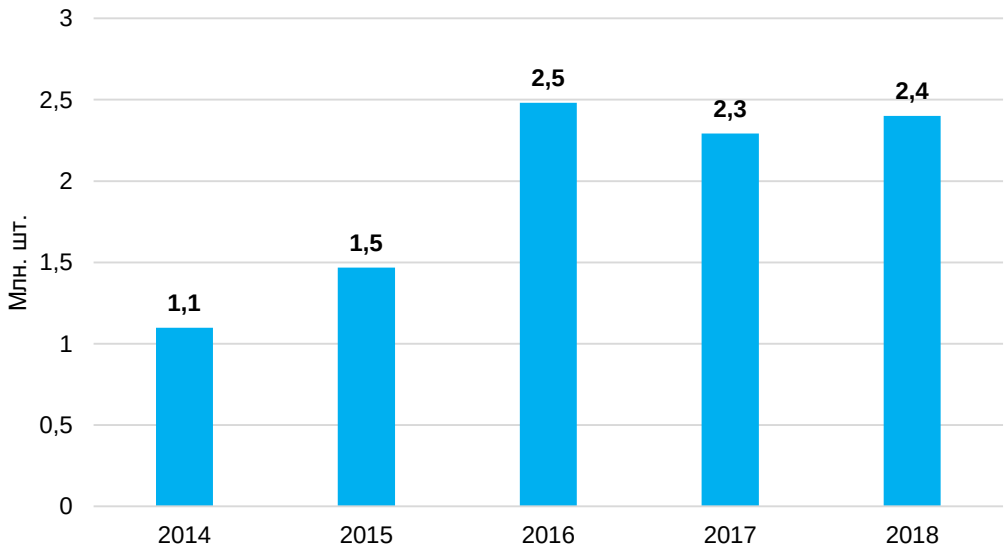
Информационная безопасность и ключевые носители в финансовом секторе

USB-токены

- Ключевой носитель - инструмент или устройство хранения закрытого или секретного (в случае с ОТП) ключа.
- На банковский сегмент приходится около 40% объема рынка USB-токенов в натуральном выражении.

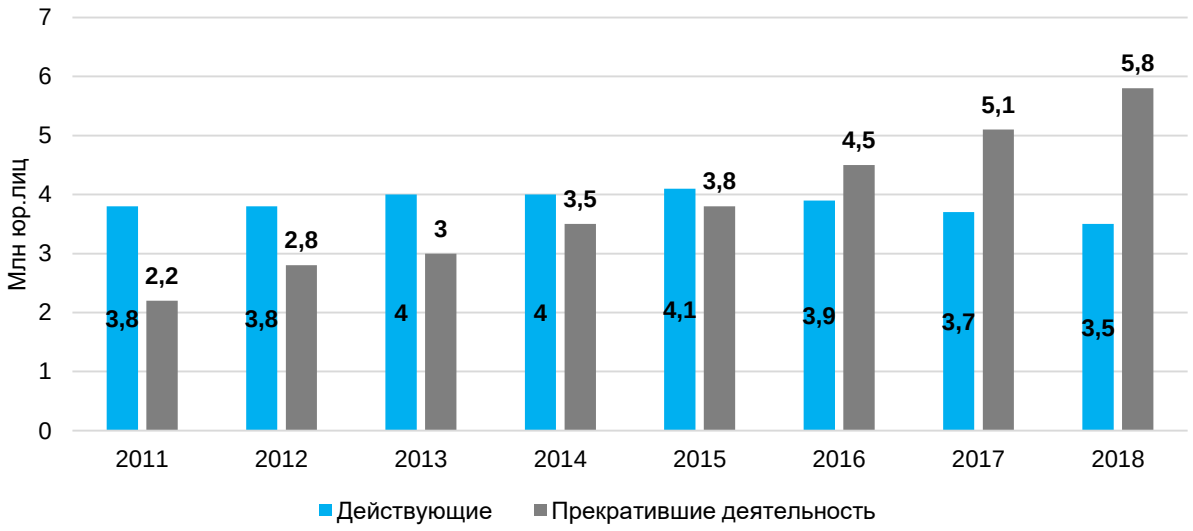
Динамика рынка USB-токенов в России 2014–2018 гг.



Факторы, влияющие на спрос

- Количество действующих коммерческих организаций по итогам 2018 г. сократилось до 3,5 млн.
- Число организаций, прекративших деятельность увеличилось почти до 6 млн по итогам 2018 г.
- Рост будет обеспечен не за счет новых клиентов, а за счет увеличения проникновения технологии в другие сегменты.

