PROTOSECURITY

Анализируй это - статистика уязвимостей веб-приложений онлайн-ритейла

denis@protosecurity.ru
https://protosecurity.ru

+7 (499) 647-5967, доб.101
+7 (916) 999-3964

Денис Безкоровайный
CISSP, CISA, CCSK
ProtoSecurity

Методология

- Данные из сервиса постоянного аудита безопасности веб-приложений.
- Данные за 2015 год, статистика ведется несколько лет.
- Данные по веб-приложениям и уязвимостям сегментированы по разным критериям, включая уровень риска, классам уязвимостей и вертикалям.
- Уровни риска основываются на методологии OWASP.
- Ключевые метрики – вероятность наличия уязвимости заданного класса, процент устранения, время до устранения уязвимости, возраст отрытых уязвимостей.
- Данные по принадлежности к вертикали внесены самими клиентами.

Какой средний возраст **критической** веб-уязвимости?

etc.ch/2NwU

Состояние защищенности веб-приложений

- Время незащищенности – количество дней в году, в которое наблюдалась открытая уязвимость
- Веб-приложения попадают в одну из категорий:
  - всегда уязвимы (365 дней в году)
  - часто уязвимы (271-364 дней в году)
  - регулярно уязвимы (151-270 дней в году)
  - иногда уязвимы (31-150 дней в году)
  - редко уязвимы (до 30 дней в году)

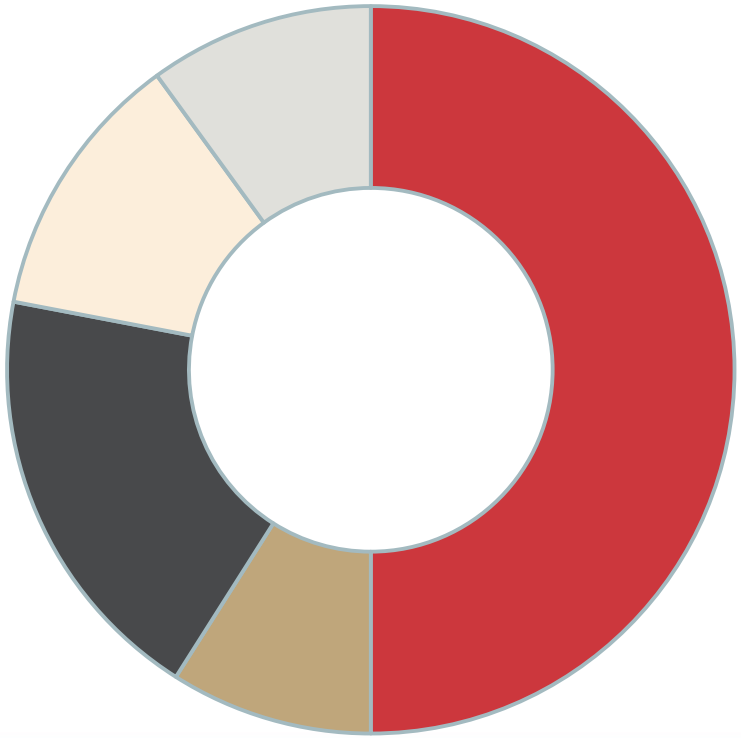
Состояние защищенности веб-приложений Ритейла

