Deloitte.

Ежегодный обзор кибербезопасности банков Узбекистана

Декабрь, 2022

MAKING AN IMPACT THAT MATTERS since 1845

Введение

Компания «Делойт» в Каспийском регионе провела свое первое комплексное исследование кибербезопасности узбекистанских банков второго уровня (далее – БВУ).

Результаты данного исследования отражены в настоящем обзоре (далее – Обзор или Отчет).

В ходе исследования мы проанализировали публичные веб-ресурсы и мобильные приложения 31 БВУ. Помимо основных веб-сайтов БВУ в исследование были включены порталы для обслуживания корпоративных и розничных клиентов. В общей сложности мы проанализировали 72 веб-адреса.

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. Безопасность HTTP
4. Защита трафика
5. Безопасность почтового сервера
6. Утечки адресов электронной почты
7. Выполнение требований по защите персональных данных
8. Открытые порты
9. Безопасность мобильного банкинга
10. Уязвимость Log4J

В географию исследования также были включены БВУ Казахстана и Азербайджана. Это позволило сравнить уровни зрелости БВУ трех стран в части используемых подходов по обеспечению кибербезопасности.

Для проведения исследования использовался набор открытых онлайн-инструментов, таких как: Google PageSpeed, SSLLabs, Talos Intellegence, Trusted Source, Haveibeenpwned и другие.

Мы искренне надеемся, что Вы найдете настоящий Отчет полезным. В случае, если у Вас возникнут какие-либо комментарии или вопросы относительно указанной в настоящем Отчете информации, просим связаться с нами.

Ремыга Владимир
Директор
Департамент по управлению рисками

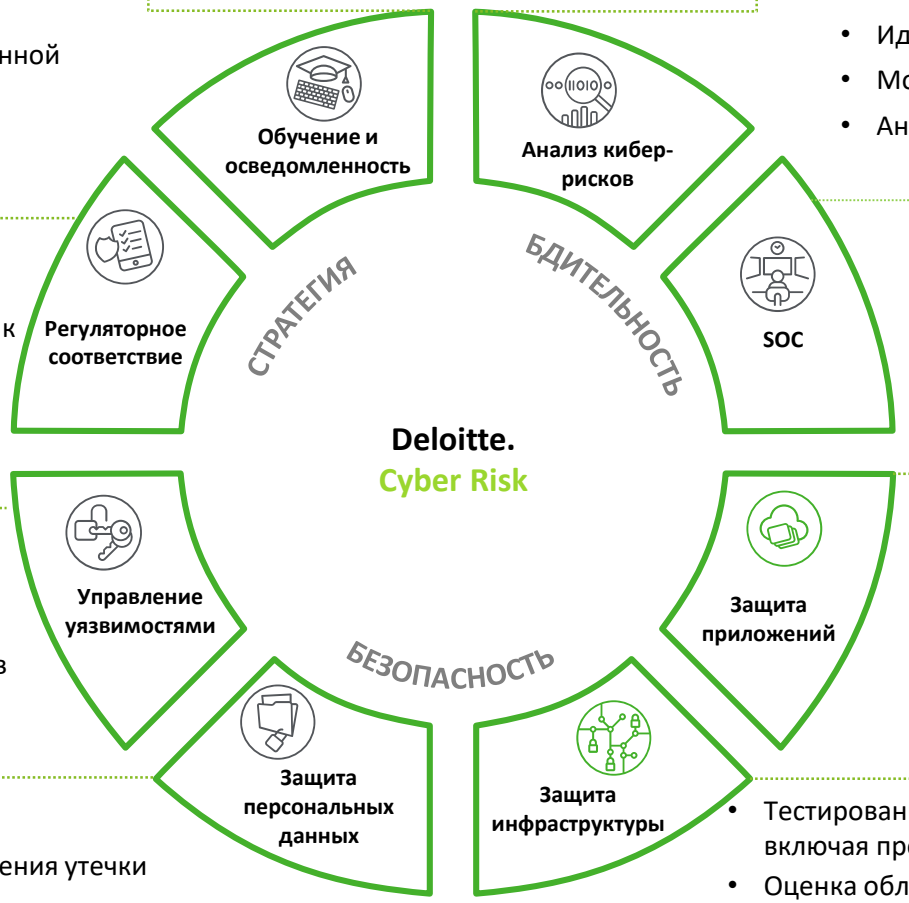
О Делойт

- Внедрение процесса повышения осведомленности об информационной безопасности
- Проведение обучения в вопросах информационной безопасности

- Внедрение процесса управления кибер-рисками
- Оценка соответствия и подготовка к сертификации: ISO 27001, PCI DSS, SOX 404
- Управление цифровыми рисками

- Разработка и выполнение процессов управления уязвимостями
- Интеграция системы инструментов управления уязвимостями

- Защита персональных данных
- Внедрение программ предотвращения утечки данных



- Идентификация рисков
- Моделирование и оценка рисков
- Анализ данных

- Аутсорсинг услуг SOC
- SOC аналитика L1 & L2 &L3
- Анализ вредоносного ПО

- Тестирование безопасности приложений и систем
- Анализ безопасности исходного кода
- Анализ безопасности разработки

- Тестирование на проникновение в инфраструктуру, включая производственные технологии (SCADA)
- Оценка облачной безопасности
- Проектирование архитектуры ИОК
- Улучшение настроек безопасности

Делойт в Узбекистане

Первоначально офис в Ташкенте был зарегистрирован в 1995 году, а позже, в 2002 году, был перерегистрирован. Аудиторская организация ООО «Делойт и Туш» имеет соответствующую регистрацию на право осуществления аудиторской деятельности на территории Республики Узбекистан и имеет более 20 лет опыта работы в сфере аудита.

«Делойт» является признанным лидером на рынке консалтинга в области ИБ. Фирму высоко оценили отраслевые аналитики, в том числе Gartner, Forrester и Kennedy.

За 20 лет деятельности в Узбекистане «Делойт» реализовал сотни успешных проектов для финансовых учреждений, государственных организаций, промышленных и торговых предприятий, сопровождая крупнейшие транснациональные проекты и являясь лидером в предоставлении услуг банковскому сектору. На сегодняшний день компания представлена главным офисом в Ташкенте, сотрудниками которых являются более 100 местных и зарубежных специалистов в области аудита, консалтинга, корпоративных финансов, налогообложения и права.

Наши специалисты разрабатывают полностью адаптируемые под потребности клиентов решения для компаний, стремясь удовлетворить растущий спрос на услуги в данной области. Наши продукты включают решения для расширенного мониторинга инцидентов, связанных с безопасностью, анализа данных по угрозам, управления киберугрозами и реагирования на инциденты и другие услуги.

Наш подход: Методология

Данный отчет призван показать важность киберзащиты от широко известных и распространенных уязвимостей. При сборе данных были использованы только общедоступные и бесплатные инструменты, такие как: бесплатные онлайн сервисы, свободно-распространяемое ПО и скрипты находящиеся в открытом доступе.

В основу методологии легли избранные практики OWASP и OSINT.

Первым шагом в сборе данных было составление списка тестируемых банков. Поскольку данный отчет выпускается впервые, мы не сопровождали его сравнительными графиками текущих и прошлогодних результатов, как мы это делаем в рамках обследования БВУ Казахстана и Азербайджана.

В дополнение к основному веб-сайту БВУ мы ввели еще две категории - корпоративных и розничных сайтов. Сайты для обслуживания юридических лиц и предпринимателей были внесены в категорию «Корпоративные», а сайты для обслуживания физических лиц – в категорию «Розничные». Главные информационные источники и точки входа посетителей на сайты БВУ, отражены в Отчете под категорией «Основные».

Детальное описание используемых инструментов приведено отдельно в начале каждого из разделов или дано непосредственно рядом с описанием проверяемых метрик и параметров.

Обращаем внимание на то, что в рамках отчета используемые термины «домен», «сайт» и «веб-сайт» имеют одинаковый смысл и значение.

Наш подход: Выбор категорий тестирования

Доступность сайтов. На сегодняшний день, веб-сайт является одним из основных инструментов взаимодействия банковских организаций с юридическими и физическими лицами. Так, производительность, включающая в себя такие метрики как время отклика, первая отрисовка контента и задержка первого ввода, играет ключевую роль в доступности веб-сайтов во время DDOS-атак. Скорость отклика непосредственно влияет на удобство использования веб-сайта – пользователь сразу получает запрашиваемый результат, без длительного времени ожидания.

Репутация домена. Репутация домена является одним из ключевых аспектов доверительных отношений в киберпространстве. Менее надежный показатель репутации домена приводит к понижению ранжирования. Это может привести к тому что письма, отправленные из домена такого банка, с большой долей вероятности будут помечены как спам.

Безопасность HTTP. Одним из эффективных методов защиты безопасности домена является корректная настройка заголовков HTTP. Поскольку сервер всегда находится в состоянии ожидания запроса, злоумышленникам не составит труда использовать предоставленный сервером ответ для компрометации сайта или нахождения слабых мест в защите, и их дальнейшая эксплуатация.

Защита трафика. В HTTPS данные шифруются с помощью протокола Transport Layer Security, и ранее, Secure Sockets Layer. Эти криптографические протоколы являются наиболее популярными методами обеспечения безопасного обмена данными в Интернете. Чтобы установить соединение SSL/TLS, на сервере должен быть установлен цифровой сертификат, подтверждающий подлинность домена и владельца сайта. Это необходимо для того, чтобы гарантировать, что пользователь посещает подлинный ресурс, а не поддельную страницу, созданную злоумышленником. Данная категория оценки подразумевает проверку на наличие более ранних версий используемых защитных протоколов шифрования. То есть, проверка на известные уязвимости, в основном связанные с SSL, но также и с устаревшими версиями TLS (TLS 1.0, 1.1).

Безопасность почтового сервера. Основная проблема при использовании электронной почты – это ее небезопасность. Уязвимости, связанные с электронной почтой, развязывают руки злоумышленникам в применении атак, компрометирующих компанию. Будь то спам-сообщения, вредоносные программы, фишинговые атаки, изощренные целевые атаки или утечка корпоративных адресов электронной почты в общий доступ.

Наш подход: Выбор категорий тестирования

Утечки адресов электронной почты. 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 люди могут использовать одинаковые или похожие варианты учетных данных в нескольких веб-приложениях, а слитый пароль и пароль корпоративной электронной почты может совпадать или отличаться лишь незначительно. В следствие чего может стать риск потери финансов, доверия клиентов и репутации.

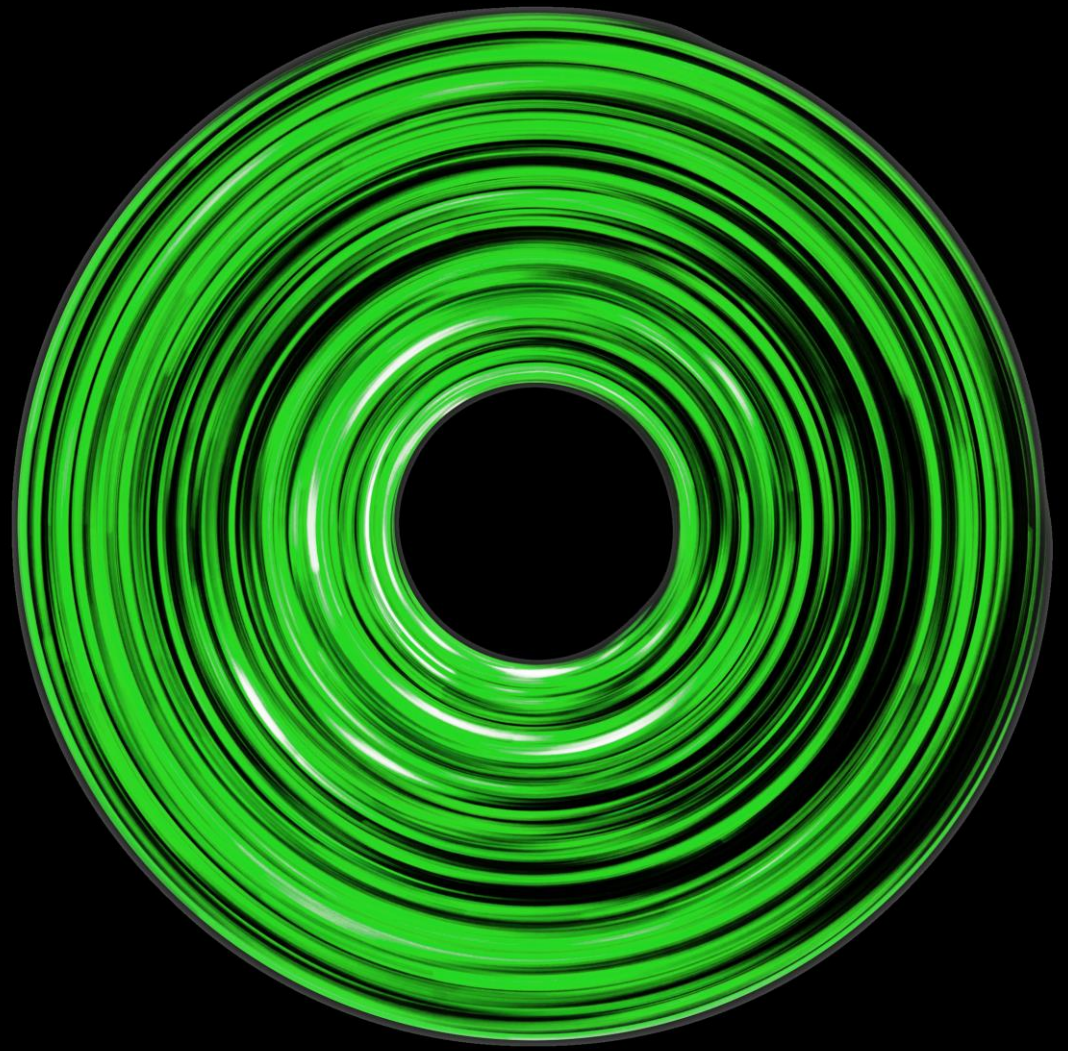
Выполнение требований по защите персональных данных. GDPR, или Общее положение о защите персональных данных - это постановление ЕС о защите данных и конфиденциальности, которое распространяется на всех лиц, находящихся на территории Европейского союза. Согласно пункту 2 статьи 3 GDPR, который касается территориального охвата, говорится, что даже компании, созданные за пределами ЕС, подпадают под требования 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 подпадает под действие GDPR.

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

Безопасность мобильного банкинга. Специфичность и достаточная открытость мобильных платформ делает пользователей мобильных устройств удобной целью для злоумышленников. Существует ряд хакерских программ и инструментов для мобильных платформ, который включает в себя: вирусы, трояны, поддельные банковские программы, программы-вымогатели и всевозможные программы-шпионы. Таким образом проверка безопасности мобильных приложений является существенно важной оценкой для защиты пользовательских данных и ресурсов банка от недоброжелателей.

Уязвимость Log4j. Уязвимость Log4Shell работает, используя функцию Log4j, которая позволяет пользователям указывать собственный код для форматирования сообщения журнала. Например, данная функция позволяет Log4j регистрировать не только имя пользователя, связанное с каждой попыткой входа на сервер, но и настоящее имя пользователя, если на отдельном сервере хранится каталог, связывающий имена пользователей и настоящие имена. Это в свою очередь дает злоумышленнику информацию касательно данных о сервере и пользователе, с целью фишинговых атак и компрометации конфиденциальных данных.

Обобщенные результаты



Резюме

Сегодня большинство руководителей банков Узбекистана вкладывают значительные ресурсы в цифровую трансформацию, которая является частью их долгосрочной стратегии повышения эффективности. Это означает, что все больше новых технологий входит в нашу повседневную жизнь - мобильный и интернет-банкинг, удаленные денежные переводы, платежи и другие инструменты стали обычным явлением в Узбекистане.

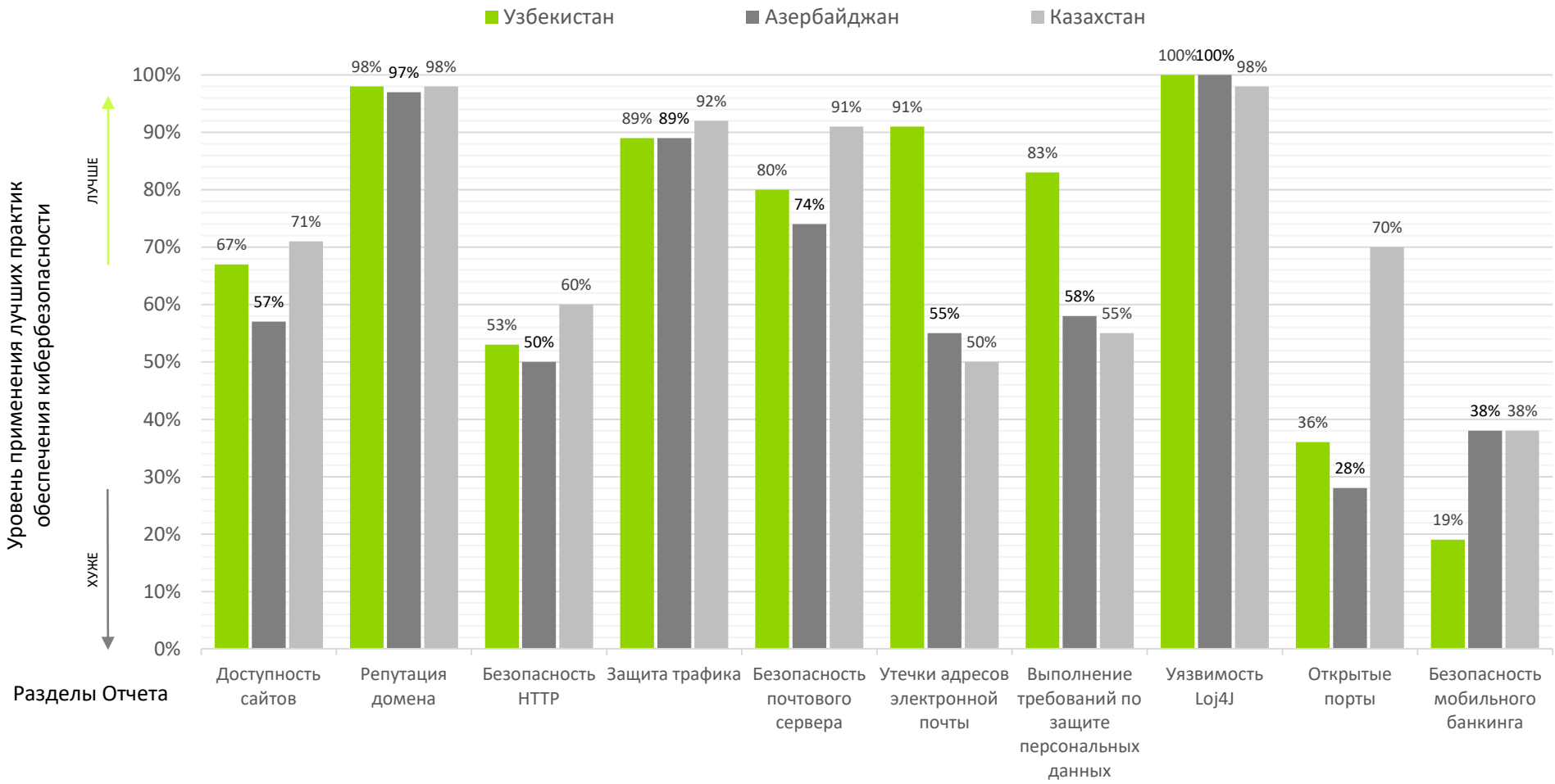
На графике, представленном на следующей странице, можно ознакомиться с показателями ВБУ Узбекистана. На это графике также приведено сравнением с показателями БВУ соседних стран – Казахстана и Азербайджана.

Результаты обзора указывают на то, что часть БВУ пока не замечает либо недооценивает сопряженных рисков. Как следствие, БВУ не следуют базовым рекомендациям по обеспечению безопасности при настройке своих онлайн сервисов. Но больше всего вопросов возникает к обеспечению безопасности работы приложений на мобильных устройствах. Именно данный факт позволяет утверждать, что обеспечение безопасности клиентов, использующих мобильные приложения БВУ, будет являться одним из ключевых вызовов в обозримой перспективе для банковского сектора в Узбекистане.

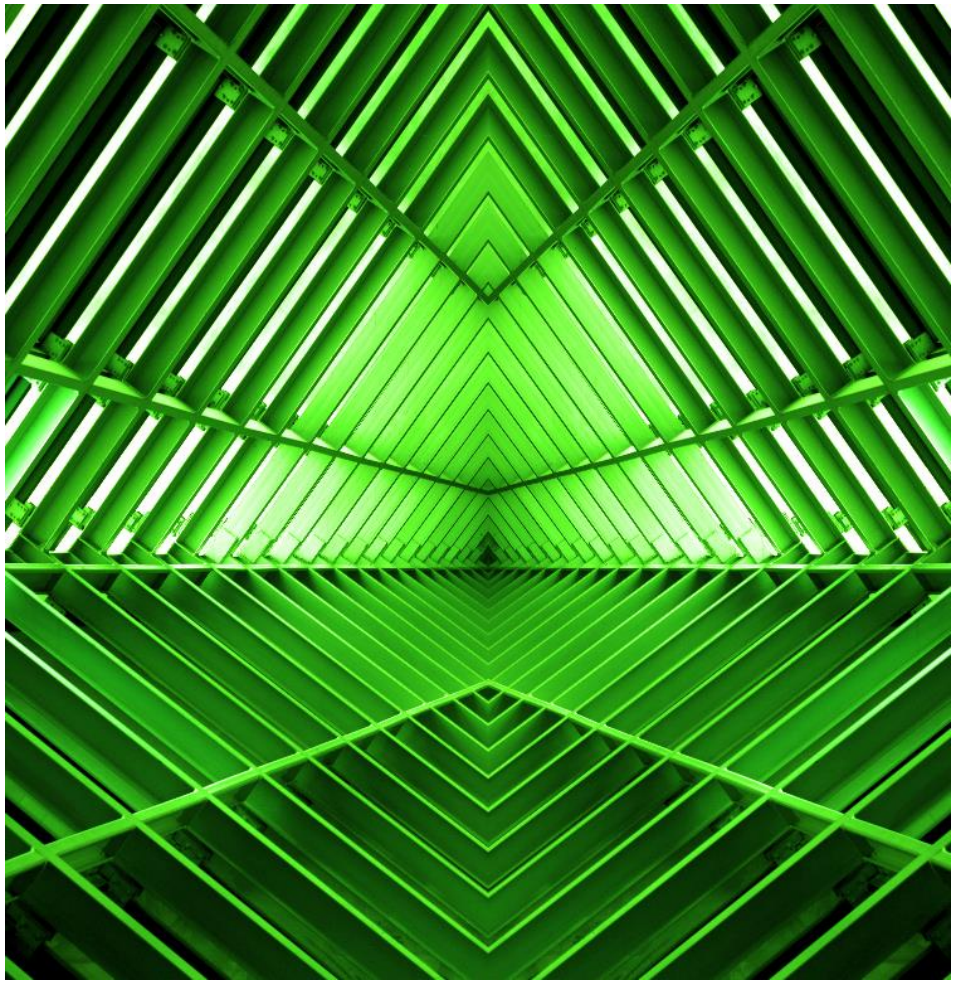
Часть выявленных недостатков может показаться незначительной. Однако хотим напомнить, что в области кибербезопасности нет «несущественных» уязвимостей. Любая из них может привести к выявлению более серьезной проблемы и стать в итоге причиной утечки конфиденциальных данных или к прямому хищению средств. В этой связи мы дополнили каждую область исследования нашими общими рекомендациями, направленными на снижение соответствующих киберрисков.

На последующих страницах настоящего отчета можно ознакомиться детальными результатами проведенного исследования.

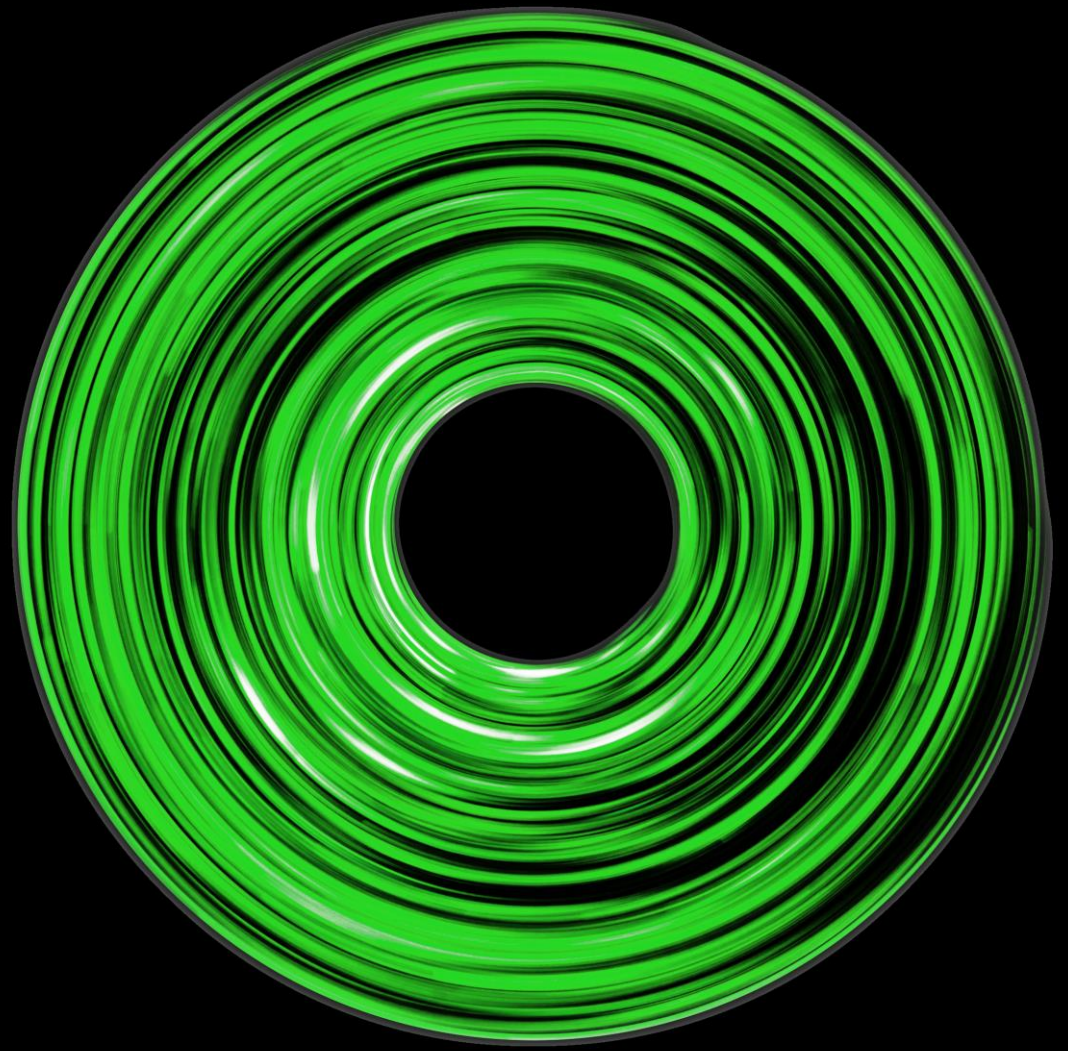
Бенчмарк показателей трех стран по каждому разделу Отчета
Обобщённый результат для все трех категорий сайтов



Содержание



1. Доступность сайтов



1. Доступность сайтов

Архитектура серверной и сетевой инфраструктуры, конфигурация интернет портала и непосредственно оптимизированный контент интернет сайта, все это основные факторы играющие ключевые роли в обеспечении высокой доступности интернет ресурсов банков для их конечных пользователей. В том числе, эти факторы являются важными в части защиты онлайн ресурсов банков от DOS-атак*.

