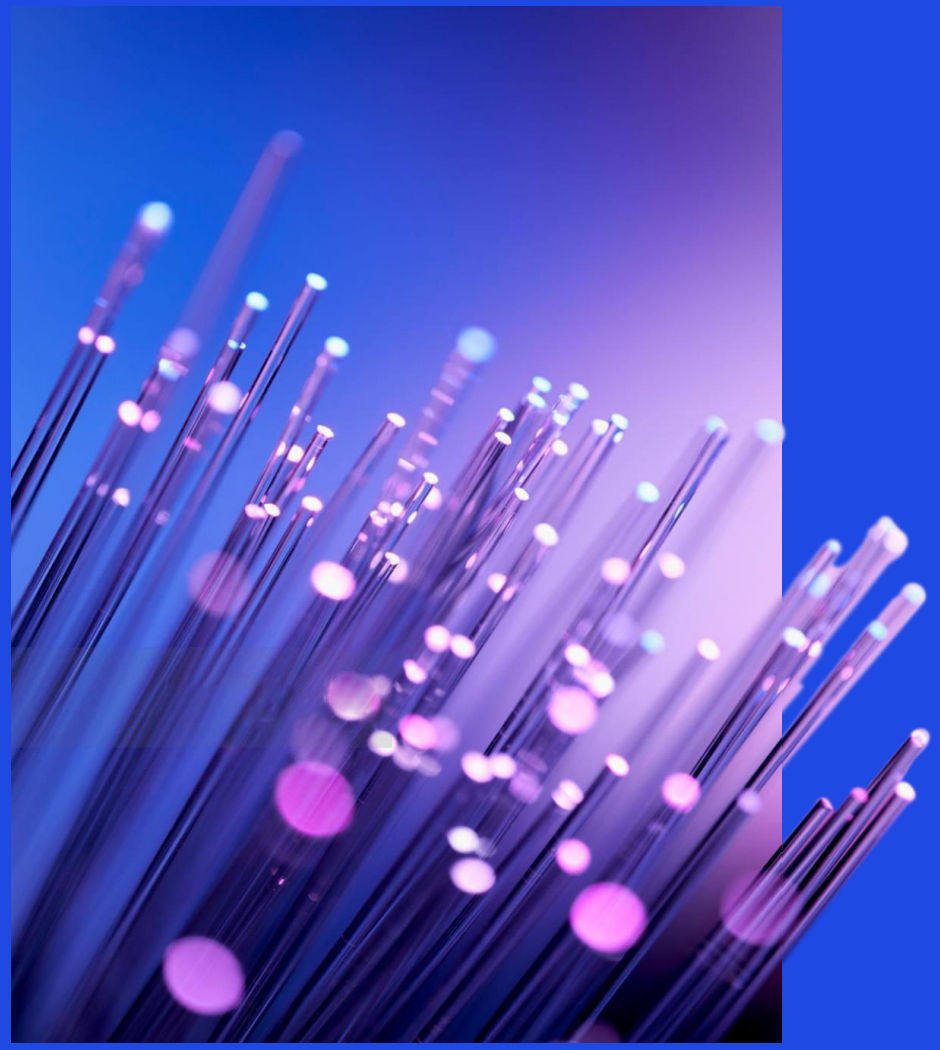
KPMG

KPMG Caspian Banks Security Review

Оценка защищенности веб-сайтов и мобильных приложений коммерческих банков

Август 2022 г.



Содержание

Приветствие

Дорогие коллеги,

Мы, команда кибербезопасности технологической практики KPMG Caspian, рады презентовать наш первый ежегодный отчет по оценке защищенности веб-сайтов и мобильных приложений коммерческих банков Каспийского региона.

Желание ускорить цифровую трансформацию в банковском секторе и переход от традиционных моделей к цифровым, выводят на первый план риски связанные с информационной безопасностью. Подтверждение данной гипотезы отражено в глобальном отчете «Global Banking CEO Outlook» от KPMG International за 2022 год.

В исследовании по оценке защищенности веб-сайтов и мобильных приложений мы попытались осветить текущее состояние основных клиентских ресурсов для 124 банков в Казахстане, Узбекистане, Кыргызстане, Армении, Грузии и Азербайджане. Наша методика основана на верхнеуровневом анализе основных критериев безопасности веб-ресурсов и мобильных приложений.

Надеемся, что данный отчет будет полезен банкам нашего региона и послужит стимулом для повышения уровня обеспечения информационной безопасности пользовательских ресурсов.

Дамир Еркин

Руководитель направления кибербезопасности группы технологического консультирования

KPMG Caspian

Введение

В связи с ускорением цифровой трансформации и переходом на удаленный режим работы риск кибербезопасности был назван наиболее серьезной угрозой для Банков в 2021 году.

Руководители сосредотачиваются на приоритетах трансформации, чтобы создать возможности, необходимые для победы в будущем после COVID. Они уделяют первостепенное внимание кибербезопасности, а также отказоустойчивости операций и цепочек поставок, чтобы минимизировать риски для роста.

Тренд банковских мошенничеств в 2021 г.

На первое место вышло мошенничество при помощи мобильных приложений. Таких операций было 50 % от общего количества.

Киберхищения с использованием банковских карт сместились на вторую позицию — 30 % от общего количества транзакций.

В то же время СМС-банкинг резко потерял популярность у злоумышленников и составляет теперь всего 12 %.

По мере того, как организации наращивают свои усилия в области цифровых технологий, важно, чтобы директора по информационной безопасности (CISO) и другие руководители высшего звена разумно инвестировали в модернизацию своих усилий в области кибербезопасности.

Угрозы роста банковской сферы согласно опросу KPMG International, в котором приняли участие 135 исполнительных директоров банков по всему миру

	2020		2021
#1	Климатический риск	#1	**Риск кибербезопасности**
#2	Новые технологические риски	#2	Налоговый риск
#3	**Риск кибербезопасности**	#3	Регуляторный риск
#4	Операционный риск	#4	Репутационный риск

25,3%
Составила доля направленных атак на банковские организации по всему миру во время пандемии Covid-19

48%
Банков планируют сконцентрироваться на совершенствовании навыков в области кибербезопасности

41%
Создают сильную культуру цифровых и кибер рисков, поддерживаемую высшим руководством

44%
Укрепляют управление операционной устойчивостью и способностью восстанавливаться после инцидентов

KPMG Global Banking CEO Outlook, 2021
https://home.kpmg/xx/en/home/insights/2022/01/global-banking-ceo-outlook.html

Введение
Современные тренды атаки

Атаки программ-вымогателей

Современные программы-вымогатели продолжают представлять серьезную угрозу для предприятий и государственных организаций. Согласно статистике банковский сектор больше других пострадал от данного вида атак.

