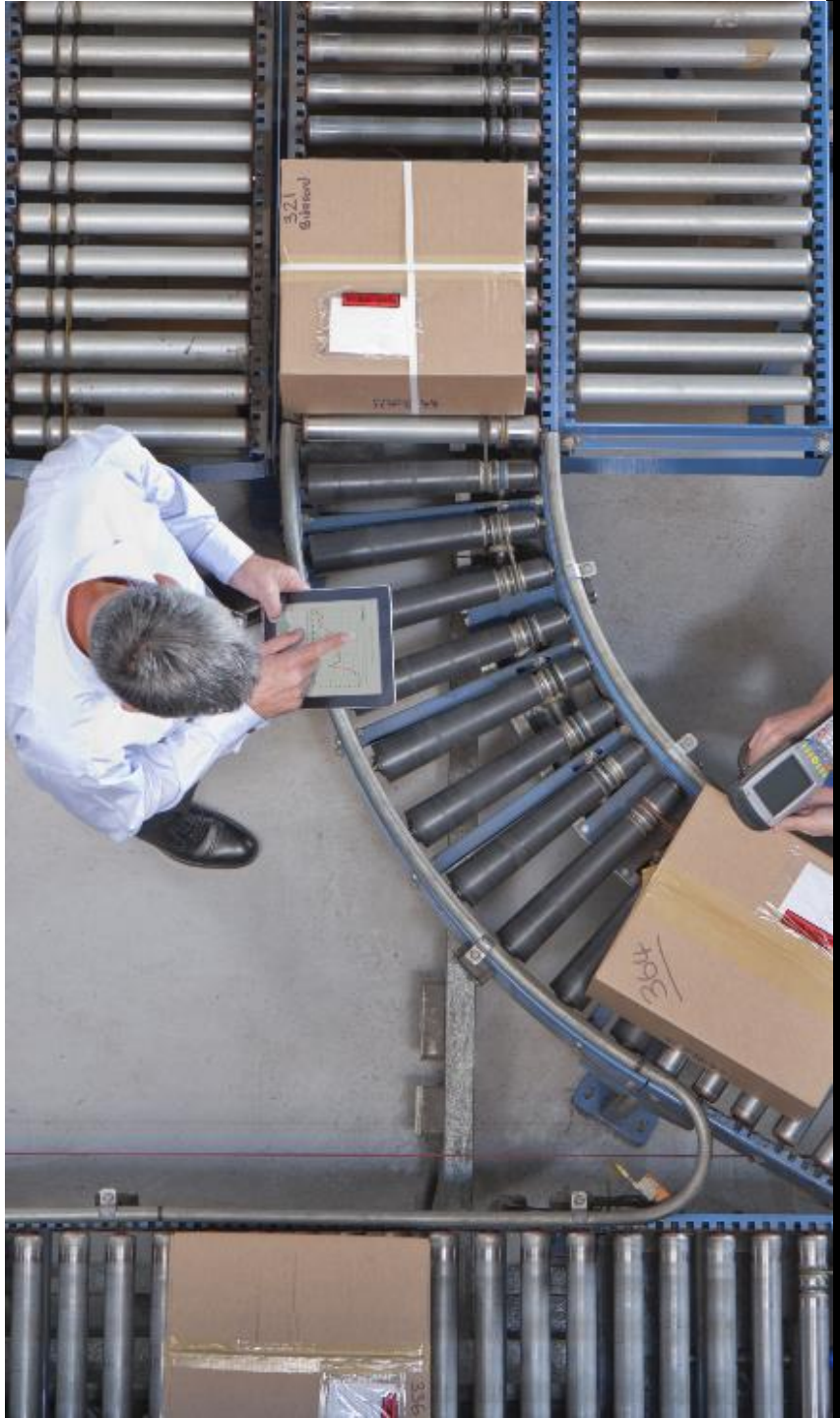
10. Безопасность мобильного банкинга

10

На сегодняшний день большинство банков предлагают своим клиентам доступ к финансовым услугам на базе мобильных решений. Это позволило существенно улучшить удобство и доступность банковских услуг в Казахстане. Однако наряду с безусловными выгодами специфичность и достаточная открытость мобильных платформ делает пользователей мобильных устройств удобной целью для злоумышленников. К тому же для таких платформ уже разработан целый арсенал хакерских программ и инструментов, включая вирусы, трояны, поддельные банковские программы, программы-вымогатели и всевозможные программы-шпионы. Это заставляет разработчиков банковских мобильных приложений помимо функциональности и удобства использования уделять серьезное внимание обеспечению высокого уровня безопасности.

