# Тема 12

Обеспечение информационной безопасности при работе в сети Интернет

# Содержание темы

- Обзор инцидентов в сфере информационной безопасности.
- Системы автоматизированного сбора и учета фактов нарушения информационной безопасности объектов информатизации.
- Методы и средства защиты информации от удаленных атак.
- Безопасность в социальных сетях.
- Рекомендации по защите персонального компьютера при работе в сети Интернет.

# Kaspersky Security Bulletin 2016

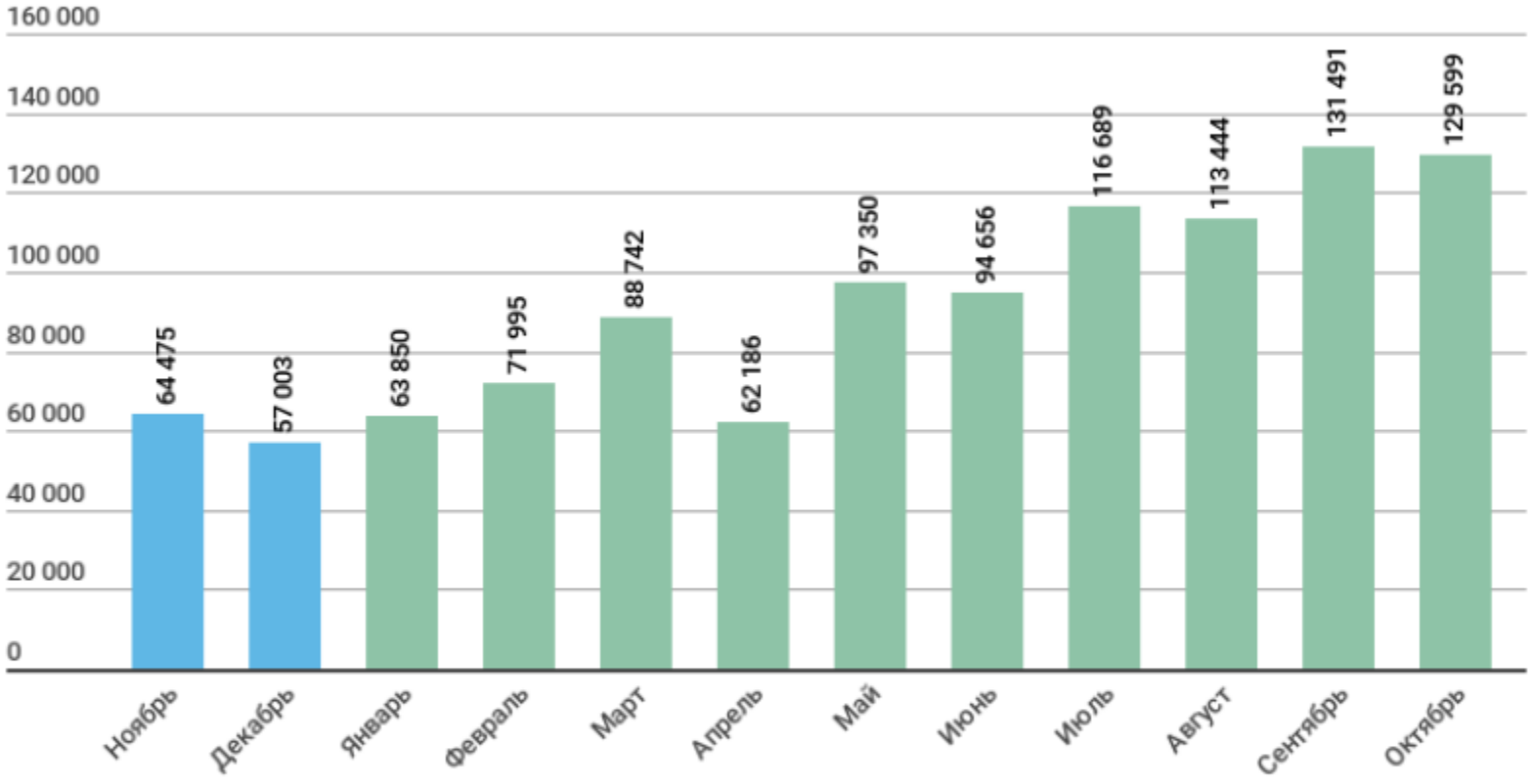
# Kaspersky Security Bulletin 2017

# Kaspersky Security Bulletin 2018

## ЦИФРЫ ГОДА

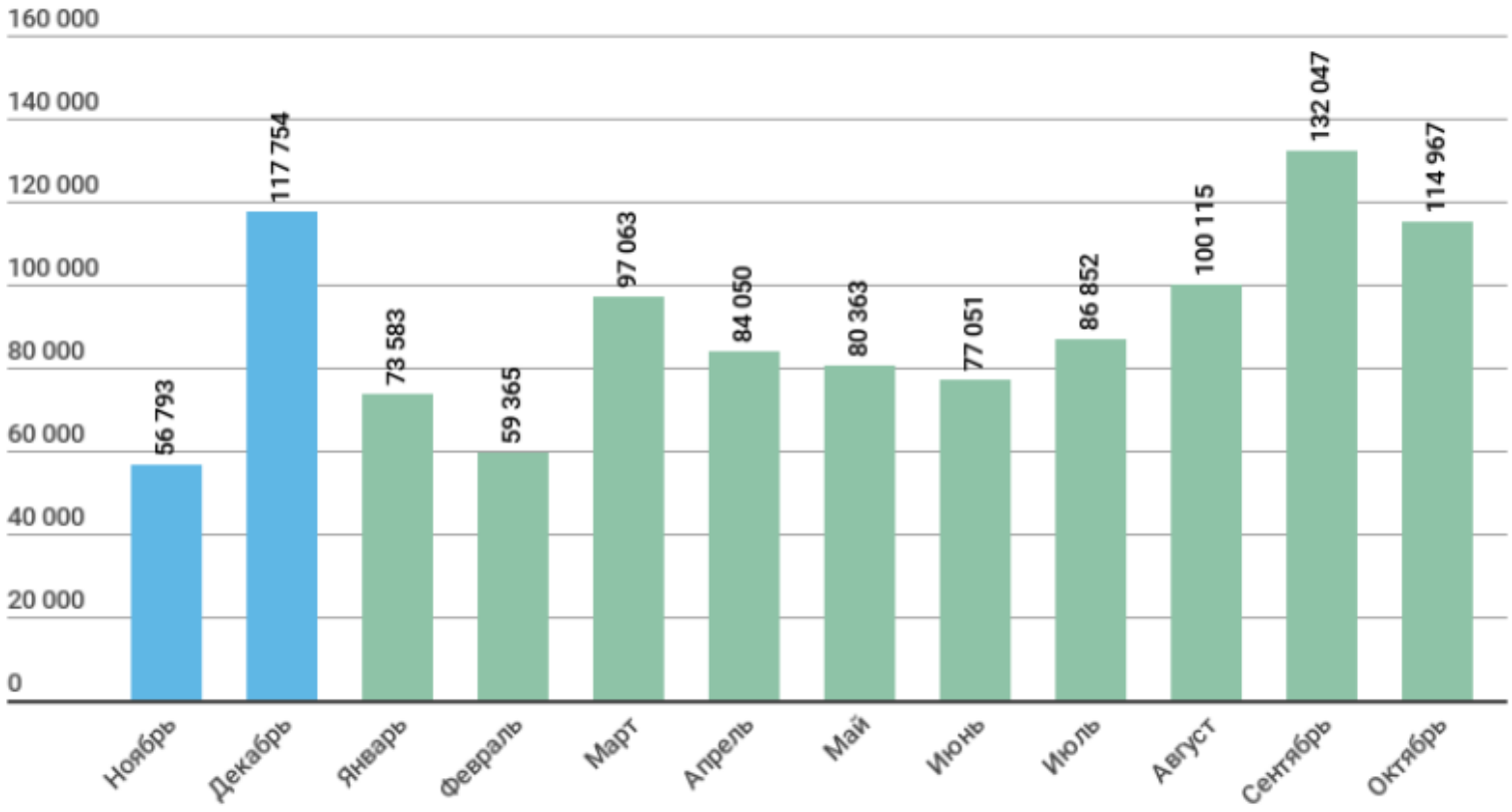
- В течение года 30,01% компьютеров интернет-пользователей в мире хотя бы один раз подверглись веб-атаке **класса Malware**.
- Решения «Лаборатории Касперского» отразили **1 876 998 691** атаку, которые проводились с интернет-ресурсов, размещенных в различных странах мира.
- Зафиксирован **554 159 621** уникальный URL, на которых происходило срабатывание веб-антивируса.
- Нашим веб-антивирусом зафиксировано **21 643 946** уникальных вредоносных объектов.
- Атаки шифровальщиков отражены на компьютерах **765 538** уникальных пользователей.
- За отчетный период майнерами были атакованы **5 638 828** уникальных пользователей.
- Попытки запуска вредоносного ПО для кражи денежных средств через онлайн-доступ к банковским счетам отражены на устройствах **830 135** пользователей.