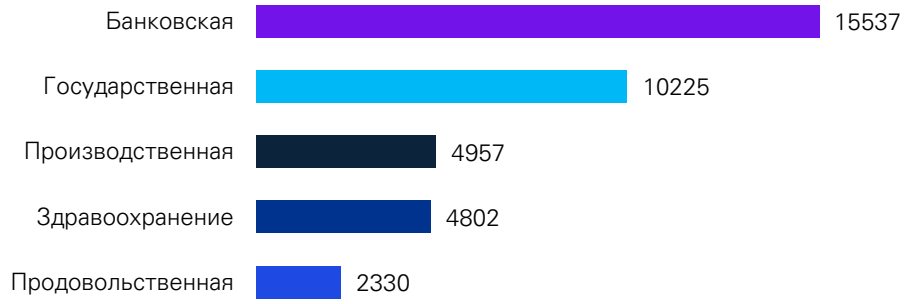
Киберпреступные группы используют более сложные бизнес-модели и внедряют новые технологии для создания эффективных и скрытных атак программ-вымогателей.

Мошенничество с картами

Индустрия кредитных карт всегда была целью хакеров и воров, и это не изменится в ближайшее время. Самые распространенные мошенничества изменились вместе с технологиями, а это значит, что мошенники всегда придумывают новые уловки, которые застают широкую публику врасплох.

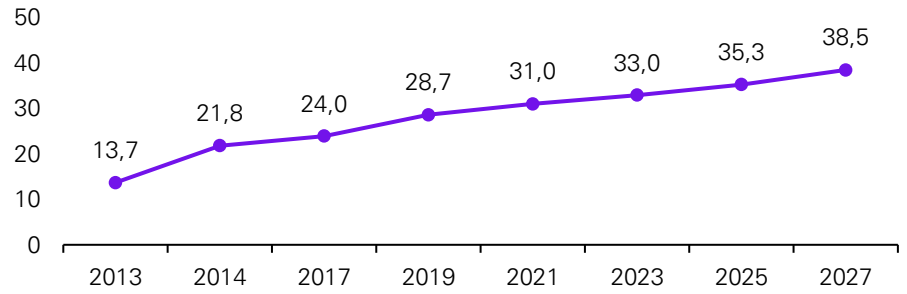
Около 30 миллиардов долларов было потеряно во всем мире в результате мошенничества с картами и кражи личных данных только в 2019 году. Хотя финансовые учреждения вовлечены в обостряющуюся гонку вооружений против киберпреступников и мошенников, потери по-прежнему необходимо учитывать.

Отрасли по всему миру, пострадавшие от программ-вымогателей в первой половине 2021г. (по количеству атак)



Attacks From All Angles: 2021 Midyear Cybersecurity Report - Security Roundup (trendmicro.com)

Прогноз киберхищений по банкам всего мира с использованием банковских карт (млрд $)



Attacks From All Angles: 2021 Midyear Cybersecurity Report - Security Roundup (trendmicro.com)

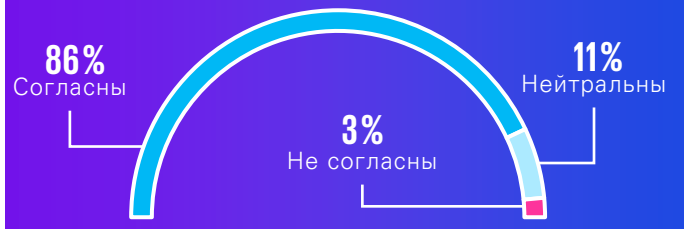
Введение
Осведомленность сотрудников

Чаще всего сотрудники являются самым слабым звеном кибербезопасности для организаций. В отчете IBM отмечается, что 95 % нарушений кибербезопасности были вызваны человеческими ошибками. По сути, если бы человеческая ошибка была каким-то образом устранена, то 19 из 20 кибервзломов могли вообще не произойти.

Несмотря на все усилия, большинство сотрудников не знают о передовых методах обеспечения ИТ-безопасности и могут стать жертвами кибератак из-за фишинговых атак, незащищенных браузеров или непреднамеренного предоставления несанкционированного доступа.

Таким образом, инвестиции в обучение и тестирование своих сотрудников на осведомленность о кибербезопасности должны быть в центре внимания организаций, если они хотят обеспечить защиту своих сотрудников и бизнеса от кибератак. Опрошенные нами ИТ-руководители согласились с этим мнением, поскольку более 80 % согласны с тем, что создание культуры осведомленности о кибербезопасности снизит риски безопасности.

Основной вывод: ИТ-директора и технические директора будут прилагать больше усилий для создания культуры осведомленности о кибербезопасности в своей организации, чтобы значительно снизить риски безопасности, такие как утечки данных.



90%
доля социальной инженерии по объему хищений

90%
доля звонков по отношению к другим каналам социальной инженерии

38%
организаций не следят за осведомленностью сотрудников в вопросах кибербезопасности

Deepfake усиливает угрозы социальной инженерии и аутентификации:

В середине октября 2021 года стало известно, что преступники завладели суммой в **$35 млн из банка в ОАЭ**, имитируя голос главы банка с помощью продвинутого искусственного интеллекта. Сообщается, что они использовали Deepfake для имитации законной коммерческой операции, связанной с банком. Это не первый случай, когда с помощью имитации голоса мошенники смогли провести крупную аферу. В 2019 году **энергетическая компания в Великобритании** потеряла **$243 тыс.** после того, как с работником компании связался человек, выдавший себя за генерального директора компании.

(Threat Zone 2020: Not waiting for thunder // BI.ZONE)

Методология оценки

Область исследования

В исследовании участвовали основные веб-сайты и мобильные приложения (одно из двух: Android или iOS) коммерческих банков стран Каспийского региона: Казахстана, Узбекистана, Кыргызстана, Азербайджана, Армении и Грузии.

HTTP-заголовки безопасности

HTTP-заголовки безопасности служат инструментами защиты от уязвимостей на стороне клиента, таких как: Cross-Site Scripting, Clickjacking, XSS, инъекции-кода и др. В исследовании оценивалось наличие следующих заголовков в ответах веб-ресурсов:

— Content-Security-Policy
— X-Content-Type-Options
— X-Frame-Options
— X-XSS-Protection
— HTTP Strict Transport Security
— Permissions Policy
— Referrer Policy
— Cross-Origin Opener Policy
— Cross-Origin Resource Policy
— Network Error Logging
— Report-To

Использованный инструмент: securityheaders.com (https://securityheaders.com/)

Оценка выполнена по шкале от A до F, где A – наивысший балл качества заголовков, а F означает низкую защищенность посетителей веб-ресурса.

Шифрование соединения, SSL-сертификат

SSL-сертификат – это цифровой сертификат, удостоверяющий подлинность веб-сайта и позволяющий использовать зашифрованное SSL соединение между веб-ресурсом и браузером пользователя.

Оценка выполнена по методологии **использованного инструмента** ssllabs.com. Рейтинг рассчитан по шкале от A+ до F.

Перенаправление на HTTPS

Принудительное перенаправление соединения с незащищенного протокола HTTP на зашифрованное соединение HTTPS является необходимым условием повышения защищенности веб-ресурса и данных пользователей.

Кибергигиена

Наряду с обеспечением безопасности данных сотрудников и клиентов банка важно ограничить использование корпоративной почты сотрудниками для регистрации на сторонних ресурсах. Взлом данных ресурсов создаёт риск утечки учетных данных сотрудников компании.

Использованный инструмент: intelx.io (https://intelx.io/)

Оценка информационной гигиены осуществлялась в соответствии с таблицей ниже.