С целью изучения банковских мобильных приложений мы сосредоточили усилия на анализе операционной системы Android, поскольку доля пользователей этой платформы, как правило, более существенная. В нашу выборку вошли 19 банков, у которых публично доступно соответствующее мобильное приложение. В ходе тестирования мы проанализировали следующие аспекты:

1) применение механизмов SSL Pinning;
2) раскрытие конфиденциальной информации в автоматически генерируемых скриншотах;
3) проверка защитных механизмов безопасности.



1. Доступность сайтов
2. Репутация домена
3. Безопасность HTTP
4. Защита трафика
5. Утечки адресов электронной почты
6. Открытые порты
7. Кибersквоттинг
8. Выполнение требований по защите персональных данных
9. Безопасность почтового сервера
10. Безопасность мобильного банкинга

10. Безопасность мобильного банкинга

10.1 SSL Pinning

Банковские мобильные решения в основном используют клиент-серверную архитектуру. В роли клиента выступает приложение, установленное на мобильное устройство, а роль сервера выполняет веб-приложение банка. Взаимодействие между мобильным клиентом и веб-сервером осуществляется через Интернет. В это связи обеспечение безопасности передаваемых данных от MITM-атак имеет решающее значение для онлайн-банкинга. Использование защитных механизмов протокола HTTPS позволяет справится с этой задачей.

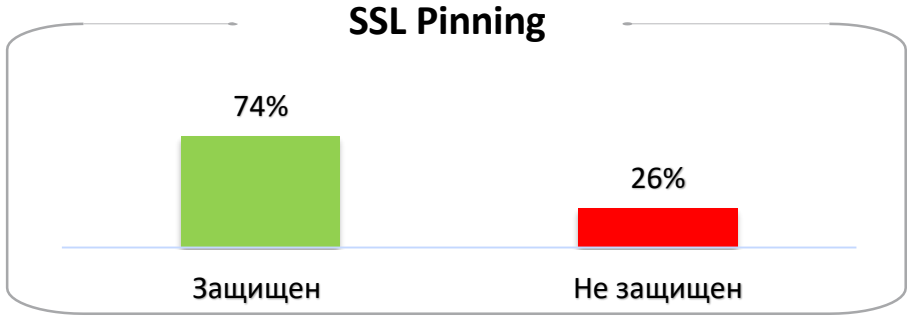
По умолчанию, устанавливая SSL-соединение по протоколу HTTPS, клиент проверяет сертификат сервера по двум критериям:

1) возможность проследить всю цепочку SSL-сертификата, от вашего личного SSL-сертификата через промежуточные до корневого сертификата доверенного удостоверяющего центра;
2) соответствие имени сервера в SSL-сертификате серверу, с которым установлено соединение.

Однако встроенный механизм сопоставления клиентом SSL-сертификатов из хранилища доверенных сертификатов устройства и тех, которые используются на веб-сервере, открывает потенциальную уязвимость. Это связано с тем, что хранилище сертификатов на устройстве можно легко скомпрометировать, просто установив небезопасный сертификат. В рамках своего исследования мы проверили мобильные приложения банков на предмет реализации механизмов SSL pinning.

SSL pinning — это внедрение SSL-сертификата, который используется на сервере, в код мобильного приложения. В этом случае приложение будет игнорировать хранилище сертификатов устройства, полагаясь только на свое хранилище. Это позволит создать защищенное SSL-соединение с банковским веб-сервером. В дополнение pinning SSL сертификата также позволяет создавать доверительное соединение с сервером, на котором установлен самоподписанный SSL-сертификат, без необходимости устанавливать дополнительный сертификат на мобильное устройство пользователя.

