Исследование финансового сектора в Центральной и Восточной Европе, IBM, 2017 г.

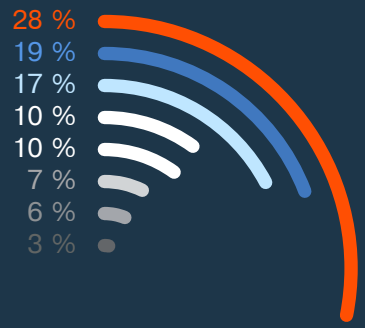
Текущая ситуация в сфере безопасности финансового сектора

Цели исследования IBM

Главная цель исследования – понять, какие проблемы стоят перед финансовыми учреждениями в плане кибербезопасности, ожидаемых будущих угроз, готовности и принимаемых мер в отношении регулирования этого сектора, а также выяснить баланс между удовлетворенностью клиентов и мерами обеспечения безопасности в целом по отрасли.

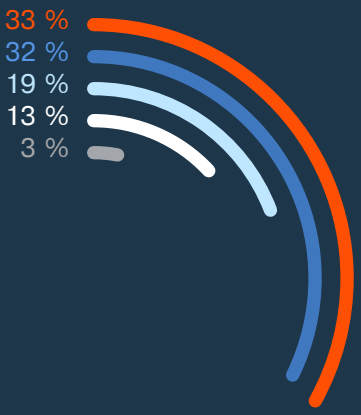
В опросе приняли участие около 200 финансовых организаций из 5 стран Центральной и Восточной Европы: России, Польши, Венгрии, Чешской и Словацкой Республик.

Респонденты по должностям:



- ИТ-директор
- Прочие ИТ-специалисты
- Директор по ИТ-безопасности
- Специалист по безопасности
- ИТ-руководитель
- Руководство
- ИТ-администратор
- Прочее

Респонденты по странам:



- Польша
- Россия
- Венгрия
- Чешская Республика
- Словакия

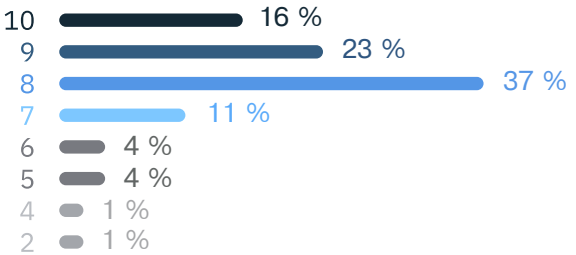
Исследование финансового сектора в Центральной и Восточной Европе, IBM, 2017 г.

Цели исследования IBM

В целом к настоящему моменту в европейском финансовом секторе сложилась относительно удовлетворительная ситуация с ИТ-безопасностью. Но полностью уверены в своих системах защиты всего 16 % опрошенных.

Текущая ситуация с ИТ-безопасностью

В: Как бы вы оценили текущую ситуацию с ИТ-безопасностью в вашей организации по шкале от 1 до 10?
(Баллы 1 – 10; 1 = защита отсутствует, 10 = максимальная безопасность)



Объем и сложность угроз растет в геометрической прогрессии. Несмотря на то что финансовый сектор жестко регулируется, мобильные, облачные и другие технологии повышают риск и требуют более серьезных мер защиты. Нет никаких сомнений в том, что в ближайшие годы финансовый сектор столкнется с дополнительными сложностями, и компаниям предстоит еще очень много работы.

Возможные атаки способны не только нанести значительные финансовые убытки, но и негативно сказаться на репутации и доверии к компании.

Цели исследования IBM

Оценивая свою ситуацию с ИТ-безопасностью, большинство финансовых организаций ответили положительно. Тех, кто совершенно не удовлетворен или очень мало удовлетворен своей ИТ-безопасностью, было немного.

С одной стороны, это неудивительно, если принять во внимание, что исследовался именно финансовый сектор, но с другой стороны, полностью защищенными считают себя “всего” 16 % организаций. Безусловно, для этой сферы это не очень большая цифра.