Оценка	Описание
5	Никаких упоминаний
4	Единичные упоминания в закрытых платных базах
3	Единичные случаи с именами, почтовыми адресами сотрудников
2	Учётные данные или массовая утечка имён, почтовых адресов сотрудников без паролей (3 года и больше с момента утечки)
1	Учётные данные сотрудников, конфиденциальные данные клиентов
0	Массовая утечка данных, упоминание в СМИ

Методология оценки

Открытые порты

Дополнительные открытые порты на серверах компаний расширяют область атаки для злоумышленников. Не редки случаи когда персонал компании не догадываются об открытых портах на своих серверах, что может привести к кибератакам.

Оценка открытых портов осуществлялась в соответствии с таблицей ниже.

Оценка	Описание
4	Только порты, использующие http с перенаправлением на основной сайт
3	Другие порты (в том числе http с другими сайтами/приложениями)
2	Другие порты со старым софтом
1	Другие порты с уязвимым софтом

Уязвимые компоненты веб-сайта

Современные веб-приложения состоят из множества компонентов, каждый из которых может содержать уязвимости. Оценка уязвимых компонентов осуществлялась в соответствии с таблицей ниже.

Оценка	Потенциальное присутствие уязвимостей
5	Нет уязвимых компонентов
4	Низкого уровня критичности
3	Среднего уровня критичности
2	Высокого уровня критичности
1	Критических

! Данное исследование не предполагало углубленного анализа и валидации уязвимостей, т.е. уязвимостей может не быть или они могут быть уже исправлены. В оценке учитывались лишь версии используемых компонентов веб-сайтов.

SSL pinning

SSL pinning – это механизм защиты мобильных приложений при котором мобильное приложение хранит в себе SSL-сертификат (или публичный ключ). Это позволяет приложению сравнивать SSL-сертификат сервера, к которому оно подключается, с тем, что хранится в приложении. В результате, мобильное приложение подключается и передаёт трафик только подлинному серверу компании.

Общая оценка защищенности учитывает только наличие данного механизма защиты т.е. «реализовано» или «не реализовано».

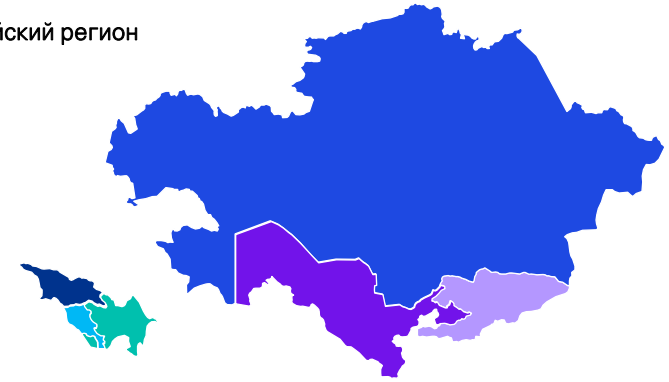
Дополнительные меры по защите мобильных приложений

Основным инструментом исследователей безопасности мобильных приложений являются смартфоны с рут привилегиями (rooted или jailbroken девайсы) и эмуляторы. Мобильные приложения способны определить их использование и реагировать. Например, приложение может выдать ошибку о неправомерном использовании или просто закрыться. Реализация защитных механизмов с определением рут привилегий и эмуляторов позволит усложнить задачу потенциальному злоумышленнику и сделать мобильное приложение более защищенным.

Общая оценка защищенности учитывает только наличие данных механизмов т.е. «реализовано» или «не реализовано». Для банков, не имеющих мобильных приложений, общая оценка защищенности не учитывала критерии «SSL pinning» и «Дополнительные меры по защите мобильных приложений».

Основные результаты

Каспийский регион



6 Стран Каспийского региона

124 Веб-сайтов коммерческих банков

101 Мобильных приложений

Средний рейтинг банков по странам

A+ **21,7%** Банков используют SSL-сертификат с оценкой A+

32,7% Мобильных приложений банков используют дополнительные меры защиты как SSL pinning, root detection и emulator detection.

89,9% Банков заботятся о шифровании трафика и используют принудительную переадресацию на HTTPS протокол.

7% Банков обладают высоким уровнем «кибергигиены». Данные пользователей/клиентов не обнаружены в слитых базах третьих сторон.

Топ 5 банков в Каспийском регионе

Название Банка	Страна	Общая оценка
HSBC Bank Armenia	Армения	96,43
Ziraat Bank Georgia	Грузия	96,00
First Heartland Jýsan Bank	Казахстан	83,86
Altyn Bank	Казахстан	82,29
Bank RBK	Казахстан	79,00

Лидеры в странах

Название Банка	Страна	Общая оценка
HSBC Bank Armenia	Армения	96,43
Ziraat Bank Georgia	Грузия	96,00
First Heartland Jýsan Bank	Казахстан	83,86
Xalq Bank	Азербайджан	78,14
Kyrgyzkommertsbank	Кыргызстан	77,00
Ravnaq-bank	Узбекистан	71,29

Казахстан

First Heartland Jýsan Bank

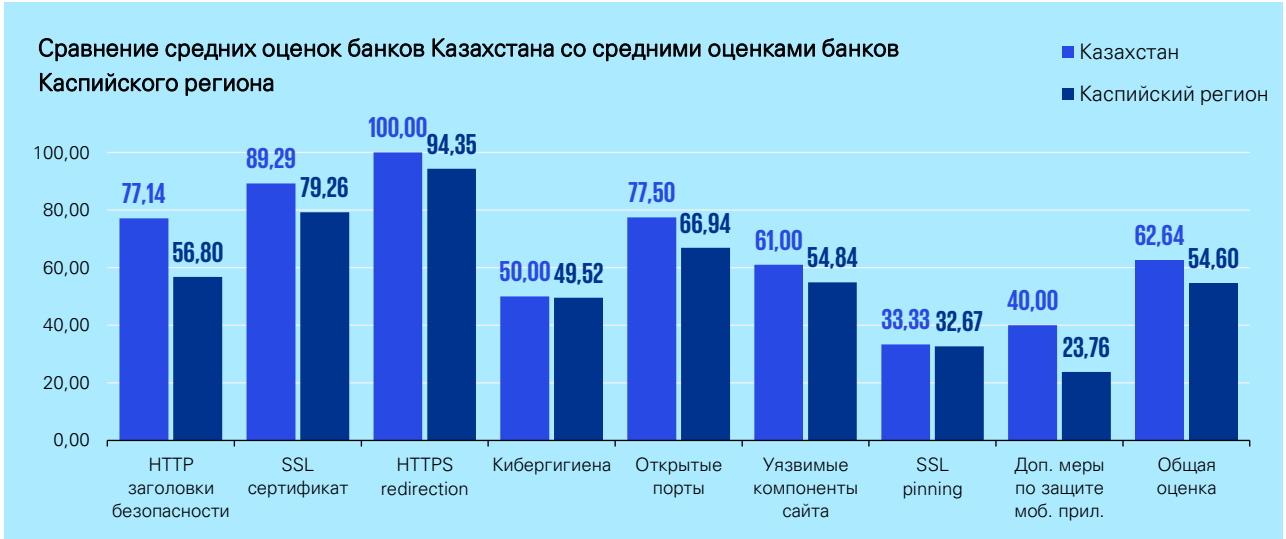
Лидер по защищенности веб-сайтов и мобильных приложений среди банков Казахстана с оценкой 83,86.