редко уязвимы
10%

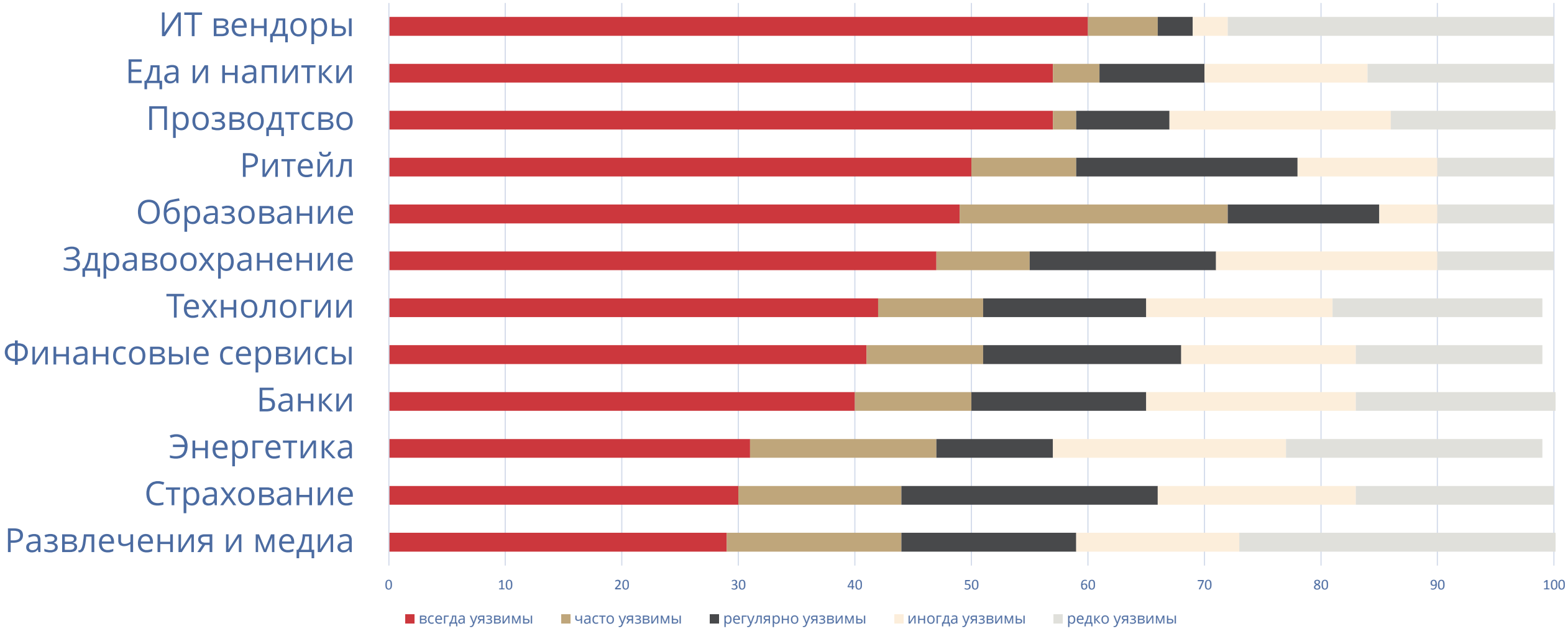
иногда уязвимы
12%

регулярно уязвимы
19%

часто уязвимы
9%



всегда уязвимы
50%


ИТ вендоры
Еда и напитки
Прозводтсво
Ритейл
Образование
Здравоохранение
Технологии
Финансовые сервисы
Банки
Энергетика
Страхование
Развлечения и медиа
0
10
20
30
40
50
60
70
80
90
100
всегда уязвимы
часто уязвимы
регулярно уязвимы
иногда уязвимы
редко уязвимы

Количество уязвимостей на 1 веб-сайт в Ритейле

23

из них 13 серьезных

По всем отраслям 5-32 всего

Средний возраст открытой уязвимости веб-приложений в Ритейле

456 дней

По всем отраслям 274-875 дней


ИТ вендоры
Ритейл
Образование
Еда и напитки
Здравоохранение
Финансовые сервисы
Прозводтсво
Банки
Страхование
Развлечения и медиа
Технологии
Энергетика
0
100
200
300
400
500
600
700
800
900
срок жизни, дней