На сегодняшний день, в мире существует множество способов оценки производительности сайтов. Тем не менее, для целей данного исследования нами были отобраны следующие три метрики:

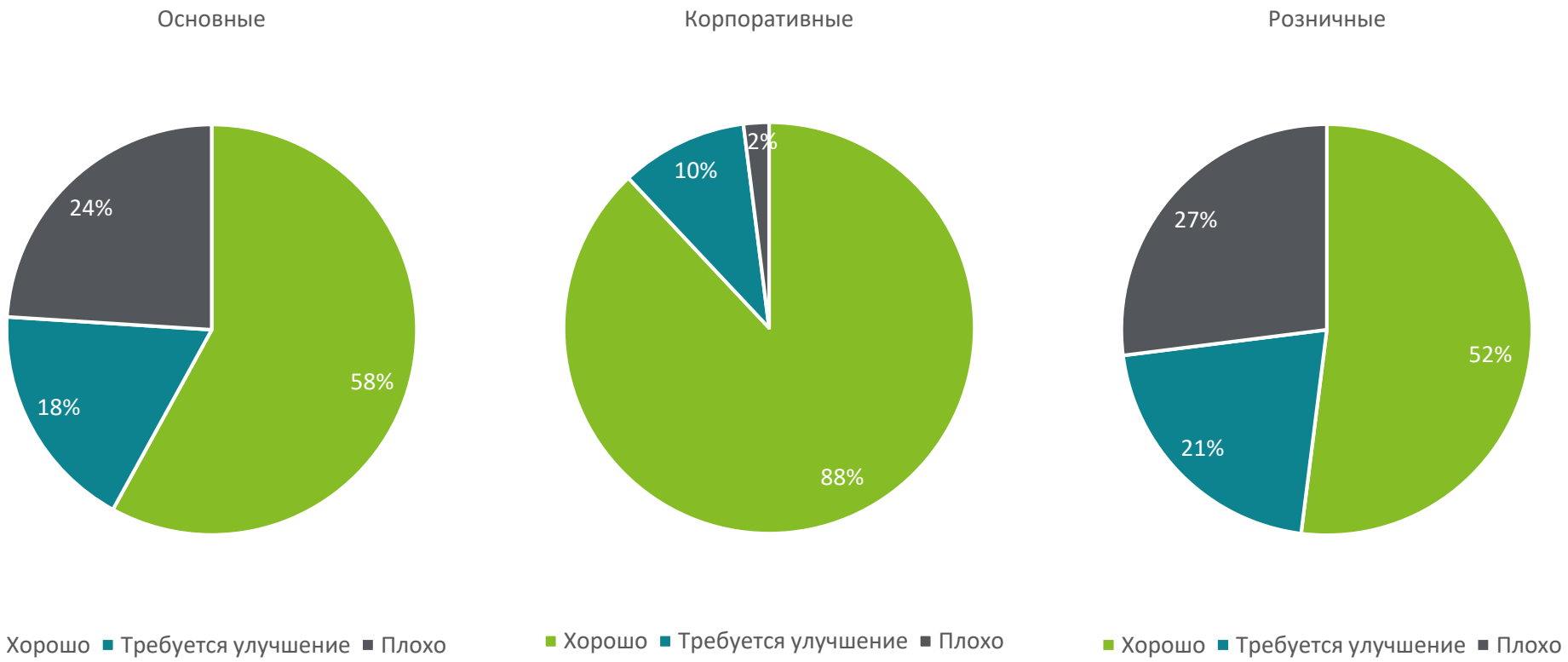
1. First Input Delay (FID);
2. Response Time (RT);
3. First Contentful Paint (FCP).

Первая оценивает производительность веб-сайта, при отображении его содержимого на стороне клиента. Последние две, измеряют время обмена информацией между сервером и клиентом.

**атака типа «отказ в обслуживании»*

1. Доступность сайтов

Обобщенный результат всех проверяемых метрик доступности для «основной», «корпоративной» и «розничной» категорий доменов.



Высокий процент доступных сайтов в корпоративной категории говорит об оптимизации страниц и обеспечении должного уровня доступности. Однако, другим категориям следует улучшить свои показатели, поскольку долгая загрузка страниц может привести к уходу пользователя со страницы, что особенно критично для основной категории сайтов, так как они являются «лицом» банка.

1. Доступность сайтов

1.1 First Input Delay (Время ожидания до первого взаимодействия с контентом)

Показатель “First Input Delay” является одним из важных параметров сайта, формирующий так называемой «первое впечатление» о скорости его работы. FID оценивает интерактивности и отзывчивости сайта, путем измерения времени необходимого браузеру для обработки первого пользовательского ввода и отображения соответствующего контента. Он измеряется в миллисекундах, таким образом и в этому случае применяется правило «чем меньше, тем лучше».

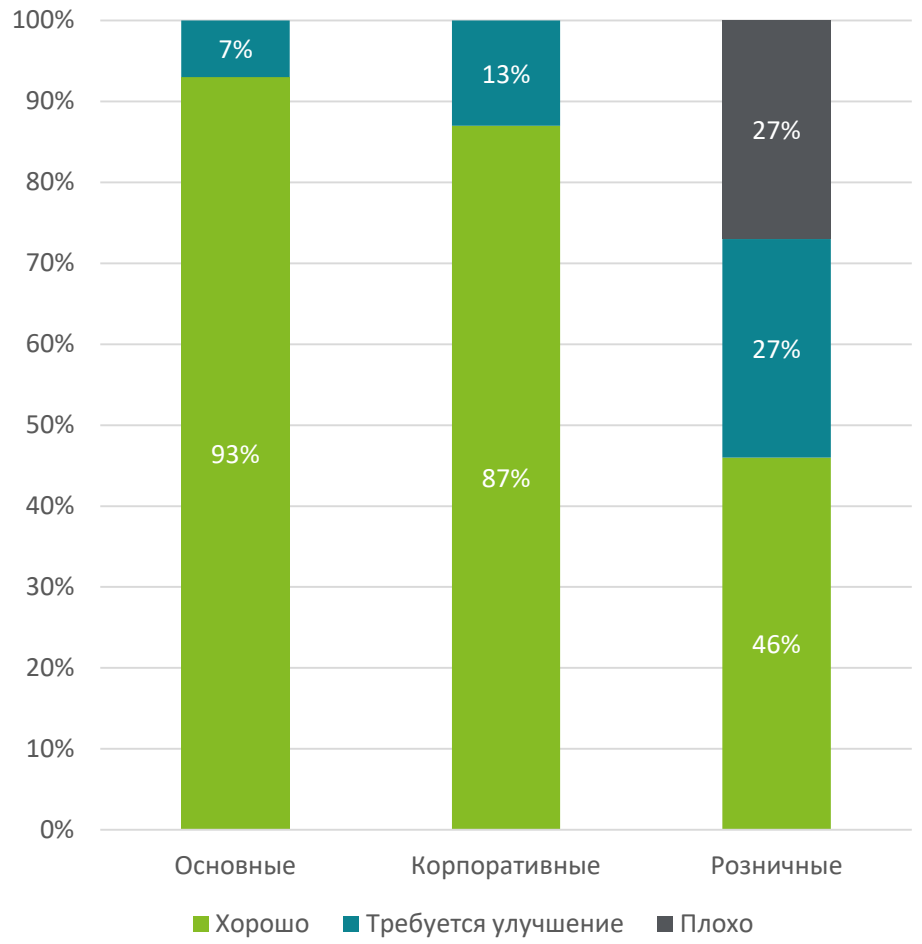
Большое значение FID может быть индикатором плохой оптимизации веб-сайта или чрезмерно «тяжелого» кода или контента, что может приводить к низкой скорости загрузки и отображения элементов веб-сайта на стороне пользователя.

Каждое значение результата интерпретировалось путем сравнения полученных результатов по следующим критериям: от 0 до 100 мс – «Хорошо», от 100 до 300 мс – «Требуется улучшение», свыше 300 мс – «Плохо».

Категории "основные" и "корпоративные" показали достаточно хорошие результаты. Очевидно что банки серьезно относятся к получению их пользователями хорошего «первого впечатления». Только в «розничной» категории оценка «хорошо» составляет 46%.

Тем не менее, для тех кто получил невысокую оценку целесообразно провести оптимизацию сайтов, путем:

- Разбития длинных задач на части.
- Оптимизации страниц для готовности к взаимодействию.
- Использовании Web-Worker API.
- Ограничения время выполнения JavaScript.



1. Доступность сайтов

1.2 Response Time (Время ответа)

Response Time (RT) - данный показатель измеряет время между запросом пользователя и моментом получения первых данных от веб-сайта. RT измеряется в миллисекундах и при оценке его результатов применяется правило «чем меньше, тем лучше».

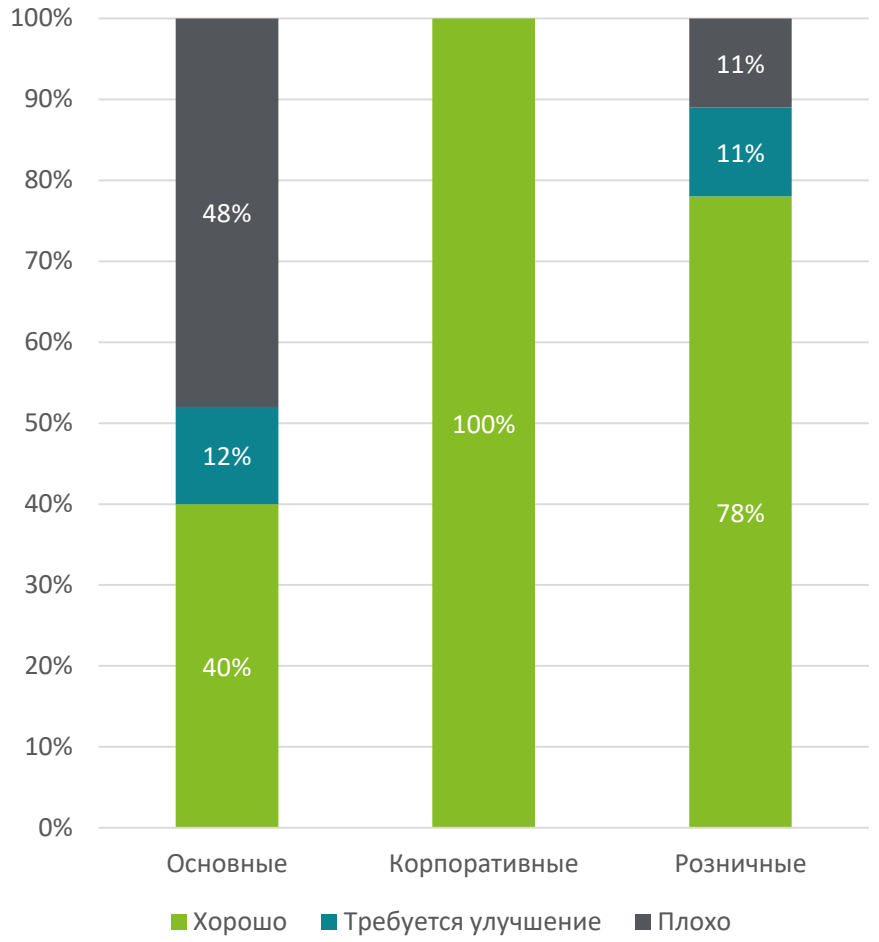
Для измерения значений RT использовался онлайн-инструмент нагрузочного тестирования K6. Тестовая конфигурация включала 20 виртуальных пользователей (VU) из Европы (Германия), которые одновременно обращались к целевому сайту. Период теста - 5 минут. Полученный результат усреднялся и фиксировался как показатель RT.

Каждое значение результата интерпретировалось путем сравнения со следующими диапазонами: до 500 миллисекунд – “хорошо”, от 500 до 1000 – “Требуется улучшение”, дольше 1000 миллисекунд – “плохо”.

Анализ показателя RT для «корпоративной» категории показал отличный результат, не было обнаружено оценки «плохо». «Розничная» категория показала оценку выше среднего, тогда как «основная» категория показала результат ниже среднего.

Существует довольно много причин которые могут влиять на показателей RT. Это значит, есть и множество возможных способов его улучшения, включая:

- Оптимизировать логику серверных приложений. Так чтобы страницы загружались быстрее.
- Оптимизировать запросы сервера к базам данных или перейдите на более быстрые системы баз данных. Также, использование кеширования обращений к базе данных, может быть полезным.
- В некоторых случаях может помочь только модернизация серверное оборудования, в части увеличения объема памяти или процессорных ресурсов.



1. Доступность сайтов

1.1 First Contentful Paint (Первая отрисовка контента)

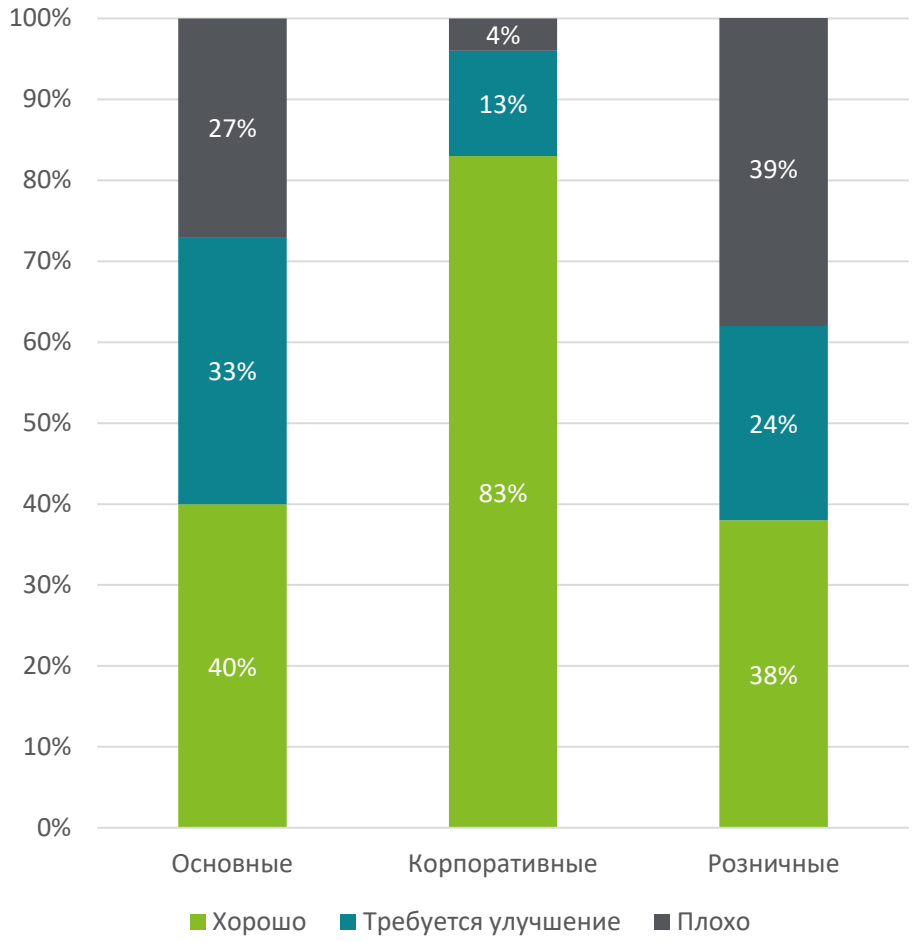
FCP измеряет время необходимое для отображения первых элементов содержимого вебсайта в окне браузера в ответ на запрос от пользователя. Позволяя пользователю убедится, что запрашиваемый ресурс доступен и обрабатывает запросы должным образом. Данный показатель измеряется в милисекундах. Таким образом, к его результатам применяется правило «чем меньше показатель, тем лучше».

В рамках исследования был использован веб-ресурс Google PageSpeed. Полученные при этом показатели времени были интерпретированы с использованием критериев оценки производительности определенных Google: от 0 до 1800 мс – «Хорошо», от 1800 до 3000 мс – «Требуется улучшение», свыше 3000 мс – «Плохо».

Результаты указывают, что данный показать для «корпоративной» категории существенно выше его аналога для «розничной» на 50%. Результат «основной» категории показал результат ниже среднего.

Для дальнейшего улучшения данного показателя владельцам сайтов рекомендуется:

- Отказаться от использования ресурсов блокирующих отрисовку контента.
- Минимизировать использование таблиц стилей (CSS), включая исключения неиспользуемых стилей.
- Повысить скорость загрузки страниц с помощью предварительного подключения.



1. Доступность сайтов

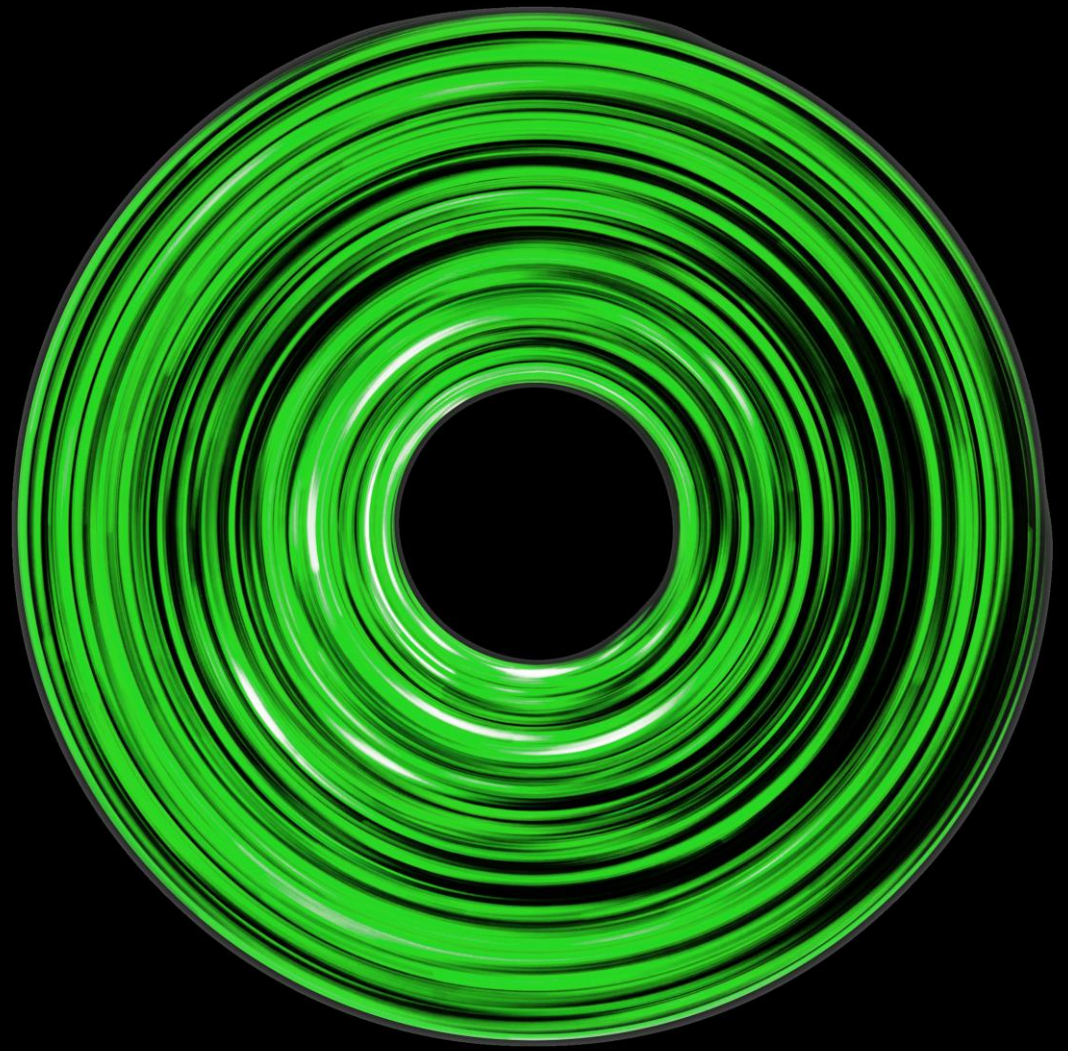
Заключение

Обобщенные результаты исследования доступности всех категорий доменов указывают на то, что производительность большинства доменов узбекистанских банков соответствует требованиям безопасности.

Наибольшее влияние на снижение результата доступности оказала первая отрисовка контента. Так, согласно Google, пользователи будут покидать сайт, если он отображает первые элементы содержимого вебсайта более трех секунд, иными словами, параметр FCP играет очень важную при этом роль, поскольку это первый момент в шкале загрузки страницы, когда пользователь может что-то увидеть на экране.

Сравнение обобщенных показателей доступности сайтов по странам:

2. Репутация домена



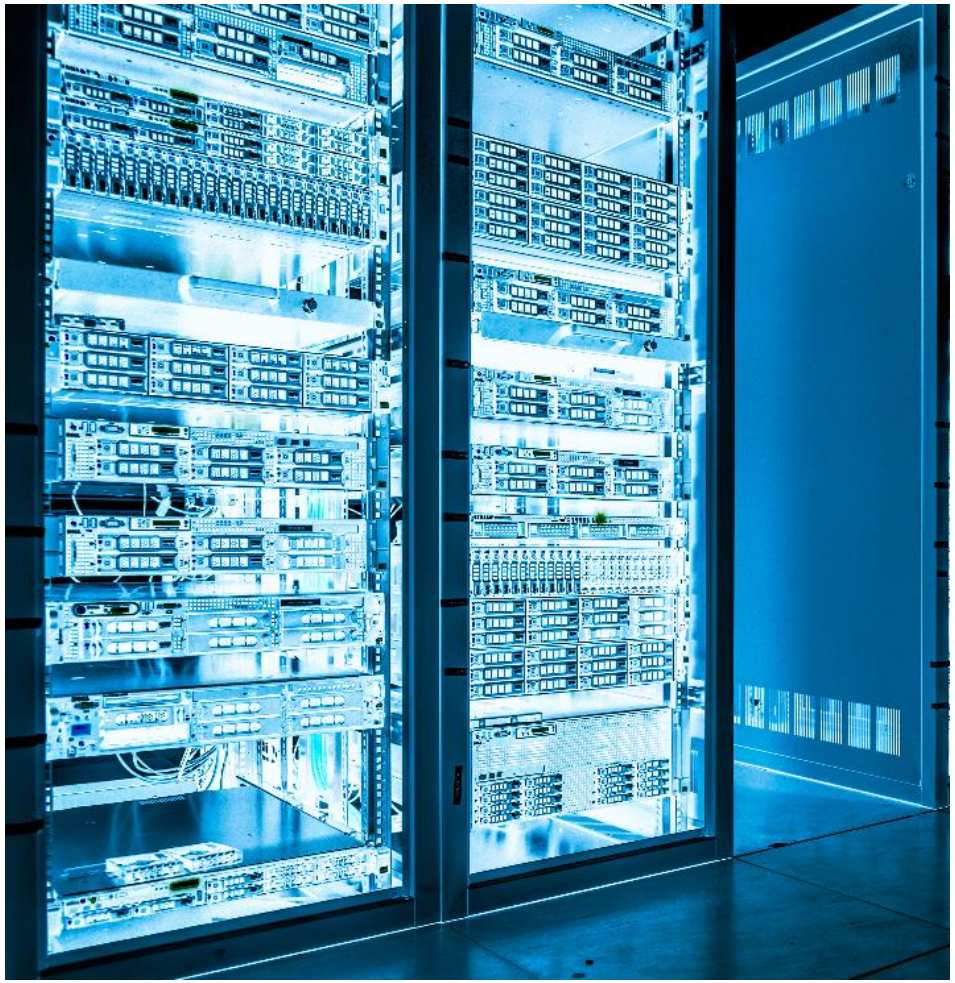
2. Репутация домена

Репутация домена играет решающую роль в доверительных отношениях в киберпространстве. С тех пор, как провайдеры электронной почты и поисковые системы начали полагаться на информацию от провайдеров репутации доменов, значимость этого фактора только возросла.

Электронные письма, отправленные из доменов с низкими показателями репутации или внесенные в черные списки поставщиками веб-репутации, могут быть промаркированы поставщиками сервисов электронной почты как спам, а их веб-ресурсы могут не отображаться в результатах поиска.

В рамках настоящего раздела, представлены результаты проведенного анализа репутации доменов банков Узбекистана, который был осуществлен с использованием трех провайдеров веб-репутации:

- Talosintelligence;
- TrustedSource;
- Barracuda Reputation System.



2. Репутация домена

2.1 Talos Intelligence

Talos Intelligence предоставляет услуги оценки репутации домена от компании Cisco. Сервис определяет и устанавливает соотношение угрозы в режиме реального времени с использованием крупнейшей в мире сети обнаружения угроз, охватывающей электронные письма, веб-запросы, экземпляры вредоносных программ, наборы данных, анализ конечных точек и сетевых вторжений.

Talos Intelligence делит репутацию доменов на четыре группы: Надежно, Хорошо, Плохо и Не классифицировано. Прежде чем присвоить домену «надежную» репутацию, Talos Intelligence собирает существенные положительные свидетельства об этом, основываясь на данных для всего домена и всех связанных с ним IP-адресов.

Результаты исследования показали, что все домены имеют «надежную» репутацию.

Репутация 100% доменов вне зависимости от категории «хорошая»

2. Репутация домена

2.2 Barracuda Reputation System

BRS предоставляет информацию о репутации домена от компании Barracuda Networks. 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, чтобы определить вероятность того, что сообщения с этих адресов являются обычными сообщениями.

Данное решение в первую очередь полагаются на вердикт репутации домена, предоставляемые BRS в качестве первого критерия для возможной блокировки сетевых атак, отправляемых по электронной почте через Интернет и другие протоколы. По аналогии с этим на индикаторы репутации BRS могут полагаться и другие Интернет решения и сервисы.

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

Результаты оценки репутации доменов узбекистанских банков согласно показаний BRS указывает, что ни один из доменов в трех категориях без исключения не попал в черный список.

100% доменов
дополнительных категорий не попали в черный список

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 собирает в реальном времени схемы трафика, упомянутые выше, с устройств безопасности McAfee.

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

Вердикт о репутации домена от TrustedSource оценивает риски по четырем категориям: высокие, средние, минимальные и неклассифицированные. TrustedSource назначает вердикт о минимальном риске доменам, для которых во время тестирования не была обнаружены какие либо подозрительные активности. Неклассифицированная репутация означает, что URL-адрес домена уже упоминался в веб-ссылке или ссылке электронной почты, но еще не был протестирован.

Результаты оценки репутации для "основных" банковских доменов по показаниям TrustedSource показывают, что 100% доменов получили оценку - Минимальный риск. Для «корпоративных» и «розничных» сайтов эта оценка составляет 92% и 87% соответственно.

