KPMG

ИБ без ИБшников. Роль CISO в эпоху ИИ

Константин Аушев
Технологическое консультирование

—

Profit Security Day

Ноябрь 2022

Начнем с картины рисков

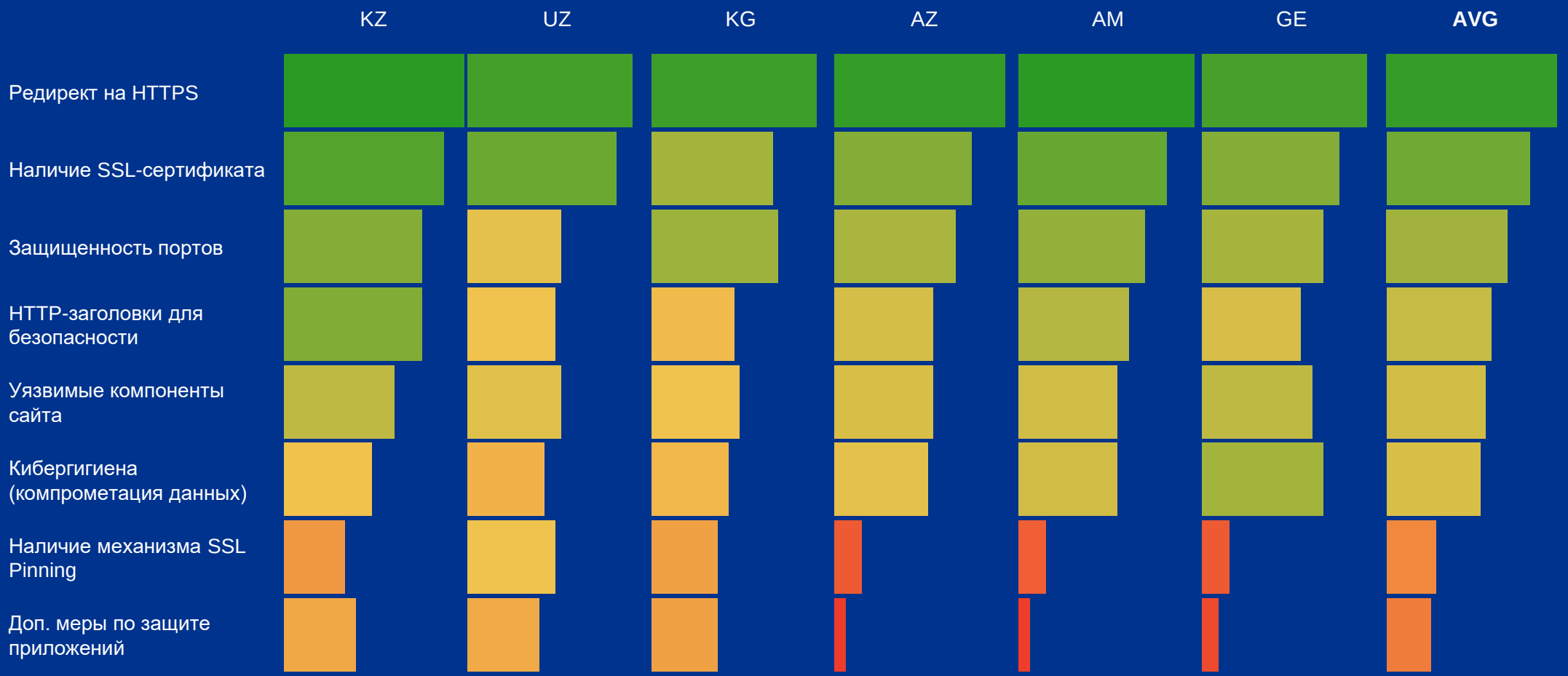
Результаты исследования KPMG по защищенности банковских приложений и веб-сайтов по региону ЦА и Кавказа

https://home.kpmg/kz/ru/home/insights/2022/09/bank-secirity-review.html

© 2022 KPMG Tax and Advisory LLC, a company incorporated under the Laws of the Republic of Kazakhstan and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

Кто ответит за ТОП 3 риска банковских приложений?