Результаты анализа показали, что чуть больше четверти (26%) казахстанских банков не применяют SSL pinning, остальные 74% используют этот механизм для защиты передаваемых данных в своих мобильных приложениях.



1. Доступность сайтов
2. Репутация домена
3. Безопасность HTTP
4. Защита трафика
5. Утечки адресов электронной почты
6. Открытые порты
7. Кибersквоттинг
8. Выполнение требований по защите персональных данных
9. Безопасность почтового сервера
10. Безопасность мобильного банкинга

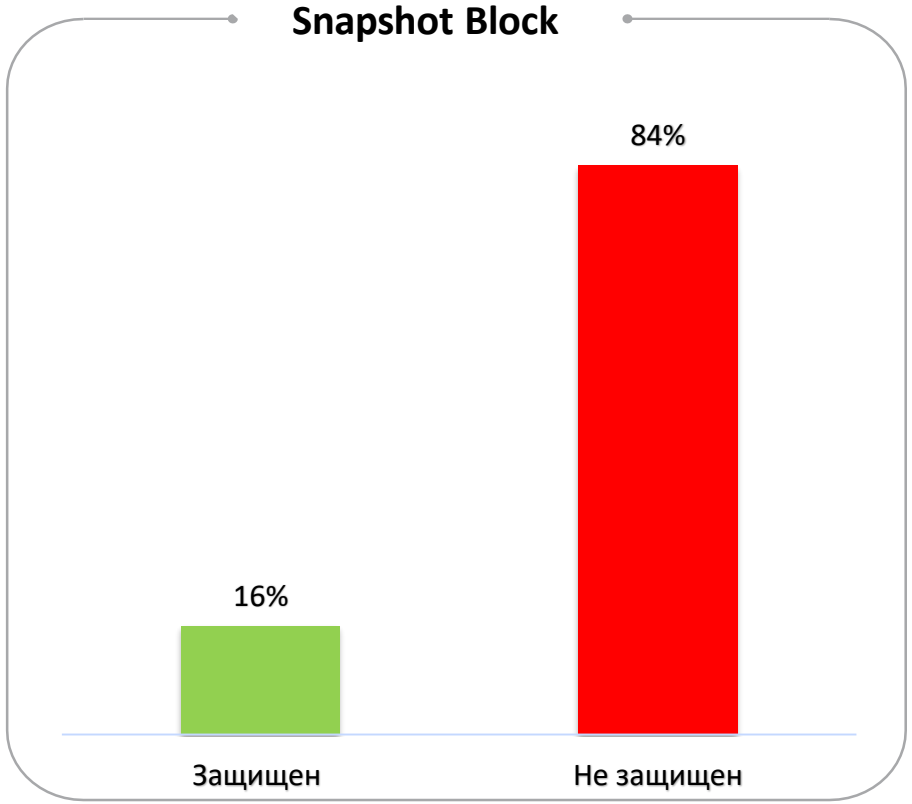
10. Безопасность мобильного банкинга

10.2 Раскрытие конфиденциальной информации в автоматически генерируемых скриншотах

Для отображения приложений, работающих на мобильном устройстве в фоновом режиме, встроенный механизм Android делает автоматический скриншот экрана приложения при переключении. Эта стандартная функция потенциально представляет собой риск для конфиденциальности, поскольку на снимок экрана могут попасть критичные данные. А те, в свою очередь, хранятся в локальном хранилище и остаются неизменными до тех пор, пока приложение не будет закрыто.

На практике встречаются шпионские программы, которые зачастую устанавливает сам пользователь, например путем «Root-тирования» устройства. Данные вредоносные программы выполняют сбор скриншотов фоновых приложений и их последующую передачу злоумышленнику. Для защиты данных в таких случаях разработчики прибегают к различным способам: например, размывают изображение на скриншоте, делая его недоступным для прочтения, или подменяют такое изображение на стандартное, на котором нет отображения каких-либо конфиденциальных данных.