4 из 12

Банков Казахстана реализовали SSL pinning в мобильных приложениях.

1 из 12

Банков Казахстана реализовавший дополнительные меры по защите мобильных приложений.



62,64 Средняя оценка защищенности банков в Казахстане

Средняя оценка Каспийского региона **54,60**

70,0% Веб-сайтов банков Казахстана имеют SSL-сертификаты с оценкой A+ и A

100% Веб-сайтов банков Казахстана используют HTTPS перенаправление

Топ 5 Банков по результатам оценки

Название Банка	Общая оценка
First Heartland Jýsan Bank	83,86
Altyn Bank	82,29
Bank RBK	79,00
Zaman Bank	78,75
Bank CenterCredit	78,71

Казахстан
Оценка защищенности веб-сайтов и мобильных приложений Банков

#	Банк	HTTP заголовки	SSL-сертификат	HTTPS redirection	Кибергигиена	Открытые порты	Уязвимые компоненты сайта	SSL pinning	Доп. меры по защите моб. приложения	Общая оценка
1	First Heartland Jýsan Bank	D	B	✓	4	4	5	✓	✗	**83,86**
2	Altyn Bank	C	B	✓	4	4	3	✓	✓	**82,29**
3	Bank RBK	A	A+	✓	3	4	3	✓	✗	**79,00**
4	Zaman Bank	A	A+	✓	2	3	5	–	–	**78,75**
5	Bank CenterCredit	D	A+	✓	2	4	5	✓	✗	**78,71**
6	Shinhan Bank Kazakhstan	D	A+	✓	3	2	5	–	–	**72,14**
7	Eco Center Bank	B	A+	✓	5	1	3	–	–	**69,46**
8	Sber Bank Kazakhstan	A	A	✓	1	4	3	–	–	**68,21**
9	ForteBank	A	A+	✓	4	3	3	✗	✗	**63,00**
10	Eurasian Bank	B	A+	✓	2	4	3	✗	✗	**58,57**
11	Al Hilal Bank	F	A	✓	2	3	3	–	–	**58,04**
12	Halyk Bank	C	A+	✓	2	4	3	✗	✗	**57,14**

Казахстан
Оценка защищенности веб-сайтов и мобильных приложений Банков

#	Банк	HTTP заголовки	SSL-сертификат	HTTPS redirection	Кибергигиена	Открытые порты	Уязвимые компоненты сайта	SSL pinning	Доп. меры по защите моб. приложения	Общая оценка
13	Freedom Bank	A	A+	✓	1	4	3	✗	✗	**56,00**
14	Home Credit Bank	D	B	✓	2	3	5	✗	✗	**55,86**
15	Kaspi Bank	B	A+	✓	3	4	1	✗	✗	**54,57**
16	VTB Bank	A	B	✓	2	2	2	–	–	**53,93**
17	KZI Bank	C	A	✓	2	3	1	–	–	**53,39**
18	Bank of China Kazakhstan	C	B	✓	2	2	2	–	–	**50,36**
19	Nurbank	C	B	✓	2	2	2	✗	✗	**40,29**
20	Otbasy Bank	C	A+	✓	2	2	1	✗	✗	**39,14**

Узбекистан

Ravnaq-bank

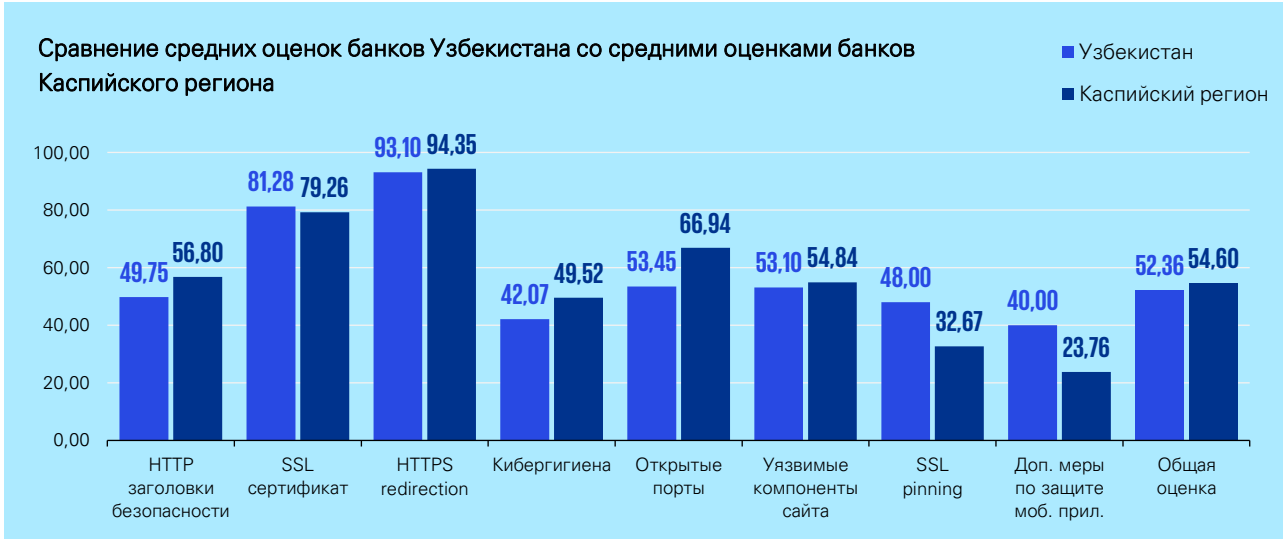
Лидер по защищенности веб-сайтов и мобильных приложений среди банков Узбекистана с оценкой 71,29.

13 из 25

Банков Узбекистана реализовали SSL pinning в мобильных приложениях.

11 из 25

Банков Узбекистана реализовали дополнительные меры по защите мобильных приложений.



52,36 Средняя оценка защищенности банков в Узбекистане

Средняя оценка Каспийского региона **54,60**

55,2% Веб-сайтов банков Узбекистана имеют SSL-сертификаты с оценкой **A+** и **A**

Сайты **O'zAgroEksportBank**, **Hi-Tech Bank**, **Trastbank** и **Davr Bank** не используют принудительное перенаправление на HTTPS.

