Противодействие мошенничеству в финансовом секторе в условиях пандемии коронавируса

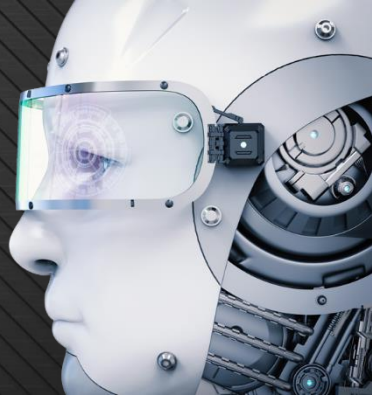
2020 г.

—

КПМГ в России и СНГ

kpmg.ru

Ситуация с мошенничеством при коронавирусе



ЧТО ПРОИСХОДИТ?

Ежедневно в мире фиксируются десятки тысяч новых заражений коронавирусом, во многих странах сохраняются значительные ограничения для граждан и компаний, что негативно отражается на экономике – вирус поставил оффлайн-бизнес на колени.

В этой связи вся жизнь и экономическая активность людей перешла в режим онлайн больше, чем когда-либо. Онлайн мы покупаем продукты, «ходим» в рестораны, оплачиваем коммунальные платежи, обновляем гардероб и бытовую технику, «ходим» в банк, получаем кредиты и пособия. Перейти в диджитал-каналы обслуживания пришлось и пожилым людям, которые ранее с этим не сталкивались.

Масштабная цифровизация граждан и расцвет онлайн-услуг привели к росту рисков мошенничества.

Пандемия коронавируса заставляет работать не только сотрудников медицинских и иных поддерживающих учреждений, которые призваны спасти жизни людей, но и мошенников, открывших для себя новые возможности в сложившейся ситуации.

Во многих отраслях ведения бизнеса наблюдается взрывной рост схем и случаев мошенничества. Особенно это проявляется в финансовом секторе – методы социальной инженерии, фишинговые атаки и использование несовершенств систем безопасности ежедневно приносят мошенникам миллионы долларов по всему миру.

Материальная «поддержка»

- Предложения оформить различные компенсации за ущерб от коронавируса, социальные выплаты и иную материальную помощь с целью сбора персональных данных и данных банковских карт и счетов
- Помощь с возвратом денег за отмененный авиаперелет, тур или иную услугу
- Предоставление кредитных каникул, уменьшение ежемесячных платежей, в т.ч. предложения оформить необходимые документы
- Предложения взять кредит на льготных условиях от имени финансовой организации

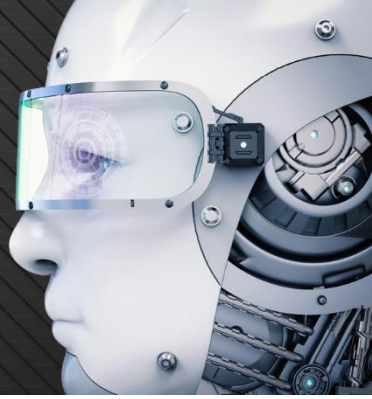
Фальшивые штрафы и товары

- Предъявление фальшивых штрафов за нарушение режима самоизоляции под видом МВД и прочих органов государственной власти
- Оформление пропусков на передвижение на платной основе (в т.ч. фальшивых)
- Покупка фальшивых лекарств от коронавируса, тест-систем, средств защиты
- Необходимость пройти осмотр или тест на вирус под предлогом штрафа
- Навязывание страховок от вируса и иных услуг
- Сбор денег на благотворительность, разработку вакцины

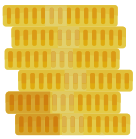
Информационная безопасность

- Фишинговые сайты о коронавирусе, страницы медицинских и финансовых организаций, предлагающих «помощь»
- Рассылки в соцсетях, мессенджерах, по почте с «выгодными» предложениями
- Сайты-клоны крупных медицинских и финансовых организаций, предлагающих фальшивые товары и услуги
- Кража персональной и платежной информации клиентов
- Взлом систем аутентификации клиентов в личном кабинете, мобильном банке и прочих сервисах

О чем говорит статистика?



МОШЕННИЧЕСКИЕ ОПЕРАЦИИ В 2019 г.*



₽ 6,4 млрд

Объем мошеннических операций с банковскими счетами

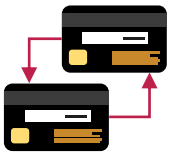
575 000+

Количество мошеннических операций с банковскими счетами

15%

Потерь было возмещено пострадавшим банками

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ**



9%

Россиян теряли крупную сумму денег из-за телефонного мошенничества

900 000+

Попыток телефонного мошенничества за январь - апрель 2020 г.

21%

Россиян никак не защищают свой телефон от подозрительных звонков

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ**

30%

Рост фишинговых рассылок в I квартале 2020 по сравнению с IV кварталом 2019

4 000+

Потенциально мошеннических сайтов коронавирусной тематики

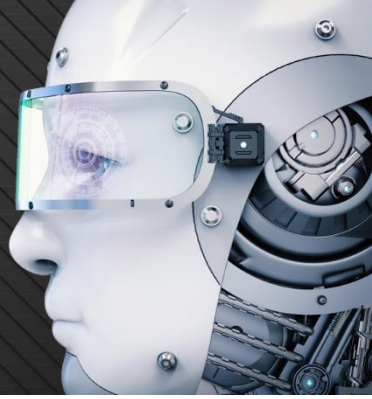
26

Количество DDoS-атак на информационные системы ПАО «Сбербанк» в 2020 году

** Источник: rbc.ru/finances/19/02/2020/5e4c02e59a7947c88583ce5e*

*** Источник: rbc.ru/finances/23/08/2019/5d5e5d359a794788daaa502e, ria.ru/20200413/1569949717.html*

Открытие банковских счетов во время самоизоляции



ПРОБЛЕМАТИКА

— С учетом текущей эпидемиологической ситуации, ЦБ РФ позволил банкам открывать счета клиентам без их личного присутствия в офисе до 1 июля 2020 года. Обязательное условие – счет открывается для проведения социально значимых операций и платежей (выплата алиментов, пенсий, оплата кредитов, получение пособий и страховых выплат, стипендий).*

— При этом рекомендуется обеспечить личную явку клиента в банк по окончании периода действия режима дистанционного открытия счетов. Для идентификации клиентов также предлагалось использовать современные средства связи, например, портал госуслуг.