Результаты нашего анализа указывают на то, что 84% банковских приложений не скрывают конфиденциальную информацию на автоматически генерируемых снимках экрана, и только в 16% случаев используются механизмы защиты.



1. Доступность сайтов
2. Репутация домена
3. Безопасность HTTP
4. Защита трафика
5. Утечки адресов электронной почты
6. Открытые порты
7. Кибersквоттинг
8. Выполнение требований по защите персональных данных
9. Безопасность почтового сервера
10. Безопасность мобильного банкинга

10. Безопасность мобильного банкинга

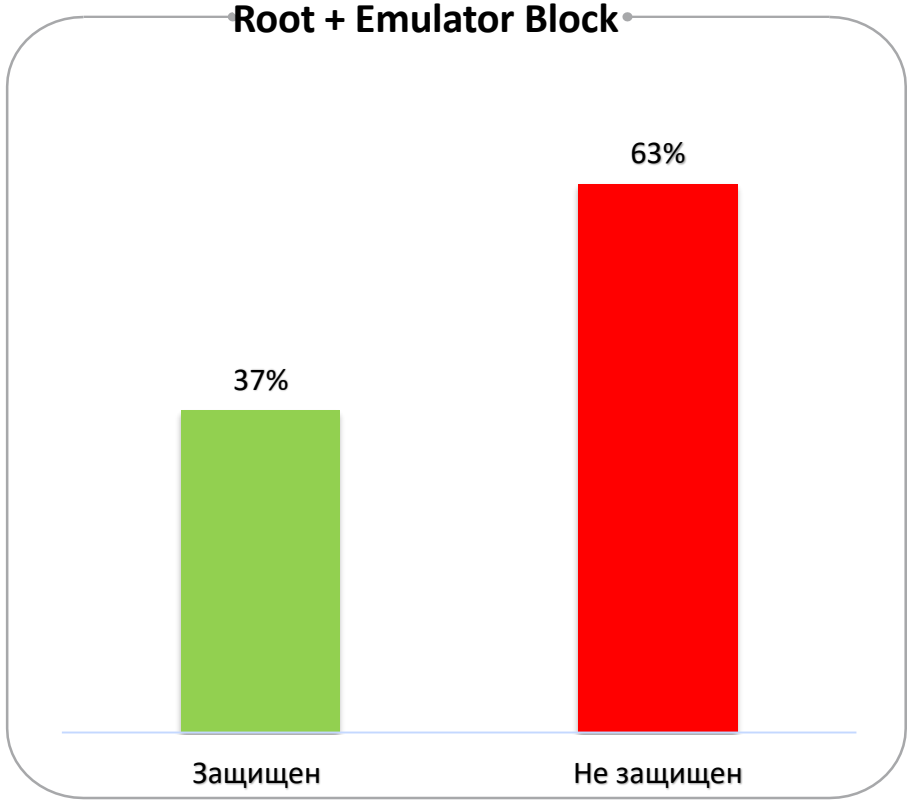
10.3 Проверка защитных механизмов безопасности

Учитывая тот факт, что банковские приложения предназначены для обработки конфиденциальной финансовой информации, разработчикам рекомендуется позаботиться о сохранности как содержащейся в них информации, так и о безопасности самих приложений. Этого можно добиться за счет применения полного перечня защитных механизмов, направленных на снижение рисков реализации злонамеренных действий на мобильном устройстве. Например, можно выполнить следующий перечень базовых проверок системного окружения:

1) реализовать механизмы обнаружения запуска мобильного устройства с привилегированным доступом («root detection»);
2) проверить вероятность запуска программы на виртуальном устройстве (проверка запуска только на базе архитектуры ARM).

В случае обнаружения нарушений с использованием одного из указанных методов приложение не должно запускаться либо его функционал должен быть существенно ограничен.