Исследование IBM показало, что подавляющее (91 %) большинство финансовых учреждений региона CEE прогнозируют дальнейший рост киберпреступности

Текущая ситуация в финансовом секторе

1. Рост числа и сложности угроз кибербезопасности

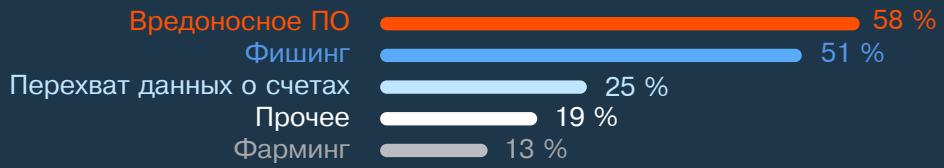
2. Необходимость соблюдения законодательных требований

3. Кибербезопасность – пункт номер один на повестке дня

4. Ежегодный рост средств, выделяемых на безопасность

Каким атакам подвергались компании?

В: Какие атаки были зарегистрированы в вашем интернет-канале?



Исследование финансового сектора в Центральной и Восточной Европе, IBM, 2017 г.

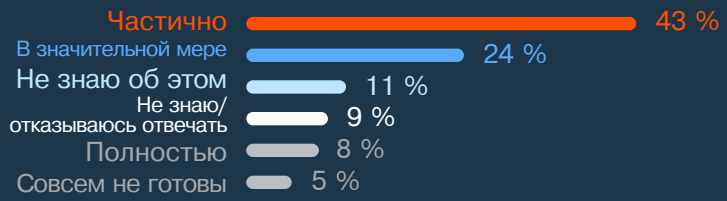
Нет никаких сомнений в том, что банки – излюбленная мишень для киберпреступников. Проще говоря, киберпреступники в основном идут туда, где есть деньги. Трудно не заметить заголовки публикаций в СМИ о многочисленных громких атаках на крупные финансовые учреждения в прошлом году.

Также все сложнее становится успевать за всеми законодательными требованиями и директивами, охватывающими все сферы: от защиты данных и платежей до безопасности передачи данных. Необходимость соблюдать все эти требования неизбежно ведет к увеличению расходов на безопасность.

Текущая ситуация в финансовом секторе

Процесс обеспечения соответствия GDPR

В: Укажите свой уровень соответствия требованиям закона (CEE, кроме России)



Более 1/2 финансовых учреждений признались, что они подверглись атакам с помощью вредоносного кода и фишинга – эти атаки уже стали практически стандартными для финансового сектора.

Несмотря на то, что финансовый сектор довольно жестко регулируется, 16 % организаций из этой сферы заявили, что они совсем не готовы к GDPR или вообще не знают о нем.

Также в качестве возможных способов атак на финансовый сектор в будущем упоминались: интернет-мошенничество, фишинг и атаки DDoS.

86 % финансовых учреждений в Европе предположили, что в ближайшем будущем им придется увеличить вложения в кибербезопасность.

Исследование финансового сектора в Центральной и Восточной Европе, IBM, 2017 г.

Инструменты для борьбы с мошенничеством

Это один из важнейших аспектов кибербезопасности. Но более 20 % финансовых учреждений в CEE ими не пользуются.

Использование средств борьбы с мошенничеством

В: Используете ли вы инструменты для противодействия мошенничеству?

Сейчас инструменты для борьбы с мошенничеством становятся решающим фактором. Так как финансовые учреждения реализуют все больше цифровых и мобильных стратегий, это – не просто залог защиты от известных и неизвестных уязвимостей, но и способ приближения скорости этой защиты к реальному времени.

Для того чтобы финансовые учреждения могли справляться с текущей ситуацией кибербезопасности, необходимо
1) Обнаружение
2) Защита и
3) Постоянное развитие.

Исследование финансового сектора в Центральной и Восточной Европе, IBM, 2017 г.