Топ 5 Банков по результатам оценки

Название Банка	Общая оценка
Ravnaq-bank	71,29
Hamkorbank	69,14
UniversalBank	64,29
Ziraat Bank Uzbekistan	62,86
O'zAgroEksportBank	61,79

Узбекистан
Оценка защищенности веб-сайтов и мобильных приложений Банков

#	Банк	HTTP заголовки	SSL-сертификат	HTTPS redirection	Кибергигиена	Открытые порты	Уязвимые компоненты сайта	SSL pinning	Доп. меры по защите моб. приложения	Общая оценка
1	Ravnaq-bank	D	A	✓	3	1	5	✓	✓	**71,29**
2	Hamkorbank	C	A+	✓	2	4	1	✓	✓	**69,14**
3	UniversalBank	D	A	✓	2	2	3	✓	✓	**64,29**
4	Ziraat Bank Uzbekistan	F	A+	✓	3	3	2	✓	✗	**62,86**
5	O'zAgroEksportBank	F	B	✗	4	3	3	–	–	**61,79**
6	Kapitalbank	D	B	✓	2	4	5	✗	✗	**60,86**
7	Xalq Banki	F	C	✓	2	3	2	✓	✓	**59,57**
8	KDB Bank O'zbekistan	B	A+	✓	2	4	3	✗	✗	**58,57**
9	Asakabank	F	A	✓	3	3	5	✗	✗	**58,43**
10	Savdogar Bank	D	B	✓	3	1	2	✓	✓	**57,86**
11	Tenge Bank	D	A+	✓	1	1	3	✓	✓	**56,71**
12	Anor Bank	B	A	✓	1	3	5	✗	✗	**56,14**

Узбекистан
Оценка защищенности веб-сайтов и мобильных приложений Банков

#	Банк	HTTP заголовки	SSL-сертификат	HTTPS redirection	Кибергигиена	Открытые порты	Уязвимые компоненты сайта	SSL pinning	Доп. меры по защите моб. приложения	Общая оценка
13	Mikrokreditbank	F	B	✓	3	2	1	✓	✓	**56,00**
14	Madad Invest Bank	F	A	✓	4	1	3	–	–	**55,54**
15	Ipoteka-bank	F	A	✓	3	2	1	✓	✗	**52,43**
16	Poytaxt Bank	D	B	✓	1	1	5	–	–	**52,32**
17	Qishloq Qurilish Bank	F	B	✓	1	2	2	✓	✓	**52,00**
18	Turon Bank	D	A	✓	1	1	2	✓	✓	**51,29**
19	InFinBank	A	A+	✓	2	2	3	✗	✗	**50,00**
20	Ipak Yo'li Bank	F	A	✓	2	2	5	✗	✗	**49,43**
21	Aloqabank	F	B	✓	4	3	2	✗	✗	**49,00**
22	Sanoat Qurilish Bank	F	B	✓	1	3	4	✗	✗	**43,00**
23	Agrobank	D	B	✓	2	2	3	✗	✗	**42,86**
24	Hi-Tech Bank	F	B	✗	2	3	1	–	–	**41,79**

Узбекистан
Оценка защищенности веб-сайтов и мобильных приложений Банков

#	Банк	HTTP заголовки	SSL-сертификат	HTTPS redirection	Кибергигиена	Открытые порты	Уязвимые компоненты сайта	SSL pinning	Доп. меры по защите моб. приложения	Общая оценка
25	Trastbank	E	A	✗	1	1	1	✓	✓	**41,57**
26	Orient Finans Bank	B	B	✓	3	1	2	✗	✗	**40,71**
27	Davr Bank	F	A	✗	1	4	2	✗	✗	**39,14**
28	TBC Bank	B	B	✓	1	1	2	✗	✗	**32,71**
29	Asia Alliance Bank	D	A	✓	1	1	2	✗	✗	**31,29**

Кыргызстан

Kyrgyzkommertsbank

Лидер по защищенности веб-сайтов и мобильных приложений среди банков Кыргызстана с оценкой 77,00.

5 из 20 банков

Реализовали SSL pinning в мобильных приложениях.

Сравнение средних оценок банков Кыргызстана со средними оценками банков Каспийского региона

49,48 Средняя оценка защищенности банков в Кыргызстане

Средняя оценка Каспийского региона **54,60**

26,1% Веб-сайтов банков Кыргызстана имеют SSL-сертификаты с оценкой **A+** и **A**

Сайты **FinanceCreditBank**, **Amanbank**, **National Bank of Pakistan Bishkek Branch** и **Bank of Asia** не используют принудительное перенаправление на HTTPS. Сайты **FinanceCreditBank** и **National Bank of Pakistan Bishkek Branch** не имеют SSL-сертификатов.

Bank of Asia и **Tolubay Bank** имеют наименьшую оценку защищенности среди всех банков Каспийского региона.

Топ 5 Банков по результатам оценки

Название Банка	Общая оценка
Kyrgyzkommertsbank	77,00
Halyk Bank Kyrgyzstan	73,00
Aiyl Bank	62,29
FINCA Bank	61,14
Capital Bank	58,86

Кыргызстан
Оценка защищенности веб-сайтов и мобильных приложений Банков

#	Банк	HTTP заголовки	SSL-сертификат	HTTPS redirection	Кибергигиена	Открытые порты	Уязвимые компоненты сайта	SSL pinning	Доп. меры по защите моб. приложения	Общая оценка
1	Kyrgyzkommertsbank	F	B	✓	3	3	5	✓	✓	**77,00**
2	Halyk Bank Kyrgyzstan	F	B	✓	2	3	5	✓	✓	**73,00**
3	Aiyl Bank	C	B	✓	2	4	5	✗	✗	**62,29**
4	FINCA Bank	A	B	✓	3	4	3	✗	✗	**61,14**
5	Capital Bank	D	B	✓	1	3	3	✓	✗	**58,86**
6	FinanceCreditBank	D	T	✗	2	4	3	–	–	**57,14**
7	Commercial bank KYRGYZSTAN	D	B	✓	3	4	3	✗	✗	**56,86**
8	Dos Credobank	D	B	✓	3	4	3	✗	✗	**56,86**
9	Eurasian Savings Bank	D	A	✓	3	2	5	✗	✗	**56,29**
10	Optima Bank	F	B	✓	1	3	1	✓	✓	**53,00**
11	Bank Bai-Tushum	C	A+	✓	2	3	2	✗	✗	**48,14**
12	Kompanion Bank	F	A	✓	2	4	2	✗	✗	**47,43**

Кыргызстан
Оценка защищенности веб-сайтов и мобильных приложений Банков

#	Банк	HTTP заголовки	SSL-сертификат	HTTPS redirection	Кибергигиена	Открытые порты	Уязвимые компоненты сайта	SSL pinning	Доп. меры по защите моб. приложения	Общая оценка
13	DemirBank	D	A+	✓	2	3	2	✗	✗	**46,71**
14	Keremet Bank	F	B	✓	3	4	1	✗	✗	**46,00**
15	BakaiBank	C	B	✓	2	3	2	✗	✗	**45,29**
16	Amanbank	F	F	✗	2	3	2	–	–	**43,21**
17	RSK Bank	F	B	✓	2	1	1	✓	✗	**42,00**
18	National Bank of Pakistan Bishkek Branch	F	T	✗	3	2	2	–	–	**41,07**
19	Kyrgyz-Swiss Bank	F	B	✓	1	3	3	✗	✗	**41,00**
20	Kyrgyz Investment and Credit Bank	C	A+	✓	2	2	1	✗	✗	**39,14**
21	EcoIslamicBank	F	B	✓	1	1	1	–	–	**28,75**
22	Bank of Asia	F	B	✗	2	2	1	✗	✗	**28,43**
23	Tolubay Bank	F	A	✓	2	1	1	✗	✗	**28,43**