# Kaspersky Security Bulletin 2018



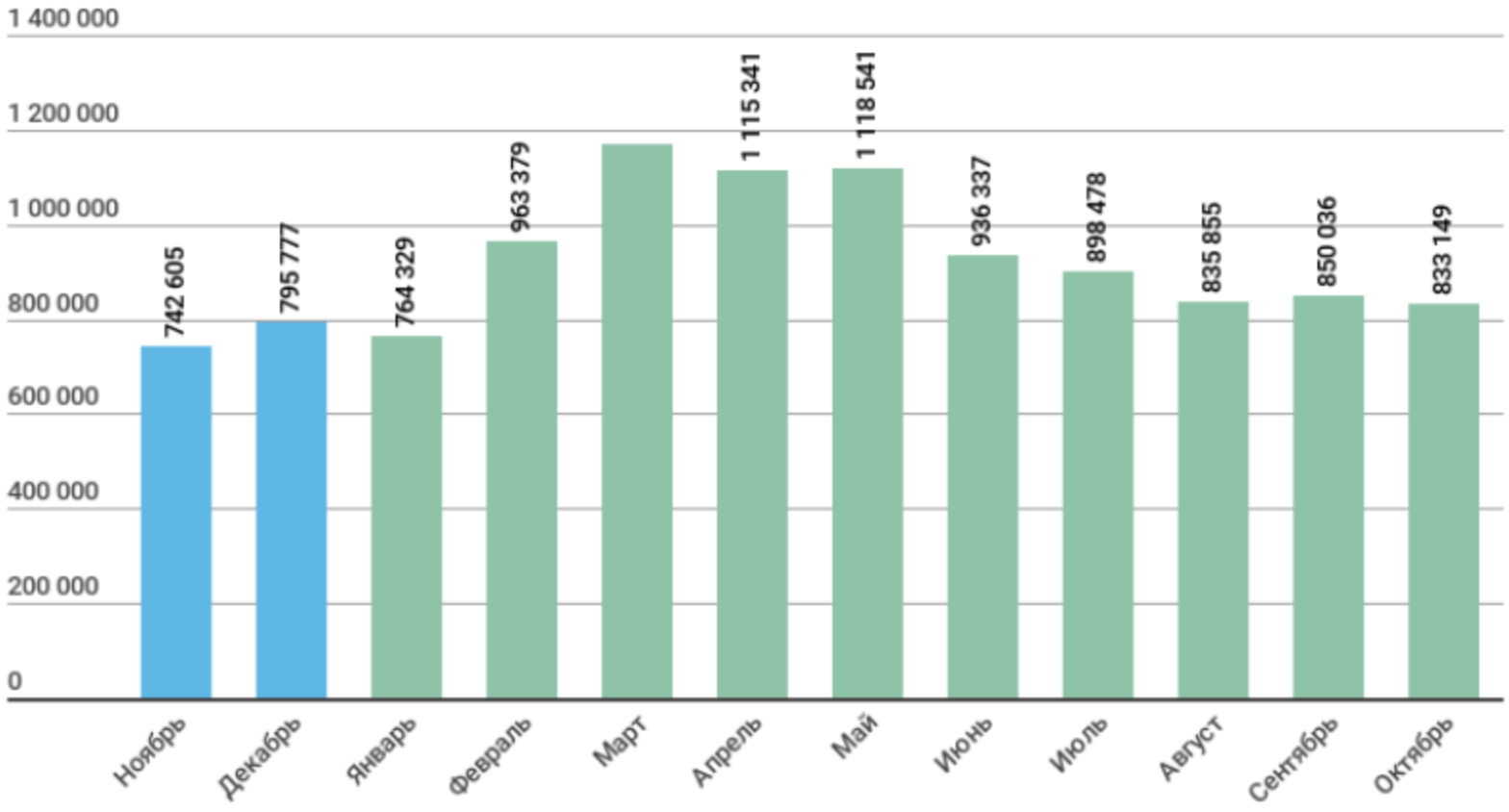

*Количество пользователей, атакованных банковским вредоносным ПО, ноябрь 2017 года – октябрь 2018 года*