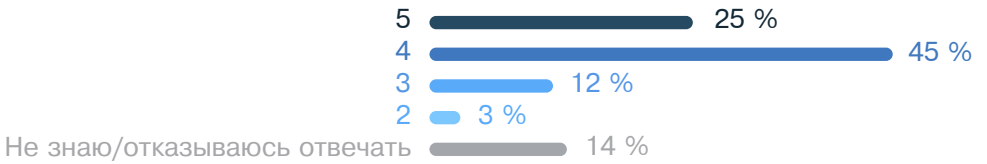
Инструменты для борьбы с мошенничеством

Хотя инструменты для борьбы с мошенничеством активно используются в 76 % финансовых учреждений в CEE, в 21 % организаций они не используются вовсе. Не очень много было и пользователей, полностью уверенных в своем инструментарии.

Если посмотреть на различные виды средств борьбы с мошенничеством, то в CEE самыми малоэффективными оказались обнаружение мошенничества и управление рисками.

Удовлетворение инструментами для борьбы с мошенничеством

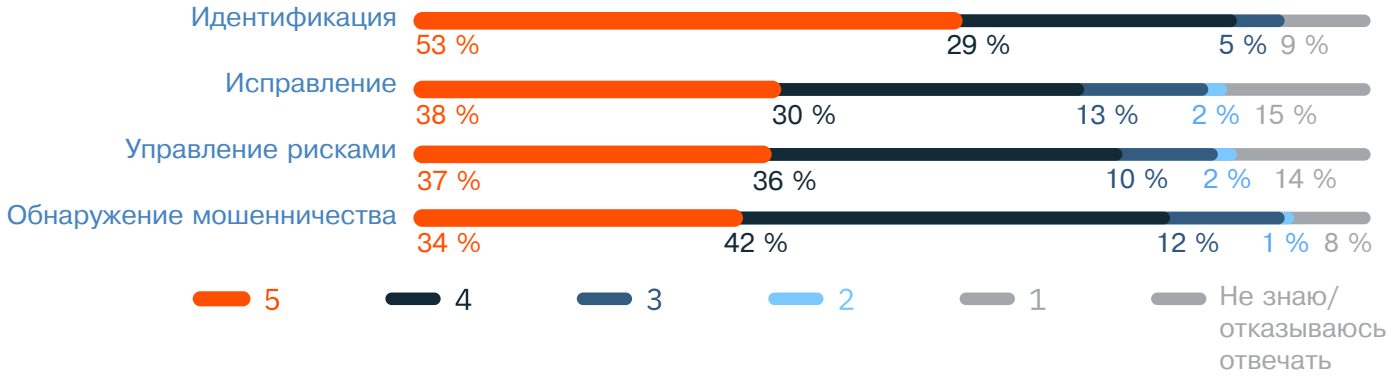
B: Как бы вы описали удовлетворение инструментарием для борьбы с мошенничеством и управления рисками со своей и клиентской стороны?

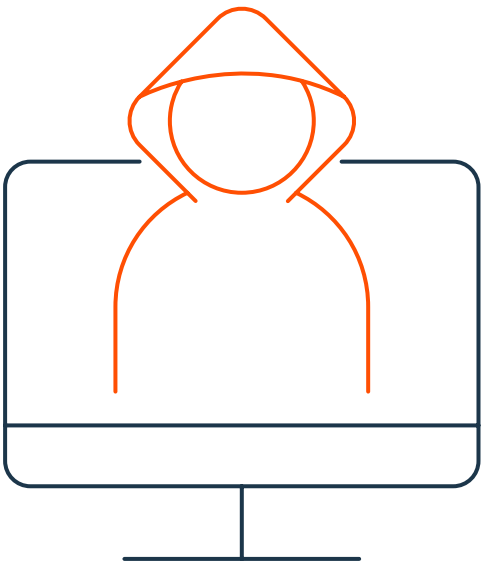


Инструменты для борьбы с мошенничеством

Эффективность инструментов для борьбы с мошенничеством

В: Насколько эффективно работают 4 следующих средства противодействия мошенничеству в вашей организации?





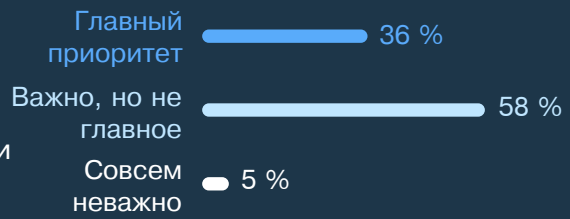
Исследование финансового сектора в Центральной и Восточной Европе, IBM, 2017 г.