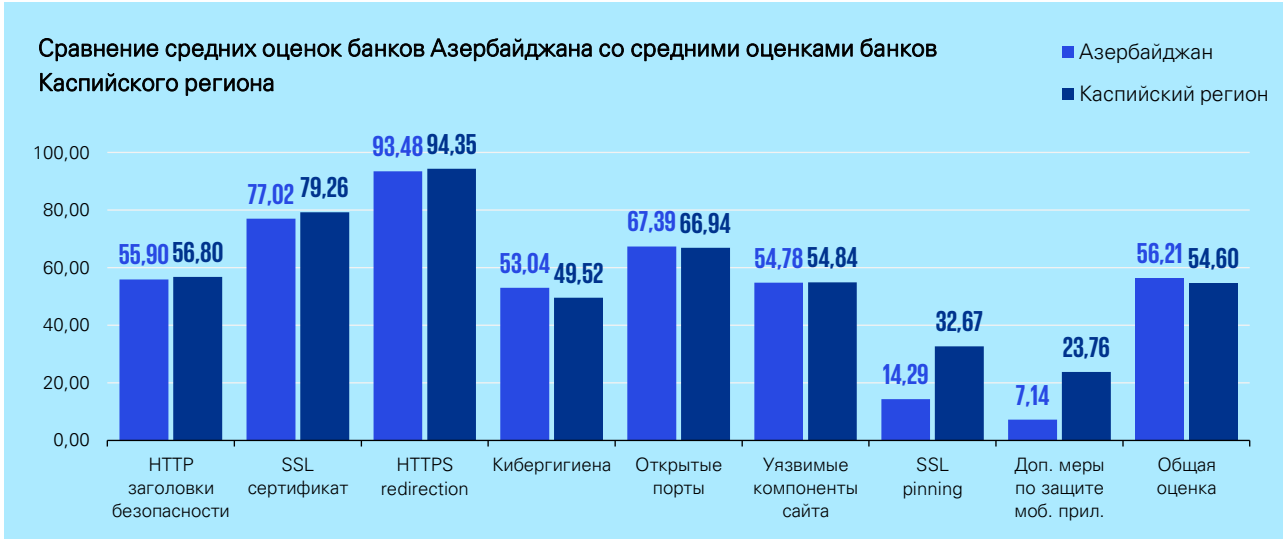
Азербайджан

Xalq Bank

Лидер по защищенности веб-сайтов и мобильных приложений среди банков Азербайджана с оценкой 78,14.

В 36,84%

мобильных приложений банков Азербайджана реализованы дополнительные защитные механизмы как SSL pinning, root detection и emulator detection.



56,21 Средняя оценка защищенности банков в Азербайджане

Средняя оценка Каспийского региона **54,60**

34,8% Веб-сайтов банков Азербайджана имеют SSL-сертификаты с оценкой **A+** и **A**

Сайты **Bank Avrasiya**, **Bank of Baku** и **AFB Bank** не используют принудительное перенаправление на HTTPS.

Топ 5 Банков по результатам оценки

Название Банка	Общая оценка
Xalq Bank	78,14
Muganbank	72,14
Yelo Bank	71,86
Premium Bank	69,29
Unibank	69,00

Азербайджан
Оценка защищенности веб-сайтов и мобильных приложений Банков

#	Банк	HTTP заголовки	SSL-сертификат	HTTPS redirection	Кибергигиена	Открытые порты	Уязвимые компоненты сайта	SSL pinning	Доп. меры по защите моб. приложения	Общая оценка
1	Xalq Bank	B	A	✓	4	1	5	✓	✓	**78,14**
2	Muganbank	B	A	✓	5	3	5	✗	✗	**72,14**
3	Yelo Bank	D	B	✓	3	3	3	✓	✓	**71,86**
4	Premium Bank	D	A	✓	5	3	5	✗	✗	**69,29**
5	Unibank	F	B	✓	5	3	1	✓	✓	**69,00**
6	International Bank of Azerbaijan	D	B	✓	2	3	3	✓	✓	**67,86**
7	Ziraat Bank Azerbaijan	A	B	✓	4	4	3	✗	✗	**65,14**
8	AzerTurkBank	D	A	✓	4	1	2	✓	✓	**63,29**
9	Kapital Bank	C	B	✓	5	3	3	✗	✗	**61,29**
10	Bank Respublika	C	B	✓	1	2	5	–	–	**60,36**
11	Pasha Bank	A	A+	✓	5	1	3	✗	✗	**57,00**
12	Yapi Kredi Bank Azerbaijan	D	A	✓	1	3	3	–	–	**56,61**

Азербайджан
Оценка защищенности веб-сайтов и мобильных приложений Банков

#	Банк	HTTP заголовки	SSL-сертификат	HTTPS redirection	Кибергигиена	Открытые порты	Уязвимые компоненты сайта	SSL pinning	Доп. меры по защите моб. приложения	Общая оценка
13	Bank Avrasiya	D	B	✗	1	3	2	✓	✓	**56,29**
14	Naxcıvanbank	D	B	✓	2	3	2	–	–	**54,82**
15	GünayBank	F	A	✓	1	4	1	–	–	**49,29**
16	Bank BTB	F	B	✓	1	2	1	✓	✓	**48,00**
17	Rabitabank	D	B	✓	1	2	5	✗	✗	**46,86**
18	Bank of Baku	F	A	✗	5	3	1	✗	✗	**46,14**
19	AccessBank	D	B	✓	1	3	3	✗	✗	**43,86**
20	AFB Bank	D	B	✗	2	4	1	✗	✗	**41,29**
21	ASB Bank	F	B	✓	1	3	1	✗	✗	**41,25**
22	TuranBank	F	B	✓	1	3	3	✗	✗	**41,00**
23	Expressbank	F	B	✓	1	2	2	✗	✗	**32,00**