Источник: KPMG Caspian Banks Security Review, 2022.



© 2022 KPMG Tax and Advisory LLC, a company incorporated under the Laws of the Republic of Kazakhstan and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

Кто ответит за ТОП 3 риска банковских приложений?

© 2022 KPMG Tax and Advisory LLC, a company incorporated under the Laws of the Republic of Kazakhstan and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

Наблюдения по контролям за процессами управления данными, третьими сторонами и разработкой – ТОП на каждом из наших 60+ аудитов ИТ и ИБ из года в год

- Отсутствие процессов управления данными
- Отсутствие процесса анализа рисков третьих сторон
- Нарушение принципа разграничений полномочий, в частности между разработчиками и администраторами
- Отсутствие принципов безопасной разработки ПО
- Отсутствие контроля за привилегированными учетными записями
- Высокий уровень износа ИТ-инфраструктуры
- Отсутствие поддержки ПО и оборудования
- Невыстроенные процессы управления инцидентами и проблемами

© 2022 KPMG Tax and Advisory LLC, a company incorporated under the Laws of the Republic of Kazakhstan and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

Наблюдения по контролям за процессами управления данными, третьими сторонами и разработкой – ТОП на каждом из наших 60+ аудитов ИТ и ИБ из года в год

CDO	Отсутствие процессов управления данными
CRO	Отсутствие процесса анализа рисков третьих сторон
CIO	Нарушение принципа разграничений полномочий, в частности между разработчиками и администраторами
CISO	Отсутствие принципов безопасной разработки ПО
CISO	Отсутствие контроля за привилегированными учетными записями
CTO	Высокий уровень износа ИТ-инфраструктуры
CIO	Отсутствие поддержки ПО и оборудования
CIO/ CRO	Невыстроенные процессы управления инцидентами и проблемами

© 2022 KPMG Tax and Advisory LLC, a company incorporated under the Laws of the Republic of Kazakhstan and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

… vs. Ключевые риски 2023

CDO	**Отсутствие процессов управления данными**
CRO	**Отсутствие процесса анализа рисков третьих сторон**
CIO	Нарушение принципа разграничений полномочий, в частности между разработчиками и администраторами
CISO	**Отсутствие принципов безопасной разработки ПО**
CISO	Отсутствие контроля за привилегированными учетными записями
CTO	**Высокий уровень износа ИТ-инфраструктуры**
CIO	**Отсутствие поддержки ПО и оборудования**
CIO/ CRO	**Невыстроенные процессы управления инцидентами и проблемами**

Источник: Internal Audit Key risk areas 2023, KPMG Global, 2022.

01 Экономическая и политическая неопределенность

02 Изменение климата

03 Поиск и удержание талантов

04 **«ESG-отчетность»**

05 **Кибербезопасность и защита ПД**

06 Сложность внедрения изменений в культуру предприятия

07 **Риски третьих сторон и цепочек поставок**

08 **Риски от дисраптеров и новых технологий**

09 **Непрерывность бизнеса и кризисное управление**

10 Риски, связанные с M&A-сделками

© 2022 KPMG Tax and Advisory LLC, a company incorporated under the Laws of the Republic of Kazakhstan and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

Хотя в ½ организаций CISO уже входит в СД/ Правление, ⅓ не может понять «язык ИБ» и обоснованность затрат на ИБ

Роль CISO как инфлюенсера в эпоху AI, Zero Trust, Digital Disruptors…:

© 2022 KPMG Tax and Advisory LLC, a company incorporated under the Laws of the Republic of Kazakhstan and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

© 2022 KPMG Tax and Advisory LLC, a company incorporated under the Laws of the Republic of Kazakhstan and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

Константин Аушев

Партнер, руководитель
Технологической практики

KPMG в Центральной Азии и на Кавказе

kaushev@kpmg.kz

kpmg.kz

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

© 2022 KPMG Tax and Advisory LLC, a company incorporated under the Laws of the Republic of Kazakhstan and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.

Document Classification: KPMG Public