2. Репутация домена

Заключение

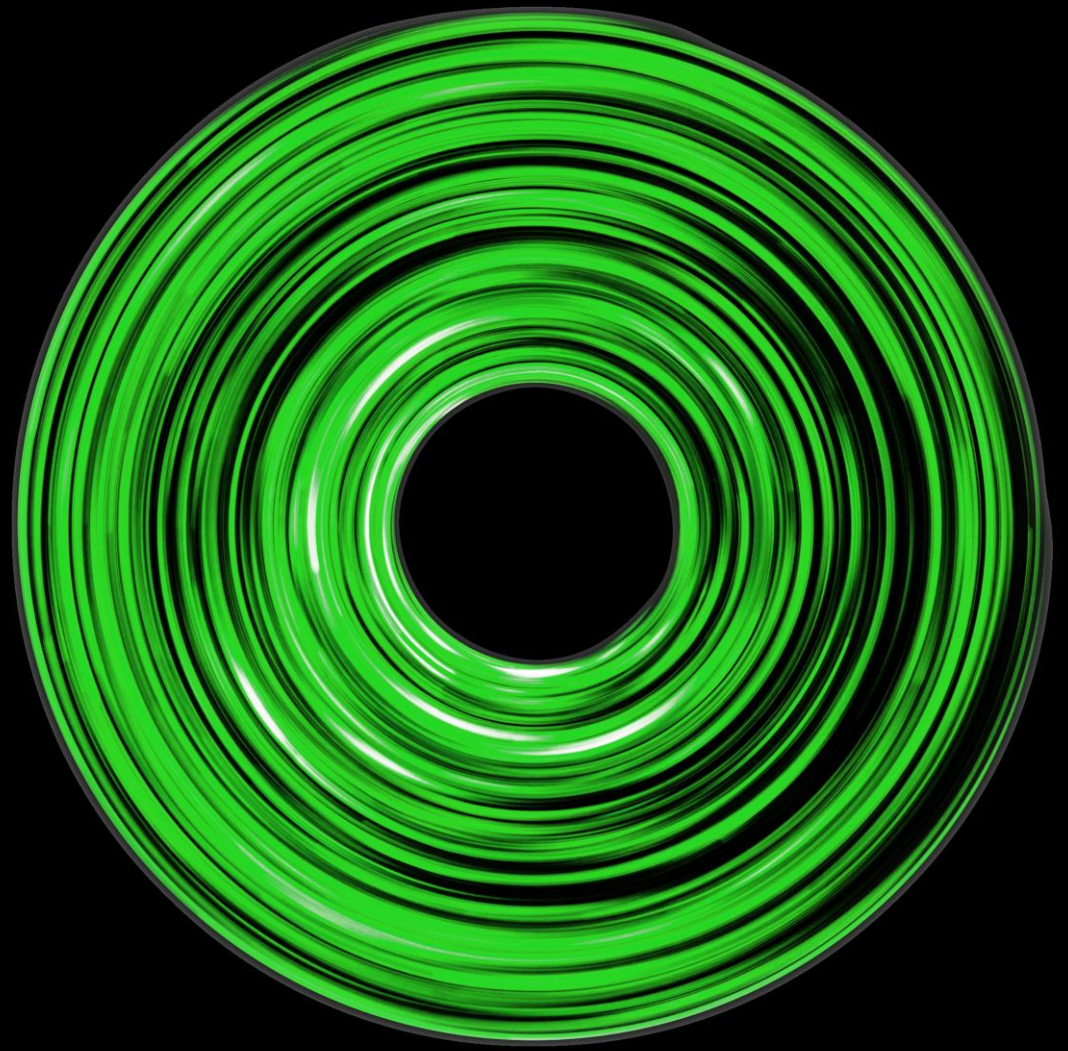
В результатах отмечены 98% банков только лишь по причине отсутствия оценки для некоторых из доменов. Таким образом, анализ репутации доменов банков Узбекистана показывает, что нет ни одного домена с сомнительной или отрицательной репутацией.

Это позволяет сделать вывод, что домены не использовались для рассылки спама, распространения вирусов и другой подозрительной активности.

Обобщенный результат репутации доменов всех категорий веб-сайтов для трех стран:

Репутация 98% доменов тестируемых банков Узбекистана является **Хорошей**	Репутация 97% доменов тестируемых банков Азербайджана является **Хорошей**	Репутация 98% доменов тестируемых банков Казахстана является **Хорошей**

3. Безопасность HTTP



3. Безопасность HTTP

Обеспечение безопасности интернет ресурсов состоит из широкого спектра защитных мер. Однако нарушение целостности хотя бы одного его компонента может привести к компрометации всего сайта. Последствия таких инцидентов могут быть весьма плачевными, включая финансовые или репетиционные потери. Именно поэтому, банкам важно обеспечить наиболее полное соблюдение всех требований кибер-безопасности. Только такой подход может минимизировать риск возможной компрометации безопасности интернет ресурсов.

Одним из базовых методов защиты безопасности интернет сайтов является корректная настройка заголовков HTTP. В рамках настоящего Обзора были проанализированы настройки следующего перечня HTTP заголовков используя общедоступный ресурс - Mozilla Observatory:

- X-Frame-Options
- Content-Security-Policy
- HTTP-Strict-Transport-Security
- X-Content-Type-Options
- X-XSS-Protection
- Set-cookie security flags
- Public-Key-Pins
- X-Powered-CMS
- X-Powered-By
- Server Header

3. Безопасность HTTP

Обобщенный результат всех проверяемых метрик доступности для «основной», «корпоративной» и «розничной» категорий доменов.

Анализ настроек безопасности HTTP всех трех категорий показывает результаты выше среднего, что говорит о том, что эти банки уделяют должное внимание данной категории обеспечения безопасности. Тем не менее почти половине банков рекомендуется осуществить соответствующие корректирующие мероприятия.

3. Безопасность HTTP

3.1 X-Frame-Options

Данный заголовок определяет, разрешено ли браузеру отображать вложенную в тег <frame> или <iframe> страницу как результат ответа HTTP на основной странице. Неправильные настройки заголовка могут быть использованы для атак типа clickjacking.
Механизм действия данной уязвимости достаточно прост: атакуемый пользователь предполагает, что взаимодействует web-сайтом банка, по крайне мере внешне он выглядит именно так. На самом деле взаимодействуя с ресурсом злоумышленников.

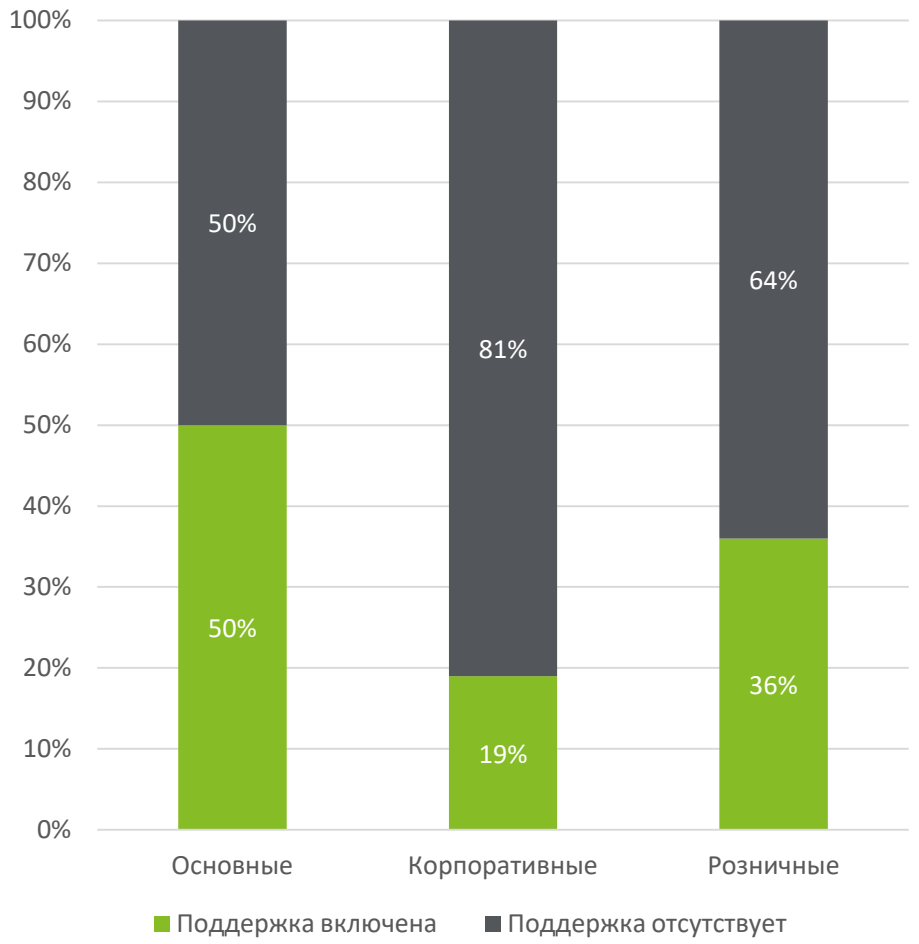
В результате настоящего исследования, обнаружено, что половина банков «основной» категории не используют поддержку данного заголовка. Для корпоративных и розничных сайтов, этот показатель оказался немного хуже, 19% и 36% соответственно.

С целью защитить интернет ресурсы от такого вида атак необходимо настроить HTTP заголовки в соответствии с тремя основными вариантами:

1. DENY: запретить отображение контента в iframe;

2. SAMEORIGIN: ограничивает возможность отображать страницу только в рамках текущего сайта;

3. ALLOW-FROM URL: разрешает определенным URL загрузку контента сайта в iframe. Обратите внимание, что не все браузеры поддерживают это параметр.



3. Безопасность HTTP

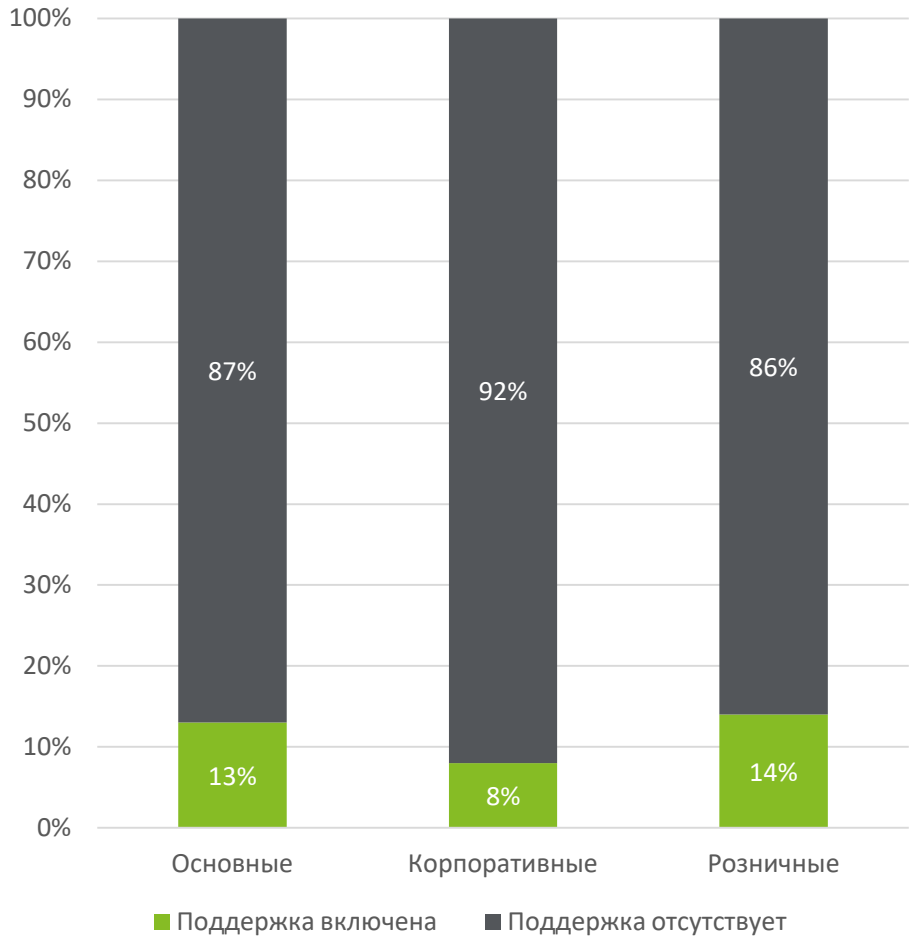
3.2 Content-Security-Policy

Заголовок Content-Security-Policy (CSP) позволяет четко разграничить допустимые источники подгружаемого содержимого веб страницы. Данный заголовок можно рассматривать как дополнительный уровень безопасности браузера, который дает возможность ограничить загрузку браузером таких ресурсов, как: JavaScript, CSS и многих других. CSP помогает в загрузке элементов страницы из заранее определенного источника, что позволяет обнаруживать и предотвращать атаки типа XSS, Formjacking и SQL Injection.

Для определения правил в CSP используется принцип «белого списка». Это позволяет определять допустимые ресурсы и препятствовать использованию других. Также, применение CSP является очень важным, поскольку данная политика может обеспечить возможность оперативного получения информации о возникновении XSS-атак. При использовании опции «report-url», браузеры как атакующего, так и жертвы будут высылать соответствующие уведомления на URL определенный администратором ресурса.

Исследование показывает, что очень малое количество банков использует поддержку данного заголовка. При этом, аналогичная картина наблюдается на корпоративных и розничных web-сайтах.

Также, исследование указывает на то, что в основном администраторы предпочитают использовать другой вариант данного заголовка - X-Content-Security-Policy. Здесь необходимо признать, что совместное использование данных заголовков может привести не корректному отображению содержимого сайта в некоторых браузерах. Тем не менее рекомендуется использовать именно Content-Security-Policy, вместо его устаревшего собрата X-Content-Security-Policy.



3. Безопасность HTTP

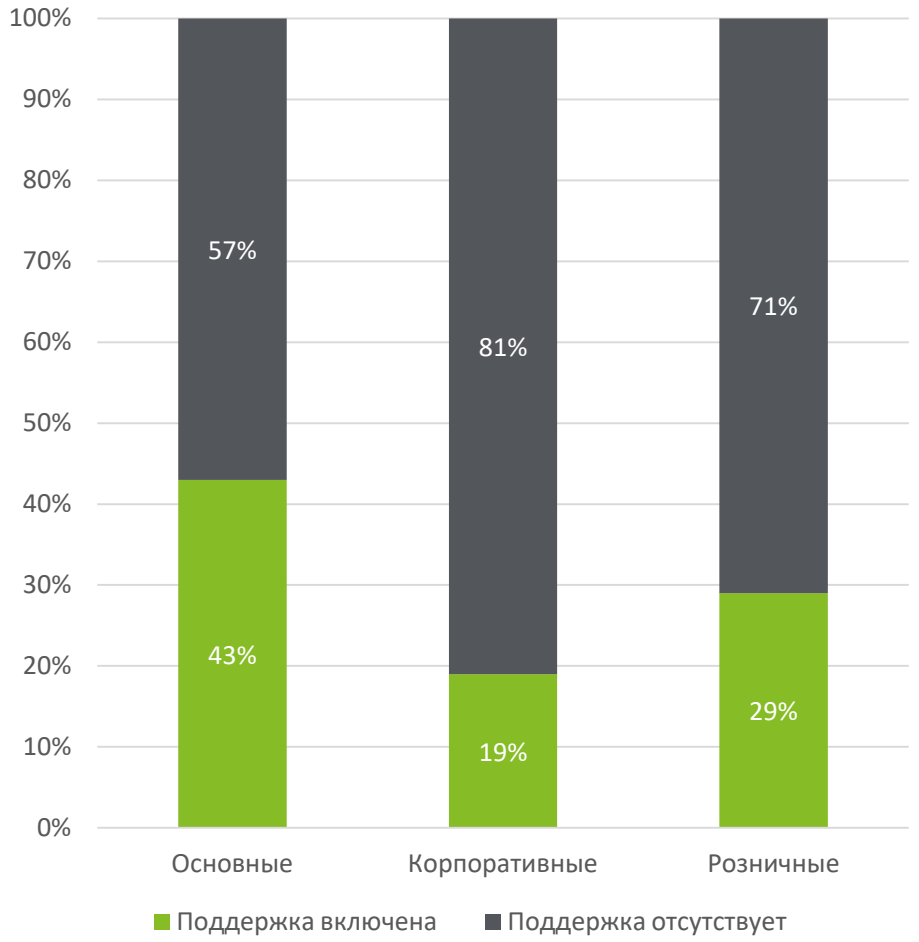
3.3 X-Content-Type-Options

Любое содержимое HTTP должно включать META-данные о его типе, чтобы браузер мог определить, что делать с заданным контентом. Например, если в заголовке типа содержимого указано изображение, браузер понимает, что его нужно отобразить. Если это HTML, то браузер отобразит разметку и исполнит любой JavaScript код.

Однако предопределение типа содержимого в коде страницы не является обязательным. Поэтому браузеры вынуждены применять технику «сниффинга» для самостоятельного определения типа содержимого, если заголовки типа контента не описаны веб-разработчиком.

Проведенный анализ показывает, что в 43% случаев для «основной» категории сайтов банки применяют заголовок X-Content-Type-Options. Результат «корпоративных» и «розничных» веб-сайтов оказался низким, 19% и 29% соответственно.

Чтобы избежать серьезных проблем с безопасностью, рекомендуется добавить строку *X-Content-Type-Option nosniff*, что не позволит браузеру определять тип контента на основании типа MIME. Включение данной строки также включает Cross-Origin Read Blocking защиту для HTML, TXT, JSON и XML файлов, за исключением SVG image/svg+xml.



3. Безопасность HTTP

3.4 HTTP-Strict-Transport-Security

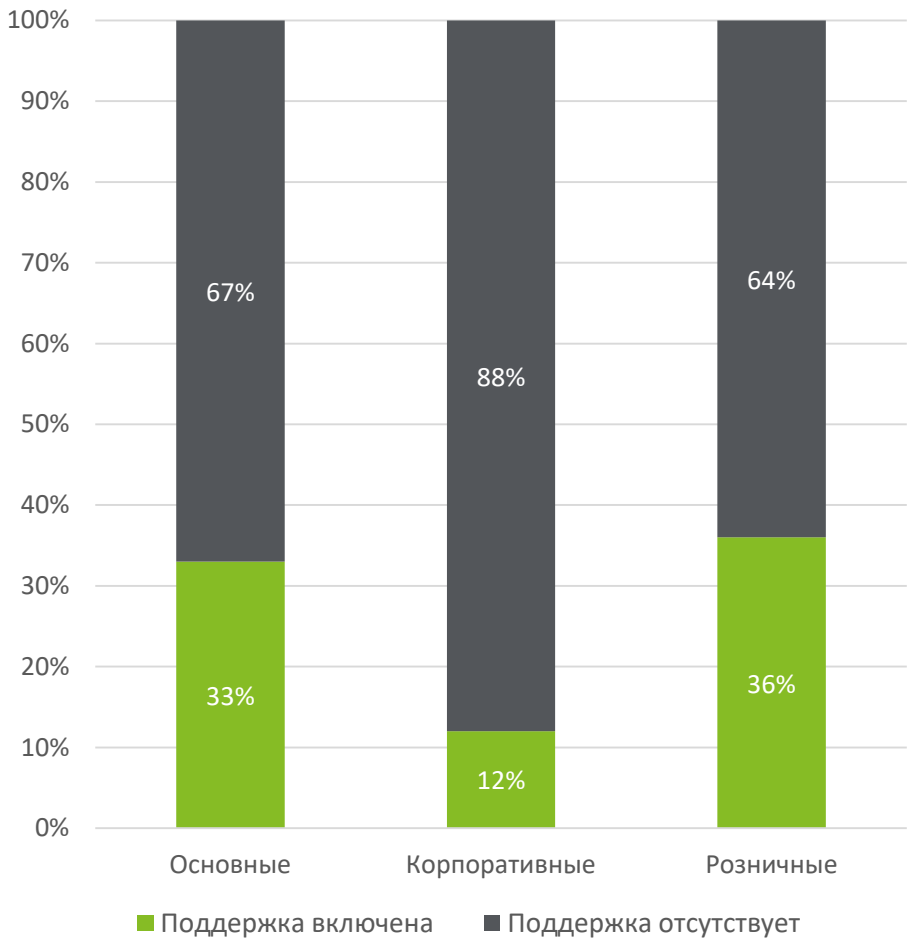
HTTP-Strict-Transport-Security (HSTS) заголовок обязывает браузер пользователя взаимодействовать с сайтом по защищенному протоколу HTTPS, не допуская передачи содержимого по небезопасному HTTP. Предназначен для предотвращения атак типа "man-in-the-middle".

Допустим, пользователь сайта – потенциальный или текущий клиент банка заходит на сайт через публичный Wi-Fi. Парольная и другая конфиденциальная информация в таких сетях нередко оказываются доступной для злоумышленников. Так как последним ничто не мешает также, подключившись к этой Wi-Fi сети, осуществить перехват передаваемой в открытом виде конфиденциальной информации.

Другой способ, когда злоумышленник используя метод 301 или 302 Redirect для перехода с протокола HTTP на зашифрованный HTTPS, может перехватить сетевой трафик передаваемый между пользователем и веб-сайтом по незащищенному HTTP. В результате злоумышленник избегает SSL-шифрование трафика и может перехватить персональные данные или даже получить данные учетной записи.

Результаты обзора показывает, что в «основной» и «розничной» категории примерно только треть доменов поддерживают Strict-Transport-Security. «Корпоративная» категория показала наихудший результат, только 12%.

Рекомендуется активировать использование HSTS. Таким образом, это обяжет браузер загружать защищенную версию сайта и игнорировать любые вызовы или запросы на перенаправление для загрузки сайта по протоколу HTTP. Это закрывает уязвимость перенаправления, существующую при использовании 301 и 302 Redirect.



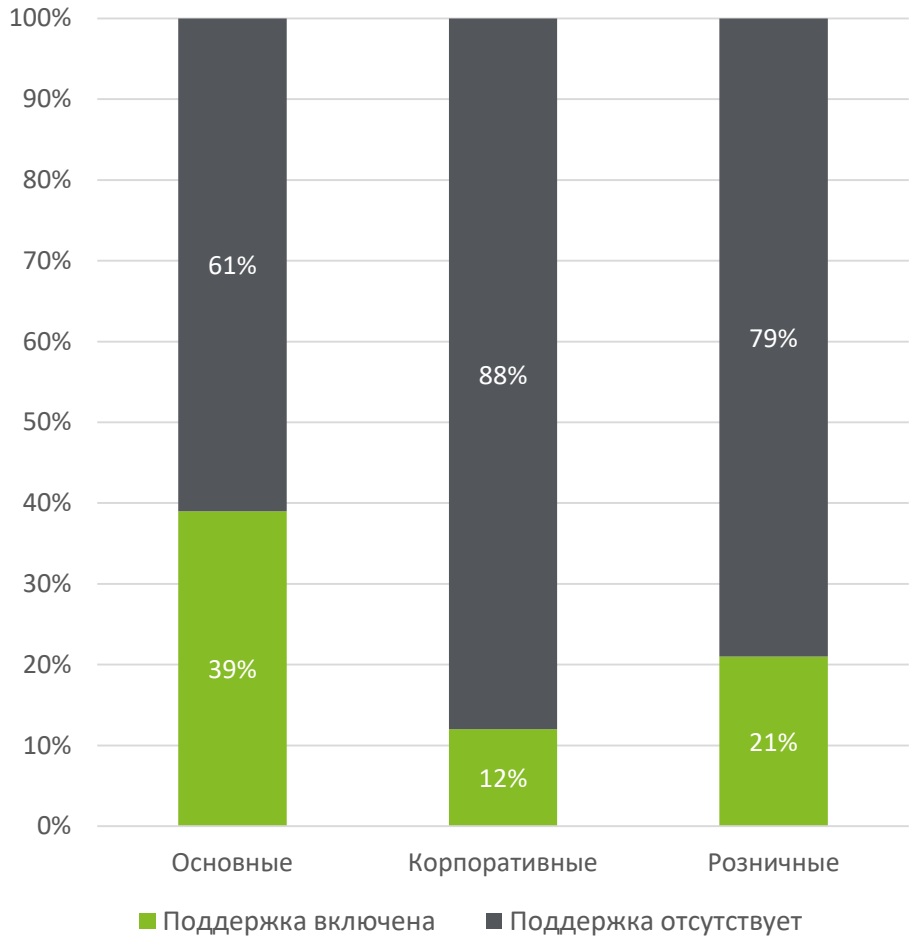
3. Безопасность HTTP

3.5 X-XSS-Protection

Заголовок X-XSS-Protection предназначен для включения фильтра направленного против атак межсайтового скриптинга (XSS), встроенного в современные веб-браузеры. Данный фильтр поддерживается Internet Explorer старше версии 8, Chrome и Safari. Обычно он включен по умолчанию, но использование в заголовках сайта будет приводить к его принудительной активации. Это особенно важно в случаях если пользователь самостоятельно отключил данную функцию браузера. В результате включение защиты от XSS, даст браузеру указание блокировать ответы в случае, если вредоносный скрипт был вставлен из пользовательского ввода. Если данная мера защиты будет отключена, вредоносный скрипт может получить доступ к содержимому cookie, сессионным токенам и прочей чувствительной информации пользователя банковских ресурсов.

Исследование показывает, что в «основной» категории лишь 39% активировали данную меру защиты. Для категорий «корпоративных» и «розничных» сайтов картина несколько хуже. Только 12% и 21% банковских сайтов соответственно активировали заголовок X-XSS-Protection.

Администраторам банковских сайтов рекомендуется принудительно активировать данный заголовок.



3. Безопасность HTTP

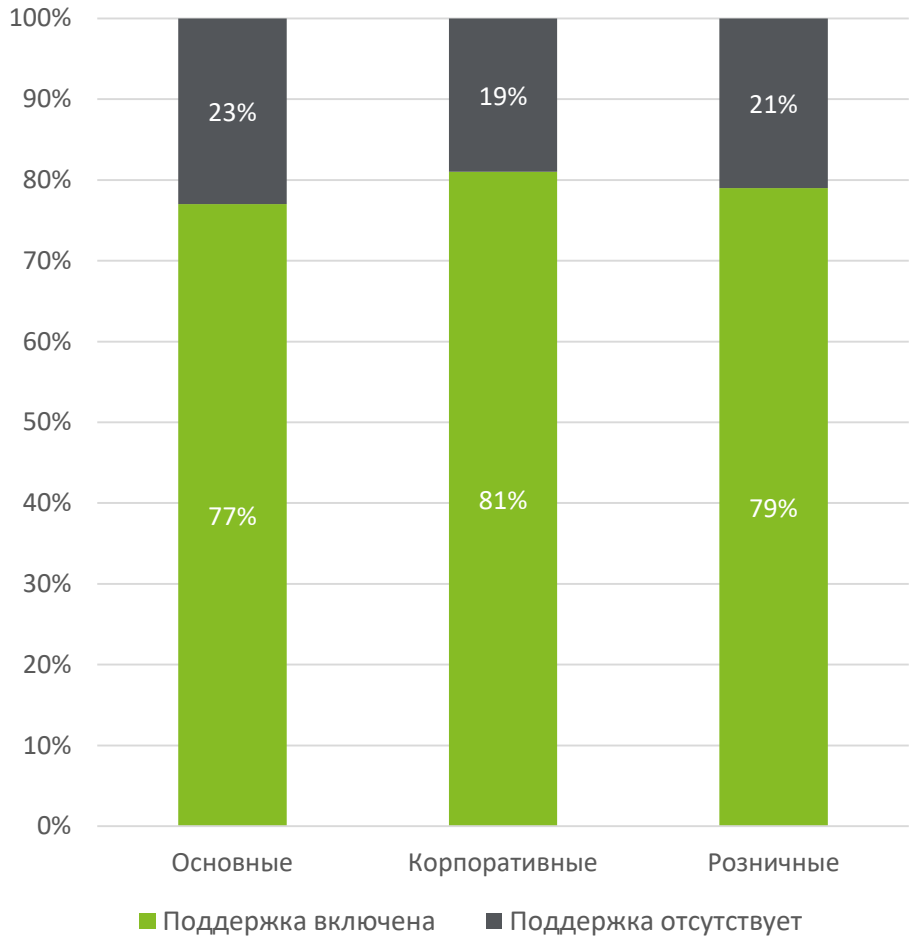
3.6 Set-cookie security flags

Веб-приложения отслеживают сеансы пользователей с помощью идентификатора сессии. Данное значение передается пользователю вместе с заголовком HTTP Set-Cookie. Интернет-браузеры хранят это значение и автоматически добавляют его к каждому создаваемому HTTP-запросу до тех пор, пока сохраненный файл cookie остается действительным.

При всей полезности, необходимо понимать, какие конкретно значения cookie важны для безопасности. Например значения содержащие ID пользователя или идентификатор сессии. Это значение должно использоваться только в безопасном HTTPS-запросе Без условно, могут быть и исключения, но это только в крайних случаях.

Информация из cookie может быть украдена с помощью JavaScript посредством таких атак, как XSS, для защиты от которых можно использовать флаги HttpOnly и secure. Это поможет предотвратить кражу сведений содержащихся cookie и минимизировать потенциальный риск.

Результаты исследования показывают, что большинство банковских сайтов, вне зависимости от категории, поддерживает безопасные настройки cookie.