# Kaspersky Security Bulletin 2018



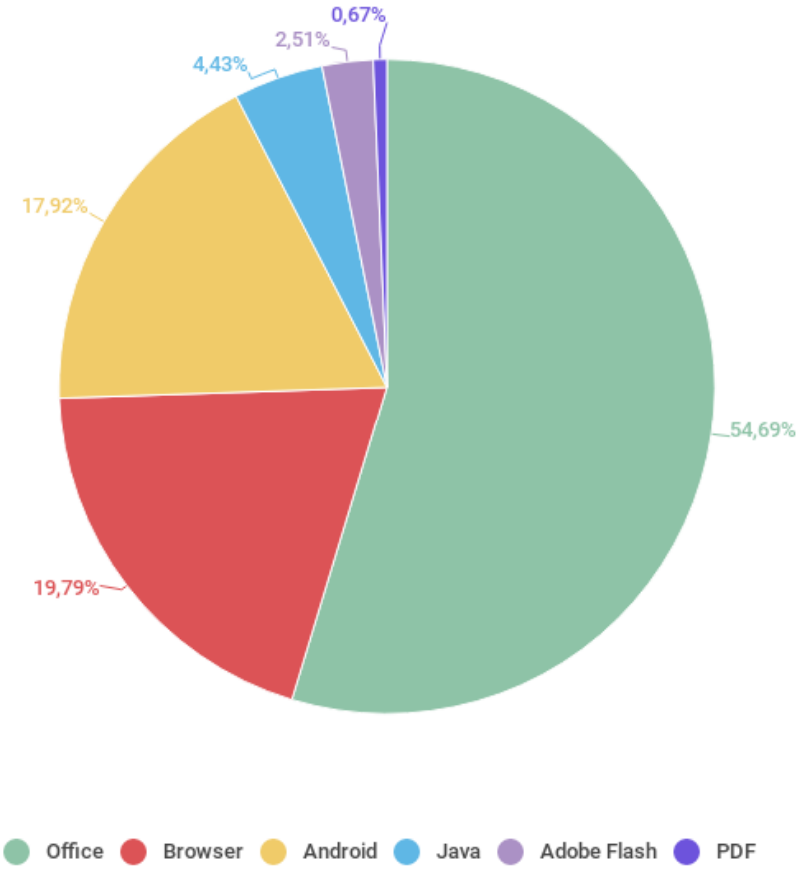

*Количество пользователей, атакованных троянцами-шифровальщиками, ноябрь 2017 года – октябрь 2018 года*

# Kaspersky Security Bulletin 2018



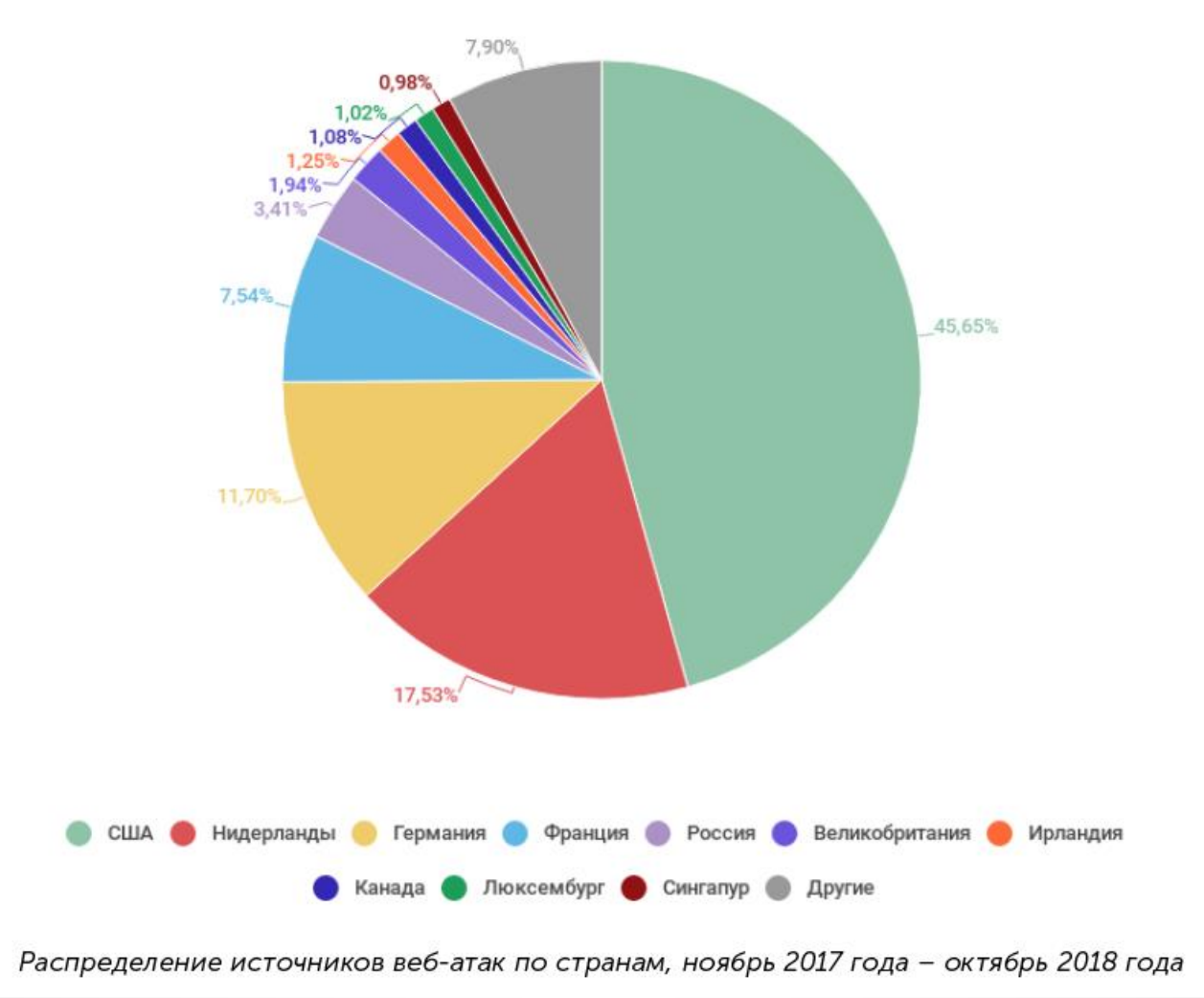

*Количество пользователей, атакованных майнерами, ноябрь 2017 года – октябрь 2018 года*