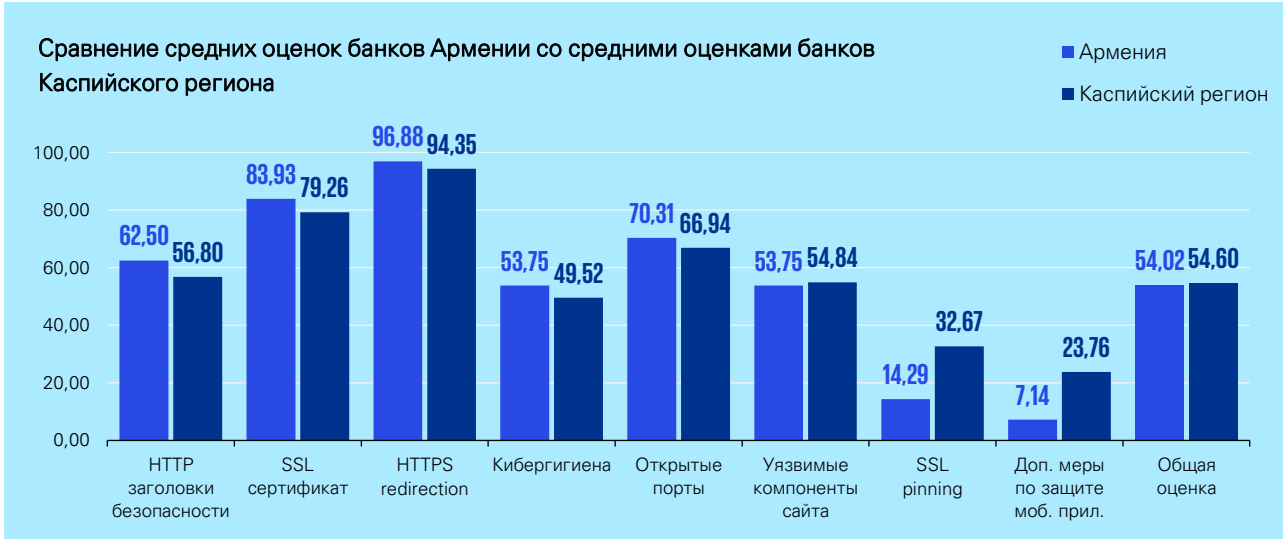
Армения

HSBC Bank Armenia

Лидер по защищенности веб-сайтов и мобильных приложений среди банков Каспийского региона с оценкой 96,43.

ACBA Bank

Реализованы SSL pinning и дополнительные меры по защите мобильных приложений..



54,02 Средняя оценка защищенности банков в Армении

Средняя оценка Каспийского региона **54,60**

62.5% Веб-сайтов банков Армении имеют SSL-сертификаты с оценкой **A+** и **A**

Сайт **ArtsakhBank** не использует принудительное перенаправление на HTTPS.

Топ 5 Банков по результатам оценки

Название Банка	Общая оценка
HSBC Bank Armenia	96,43
ACBA Bank	75,00
EvocaBank	71,71
Byblos Bank Armenia	60,14
AraratBank	59,71

Армения
Оценка защищенности веб-сайтов и мобильных приложений Банков

#	Банк	HTTP заголовки	SSL-сертификат	HTTPS redirection	Кибергигиена	Открытые порты	Уязвимые компоненты сайта	SSL pinning	Доп. меры по защите моб. приложения	Общая оценка
1	HSBC Bank Armenia	C	A+	✓	5	4	5	–	–	**96,43**
2	ACBA Bank	A	A+	✓	2	3	3	✓	✓	**75,00**
3	EvocaBank	C	A	✓	4	4	5	✗	✗	**71,71**
4	Byblos Bank Armenia	A	B	✓	4	3	3	✗	✗	**60,14**
5	AraratBank	C	A	✓	4	4	2	✗	✗	**59,71**
6	ArtsakhBank	D	B	✗	4	2	5	✗	✗	**55,29**
7	ID Bank	D	B	✓	3	2	5	✗	✗	**54,86**
8	InecoBank	C	A+	✓	2	1	2	✓	✗	**53,14**
9	ArmSwissBank	B	A	✓	2	3	3	✗	✗	**52,14**
10	Mellat Bank	F	A	✓	4	2	1	–	–	**51,79**
11	Converse Bank	D	A	✓	2	3	3	✗	✗	**49,29**
12	AmeriaBank	F	A	✓	1	4	2	✗	✗	**42,00**

Армения
Оценка защищенности веб-сайтов и мобильных приложений Банков

#	Банк	HTTP заголовки	SSL-сертификат	HTTPS redirection	Кибергигиена	Открытые порты	Уязвимые компоненты сайта	SSL pinning	Доп. меры по защите моб. приложения	Общая оценка
13	ArmEconomBank	F	B	✓	2	4	1	✗	✗	**42,00**
14	Unibank	A	A+	✓	2	1	1	✗	✗	**37,00**
15	ArmBusinessBank	F	B	✓	1	3	1	✗	✗	**33,00**
16	Ardshinbank	D	B	✓	1	2	1	✗	✗	**30,86**

Грузия

Ziraat Bank Georgia

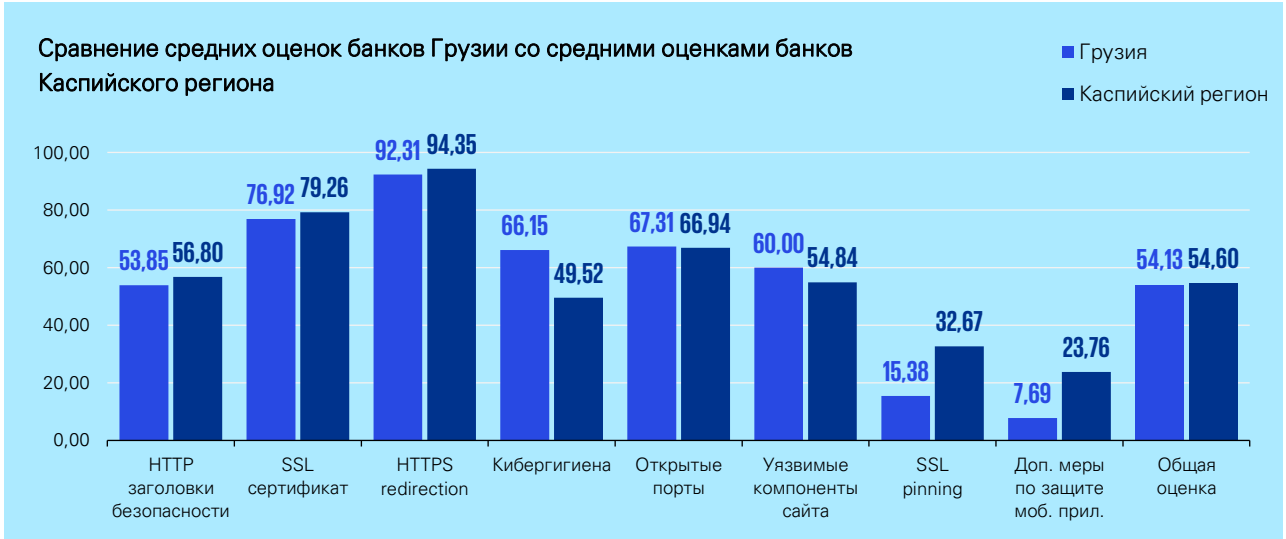
Лидер по защищенности веб-сайтов и мобильных приложений среди банков Грузии с оценкой 96,00.

Basisbank

Не имеет никаких упоминаний в публично известных и доступных утечках данных.

2 из 13

Банков Грузии реализовавших SSL pinning в мобильном приложении.



54,13 Средняя оценка защищенности банков в Грузии

Средняя оценка Каспийского региона **54,60**

61,5% Веб-сайтов банков Грузии имеют SSL-сертификаты с оценкой **A+** и **A**

Сайты **Silk Road Bank** и **Isbank Georgia** не используют принудительное перенаправление на HTTPS. Сайт **Isbank Georgia** не имеет SSL-сертификата.

Cartu Bank имеет наименьшую оценку защищенности среди всех банков Каспийского региона.