3. Безопасность HTTP

3.7 Public-Key-Pins

Данный заголовок инструктирует интернет-браузер запомнить используемый веб-сервером SSL-сертификат. Такой сертификат содержит в себе информацию, в частности, о названии сайта, сроке действия сертификата и длине используемых криптографических ключей. Сертификаты также содержат дополнительную информацию: название Удостоверяющего Центра (УЦ). При отправке клиентам информации открытого ключа браузер проводит проверку подлинности веб-сайта. Для этого, он сверяется с УЦ, который представляет собой доверенную сторону, выпускающую сертификаты веб-серверов.

В результате, при последующем взаимодействии с сайтом интернет-браузер пользователя не будет принимать сертификаты с другими открытыми ключами. Это призвано помочь предотвратить атаки на пользователей с помощью поддельных сертификатов, например в случаях, когда УЦ выпустивший сертификат был скомпрометирован или взломан с целью выпуска поддельных сертификатов.

Результаты исследования подтвердили, что все без исключения банки применяют заголовок Public-Key-Pins в каждой из исследуемых категорий.

100%
веб-сайтов
применяют
Public Key Pins

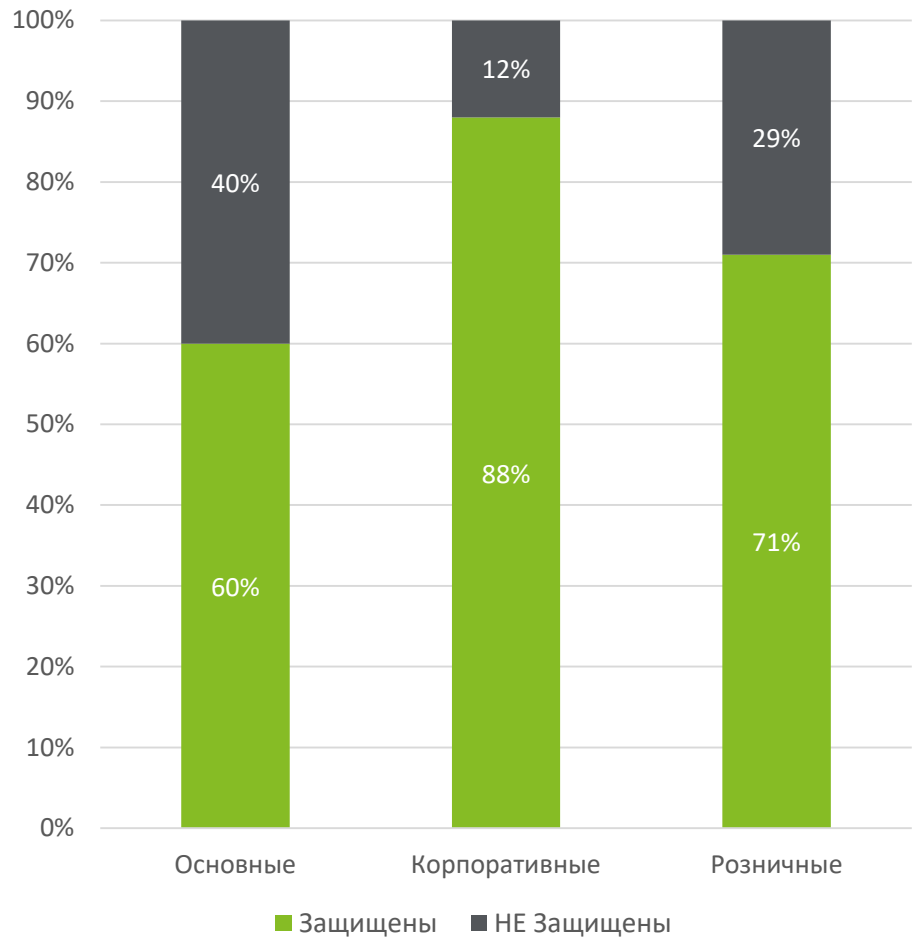
3. Безопасность HTTP

3.8 X-Powered-By

Заголовок X-Powered-By, по аналогии с предыдущим X-Powered-CMS, содержит информацию об используемых веб-сервером технологиях.

Такая информация также не несет серьезной опасности, при условии регулярного обновления программного обеспечения сервера. Однако, по возможности, лучше скрыть название и версию. Несоблюдение этого правила может сократить время, необходимое злоумышленникам для сбора информации и определения последующих векторов атаки.

Результаты исследования показывают, что в «основной» категории 60% доменов активировали данную меру защиты. Стоит отметить, что «корпоративная» категория показала наилучший результат 88%. Также «Розничная» категория показала хорошие результаты, 71%, что выше уровня «основной» категории.



3. Безопасность HTTP

3.9 X-Powered-CMS

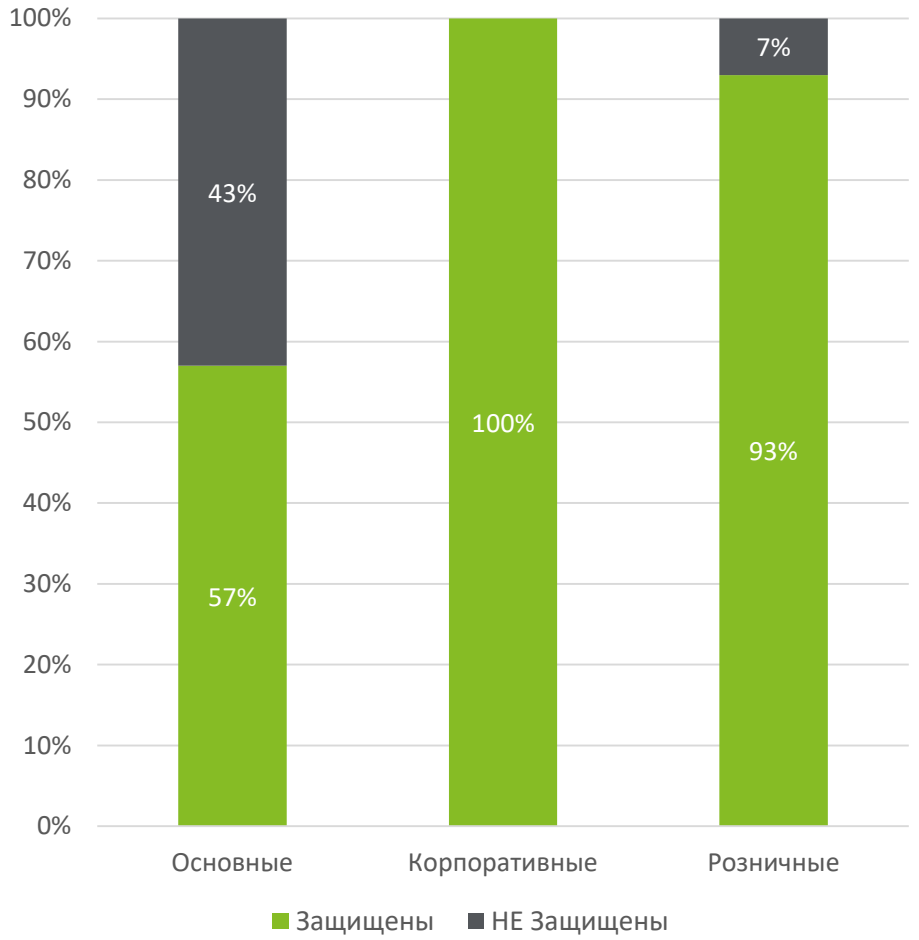
Заголовок X-Powered-CMS содержит имя и версию Content Management System (CMS), используемой для формирования ответа интернет-сайта, например, Битрикс или Express.

Сама по себе, такая информация не несет серьезной опасности. В особенности при условии регулярного обновления программного обеспечения сервера. Однако, лучше скрывать названия и версии технологий от посторонних глаз. Поскольку несоблюдение этого правила может сократить время, необходимое злоумышленникам для сбора информации и определения последующих векторов атаки.

Как показывает исследование, банки критично относятся к скрытию данной информации для Корпоративных и Розничных категорий интернет-сайтов.

«Корпоративная» категория показала наилучший результат, иными словами все банки этой категории применяют данную меру защиты. В «Основной» же категории веб-адресов, только 57% банков скрывают заголовок X-Powered-CMS.

Рекомендуется скрыть или подменить информацию о своей CMS. Так время необходимое на поиск потенциальных уязвимостей многократно возрастает, что обеспечивает дополнительную безопасность.



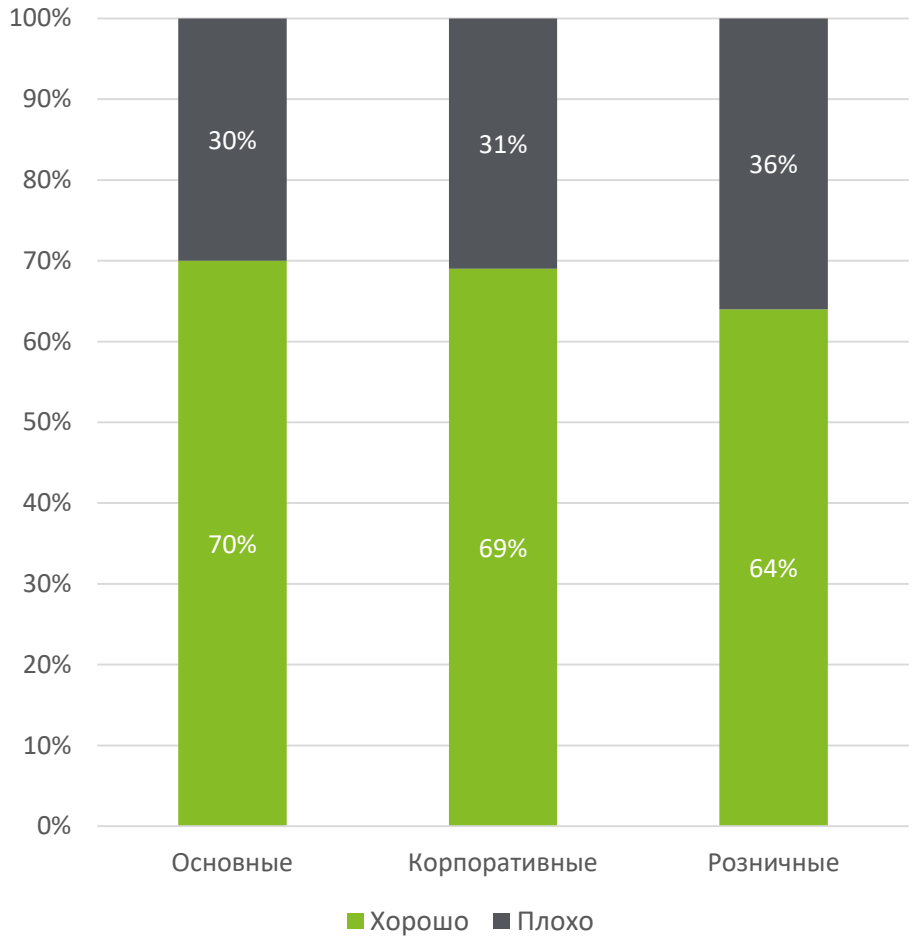
3. Безопасность HTTP

3.10 Server Header

Заголовок сервера предоставляет собой ответ содержащий информацию о программном обеспечении используемом сервером для обработки запросов. Часто встречаемые значения включают nginx/x.x.x, Apache/x.x.x и Microsoft-IIS/x.x.

Аналогично предыдущим двух заголовкам, такая информация не несет серьезной опасности. При условии регулярного обновления программного обеспечения сервера. Однако, по возможности, лучше скрыть название и версию используемого сервером программного обеспечения. Несоблюдение этого правила может сократить время, необходимое злоумышленникам для сбора информации и определения последующих векторов атаки.

Результаты исследования показывают, что большинство банковских сайтов, вне зависимости от категории, следят за безопасностью и скрывают заголовок сервера. Стоит отметить результаты «основной» и «корпоративной» категорий, безопасность которых составила 70% и 69% соответственно.



3. Безопасность HTTP

Заключение

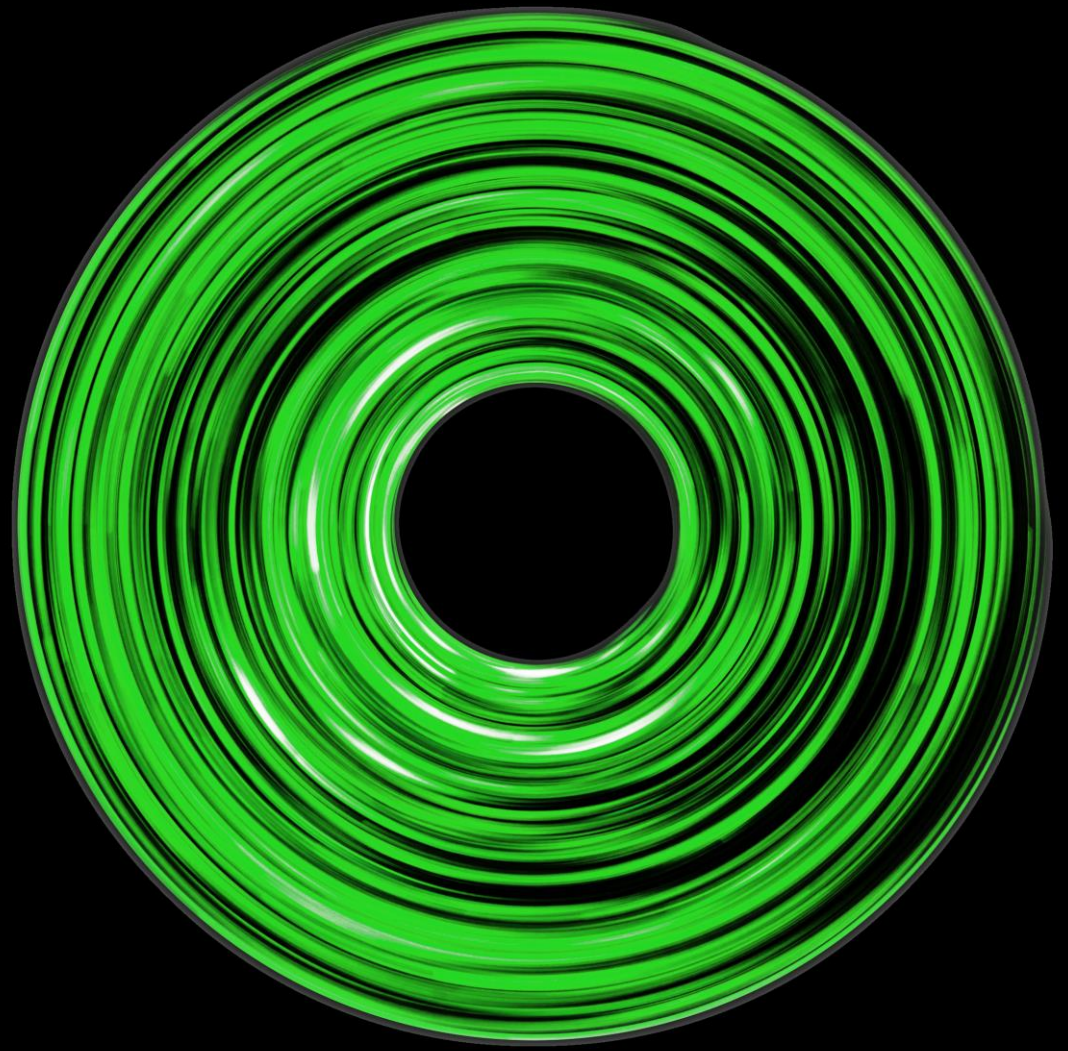
Настройка и поддержание безопасности банковских веб-ресурсов является сложной задачей, которая включает в себя большое количество мер защиты. Нарушение целостности любого из них может быть фатальным для всего сайта.

HTTP заголовки являются хорошей отправной точкой для надежной защиты веб-сайтов. Особенно принимая во внимание, что большинство из них достаточно легко реализовать на практике. Соблюдая требования лучших практик HTTP безопасности, заголовки обеспечивают дополнительный уровень безопасности поверх любых других мер защиты.

Обобщенный результат безопасности HTTP всех трех категорий узбекистанских банков показал, что в целом в 53% случаев данная мера обеспечения безопасности активно используется. Тем не менее, для другой 47% доли случаев все же рекомендуется воспользоваться рекомендациями по их использованию.

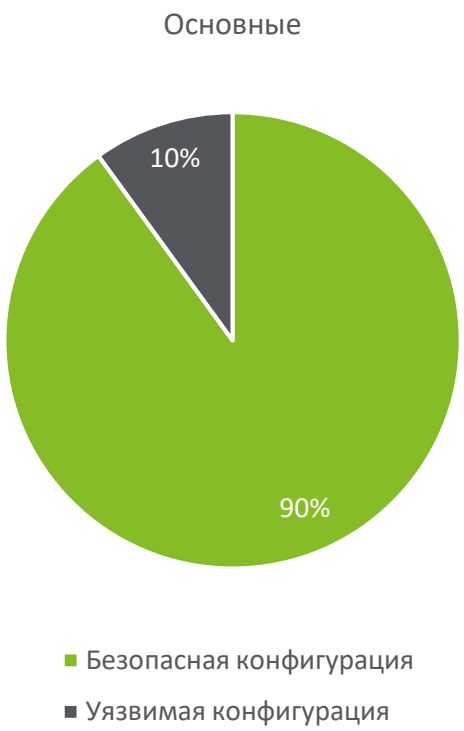
Обобщенный результат безопасности HTTP для всех категорий доменов по странам:

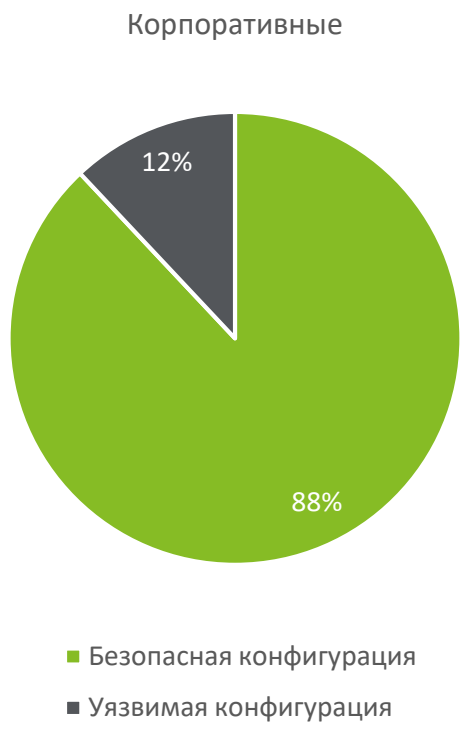
4. Защита трафика

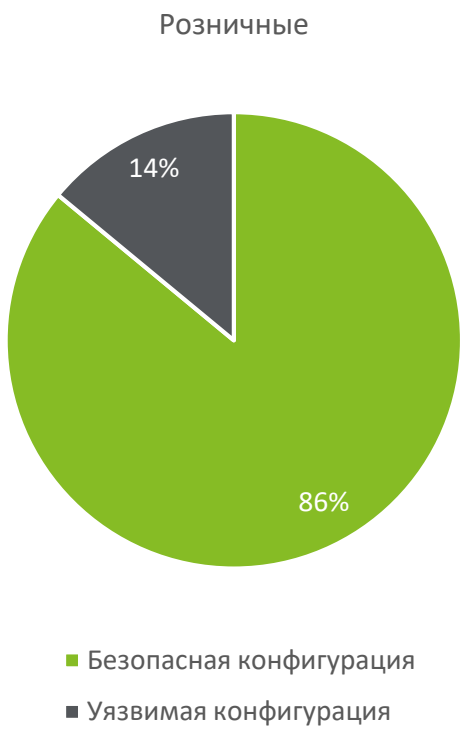


4. Защита трафика

Обобщенный результат всех проверяемых метрик доступности для «основной», «корпоративной» и «розничной» категорий доменов.







Результат нашего анализа показывает, что подавляющее число банков в должной мере понимает важность защиты трафика сайта вне зависимости от категорий доменов.

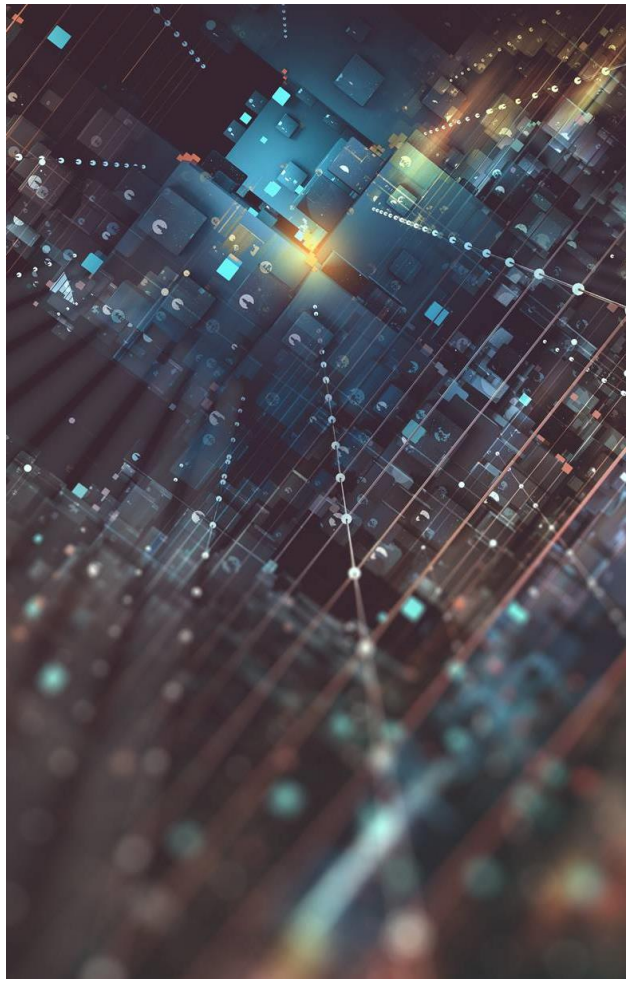
4. Защита трафика

Сегодня как потребители, так и компании выбирают услуги партнеров на основе HTTPS, который представляет собой защищенную версию распространенного протокола HTTP для доступа к веб-ресурсам. В HTTPS данные шифруются с помощью протокола Transport Layer Security (TLS) и предыдущей версии, Secure Sockets Layer (SSL). Эти криптографические протоколы являются наиболее популярными методами обеспечения безопасного обмена данными в Интернете.

Для SSL/TLS соединения, на сервере должен быть установлен цифровой сертификат, подтверждающий подлинность веб-сайта и владельца сайта. Это необходимо для того, чтобы гарантировать, что пользователь посещает подлинный ресурс, а не поддельную страницу, созданную злоумышленником.

Используя общедоступный ресурс SSLlabs были протестированы веб-серверы на наличие следующих уязвимостей:

- Weak DH parameters
- BEAST attack
- Heartbleed
- Ticketbleed
- OpenSSL CCS vuln. (CVE-2014-0224)
- OpenSSL Padding Oracle vuln. (CVE-2016-2107)
- ROBOT
- GOLDENDOODLE
- OpenSSL 0-Length (CVE-2019-1559)
- POODLE
- FREAK attack
- DROWN attack
- Поддержка TLS 1.1, TLS 1.0
- Поддержка SSL 3.0, SSL 2.0
- Поддержка RC4



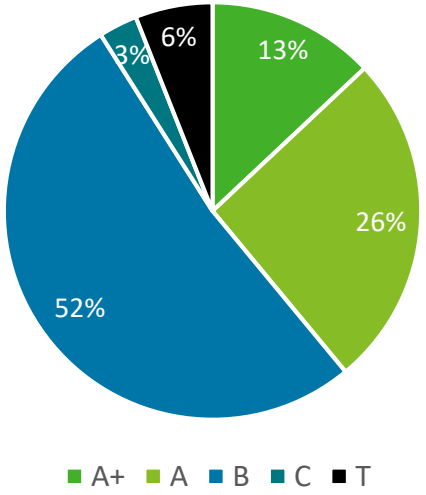
4. Защита трафика

4.1 SSL Labs

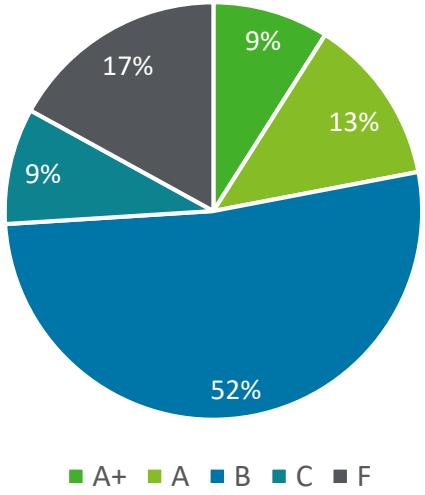
Предупреждения и ограничения, встроенные в браузеры, упростили определение того, насколько надежное шифрование использует сайт или сервис. Для оценки этих параметров использовался сервис Qualys SSL Labs и используемый этим сервисом рейтинг в порядке убывания A+, A, B, C, F. Так же SSL Labs может присвоить рейтинг T доменам чьи сертификаты оказались ненадежными.

Наилучшая оценка (A+) наблюдается у категорий «основные» и «корпоративные», однако стоит учесть, что 6% веб-адресов «основной» категории классифицируется как ненадежные. Также в «розничной» категории наблюдается самый высокая доля хороших оценок «A» и «B», 18% и 55% соответственно.

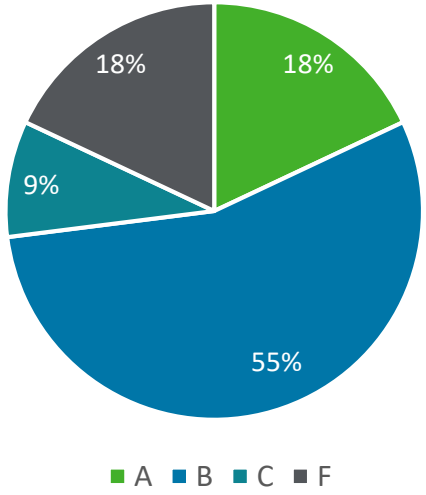
Основные



Корпоративные



Розничные



4. Защита трафика

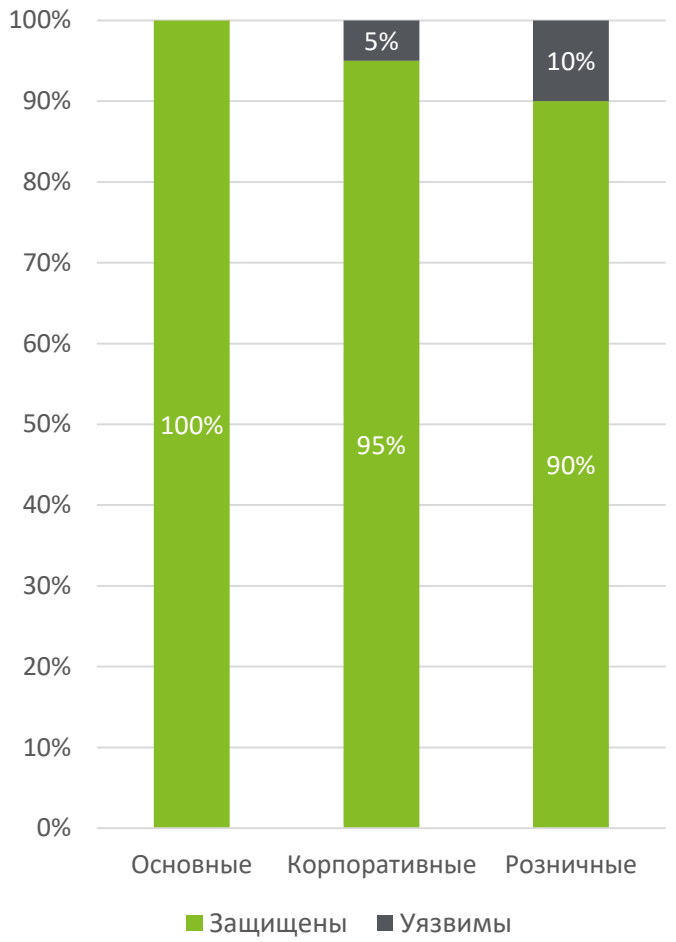
4.2 Слабые параметры Диффи-Хеллмана

Для безопасной зашифрованной связи между двумя участниками необходим предварительный обмен ключами по какому-либо защищенному физическому каналу, например, бумажные списки ключей, передаваемые доверенным курьером. Метод обмена ключами Диффи-Хеллмана позволяет двум сторонам, не знающим друг друга, обмениваться секретным ключом по незащищенному каналу связи. Далее этот ключ может быть использован для шифрования последующих сообщений с помощью некоторого алгоритма шифрования с симметричным ключом.