# Kaspersky Security Bulletin 2018



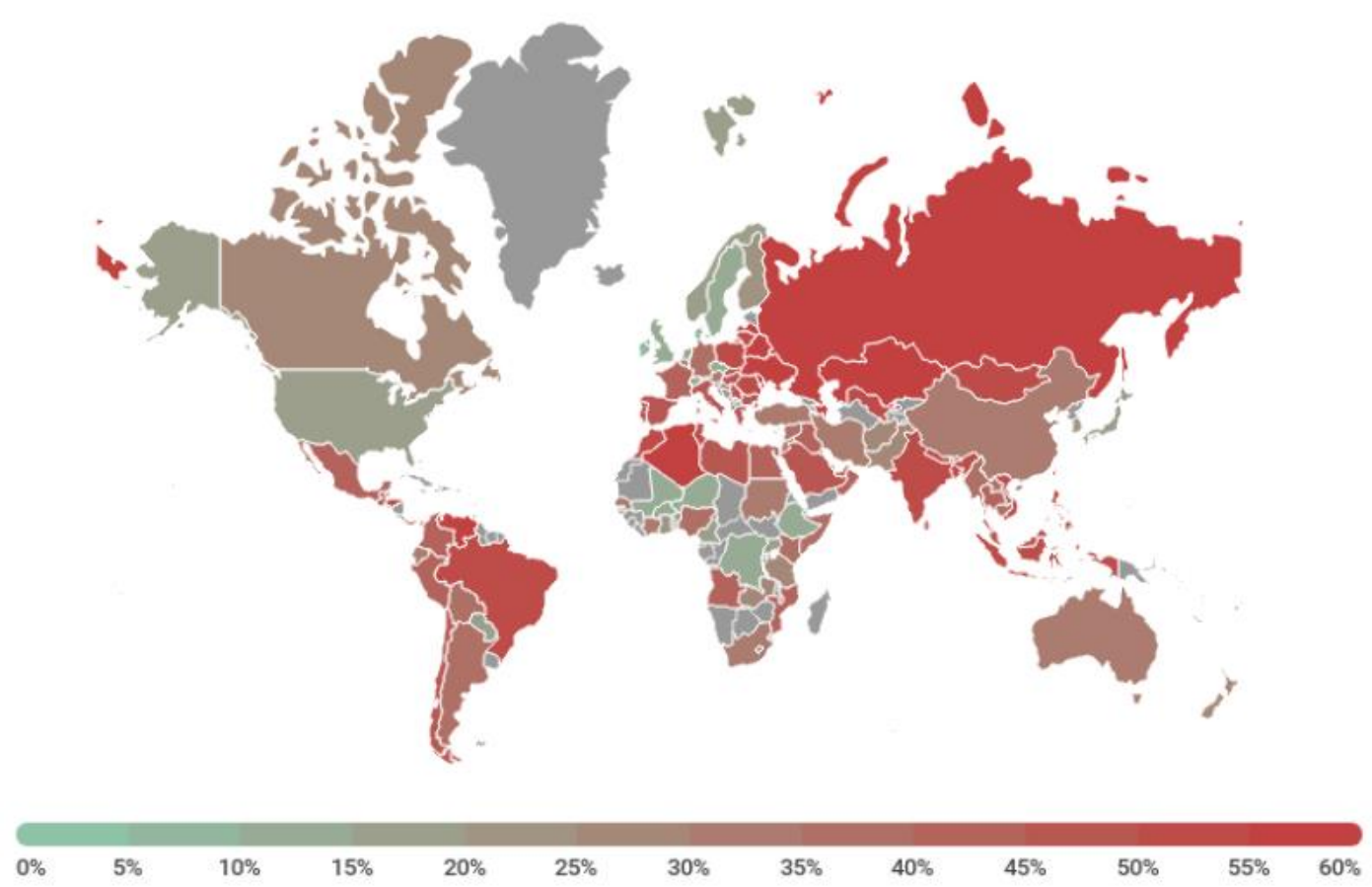

*Распределение эксплойтов, использованных в атаках злоумышленников, по типам атакуемых приложений, ноябрь 2017 года – октябрь 2018 года*