Топ 5 Банков по результатам оценки

Название Банка	Общая оценка
Ziraat Bank Georgia	96,00
Liberty Bank Basisbank	66,86
Basisbank	64,29
Halyk Bank Georgia	62,29
Bank of Georgia	58,57

Грузия
Оценка защищенности веб-сайтов и мобильных приложений Банков

#	Банк	HTTP заголовки	SSL-сертификат	HTTPS redirection	Кибергигиена	Открытые порты	Уязвимые компоненты сайта	SSL pinning	Доп. меры по защите моб. приложения	Общая оценка
1	Ziraat Bank Georgia	A	A+	✓	4	4	5	✓	✓	**96,00**
2	Liberty Bank	D	B	✓	4	3	2	✓	✗	**66,86**
3	Basisbank	D	A	✓	5	2	5	✗	✗	**64,29**
4	Halyk Bank Georgia	D	A	✓	2	4	5	✗	✗	**62,29**
5	Bank of Georgia	B	A+	✓	4	4	1	✗	✗	**58,7**
6	TBC Bank	D	A	✓	2	4	3	✗	✗	**54,29**
7	Silk Road Bank	D	A	✗	4	4	2	✗	✗	**54,00**
8	Credo Bank	F	B	✓	4	1	5	✗	✗	**51,00**
9	ProCredit Bank	D	A+	✓	2	2	3	✗	✗	**45,71**
10	PASHA Bank Georgia	D	C	✓	2	2	3	✗	✗	**41,43**
11	Isbank Georgia	F	T	✗	4	2	3	✗	✗	**40,86**
12	TeraBank	F	B	✓	4	2	1	✗	✗	**40,00**
13	Cartu Bank	F	A	✓	2	1	1	✗	✗	**28,43**

KPMG Caspian

Преимущества KPMG

1. Методология
KPMG обладает методикой проведения обследований и успешно реализовало ряд консалтинговых проектов в области комплексных ИТ и ИБ аудитов.

2. Опытная команда
Команда консультантов KPMG имеет опыт работы в аудите операторов платежных систем и платежных организаций, коммерческих банков и финансово-кредитных организаций.

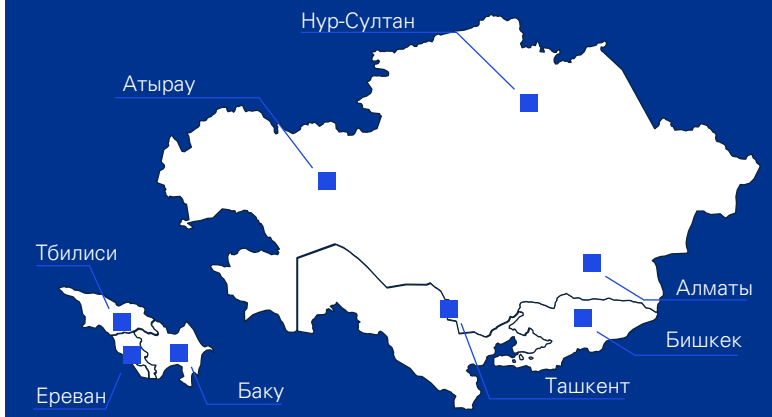
3. Отраслевая экспертиза
КПМГ имеет большой опыт оказания услуг аудита ИТ в крупных компаниях на территории региона Центральной Азии и Кавказа.

4. Квалификация
Наша команда консультантов имеет подтвержденную профессиональную квалификацию и практический опыт проведения ИТ и ИБ аудитов.

5. KPMG International
Являясь членом сети международных фирм KPMG International наша команда обладает доступом к методологиям и ресурсам фирм KPMG по всему миру.

KPMG Caspian

Команда KPMG Central Asia and Caucasus включает в себя следующие страны: Казахстан, Узбекистан, Кыргызстан, Азербайджан, Армения и Грузия



+30
Профессиональных сертификатов в области управления, ИТ и ИБ

+150
Проектов за последние 5 лет для +80 клиентов в 6 странах

46
Сотрудников группы Технологического консультирования

KPMG Caspian ○●○

KPMG Caspian
Предоставляемые услуги

Кибербезопасность:

— Аудит информационной безопасности
— Тестирование на проникновение
— Этичный взлом и расследование кибератак
— Соответствие стандартам
— Разработка стратегии ИБ
— Оценка уровня зрелости ИБ
— Непрерывность бизнеса

Цифровая трансформация:

— Трансформация клиентского опыта
— Подбор и внедрение технологий для постоянного мониторинга клиентского опыта
— Модернизация корпоративной архитектуры
— Выстраивание, внедрение и реализация архитектуры данных, приложений, инфраструктуры, безопасности
— Разработка цифровых бизнес-моделей
— Проектирование новых продуктов

Корпоративное управление ИТ:

— Разработка ИТ стратегии
— Анализ и разработка моделей корпоративного управления ИТ
— Оценка уровня зрелости ИТ-процессов
Аудит и аттестация ИТ
— Комплексный анализ информационных систем, инфраструктуры и качества управления ИТ
— Оценка и внедрение ИТ-контролей, контрольных процедур в области управления ИТ-рисками

Внедрение технологий и управление ИТ проектами:

— Выбор ИТ-решения
— Оценка эффективности и контроль внедрения информационных систем
— Трансформация корпоративных решений
— Оценка рисков и разработка плана миграции корпоративных приложений в облако
— Внедрение и сопровождение корпоративных систем

Управление данными и продвинутая аналитика:

— Аудит качества данных
— Повышение качества данных
— Сложная аналитика и прогнозирование
— Построение эконометрических моделей
— Визуализация данных. Проектирование и внедрение современных BI-решений (SAS, SAP, Qlik, IBM, MS Power BI и др.)

KPMG

KPMG Caspian

KPMG Caspian
Методология Cyber Maturity Assessment

Будучи экспертами в информационной безопасности, а также обладая обширным опытом работы с компаниями в различных отраслях экономики, мы предлагаем услуги в области информационной безопасности, затрагивающие как организационные, так и технические аспекты, которые будут эффективными именно для вашего бизнеса.

Cyber Maturity Assessment - это патентованная методология KPMG, основанная на ведущих стандартах информационной безопасности, таких как:
— Модель зрелости информационного обеспечения (IAMM)
— Финансовое управление киберрисками Американского национального института стандартов (ANSI)
— ISO 27001
— NIST
и других подобных стандартах в сочетании с нашим глобальным пониманием передовых практик.

— Тщательное соответствие ведущим стандартам для реализации концепции «Выполнить однажды, сообщать многократно»
— Риск-ориентированный подход для согласования с устойчивыми процессами управления рисками предприятия
— Оценка зрелости по девяти ключевым доменам для обеспечения полного и всестороннего представления о киберзрелости организации

The Cyber Maturity Assessment также доступен в качестве онлайн-платформы для последовательного сбора и использования данных.

Контакты

ТОО «КПМГ Такс энд Эдвайзори»
A25D6T5 Алматы, пр. Достык 180
E-mail: company@kpmg.kz
Тел./факс: +7 (727) 298-08-98, 298-07-08

Константин Аушев

Партнер

Руководитель группы
технологического консультирования

T +7 7272 980898 x62210
kaushev@kpmg.kz

Дамир Еркин

Менеджер

Руководитель направления кибербезопасности
группы технологического консультирования

T +7 7172 552888 x61689
damiryerkin@kpmg.kz

kpmg.kz