Веб-сайты, использующие одну из немногих распространённых 1024-битных групп Диффи-Хеллмана, могут быть подвержены пассивному перехвату злоумышленниками, обладающими соответствующими ресурсами. Чтобы повысить надежность обмена ключами, следует использовать более крупные простые числа, например, 2048-битные простые числа. Безопаснее будет перейти на протокол Диффи-Хеллмана, использующий эллиптические кривые. Эллиптические кривые не страдают от распространенных проблем предварительного вычисления, что означает, что атаки на параметры, которые едва поддаются вычислению, могут скомпрометировать лишь одно соединение, а не все, использующие данную группу.

Слабые настройки розничной категории дают основание полагать, что настройка их безопасности не является приоритетной. Однако, не стоит забывать, что нередко пользователи используют одни и те же данные для входа, а значит при перехвате злоумышленниками данных одного из веб-сайтов, может означать получение доступа к данным на более защищенном веб-сайте.

Согласно результатам Обзора, параметры Диффи-Хеллмана среди всех категорий доменов настроены безопасно. Только 5% корпоративных доменов и 10% доменов розничных категорий были оценены как уязвимые.



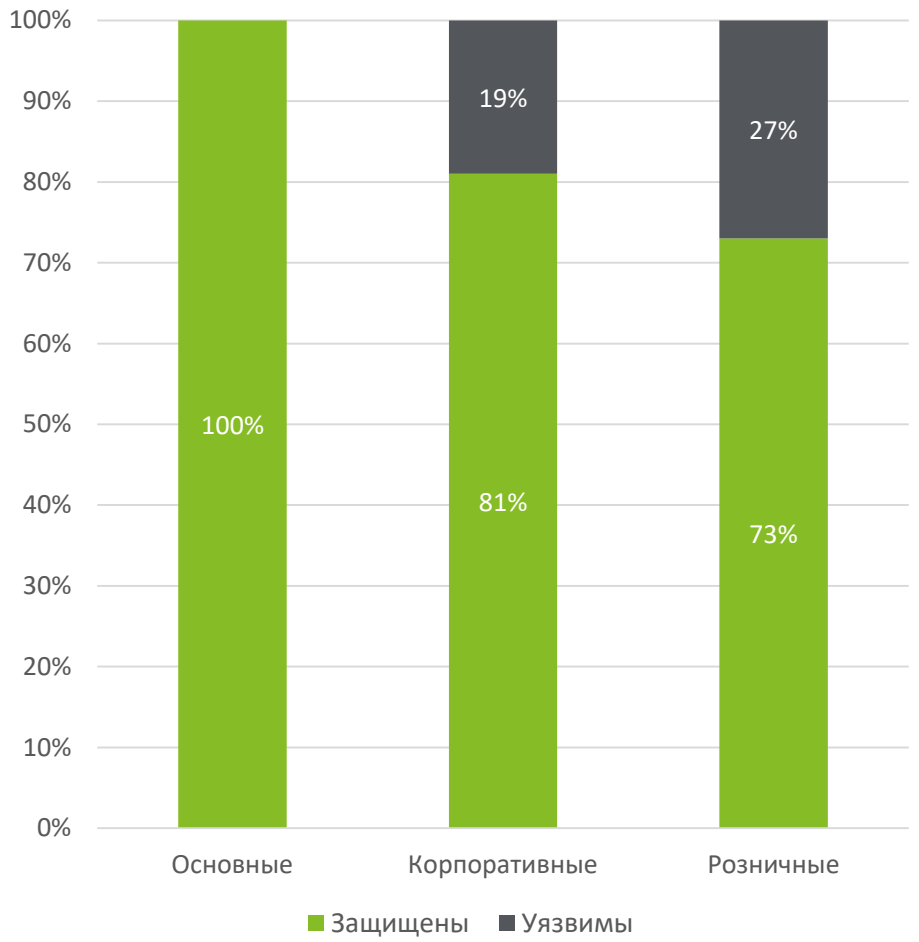
4. Защита трафика

4.3 Поддержка RC4

RC4, также известный как ARC4 или ARCFOUR – потоковый шифр, широко используемый в компьютерных сетях (в протоколах SSL и TLS, алгоритмах беспроводной безопасности WEP и WPA), а также различных системах информационной безопасности. Алгоритм RC4, как и любой шифр потока, основан на псевдо-случайном генераторе битов. Ключ записан на ввод генератора, а псевдо-случайные биты считываются на выходе. Длина ключа может быть от 40 до 2048 битов.

RC4 больше не считается безопасным, и целесообразность его применения требует тщательного рассмотрения. Так, поддержка RC4 на веб-сайте позволяет расшифровать часть зашифрованного трафика HTTPS (например, идентификатор сеанса, передаваемый в Cookies) за десятки часов. Также становится возможной реализация атаки типа Man-in-the-Middle, подслушивая и сохраняя зашифрованный трафик, и исполнение большого количества запросов от имени жертвы.

Согласно результатам обзора, ни один из доменов основной категории не поддерживают устаревший и ненадежный RC4. В то же время домены корпоративных и розничных категорий отключили поддержку в 81% и 73% сайтов соответственно.



4. Защита трафика

4.4 Поддержка SSL 2.0 и SSL 3.0

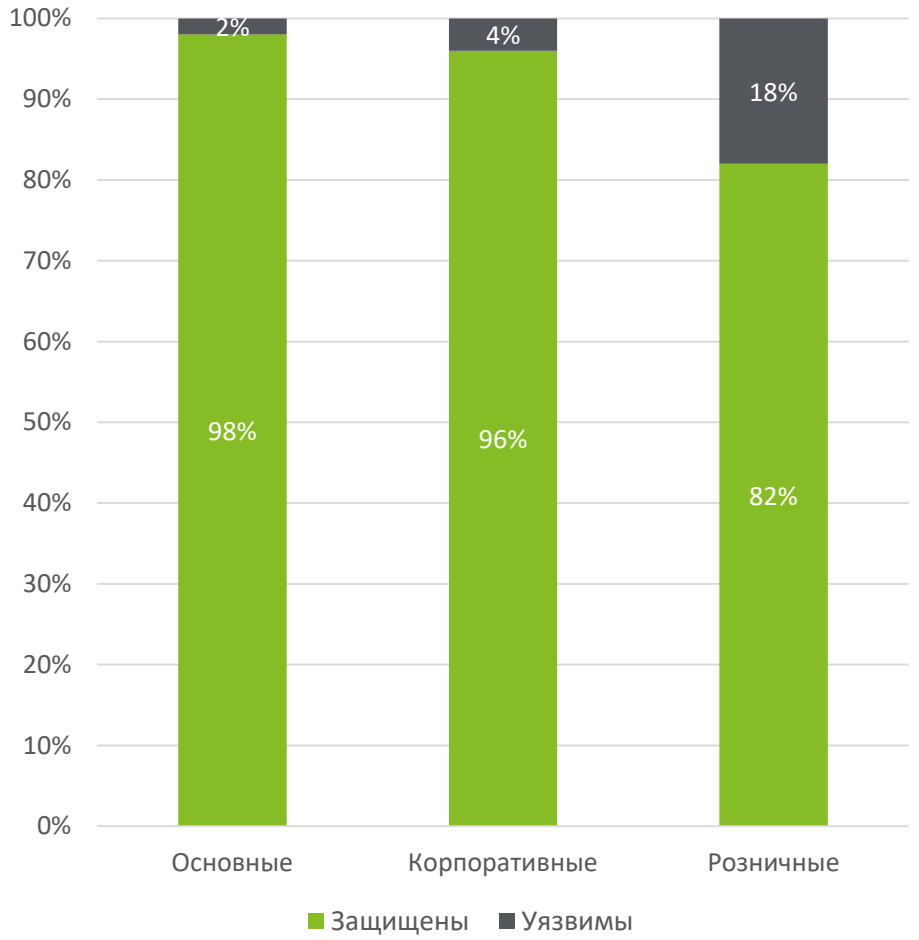
SSL и TSL являются протоколами шифрования и авторизации. С помощью этих протоколов передача данных осуществляется безопасно с сервера на сервер или с сервера на клиент. TSL является улучшенной версией SSL. Тем не менее, некоторые общедоступные веб-ресурсы по-прежнему поддерживают SSL для шифрования.

В 1995 году SSL был впервые опубликован Netscape как SSL 2.0. Однако, эта версия, имела серьезную уязвимость, что привело к замене в 1996 году на более новую версию, SSL 3.0.

Ряд уязвимостей был обнаружен в SSL 2.0 и 3.0 с 90-х годов, некоторые из которых были подтверждены IEFT в 2011 и 2015 годах. Многие из этих уязвимостей больше не несут угрозы, но на практике SSL не так надежен, как должно быть.

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

Оценка поддержки SSL 2.0 и SSL 3.0 показал, что почти у всех проверенных доменов протоколы шифрования SSL были отключены, что в свою очередь означает хорошую защищенность.



4. Защита трафика

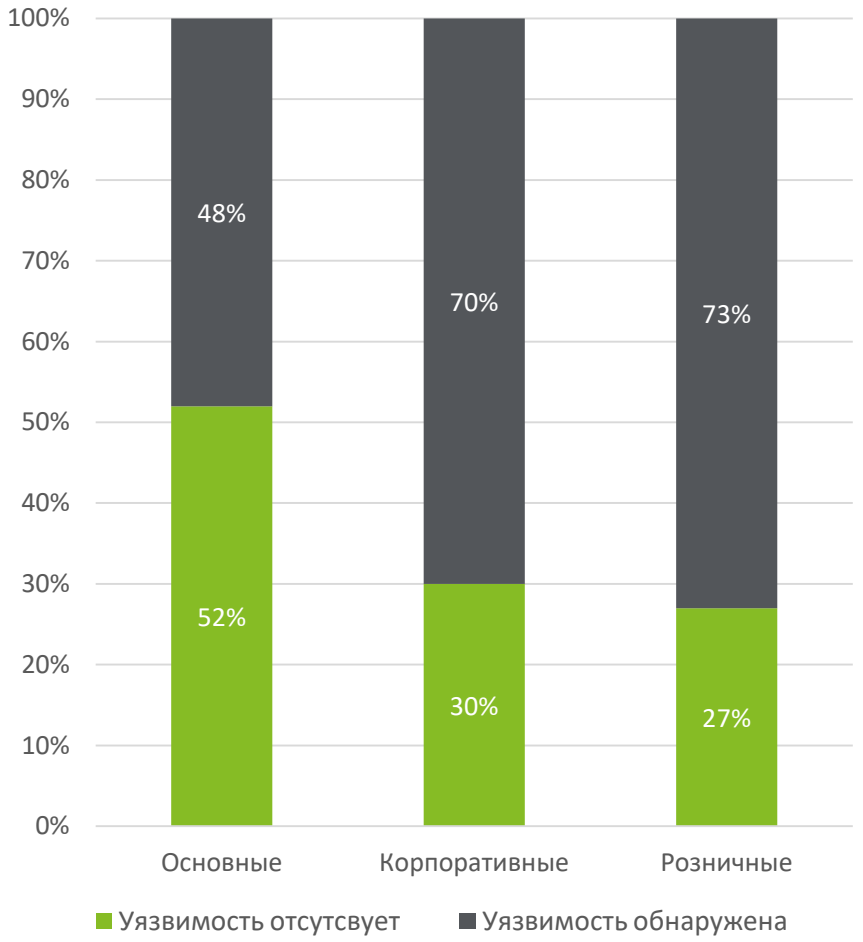
4.5 Устаревшие версии TLS

Transport Layer Security гарантирует зашифрованную связь для обеспечения безопасности и конфиденциальности. TLS версии 1.0 существует с 1999 года, и представляет собой развитие более старого протокола шифрования SSL. В настоящее время существует также более современный TLS 1.2, который появился в августе 2008 года, и самый актуальный TLS 1.3, выпущенный в августе 2018 года.

В 2011 году была обнаружена уязвимость в 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 отключили поддержку TLS 1.0 и TLS 1.1. Отключение этих протоколов также рекомендуется на стороне сервера.

В результате исследования, мы обнаружили, что более 70% корпоративных и розничных доменов, сохранили поддержку устаревших версий TLS. Одновременная поддержка старых и более новых версий TLS, дают основание полагать, что старые версии были сохранены для обеспечения совместимости со старыми версиями браузеров. В то время как результаты «основной» категории показывают, что только у 52% веб-адресов установлены новые версии сертификатов и отключены старые версии.

Оставшимся веб-сайтам рекомендуется отключить поддержку устаревших версий, поскольку их наличие повышает риски потенциальной угрозы расшифровки данных.



4. Защита трафика

4.6 Уязвимость BEAST

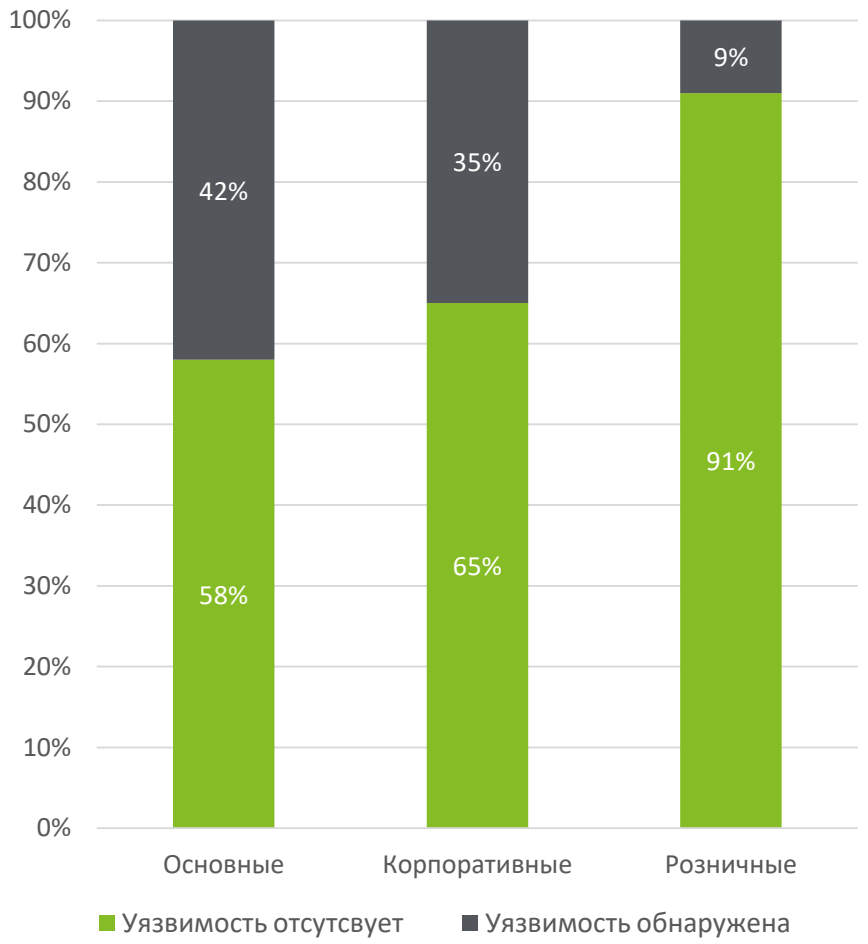
Злоумышленники могут расшифровать данные, передаваемые между двумя участниками, использующими TLS 1.0, SSL 3.0 и ниже. Для осуществления данной атаки, злоумышленник и жертва , атакующий и жертва должны находиться в одной и той же сети (man-in-the-middle).

Используя метод BEAST, пароли могут быть разбиты на небольшие пакеты и расшифрованы. Хакеры, расшифровывающие за две секунды один байт данных, за полчаса могут получить доступ к учетным данным, используя систему аутентификации из 1000-2000 символов.

Наиболее эффективным способом защиты пользователей от атак типа BEAST является отключение на стороне сервера поддержки протокола SSL и протокола TLS старше версии 1.2.

В результате исследования обнаружено, что несмотря на поддержку устаревшего протокола SSL и версий TLS старше 1.2, большинство розничных веб-сайтов митигировали уязвимость BEAST на стороне сервера. Однако, в случае «основных» и «корпоративных» веб-сайтов близость процентов уязвимости BEAST и поддержке устаревших протоколов говорит об отсутствии митигации данной уязвимости.

Оставшимся веб-сайтам рекомендуется отключить поддержку устаревших версий TLS или провести митигацию уязвимости Beast, так как поддержка старых версий TLS повышает риски потенциальной угрозы перехвата данных.



4. Защита трафика

4.7 SSL Renegotiation

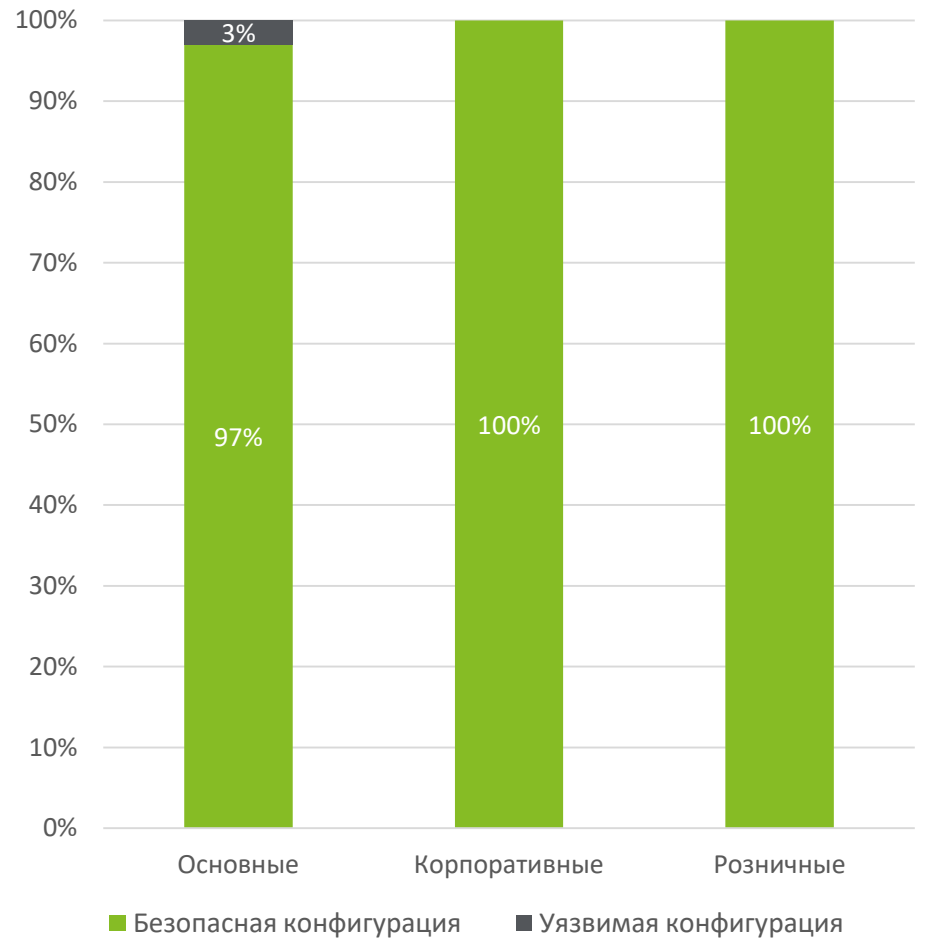
SSL Renegotiation – возобновление воссоединения с сервером с имеющимися аутентификационными данными внутри существующего защищенного сеанса.

Неправильная конфигурация SSL Renegotiation может стать причиной таких атак как Denial of Service (DOS) или атака инъекционного типа Man-in-the-Middle (MITM) в HTTPS-сессии. Поэтому, некоторые разработчики предпочитают отключать SSL Renegotiation на стороне сервера.

Однако при отключении функции Renegotiation и отсутствии индикации статуса безопасности возникают проблемы: некоторые серверы будут безопасны, другие нет, и браузеры ничего не могут сделать, не обладая информацией о надежности сервера. Это доставляет неудобства пользователям и заставляет их вручную настраивать уровни защиты.

Результаты нашего исследования показывают, что большинство сайтов, за исключением одного, обеспечивают поддержку правильной конфигурации данного параметра.

Рекомендуется настроить сервер на пропуск только безопасного SSL Renegotiation и ограничение количества SSL подключений.



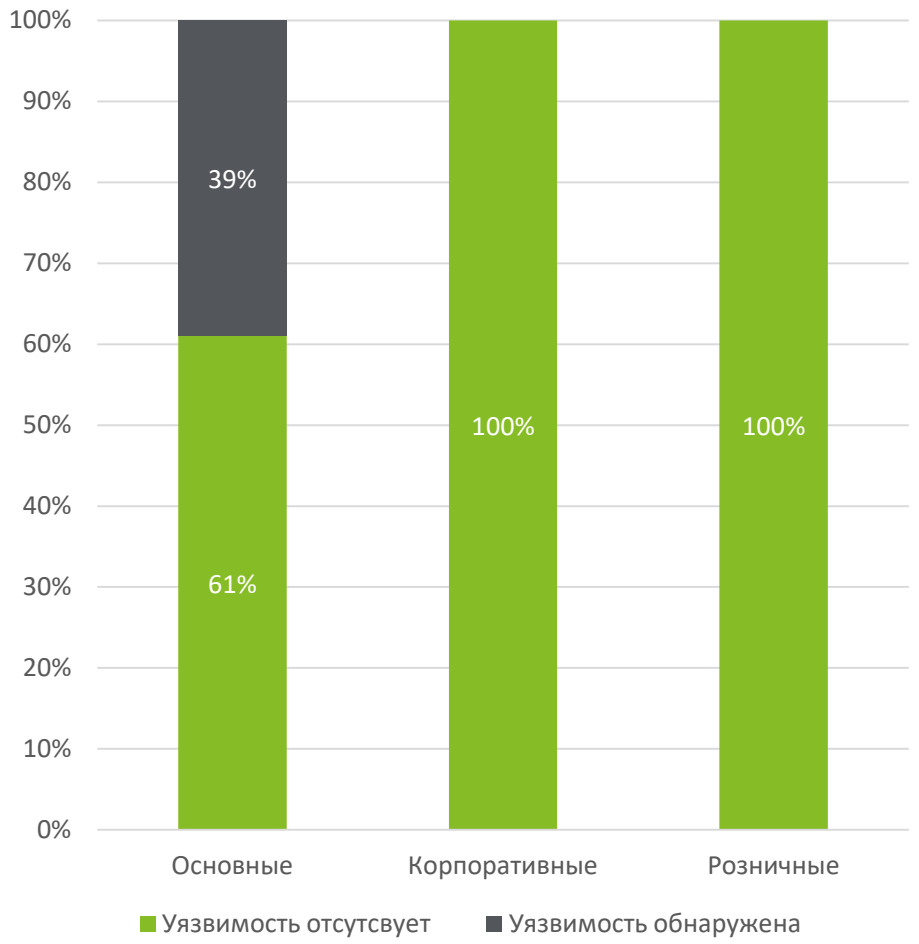
4. Защита трафика

4.8 SSL Уязвимость Ticketbleed

В начале 2017 года стало известно об уязвимости, наносящей вред исключительно продуктам F5. 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 от других подключений.

Исследование показывает, что в "корпоративных" и "розничных" категориях отсутствует уязвимость Ticketbleed, в то время как 39% доменов основной категории сайтов подвержена данной уязвимости.

Веб-сайтам уязвимым к Ticketbleed рекомендуется обновление версии TMOS для укрепления защиты домена.



4. Защита трафика

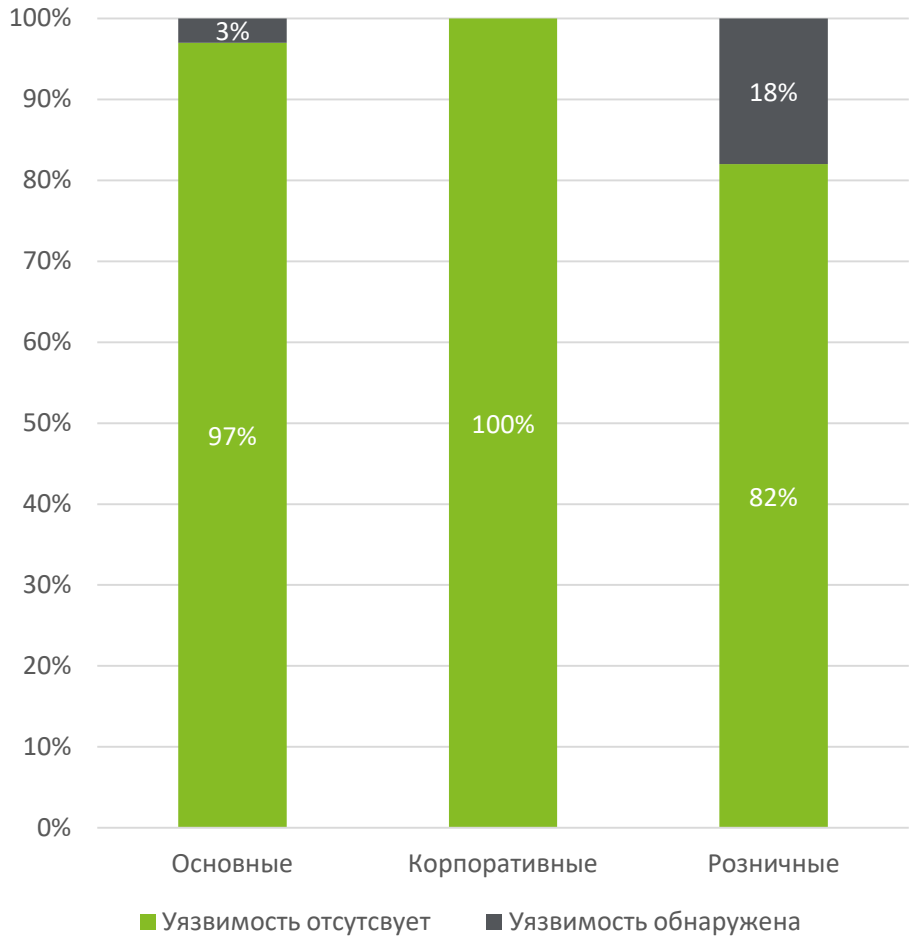
4.9 SSL Уязвимость Poodle (SSLv3)

Осенью 2014 года стало известно о новой атаке для давно устаревшего протокола SLL версии 3.0. Для взлома данная уязвимость использует особенности CBC схемы шифрования характерной для SLL v3 и некоторых имплементаций TLS.

По своей концепции данная уязвимость весьма схожа с уязвимостью BEAST. Для успешной эксплуатации POODLE злоумышленник должен быть способен внедрить вредоносный JavaScript в браузер жертвы, а также должен иметь возможность наблюдать и манипулировать зашифрованным сетевым трафиком в сети.

Результаты исследования показали, что у 97% «основой» и 100% «корпоративной» категорий данная уязвимость отсутствует, в то время как 18% веб-адресов «розничной» категории показали уязвимость к атакам.

Во избежание POODLE-атак рекомендуется полное отключение поддержки протокола SSL и устаревших версий TLS. Особенно для корпоративной категории сайтов.



4. Защита трафика

4.10 SSL Другие уязвимости

В дополнение к вышеуказанным наблюдениям, в рамках настоящего Обзора был проверен каждый веб-сайт на следующие уязвимости: ROBOT, GOLDENDOODLE, FREAK, DROWN и Heartbleed.