# Kaspersky Security Bulletin 2018



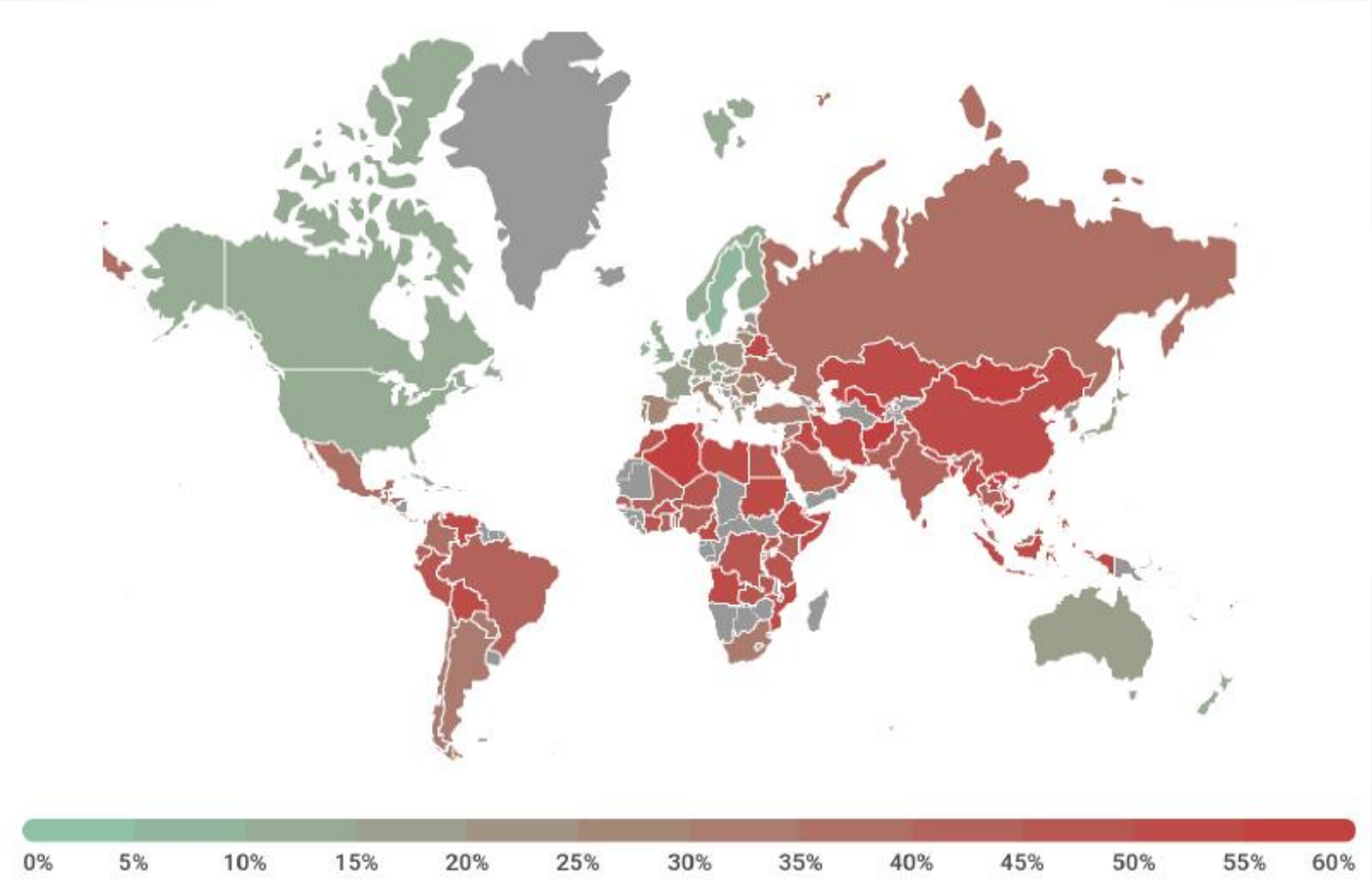

*Распределение источников веб-атак по странам, ноябрь 2017 года – октябрь 2018 года*