В рамках данного исследования мы проанализировали мобильные приложения банков на предмет наличия защитных механизмов. Полученные результаты свидетельствуют о том, что в 63% рассматриваемых приложений не реализованы упомянутые выше защитные механизмы, тогда как в остальных 37% приложений такие механизмы защиты применяются.



1. Доступность сайтов
2. Репутация домена
3. Безопасность HTTP
4. Защита трафика
5. Утечки адресов электронной почты
6. Открытые порты
7. Кибersквоттинг
8. Выполнение требований по защите персональных данных
9. Безопасность почтового сервера
10. Безопасность мобильного банкинга

10. Безопасность мобильного банкинга

10.4 Заключение

Современные мобильных платформы (Android и iOS) имеют богатый набор встроенных механизмов защиты. Однако очень часто разработчики, стремясь выпустить новый релиз или дополнительный функционал как можно скорее, допускают непростительные ошибки с точки зрения защиты приложения и обрабатываемых в нем данных. Это приводит к возникновению уязвимостей, которыми непременно воспользуются киберпреступники.

Результаты нашего поверхностного исследования мобильных приложений казахстанских банков указывают на то, что вопросам защиты и безопасности уделяется недостаточно внимания. Такое положение дел может впоследствии открыть прямой путь к организации целенаправленных кибератак как на отдельных клиентов, так и на банки в целом.

В качестве рекомендаций разработчикам банковских мобильных приложений, помимо реализации базовых и расширенных механизмов защиты, мы советуем уделить особое внимание вопросам безопасности бэкенд-серверов и защиты передаваемых данных между приложением и сервером.

1. Доступность сайтов
2. Репутация домена
3. Безопасность HTTP
4. Защита трафика
5. Утечки адресов электронной почты
6. Открытые порты
7. Киберсквоттинг
8. Выполнение требований по защите персональных данных
9. Безопасность почтового сервера
10. Безопасность мобильного банкинга

Deloitte.

deloitte.kz

О «Делойте»

Наименование «Делойт» относится к одному либо любому количеству юридических лиц, включая их аффилированные лица, совместно входящих в «Делойт Туш Томацу Лимитед», частную компанию с ответственностью участников в гарантированных ими пределах, зарегистрированную в соответствии с законодательством Великобритании (далее — ДТТЛ). Каждое такое юридическое лицо является самостоятельным и независимым юридическим лицом. ДТТЛ (также именуемая «международная сеть «Делойт») не предоставляет услуги клиентам напрямую. Подробная информация о юридической структуре ДТТЛ и входящих в нее юридических лиц представлена на сайте www.deloitte.com/about.

«Делойт» предоставляет услуги в области аудита, консалтинга, финансового консультирования, управления рисками, налогообложения и иные услуги государственным и частным компаниям, работающим в различных отраслях экономики. «Делойт» — международная сеть компаний, в число клиентов которой входят около четырехсот из пятисот крупнейших компаний мира по версии журнала Fortune. «Делойт» имеет многолетний опыт практической работы при обслуживании клиентов в любых сферах деятельности более чем в 150 странах мира и использует свои обширные отраслевые знания и опыт оказания высококачественных услуг для решения самых сложных бизнес-задач клиентов. Более 264 тысяч специалистов «Делойта» по всему миру привержены идеям достижения результатов, которыми мы можем гордиться. Для получения более подробной информации заходите на нашу страницу в Facebook, LinkedIn или Twitter.

Настоящее сообщение содержит информацию только общего характера. При этом ни компания «Делойт Туш Томацу Лимитед», ни входящие в нее юридические лица, ни их аффилированные лица (далее — «сеть «Делойт») не представляют посредством данного сообщения каких-либо консультаций или услуг профессионального характера. Прежде чем принять какое-либо решение или предпринять какие-либо действия, которые могут отразиться на вашем финансовом положении или состоянии дел, проконсультируйтесь с квалифицированным специалистом. Ни одно из юридических лиц, входящих в сеть «Делойт», не несет ответственности за какие-либо убытки, понесенные любым лицом, использующим настоящее сообщение.