Ни один из веб-сайтов местных банков неуязвим для атак из указанного списка.

100%
веб-сайтов
не имеют уязвимостей
для указанных атак

4. Защита трафика

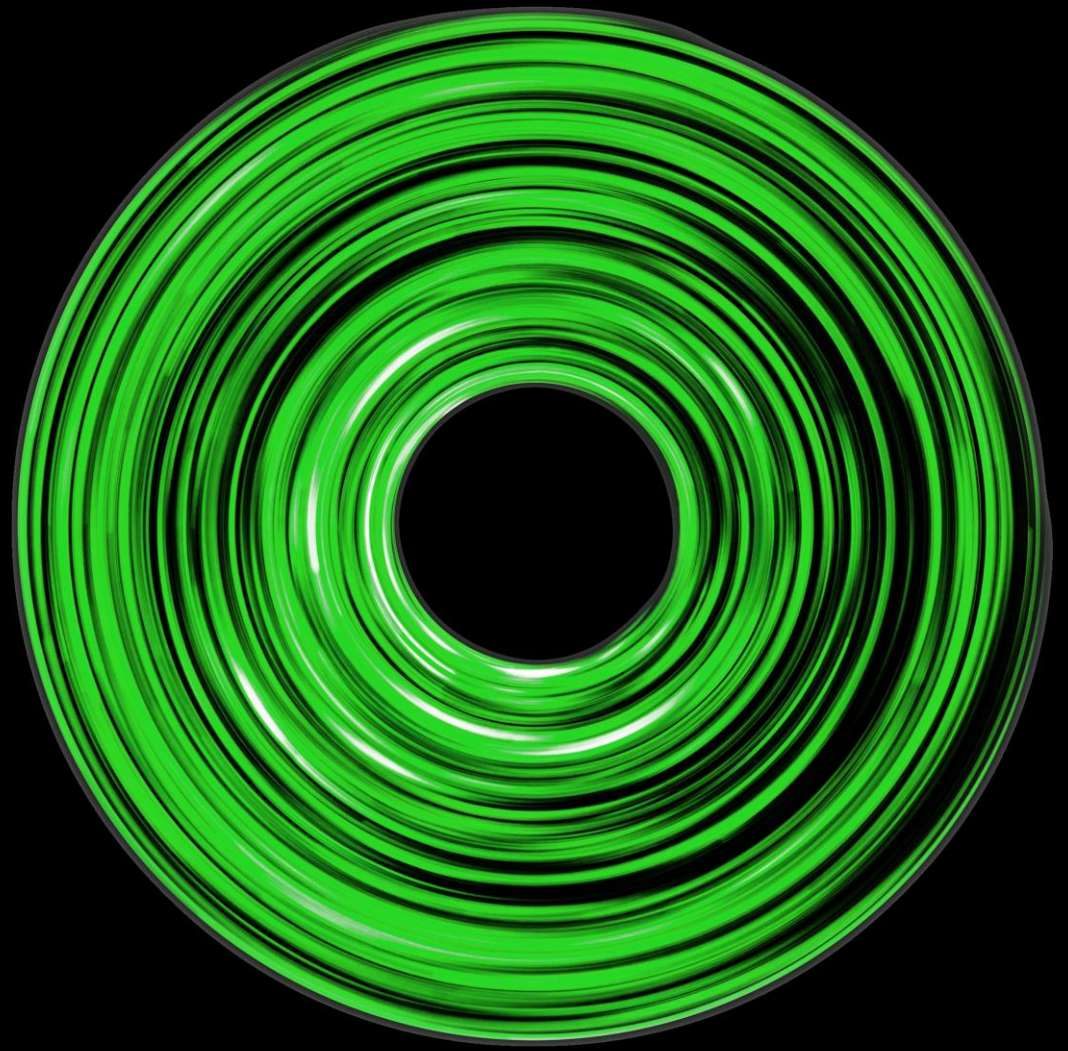
Заключение

Внедрение TLS имеет первостепенное значение для обеспечения безопасности данных в Интернете как самих банков, так и клиентов. Однако неправильно настроенные веб-серверы могут подвергать данные угрозе, а не защищать их.

Обобщенная оценка показала, что для большинство сайтов банков Узбекистана конфигурация SSL/TLS настроена на должном уровне с показателем в 89%. Тем не менее, некоторые банки по-прежнему поддерживают устаревшие версии протоколов, что делает их уязвимыми к потенциальным атакам.

Обобщенный результат для всех категорий в области защиты трафика по странам:

5. Безопасность почтового сервера



5. Безопасность почтового сервера

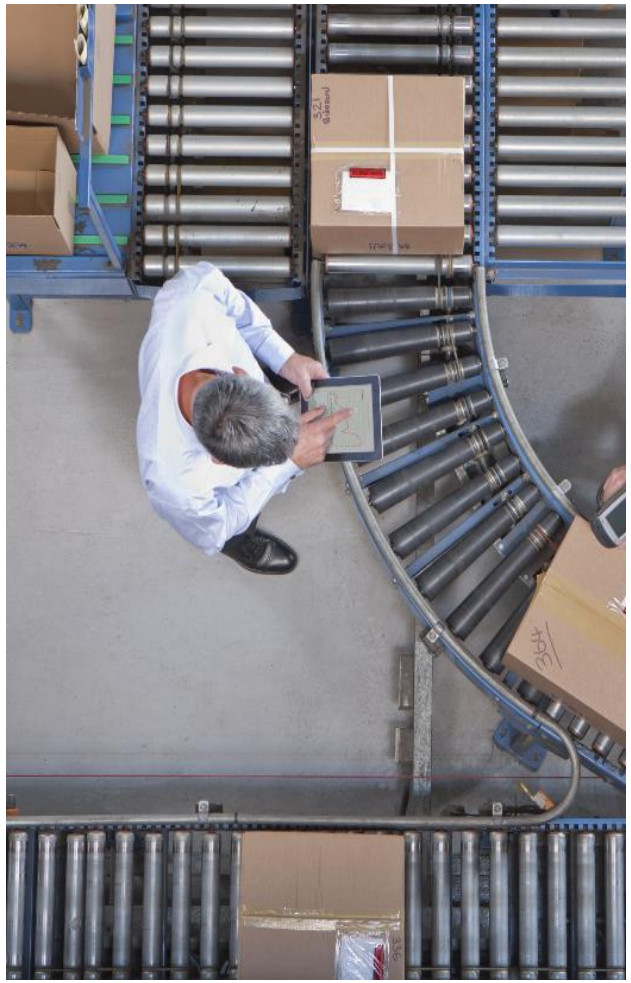
Распространенной точкой входа для злоумышленников, стремящихся закрепиться в корпоративной сети и получить ценные банковские данные, является электронная почта. Основная проблема при использовании электронной почты – это ее небезопасность. Уязвимости связанные с электронной почтой развязывают руки злоумышленникам 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 электронную почту.

Прежде чем применять комплексные методы защиты, важно убедиться, что применяются базовые параметры безопасности для защиты сотрудников компании и общего повышения репутации электронной почты. Так очень часто фильтры спама будут игнорировать письма отправленные с сервера банка, не воспринимая их, как вредоносные.

Для анализа основных настроек безопасности почтовых серверов был составлен список почтовых (MX) серверов по серверному имени каждого банка (с помощью MX Lookup). После с помощью инструмента диагностики SMTP с сайта mxtoolbox.com были проверены следующие настройки безопасности:

- SMTP Valid Hostname
- SMTP Banner
- SMTP TLS
- SMTP Open Relay
- SMTP Connection Time
- DMARC
- Domain Keys Identifies Mail

Также с помощью сайта checktls.com была проведена проверка валидности сертификатов TLS.



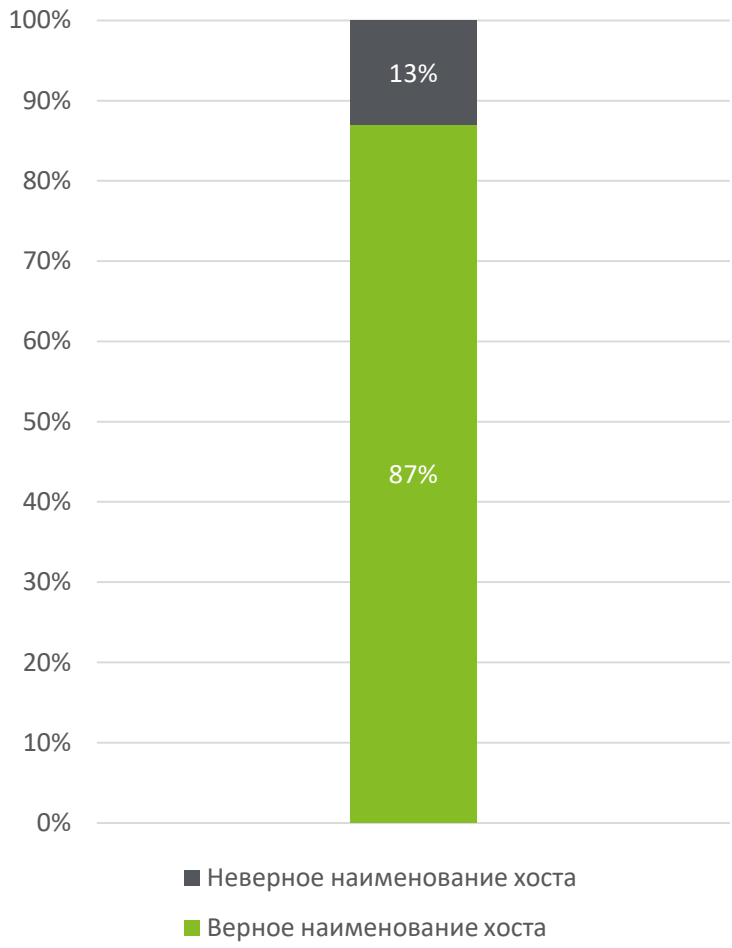
5. Безопасность почтового сервера

5.1 SMTP Valid Hostname

Тест проверяет, 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 того, что могут возникнут проблемы при доставке электронной почты посредством служб защиты от спама.

MxToolbox выдает две оценки корректности названия хоста: верное наименование или неверное наименование.

По результатам исследования 87% банков Узбекистана имеют верное наименование хоста.



5. Безопасность почтового сервера

5.2 Проверка SMTP Banner

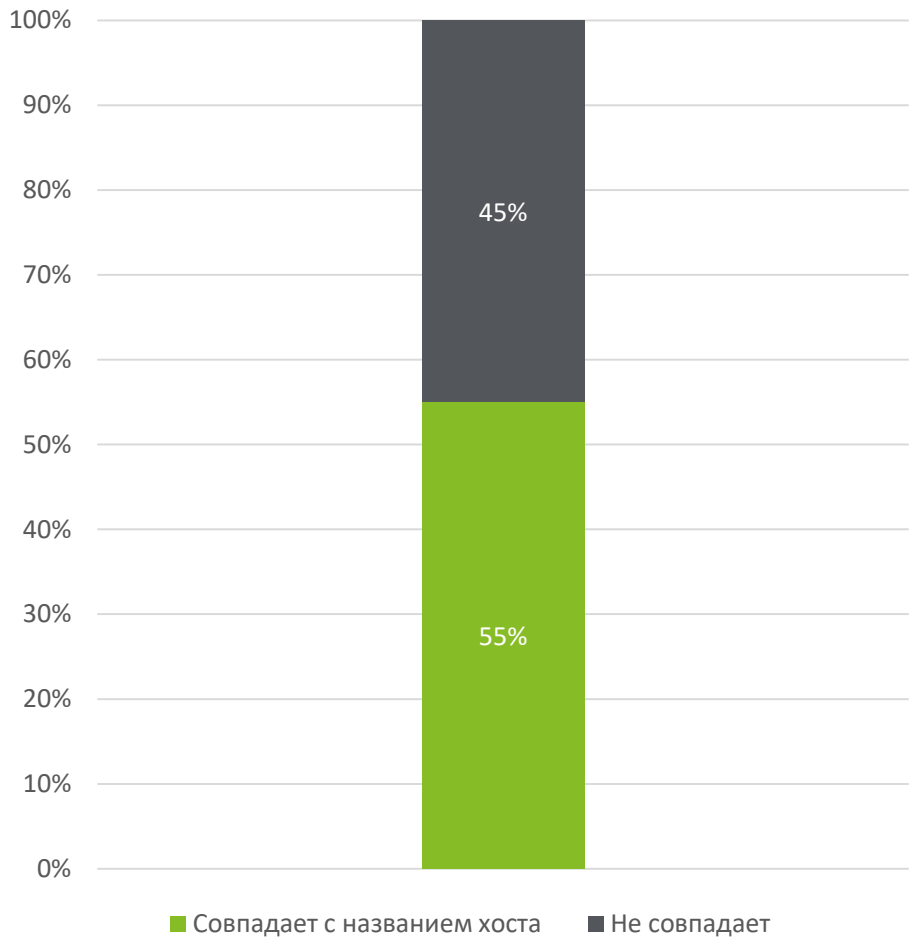
Сервера электронной почты отвечают на соединения на 25 порт с помощью строки текста, который называется SMTP-баннер. Основная цель - объявить сервер и любую информацию, которую администратор хотел бы предоставить стороне устанавливающей соединение. Лучше всего указать имя сервера в баннере SMTP, чтобы любой, кто подключается к IP-адресу, имел представление о том, к кем он «общается».

Еще недавно многие сервера «маскировали» свои SMTP баннеры, заменяя символы звездочками для всех, кто находится за пределами локальной сети. Логика, лежащая в основе этого заключалась в том, что владельцы не хотели разглашать какую-либо информацию о себе из-за страха предоставить информацию, которая может помочь им при возможной атаке на сервер. Выгоды от этого минимальны, и многие сервера выполняют проверку баннеров как часть защиты от спама, поэтому такая практика сопряжена с негативными факторами.

Некоторые почтовые сервера могут использовать несоответствующий или замаскированный баннер, как индикатор возможного источника спама в системе скоринга, но большинство не будет отклонять входящую почту исключительно на этом основании.

Если у сервера нет PTR записи в DNS или запись не совпадает с именем хоста, то рекомендуется организовать/актуализировать данную обратную (PTR) запись, которая будет соответствовать имени хоста вашего почтового сервера.

Согласно результатам тестирования, 55% имен хостов совпадают с обратной записью (PTR) и 45% из них не совпадают.



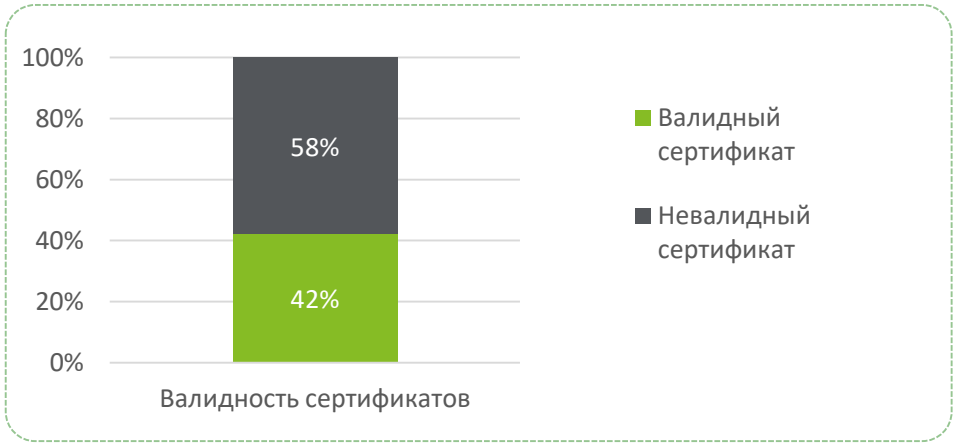
5. Безопасность почтового сервера

5.3 SMTP TLS

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.

Согласно полученным результатам, 80% почтовых серверов поддерживают TLS. В 20% почтовых серверов при попытке установить защищенное SMTP соединение выдали ошибку.

Также в ходе исследования помимо наличия поддержки TLS, была проведена проверка на валидность сертификатов. При проверке выяснилось, что среди 80% почтовых серверов, которые поддерживают TLS, только 42% успешно прошли проверку на валидность сертификатов.



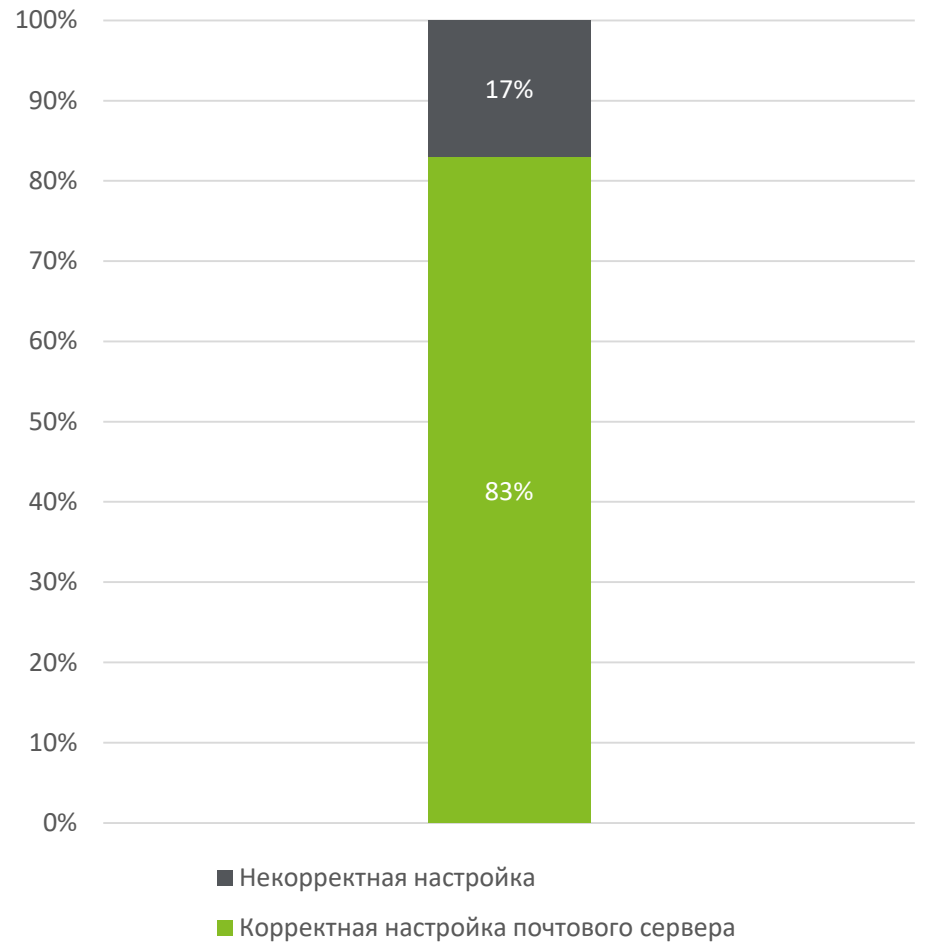
5. Безопасность почтового сервера

5.4 SMTP Open Relay

Многие почтовые сервера теперь делают вид, что принимают неправильно адресованное письмо, но затем отбрасывают это сообщение, не пересылая отправителю ответ на него. Этот метод используется для предотвращения атак направленных на сбор информации. При такой атаке злоумышленник пытается отправить тысячи автоматически сгенерированных сообщений электронной почты из вашего сервера в попытках найти действительные почтовые адреса. 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 адрес действительный.

Во время исследования были сымитированы отправки сообщений на заведомо ошибочный адрес электронной почты (test@example.kz). Далее, на основании полученных ответов определяли, является ли сервер открытым ретранслятором, т.е. принимает ли он почту от неизвестного сервера, и затем передает ее соответствующему серверу.

По результатам исследования 83% банков получили рейтинг «Корректная настройка», а 17% - «Не корректная настройка».



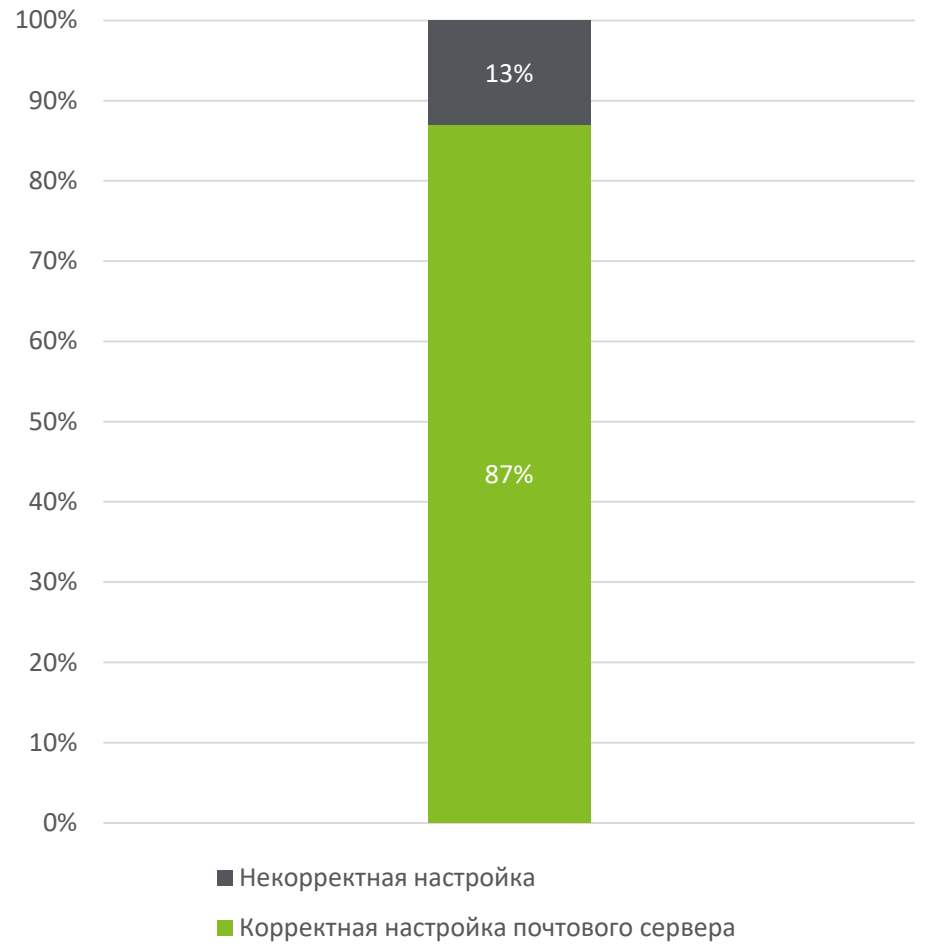
5. Безопасность почтового сервера

5.5 SMTP Connection Time

В процессе проверки SMTP Connection Time, устройство подключается к почтовому серверу через открытые порты и иногда подключение занимает гораздо больше времени, чем ожидалось. Это может указывать на то, что почтовый сервер находится под большой нагрузкой.

Результат ответа на запрос проверки времени соединения измеряется в секундах. Показатели меньше 5 с считаются быстрым временем ответа и попадают в категорию «Хорошо», ответ от 5 с до 8 с – «Предупреждение», и выше 8 с – «Опасно».

В результате исследования ни один почтовый сервер не получил оценку «Опасно», однако, 13% почтовых серверов отвечали в пределах 5 - 8 секунд. Это не означает, что возникнут проблемы с пересылкой почты. Пока это только предупреждение о том, что ситуация не является оптимальной. При увеличении объемов корреспонденции или уменьшении полосы пропускания каналов передачи данных это может привести к возникновению задержек с пересылкой электронной почты.



5. Безопасность почтового сервера

5.6 Domain Keys Identified Mail

Технология DomainKeys Identified Mail (DKIM) используется для предотвращения «спуфинга» при отправке писем из вашего домена.

Спуфингом называется изменение письма злоумышленником, которое позволяет ему выдать себя за другое лицо. 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.

По результатам обзора было определено, что все банки применяют собственный ключ DKIM для всех исходящих сообщений.

100%
доменов
применяют технологию DKIM

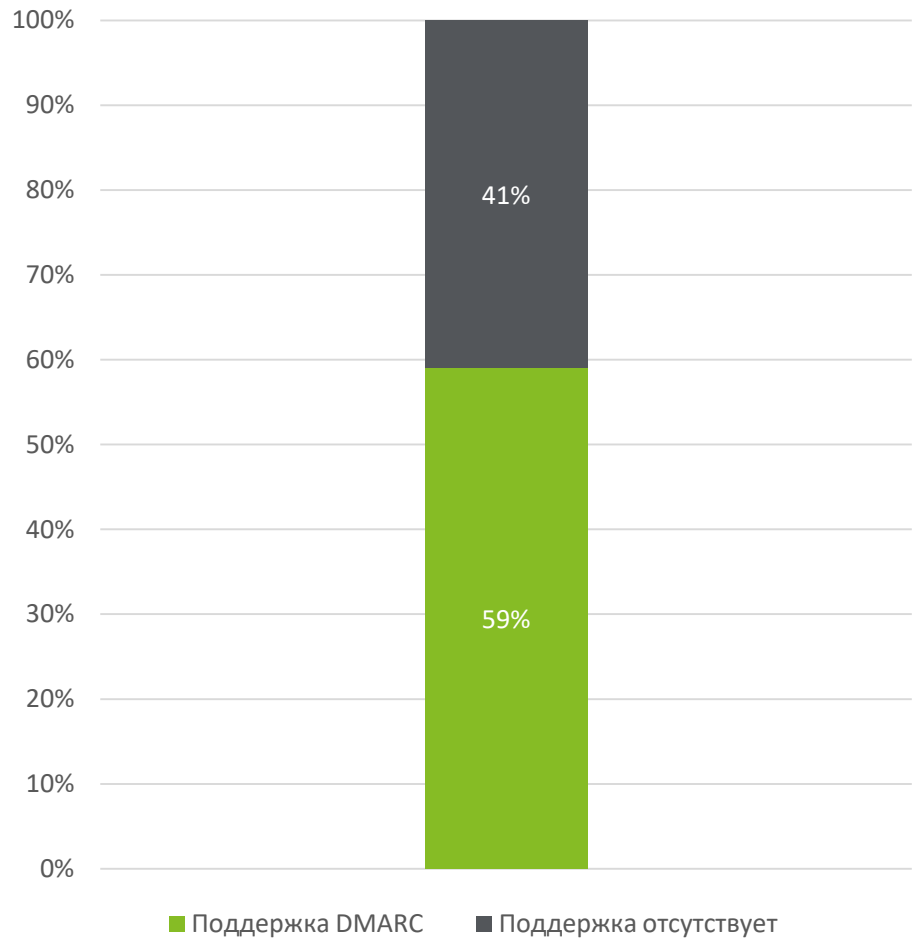
5. Безопасность почтового сервера

5.7 Domain -based Message Authenticator Reporting and Conformance

Domain-based Message Authentication Reporting and Conformance (DMARC) — один из механизмов защиты организаций от фишинговых атак с использованием собственного почтового сервера. Ведь не секрет, что для успешной фишинговой атаки письмо должно быть максимально похожими на легальное. Залогом успеха в таком случае будет возможность отправки письма непосредственно посредством почтового сервера атакуемой организации.
В защищенном исполнении, почтовый сервер проверяет соответствует ли сервер email адреса в строке «От:» идентификаторам проверки SPF и подписи DKIM. Если совпадение абсолютное, письмо признается легитимным и отправляется во почтовый ящик получателя. Если же есть малейшие несоответствия, такое сообщение обрабатывается согласно настроенной политике DMARC.

Результат исследования показал, что больше половины почтовых серверов применяют данный механизм защиты (59%) и 41% - не применяют DMARC.

Для улучшения показателя безопасности, рекомендуется начать с нестрогого правила DMARC, ежедневно проверять отчеты и изучать возникшие проблемы, отправить в карантин небольшой процент писем и назначить правило отклонения для всех писем, не прошедших аутентификацию.