Процент устранения уязвимостей веб-приложений Ритейла

48%

По всем отраслям 24% - 66%

Средний срок устранения уязвимости

205 дней

В среднем по всем отраслям 150 дней

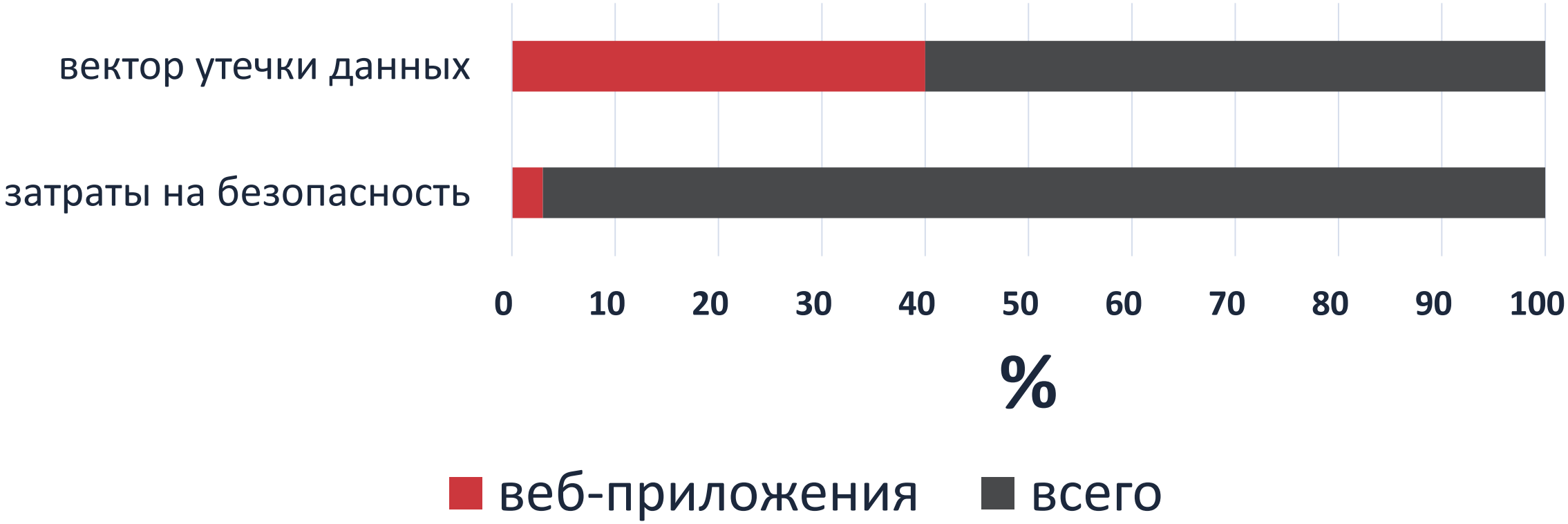
Подытожим данные по веб-приложениям Ритейла

- Более **50%** сайтов Ритейла **всегда** содержат уязвимости.
- На каждый веб-сайт Ритейла в среднем приходится **23** уязвимости, из которых **13** – с критическим и высоким риском.
- Из этих 23 уязвимостей около **48%** будут рано или поздно устранены.
- Устранение каждой из уязвимостей займет в среднем более **200** дней.

Выводы

- Даже при обнаружении уязвимостей не хватает ресурсов на их устранение
- Даже серьезные уязвимости устраняются долго
- Регулируемые отрасли показывают схожие результаты с другими
- Ритейл по некоторым показателям среди «лидеров»

Куда направлять усилия?



1 Verizon 2016 Data Breach Investigations Report
2 Gartner Inc., “Market Share: Security Software, Worldwide, 2015”, Sid Deshpande, Ruggero Contu, 06 April 2016

Security as a Service

by ProtoSecurity

Вопросы?

- denis@protosecurity.ru
- https://protosecurity.ru

Какой средний возраст **критической** веб-уязвимости?

300 дней!

Результаты опроса
http://directpoll.com/r?XDbzPBd3ixYqg8EFREIrBV1vNkd5vAYDdCsIT7a9h