Удобство клиентов

Обеспечение безупречного обслуживания клиентов – первостепенная задача почти для всех финансовых учреждений в CEE. Но как же найти оптимальный баланс между удобством клиентов и требованием высочайшей кибербезопасности?

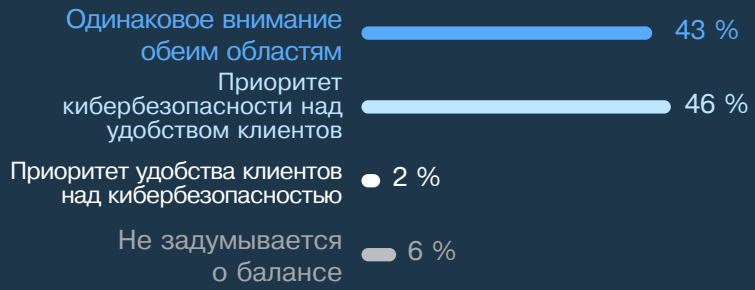
Значимость обеспечения беспрепятственной и удобной работы интернет-клиентов

В: Если говорить о кибербезопасности, какое значение ваша организация придает интернет-безопасности при условии сохранения удобного интерфейса для интернет-клиентов? Удобство/удовлетворенность клиентов – это:



Баланс между кибербезопасностью и удобством интернет-клиентов

В: Как, по-вашему, ваша организация сочетает кибербезопасность и удобство интернет-клиентов?



Исследование финансового сектора в Центральной и Восточной Европе, IBM, 2017 г.

Удобство клиентов

Одна из задач, стоящих сегодня перед финансовыми учреждениями – поиск оптимального баланса между удобством клиентов и эффективной киберзащитой, позволяющей обслуживать их с оптимальной степенью безопасности.

Каждый клиент, организация, каждая фокус-группа требует своего уровня безопасности, позволяющего надежно защитить их, не жертвуя удобством их работы.

Достичь оптимального баланса можно с помощью технологий идентификации нового поколения (например, биометрической) и поведенческой аналитики, обеспечивающей высокий уровень безопасности и вместе с тем удобный интерфейс.

46 %

Хотя 46 % финансовых учреждений выбирают безопасность, 43 % организаций пытаются уравновесить обе области. В условиях цифровой трансформации при предложении новых услуг так или иначе придется подвергать системы дополнительному риску.

60 %

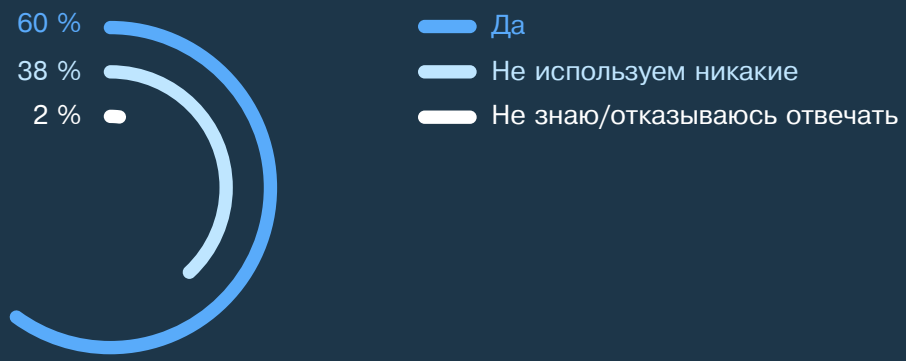
Большинство (60 %) организаций считает, что их средства обеспечения безопасности воспринимаются клиентами как лишние препятствия.

Исследование финансового сектора в Центральной и Восточной Европе, IBM, 2017 г.

Удобство клиентов

Средства контроля безопасности: неудобство и помеха для работы

В: Как вы считаете, есть ли в вашей организации средства контроля безопасности, которые воспринимаются клиентами как неудобство или преграда, мешающая работе?



Исследование финансового сектора в Центральной и Восточной Европе, IBM, 2017 г.