5. Безопасность почтового сервера

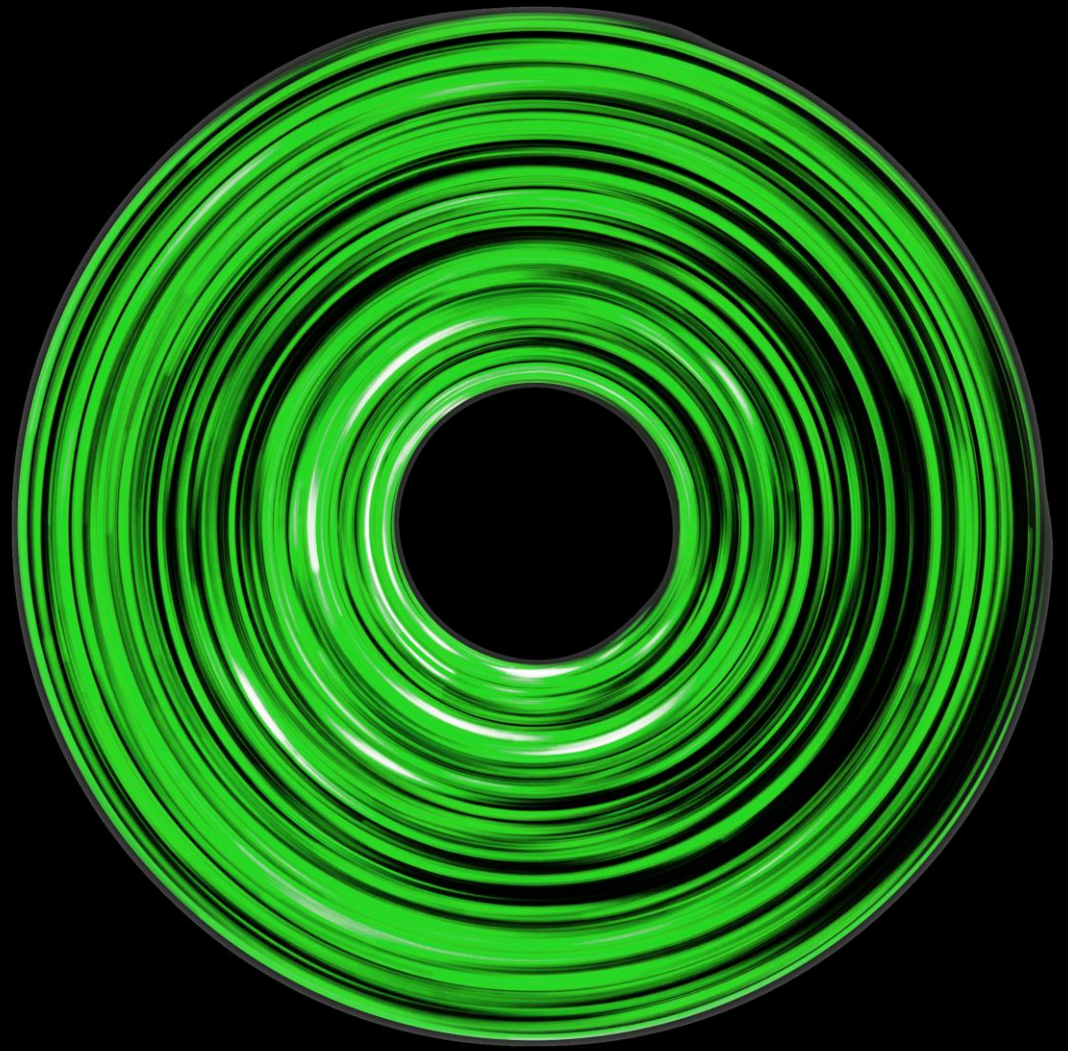
Заключение

Несмотря на активное использование сотрудниками банков всевозможных мобильных мессенджеров, электронная почта остается одним из официальных инструментов коммуникации. При этом это касается взаимодействия как с внутренними банковскими структурами, так и с внешними организациями. В этой связи, обеспечение высокого уровня безопасности при работе с электронной почтой является одной из важных задач.

Обобщенные результаты показывают хорошие результаты. Тем не менее, некоторые из мер, повышающих уровень защиты данной услуги, еще не нашли применения в части банков Узбекистана. В связи с этим мы рекомендуем уязвимым банкам этой части внедрить необходимые меры защиты на почтовых серверах.

Обобщенный результат безопасности почтовых серверов по странам:

6. Утечки адресов электронной почты



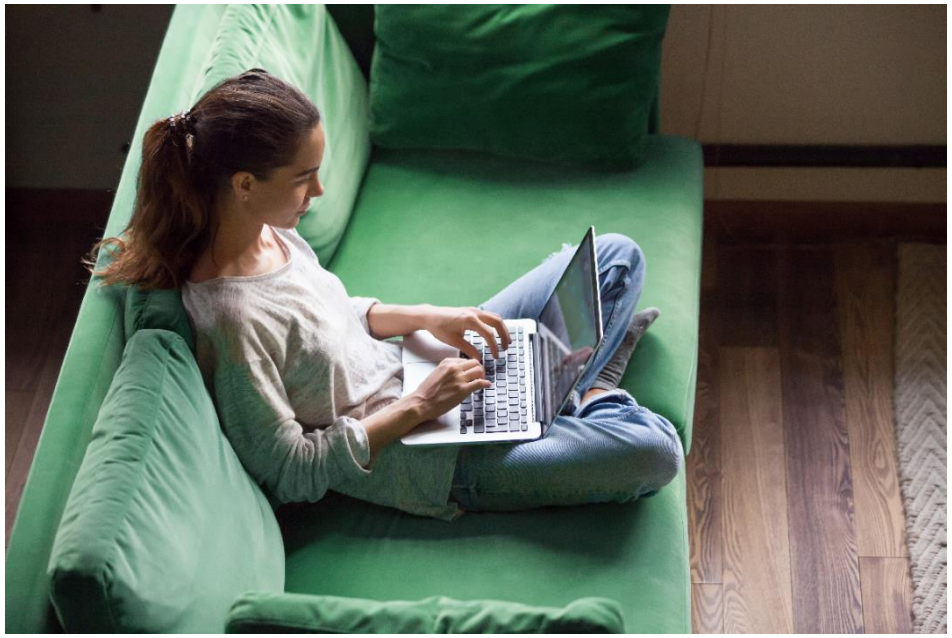
6. Утечки адресов электронной почты

В мире, факты утечек данных фиксируются довольно часто. Это является одним из недостатков цифрового мира. Даже в тех случаях, когда организация ответственно подходит к защите своих информационных ресурсов, и применяет наиболее современные технические инструменты защиты. Человеческий фактор по-прежнему остается одной из наиболее существенных уязвимостей.

Сотрудники организаций, слабо осведомленные в вопросах кибербезопасности, часто используют корпоративные электронные адреса для регистрации на сторонних веб-ресурсах. При этом сама по себе, такая утечка корпоративного адреса электронной почты уже может сулить его возможное использования для целей рассылки нежелательной электронной корреспонденции (SPAM). Но усугубляет данную ситуацию то обстоятельство, что зачастую сотрудники используют одни и те-же пароли. Либо пароли в которых изменяется только один-два символа. В результате, в руках злоумышленников может оказаться как адрес корпоративной электронной почты, так и пароль к ней.

Имея доступ к корпоративным электронным письмам можно например получить доступ к конфиденциальной или персональной информации клиентов. Также он может быть использован и для проведения фишинговых атак на других сотрудников организации. Конкретные последствия таких утечек трудно предугадать, но скорее всего они будут негативными.

В сети Интернет 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, была ли какая-либо конкретная электронная почта подвержена утечке. Если, такие утечки имелись, то сервис предоставит подробную информацию о ней.



6. Утечки адресов электронной почты

6.1 Наш поход к оценке и результаты

Для целей настоящего Обзора, была изучена общедоступная информация из социальных сетей (например, LinkedIn). На основе полученных таким образом данных был сформирован целевой список сотрудников казахстанских банков. На следующем шаге, используя Интернет-ресурс Hunter.io были определены используемые банками шаблоны электронной почты и сгенерирован перечень целевых электронных адресов для каждого банка. Сформированные нами списки электронных адресов были проверены на предмет их наличия в списках утечек. Для этих целей был использован Интернет-сервис haveibeenpwned.com.

Полученные статистические данные сведены на графиках с права.

Результаты указывают на то, что из всех проверенных банков только у двух были найдены утечки почтовых адресов в количестве не больше двух.

Всего
2 банка
с количеством утечек
не больше 2

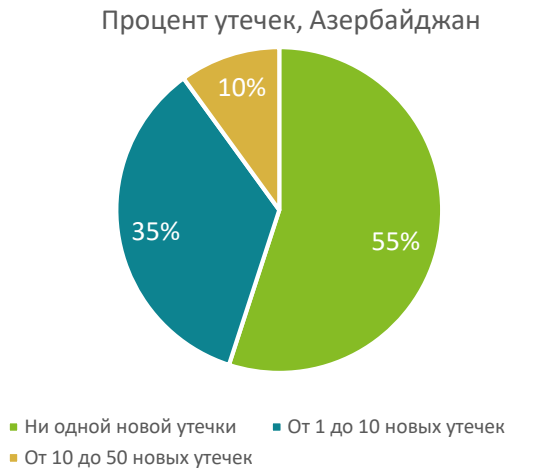
6. Утечки адресов электронной почты

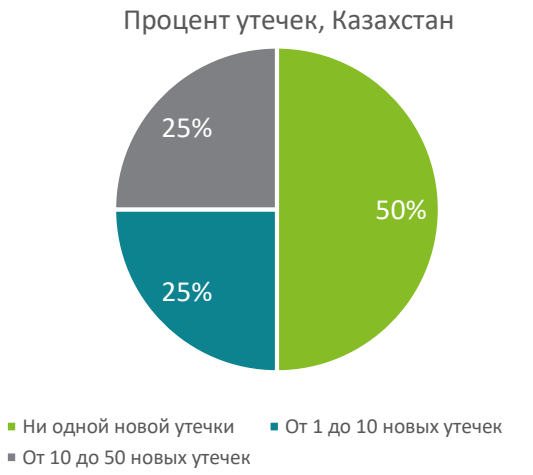
Заключение

Для снижения рисков возможных утечек адресов электронной почты рекомендуется разработать и поддерживать в актуальном состоянии программу обучение сотрудников в вопросах кибербезопасности. Формирование данной программы можно осуществить на основе следующего перечня мероприятий:

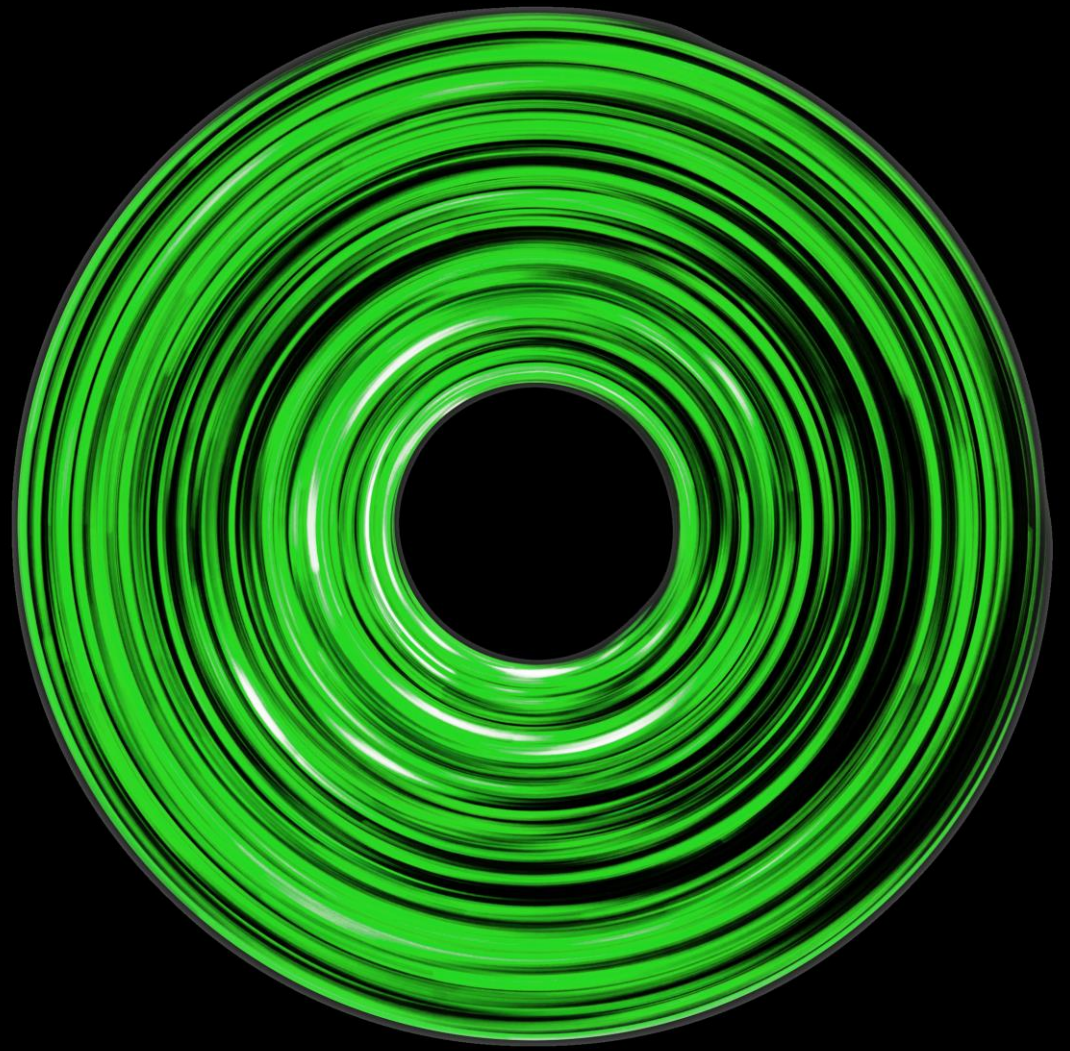
- Проведение фишинг-теста, направленного на оценка текущего уровня информированности сотрудников и определение зон риска;
- Подготовка материалов по обучению персонала в областях кибербезопасности. Особое внимание необходимо уделить тем вопросам, где на первом этапе были выявлены основные пробелы. Помимо курса обучения, материалы могут включать: стенды и листовки наглядной агитации, специальные информационные видео ролики, для использования в качестве заставки экрана, а также информационных картинок в форме фонового изображения для использования на всех компьютерах организации.
- Проведение интерактивных семинаров или онлайн обучения с презентацией подготовленных материалов. В завершении обучения сотрудники должны пройти тестирование для оценки полученных знаний.

Обобщенный результат утечек адресов электронной почты по странам:





7. Выполнение требований по защите персональных данных

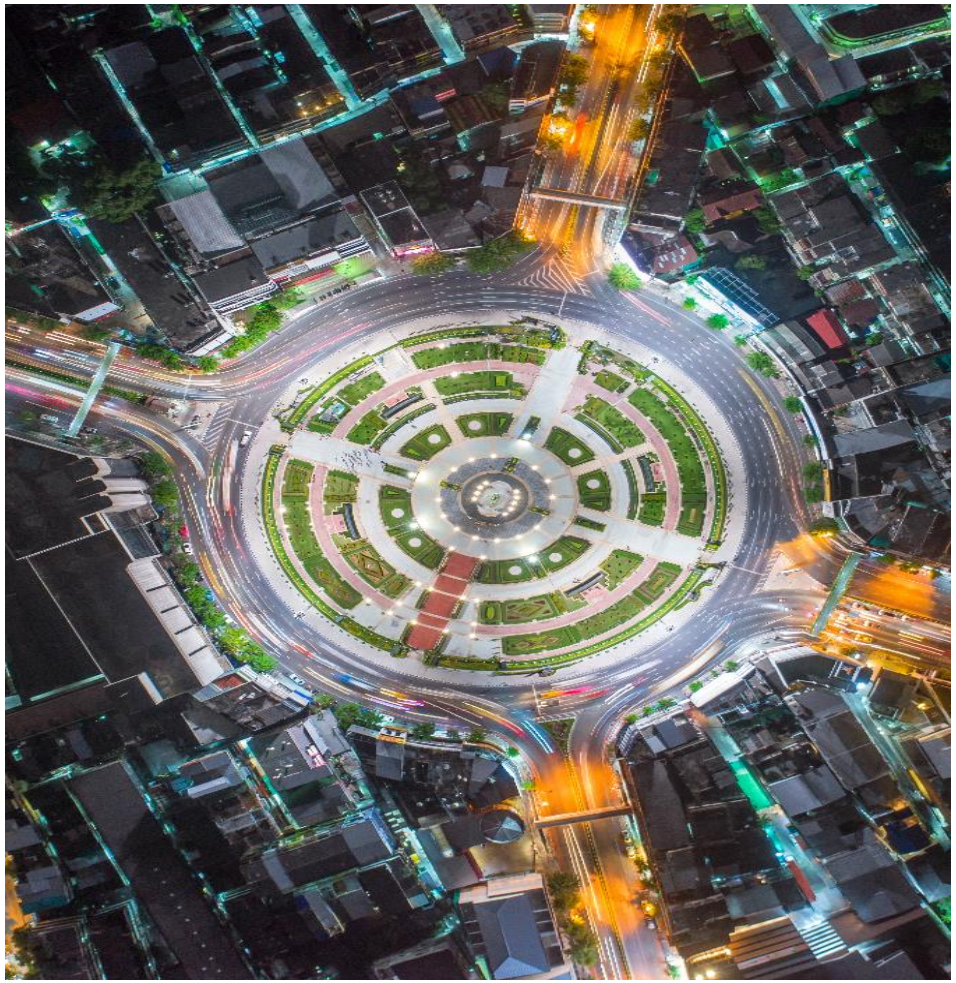


7. Выполнение требований по защите персональных данных

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, которые связаны 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, 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 COOCKIE для технической работы сайта без предварительного согласия со стороны пользователя.

Следует отметить, что для целей настоящего Обзора случаи отсутствия сбора сведений посредством COOKIE трактовались как соответствие требованиям GDPR.



7. Выполнение требований по защите персональных данных

Обобщенный результат всех проверяемых метрик доступности для «основной», «корпоративной» и «розничной» категорий доменов.

Подавляющее большинство доменов банков Узбекистана соответствует требованиям GDPR. Однако, следует отметить, что отсутствие сбора сведений cookie засчитывается за соответствие требованиям.

7. Выполнение требований по защите персональных данных

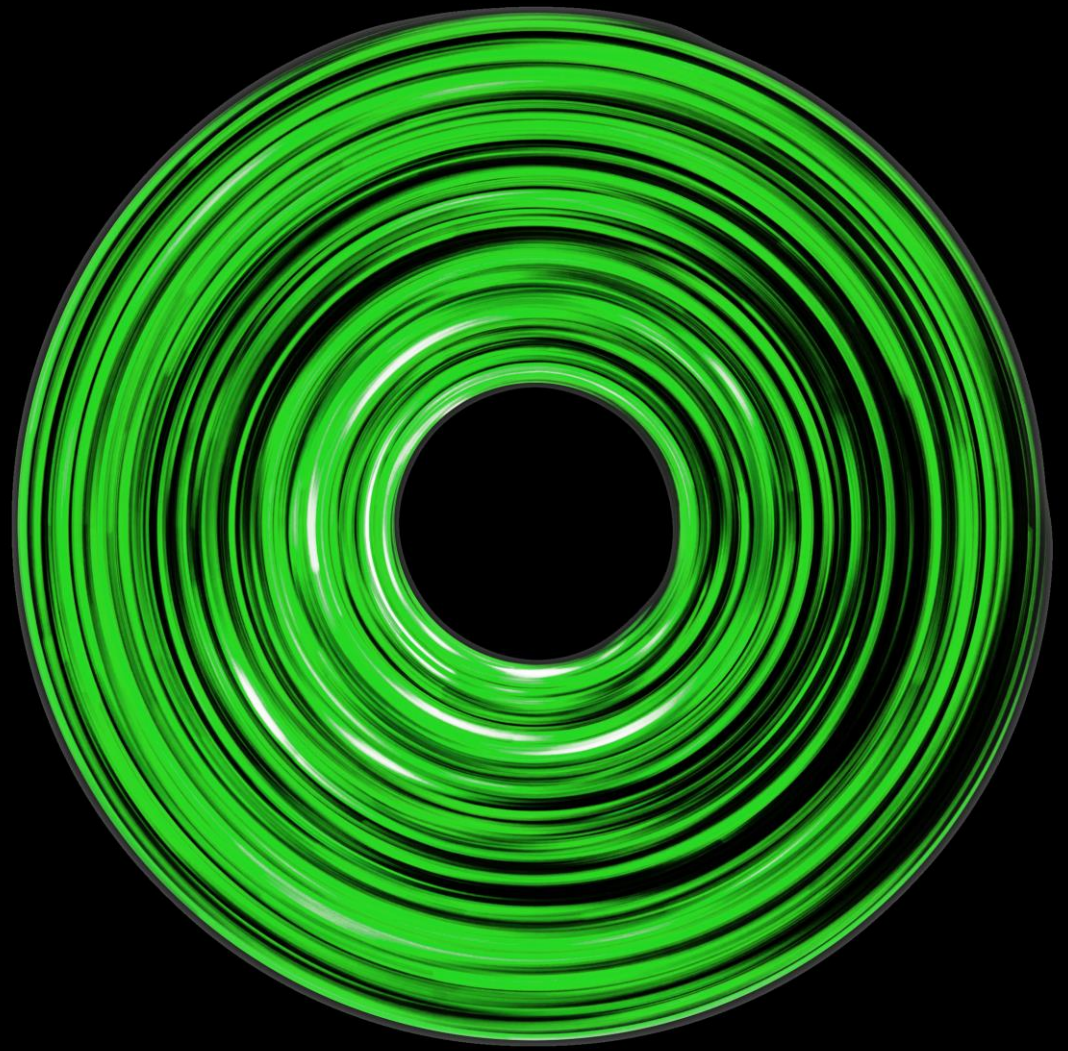
Заключение

В пункте 2 статьи 3 GDPR, который касается территориального охвата, говорится, что даже компании, созданные за пределами ЕС, подпадают под требования 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 являющегося гражданином Европейского Союза, 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 Узбекистане.

Обобщенный результат выполнения требований GDPR для всех категории веб-сайтов по странам:

8. Открытые порты



8. Открытые порты

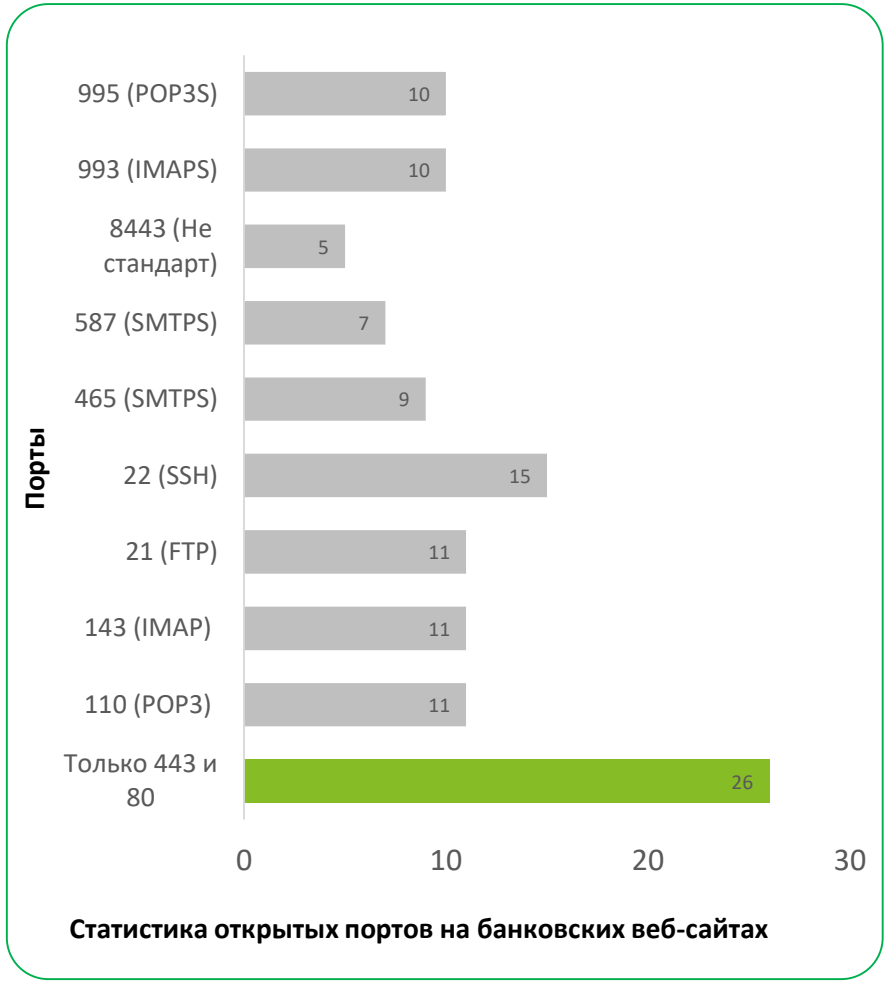
Передовая практика утверждает, что порты (сервисы), которые не являются обязательными для работы веб-сайта, должны быть закрыты или отфильтрованы.

В рамках настоящего Обзора был проанализирован перечень открытых портов на банковских веб-сайтах. Для определения состояния портов использовался онлайн сервис сканирования nmap.online-domain-tools.com. При этом изучение было ограничено 100 портами, на которых располагаются наиболее распространённые онлайн сервисы.

Результаты анализа открытых портов на веб-сайтах банков указывают, что только 36% придерживаются рекомендации использовать исключительно порты 80 и 443. Однако количество банков с запущенными дополнительными сервисами существенное, их доля составила 64%.

Основная доля дополнительных сервисов которые используют банки это сервисы работы с электронной почтой:

- порт 110 – (POP3) наиболее распространённый метод получения электронной почты.
- порт 143 – (IMAP) еще один сервис для работы с электронной почтой.
- порт 465 – (SMTPS) используется для отправки электронной почты, в основном между почтовыми серверами.с TLS/SSL шифрованием
- порт 587 – (SMTP) порт в основном используемый для отправки почты конечными пользователями. Поддерживает TLS.
- порт 993 – (IMAPS) тоже самое, что и порт 143, но с TLS/SSL шифрованием.
- порт 995 – (POP3S) тоже самое, что и POP3 но с TLS/SSL шифрованием.