# Kaspersky Security Bulletin 2018




*География веб-атак вредоносного ПО, ноябрь 2017 года – октябрь 2018 года*

# Kaspersky Security Bulletin 2018



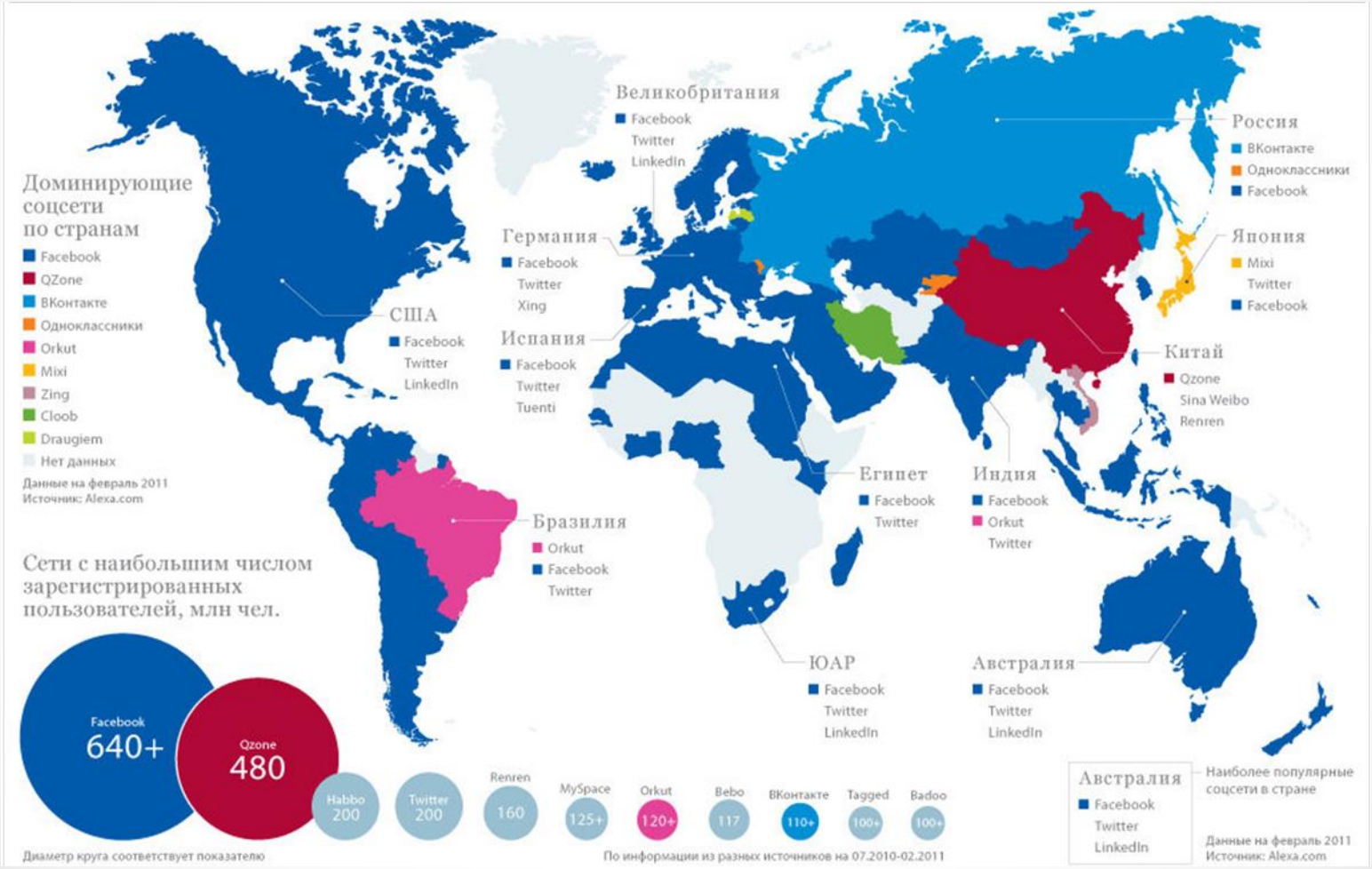

*География локальных заражений вредоносным ПО, ноябрь 2017 года – октябрь 2018 года*

# Защита информации от удаленных атак

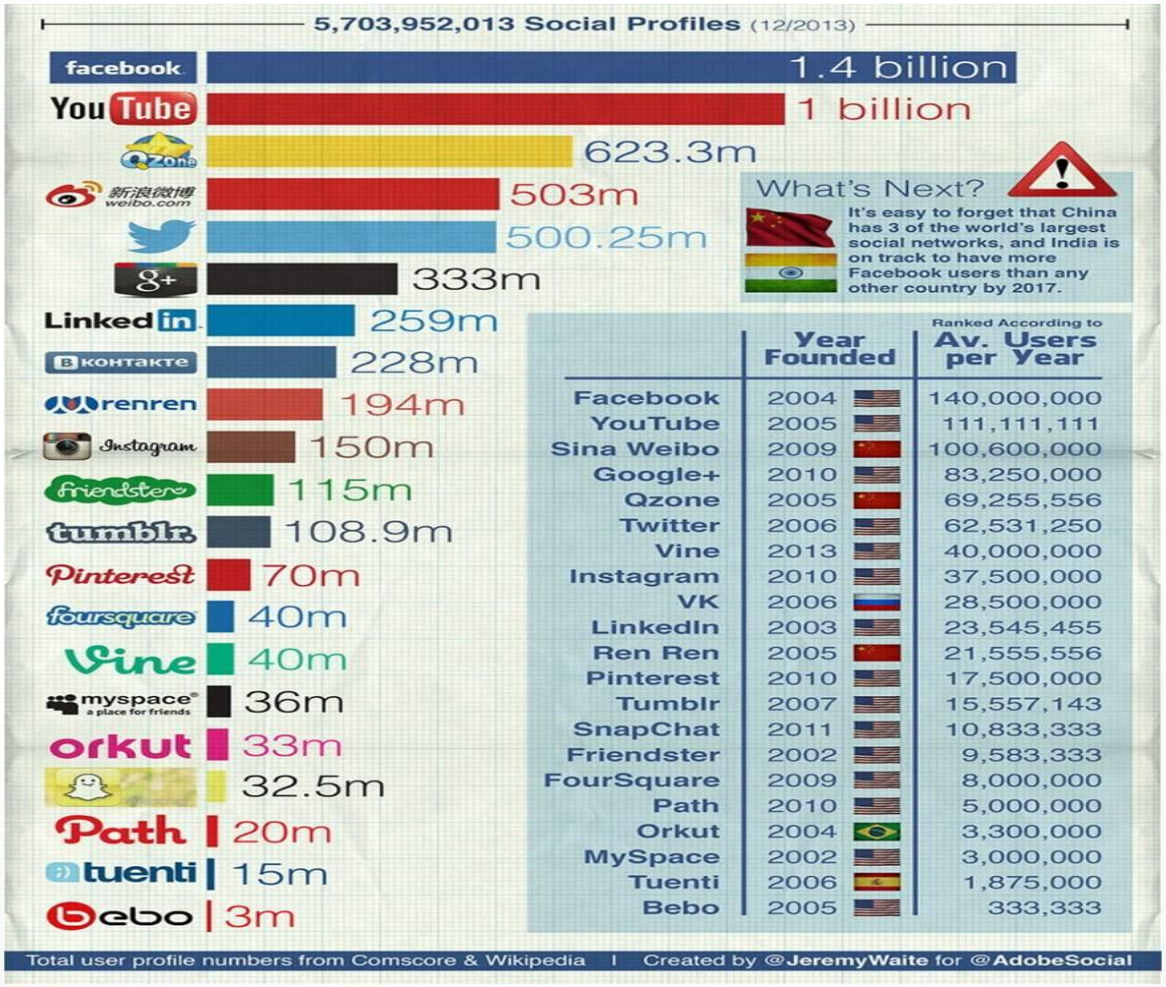
**Через сеть Интернет нарушитель может**:

- вторгнуться во внутреннюю сеть предприятия и получить несанкционированный доступ к конфиденциальной информации;
- незаконно скопировать важную и ценную для предприятия информацию;
- получить пароли, адреса серверов и их содержимое;
- входить в информационную систему предприятия под логином зарегистрированного пользователя и т. п.

# Безопасность в социальных сетях



# Безопасность в социальных сетях



# Безопасность в социальных сетях

**ИНФОРМАЦИОННЫЙ ВЗРЫВ – ГЕНЕРАЦИЯ КОНТЕНТА В МИРЕ:**

- Классические СМИ – 1 млн. документов в сутки;
- Пользовательский контент (твиты, блоги, форумы, соцсети, отзывы, комментарии) – свыше 1 млрд. в сутки;
- Ежегодный прирост – 25%.

# Безопасность в социальных сетях

**92%** – уровень доверия к социальным сетям

**47%** – уровень доверия к ТВ, радио, прессе

# Рекомендации

Чтобы обезопасить себя и сохранить свою личную информацию конфиденциальной, необходимо соблюдать некоторые правила:

1. **Электронная почта.** Для того чтобы зарегистрироваться в социальных сетях, необходимо иметь отдельную электронную почту. Нельзя проходить регистрацию и указывать адрес рабочей почты или почты, которая связана с важными услугами – электронные кошельки, банковские услуги или оплата коммунальных платежей.

# Рекомендации

Чтобы обезопасить себя и сохранить свою личную информацию конфиденциальной, необходимо соблюдать некоторые правила:

1. **Электронная почта.** Для того чтобы зарегистрироваться в социальных сетях, необходимо иметь отдельную электронную почту.

Нельзя проходить регистрацию и указывать адрес рабочей почты или почты, которая связана с важными услугами – электронные кошельки, банковские услуги или оплата коммунальных платежей.

# Рекомендации

2. **Пароль.** Именно он является первой линией защиты для злоумышленников.

Для каждого сервиса необходимо использовать **отдельный пароль** и держать его в сохранности.

Необходимо подобрать базовое слово, которое можно дополнять другими символами или цифрами для каждой социальной сети в отдельности.

# Рекомендации

3. **Минимизация информации, которая публикуется в социальной сети.**

Возможно, и стоит поделиться свежей фотографией с друзьями, но не нужно демонстрировать всему миру свою личную жизнь.

4. **При переходе на ссылки из посторонних источников необходимо быть максимально внимательным.** Особенно если они получены от незнакомых людей.

# Рекомендации

5. **Не нужно использовать социальные сети в качестве главного хранилища информации и фотографий**.

Необходимо помнить, что это не персональный сайт, это ресурс, который принадлежит другим владельцам и обычно в набор стандартных инструментов не включены резервные копии.

6. **В социальных сетях не рекомендуется добавлять незнакомых людей.**

Злоумышленники могут создавать вымышленные аккаунты для получения той информации, которая доступна только пользователям из списка друзей.

# Рекомендации

7. **Посещать социальные сети с рабочего места нельзя.**

Любая соцсеть – это распространение вирусов и других шпионских программ, что может привести к заражению не только персонального компьютера, но и всей корпоративной сети.

Это чревато потерей тех информационных данных, которые составляют коммерческую тайну организации.

# Рекомендации

8. **Нельзя отправлять важные данные и документы посредством социальных сетей.**
9. **Нельзя публиковать фото документов.**

Нынешние соцсети содержат огромный функционал, который позволяет сделать личную информацию доступной только для определенного круга лиц. Чтобы активировать эту защиту, необходимо настроить конфиденциальность в собственном аккаунте.