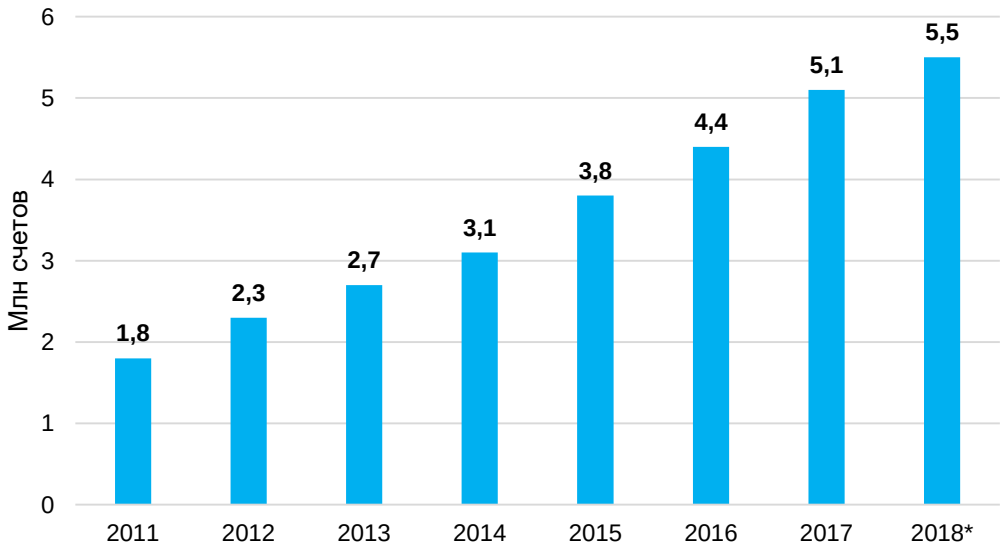
Динамика действующих и прекративших свою деятельность коммерческих организаций, 2011–2018 гг.



Факторы, влияющие на спрос

- Все больше взаимодействий переходит в цифровую реальность.
- Растет **реальное** осознание проблем информационной безопасности со стороны конечных клиентов и заказчиков.
- Интенсификация перевода взаимодействия в электронный вид между банками и их клиентами.

Динамика счетов юрлиц с дистанционным доступом, 2011–2018 гг.



Факторы, влияющие на спрос

- **Рост числа субъектов регулирования**.
  - Законопроект ЦБ «Об установлении обязательных для не кредитных финансовых организаций требований к обеспечению защиты информации при осуществлении деятельности в сфере финансовых рынков».
  - Распространяется на НПФ, ПИФы, проф.участники рынка ценных бумаг, депозитарии, ломбарды и др.
  - Рост количества носителей – не более чем на 20 000 устройств.
- **Смена технологически парадигмы** маловероятна в долгосрочной перспективе.
- **Применение биометрии в сегменте юр.лиц** возможно с вероятностью около 20% в среднесрочной перспективе – до 2024 г. К 2027 г. вероятность наступления события – около 40%.
- **Требования регулятора** будут расти. Необходимость им соответствовать – по умолчанию.

Актив Консалтинг

- **Аудит информационной безопасности**
  - Аудит защищенности информационных систем
  - Тестирование на проникновение внешнего и внутреннего периметров
  - Проверка устойчивости к DDoS атакам
  - Защита от методов социальной инженерии
- **Консалтинг и обучение**
  - Разработка внутренних нормативных документов ИБ
  - Проектирование системы управления ИБ (СУИБ)
  - Создание методологии безопасного жизненного цикла разработки
  - Разработка программы обучения ИБ
- **Аутсорсинг процессов и ролей**
  - Сопровождение СЗИ, СКУД и различных систем мониторинга инфраструктуры
  - Предоставление внешнего центра мониторинга и реагирования на инциденты ИБ (SOC)
  - Сопровождение безопасного цикла разработки ПО
- **Оценка соответствия стандартам**
  - Консолидация требований, необходимых к исполнению
  - Приведение инфраструктуры в соответствие требованиям регуляторов
  - Аудит соответствия требованиям регуляторов
- **Интеграция средств защиты информации**
  - Проектирование и внедрение средств защиты информации
  - Внедрение защитных систем глубокого обучения
  - Внедрение систем контроля и управления доступом (СКУД)
- **Компьютерная криминалистика**
  - Выездные мероприятия по сбору свидетельств инцидентов
  - Исследование и анализ вредоносного ПО
  - Расследование инцидентов кибербезопасности

Контактная информация

Мария Грудева

Электронная почта:

grudeva@aktiv-company.ru

Сайт:

www.aktiv-company.ru

Телефон:

+7 495 925-77-90