Статистика открытых портов на банковских веб-сайтах

8. Открытые порты

Заключение

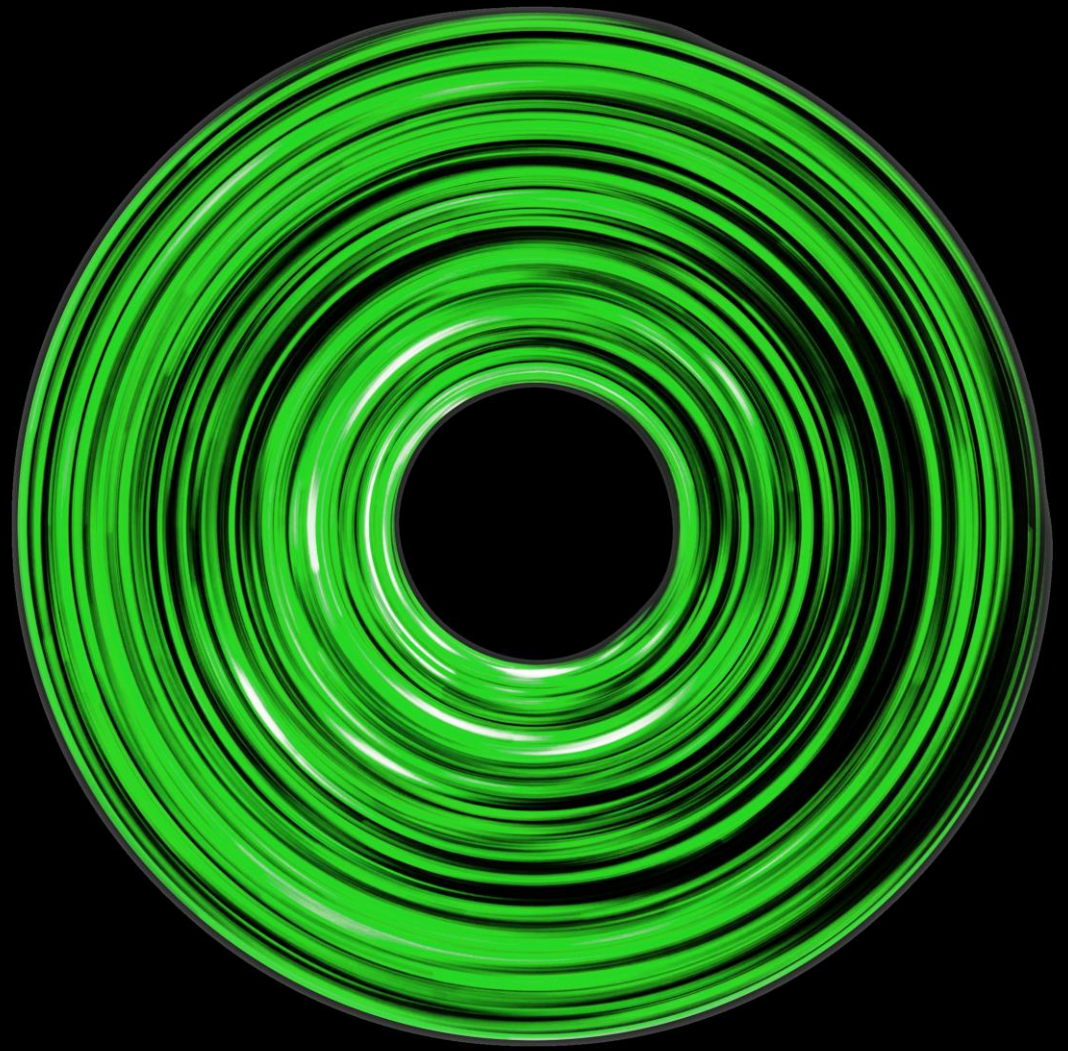
Обобщенный результат анализа открытых портов указывает, что помимо стандартной пары портов 80 и 443, на этих же IP адресах банки активно пользуются такими сервисами как: электронная почта, SSH и даже FTP.

Необходимо отметь, что результаты анализа показали использование сервисов на портах, которые большинство провайдеров Интернета и облачных хостинг-провайдеров в мире блокируют, рекомендуя к использованию их более защищенные аналоги. В данном случае речь о переходе на порт 587. Также может быть использован порт 2525. Несмотря на то, что он не признан как официальный порт SMTP, но он широко используется и поддерживается большинством Интернет провайдеров в мире.

Общий результат по открытым портам для Узбекистана показал, что всего у 36% веб-адресов открыты только нужные порты. Следует признать само по себе это не несет существенных рисков. Тем не менее, банкам очень важно обеспечивать эффективную работу процессов управлению уязвимостями, изменениями и инцидентами ИБ.

Обобщенный результат по открытым портам по странам:

9. Безопасность мобильного банкинга



9. Безопасность мобильного банкинга

На сегодняшний день большинство банков предлагают своим клиентам доступ к финансовым услугам на базе мобильных решений. Это позволило поднять уровень удобства и доступности банковских услуг в Казахстане на небывалый, высокий уровень.

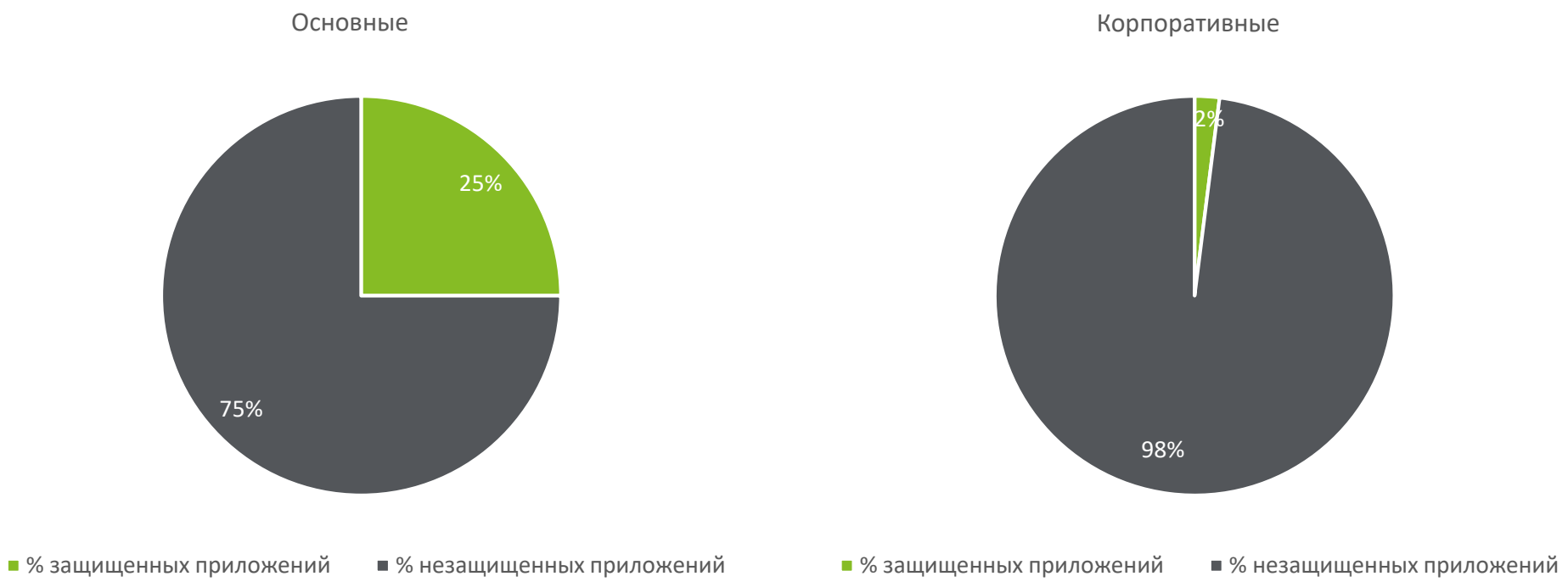
Однако, в купе с безусловными выгодами, специфичность и достаточная открытость мобильных платформ делает пользователей мобильных устройств удобной целью для злоумышленников. К тому же, для мобильных платформ уже разработан целый арсенал хакерских программ и инструментов, включая: вирусы, трояны, поддельные банковские программы, программы-вымогатели и всевозможные программы-шпионы. Это заставляет разработчиков банковских мобильных приложений помимо функциональности и удобства использования уделять много внимания обеспечению высокого уровня безопасности.

С целью изучения банковских мобильных приложений были проверены банковские приложения на двух основных платформах – Android и iOS. В рамках исследования были изучены следующие параметрам безопасности:

- Подверженность атакам типа SSL Pinning.
- Раскрытие конфиденциальной информации в автоматически генерируемых скриншотах.
- Проверка защитных механизмов безопасности.

9. Безопасность мобильного банкинга

Обобщенный результат всех проверяемых мобильных приложений для «основной» и «корпоративной» категорий



Наше исследование показало, что только 25% банков «основной» категории приложений уделяют достаточно внимания безопасности своих мобильных приложений. Банки, у которых имеются корпоративные приложения, совсем не защищены, и всего лишь одно приложение (2%) соответствует требованиям безопасности.

9. Безопасность мобильного банкинга

9.1 Подверженность атакам типа SSL Pinning

SSL pinning – это атака на владельца мобильного телефона, при которой встроенный механизм сопоставления клиентом SSL сертификатов обходится путем простой установки «небезопасных» сертификатов.

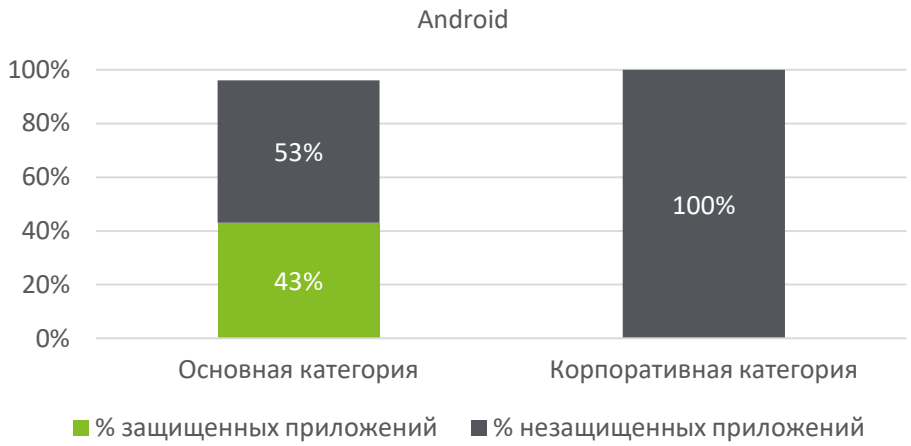
Одним из простых способов защиты от данной угрозы является внедрение SSL сертификата, в непосредственно код мобильного приложения. В этом случае приложение будет игнорировать хранилище сертификатов устройства, полагаясь только на то что «жестко» прописано в программе. В итоге это позволит безопасно обмениваться данными с банковским веб-сервером.

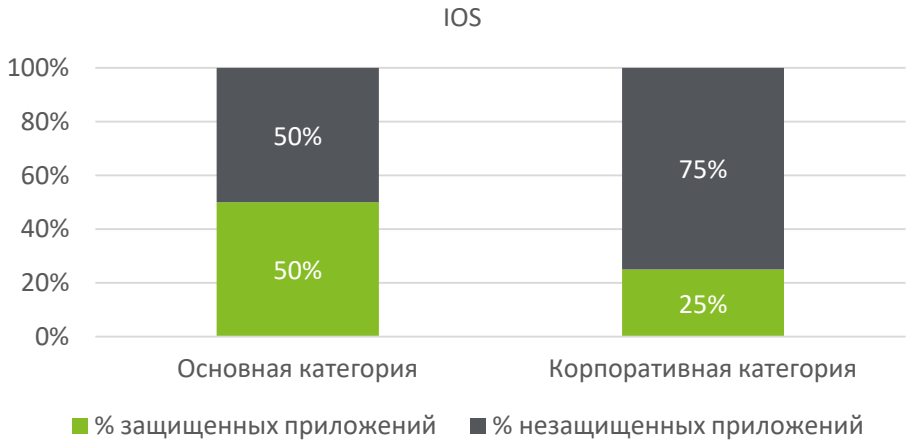
Для проверки SSL Pinning был создан и установлен поддельный сертификат в смартфоны для обоих тестируемых платформ. После чего трафик пропускался через специально настроенный прокси сервер и осуществлялся его перехват для последующего анализа. На мобильных устройствах вводились случайные данные для входа, после чего анализировался перехваченный траффик в поисках введенных учетных данных.

Если в передаваемом трафике перехватывались в открытом виде введенные в мобильном приложении учетные данные, то приложение получало рейтинг не защищенного. И наоборот, в случае если передаваемые данные оставались зашифрованными не смотря на подложный сертификат, то такое приложения считалось защищенным от SSL Pinning.

В результате проверки SSL Pinning для устройств Android показало, что текущий результат защищенности составляет 43% в основной категории, а результат проверки корпоративных приложений показал отсутствие защищенности.

Касательно проверки SSL Pinning для устройств IOS, исследование показывает, что половина приложений категорий «основной» и только 25% категорий «корпоративный» являются безопасными.





9. Безопасность мобильного банкинга

9.2 Раскрытие конфиденциальной информации в автоматически генерируемых скриншотах

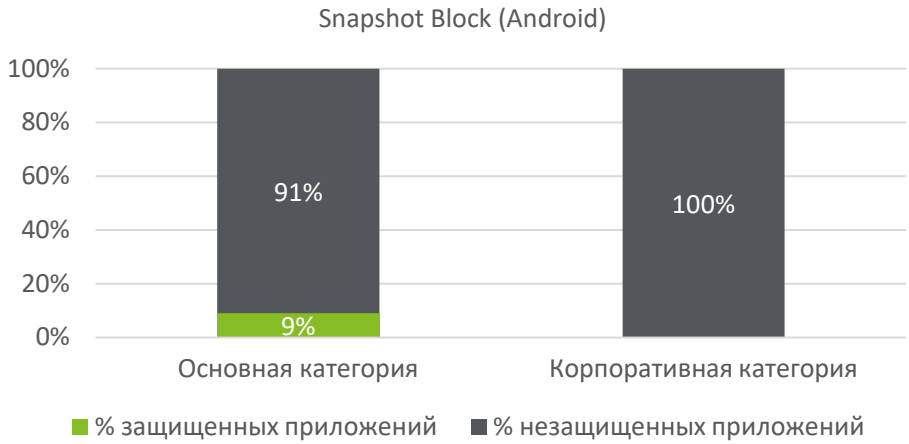
Для отображения приложений запущенных в фоновом режиме на мобильном устройстве, встроенный механизм Android или IOS делает автоматический скриншот экрана приложения при переключении. Эта стандартная функциональность потенциально представляет собой риск для конфиденциальности, поскольку критичные данные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

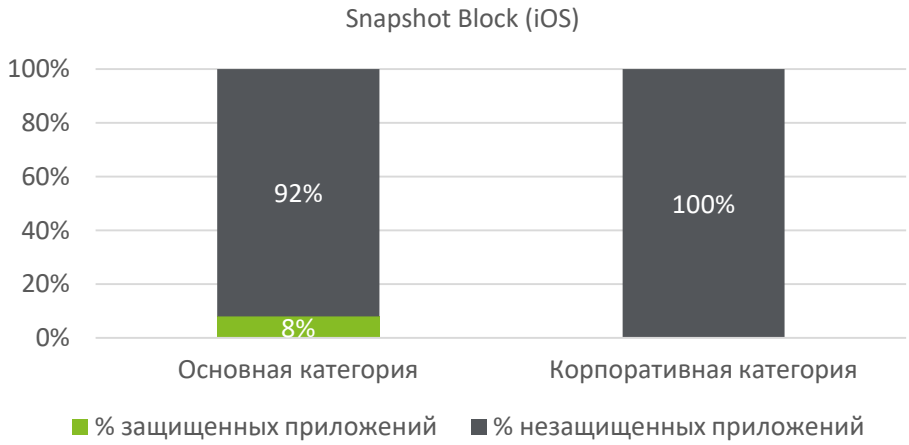
На практике встречаются шпионские программы, которые зачастую установил сам пользователь. Данные программы выполняют сбор скриншотов фоновых приложений и их последующую передачу злоумышленнику. Для защиты конфиденциальной информации от такого вида угроз разработчики прибегают к различным хитростям. Например: размывают изображение на скриншоте делая его невозможным для понимания или подменяют его на стандартное, на котором нет отображения каких либо конфиденциальных данных.

Чтобы проверить препятствует ли приложение снятию скриншотов или записи экрана устройства, осуществлялась проверка возможности сделать снимок экрана, а также можно ли при наличии данной блокировки отключить её в настройках приложения.

По итогам исследования для устройств Android выяснилось, что показатель безопасности для основной категории составил только 9%. Одновременно с этим, приложения корпоративной категории и вовсе оказались на 100% незащищенными.

При проверке мобильных приложений для IOS устройств, показатель защищенности мобильного приложения от перехвата скриншота для «основной» категории составил 8% в то время как результат «корпоративной» категории совсем не показал хороших результатов.





9. Безопасность мобильного банкинга

9.3 Проверка защитных механизмов безопасности

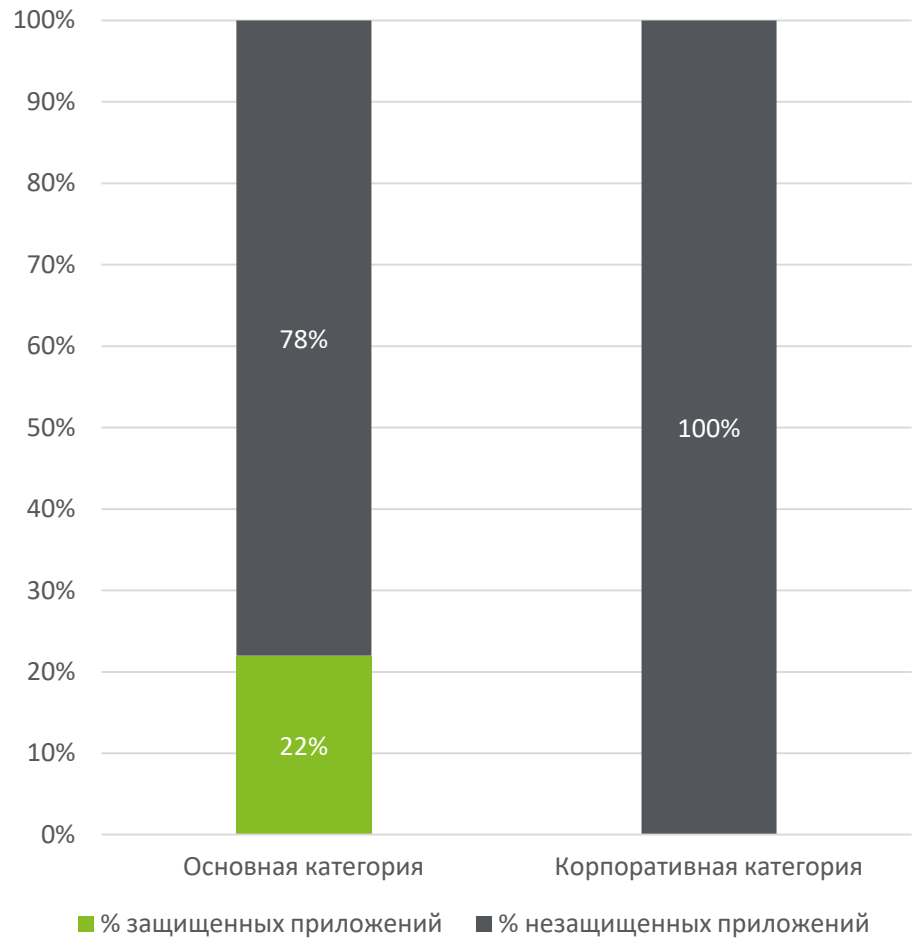
Учитывая тот факт, что банковские приложения разработаны для обработки конфиденциальной финансовой информации, разработчикам рекомендуется позаботиться о безопасности как хранящейся информации, так и безопасности самих приложений. Этого можно добиться за счет реализации полного перечня защитных механизмов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

- Реализацию механизмов обнаружения запуска мобильного устройства с привилегированным доступом («root detection»).
- Обнаружение запуска программы на виртуальном устройстве (проверка запуска только на базе архитектуры ARM).

В случае обнаружения нарушений в одном из указанных методов приложение не должно запускаться либо его функционал должен существенно ограничиваться.

Если при попытке запуска приложение отказывалось запускаться на эмуляторе, мы проверяли удастся ли запустить приложение на настоящем устройстве с возможностью скрытия рут прав. Если приложение запускалось при отключенном скрытии рут прав, данное приложение заносилось в категорию не защищенных.

Данная проверка осуществлялась только для приложений Android, и по ее итогам, показатель уязвимости «основной» категории составил 78%. Показатели приложений «корпоративной» категории оказались также неутешительными, так как все 100% приложений оказались не безопасными.



9. Безопасность мобильного банкинга

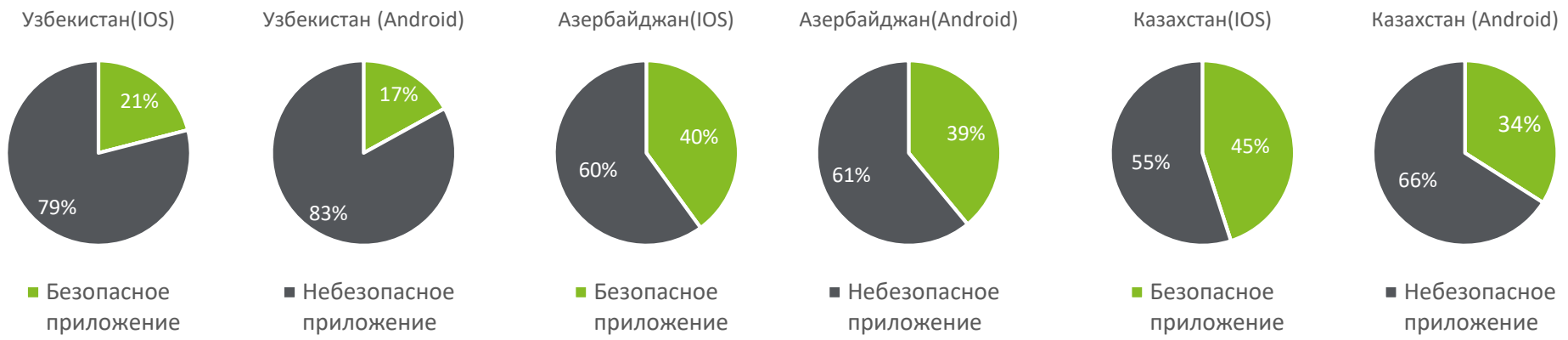
Заключение

Современные мобильных платформы (Android и IOS) имеют богатый набор встроенных механизмов защиты. Однако, очень часто разработчики в погоне за быстротой выпуска нового релиза или дополнительного функционала допускают непростительные ошибки с точки зрения защиты приложения и обрабатываемых в нем данных. В итоге это приводит к появлению уязвимостей, которыми непременно воспользуются киберпреступники.

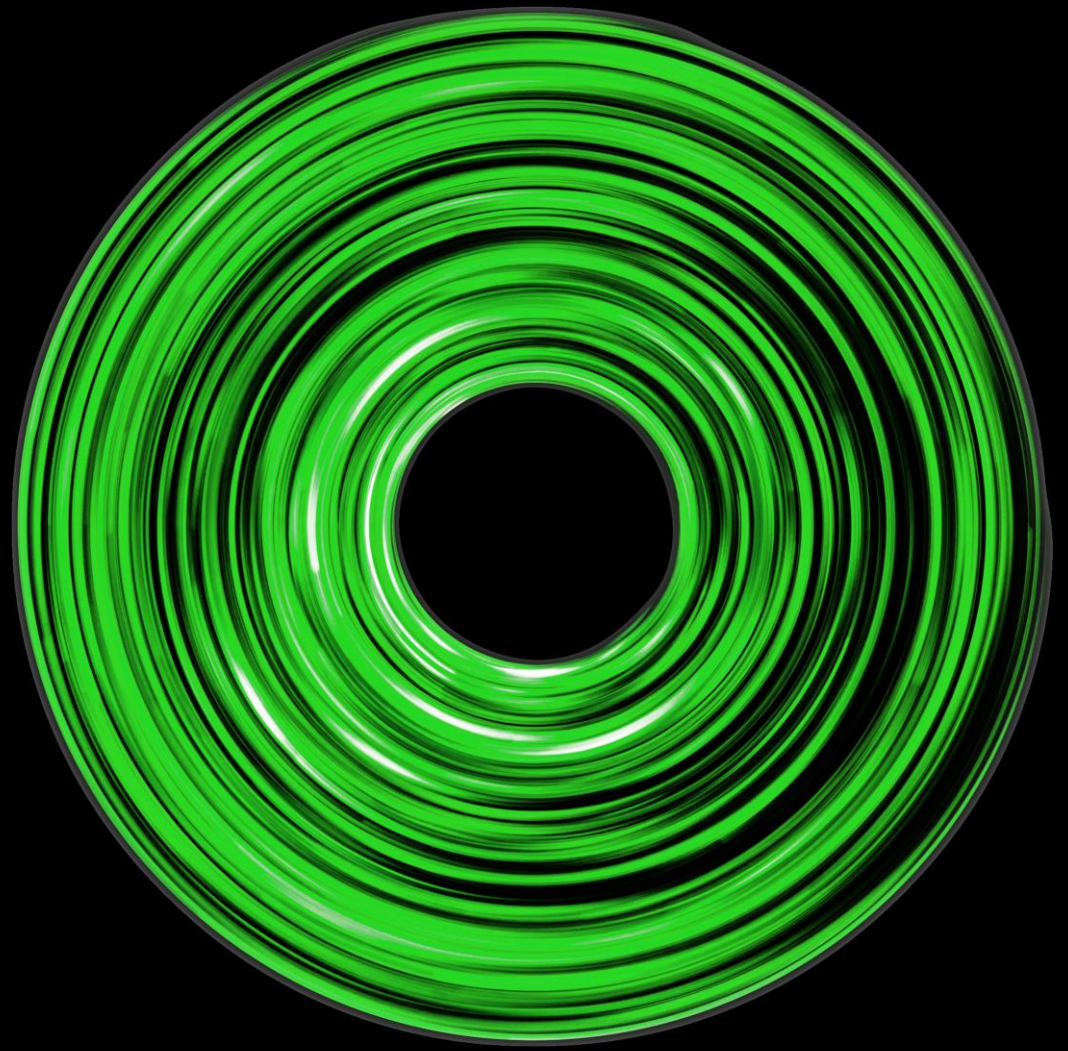
Результаты нашего исследования мобильных приложений узбекистанских банков указывают, на то что вопросам защиты и безопасности уделяется недостаточно внимания. Такая ситуация может в последствии открыть прямой путь для проведения целенаправленных кибер-атак, как на отдельных клиентов, так и банки в целом.

В качестве рекомендаций разработчикам банковских мобильных приложений, помимо реализации базовых и расширенных механизмов защиты, мы хотели бы обратить отдельное внимание на вопросы безопасности бак-энд серверов и защиты передаваемых данных между приложением и сервером.

Обобщенный результат для SSL Pinning и раскрытия конфиденциальной информации проверяемых мобильных приложений разделенный по платформам:



10. Уязвимость Log4J



10. Уязвимость Log4j

В библиотеке протоколирования Apache Log4j в версиях от 2.0.0 и до 2.15.0 была обнаружена уязвимость. Log4j отвечает за регистрацию событий - ошибок и обычных системных операций - и передает диагностические сообщения о них системным администраторам и пользователям. Данное ПО является открытым и предоставляется Apache Software Foundation.

Об уязвимости названной Log4Shell стало известно в декабре 2021 года. Эта уязвимость работает, используя функцию Log4j, которая позволяет пользователям указывать собственный код для форматирования сообщения журнала. Например, данная функция позволяет Log4j регистрировать не только имя пользователя, связанное с каждой попыткой входа на сервер, но и настоящее имя пользователя, если на отдельном сервере хранится каталог, связывающий имена пользователей и настоящие имена. Для этого сервер Log4j должен связаться с сервером, хранящим реальные имена.

По итогам исследования выявилось то, что все веб-адреса банков Узбекистана защищены от уязвимости Log4Shell.

100%
всех доменов
защищены от уязвимости Log4Shell

10. Уязвимость Log4j

Заключение

Одной из основных проблем, связанных с Log4Shell, является место Log4j в экосистеме программного обеспечения. Логирование является фундаментальной функцией большинства программ, что делает Log4j чрезвычайно распространенным. Помимо таких популярных игр, как Minecraft, он используется в облачных сервисах, таких как Apple iCloud и Amazon Web Services, а также в широком спектре программ - от инструментов разработки программного обеспечения до средств обеспечения безопасности.

К большому сожалению, из-за повсеместной распространенности эксперты уверены, что проблема логирования Java-программ имеет все шансы стать худшей уязвимостью 2021 года.

Несмотря на то, что ни у одного домена банка Узбекистана не обнаружена уязвимость Log4Shell, рекомендуется проводить проверки своих систем на следы атак, проводить профилактические работы, а так же устанавливать необходимые обновления ПО.

Обобщенный результат уязвимости Log4j для всех категорий доменов:

100%
всех доменов
Узбекистана
защищены от
уязвимости Log4Shell

100%
всех доменов
Азербайджана
защищены от
уязвимости Log4Shell

98%
всех доменов
Казахстана
защищены от
уязвимости Log4Shell

Deloitte.