— Очевидно, в отсутствие в банке инструментов работы с биометрическими данными, а также систем, способных выявить цифровой фрод (цифровые подделки документов), применить предложенный подход будет затруднительно.

КПМГ и наш технологический партнер, компания Oz Forensics, представляем решения Oz Biometry и Oz Text, которые призваны решить обозначенные проблемы.

ПРЕДПОСЫЛКИ СОЗДАНИЯ РЕШЕНИЙ

— Переход финансовых услуг в дистанционный цифровой формат, что требует надежной идентификации клиентов и подтверждения валидности документов

— Цифровые сканы документов являются ключевым источником информации в дистанционном банковском обслуживании

— Современные технологии по корректировке и манипуляциям с фотоизображениями широко известны и легко доступны, корректировка изображений не требует специальных навыков

— В сети Интернет размещено большое количество инструкций по манипулированию изображениями и биометрическими данными, использующимися для аутентификации (подмена или фальсификация объекта сканирования, фальшивые фото и видео)

ПРЕИМУЩЕСТВА РЕШЕНИЙ

— Снижение цифрового фрода в бизнес-операциях в целом

— Достоверная идентификация и аутентификация клиентов

— Снижение нагрузки на отделения и сотрудников, работающих в жестких условиях из-за вируса

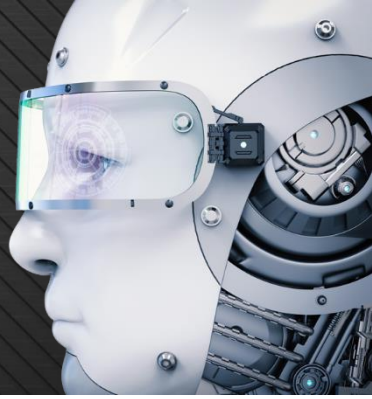
— Снижение финансовых потерь вследствие потенциальных выплат пострадавшим от мошенничества

— Улучшение репутации на рынке и повышение доверия клиентов к финансовой организации

— Минимизация вероятности претензий от ЦБ РФ из-за ненадежной идентификации личности клиента

** Источник: cbr.ru/StaticHtml/File/59420/20200410_in-014-12_62.pdf*

Анализ и выявление подозрительных операций



ПРОБЛЕМАТИКА

— Несмотря на то, что банки получили возможность не приостанавливать работу из-за коронавируса, ограничения на перемещения граждан перевели большую часть финансовых операций в режим онлайн. Все меньше клиентов посещают отделения банков, чтобы оплатить коммунальные услуги, оформить вклад или кредит, сделать перевод или получить пенсию.

— Огромное количество онлайн-транзакций и активное использование мошенниками приемов социальной инженерии требует повышенного внимания к операциям, которые клиенты проводят в дистанционных каналах обслуживания и при торговле на бирже. Это приводит к повышению нагрузки на сотрудников, отслеживающих и предотвращающих сомнительные операции.

— Очевидно, в отсутствие в банке инструментов для работы с большим объемом данных и автоматизированной идентификации подозрительных операций, невозможно обеспечить должный уровень безопасности финансов клиентов, которые нам доверяют.

КПМГ и наш технологический партнер, компания WhyHappen, представляем решения WhyHappen FMS и WhyHappen Trading, которые призваны решить обозначенные проблемы.

ПРЕДПОСЫЛКИ СОЗДАНИЯ РЕШЕНИЙ

— Обеспечение соответствия требованиям регуляторов в части 167-ФЗ, выявления сомнительных операций по 115-ФЗ, противодействия неправомерному использованию инсайдерской информации (Market Abuse Regulation, 224-ФЗ)

— Рост мошенничества в дистанционных каналах обслуживания клиентов (мобильный банкинг, онлайн-кредитование и пр.)

— Необходимость автоматизированного контроля за большим объемом операций и блокирования подозрительных транзакций

— Упрощение работы сотрудников службы безопасности, внутреннего аудита и антифрод-специалистов

ПРЕИМУЩЕСТВА РЕШЕНИЙ

— Снижение уровня мошенничества (fraud rate) бизнес-операциях в целом

— Анализ транзакций в режиме реального времени, блокирование сомнительных операций

— Возможность интеграции с внутренними и внешними ИТ-системами и инструментами

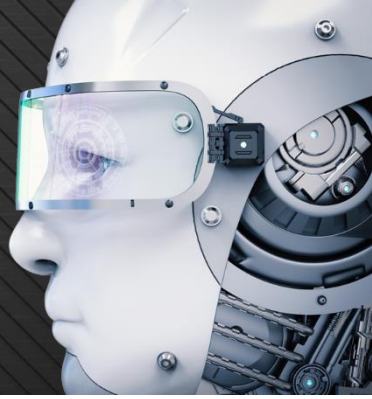
— Снижение нагрузки на сотрудников, ответственных за противодействие мошенничеству

— Снижение финансовых потерь, вызванных мошенничеством

— Улучшение репутации на рынке и повышение доверия клиентов к финансовой организации

— Минимизация вероятности несоответствия требованиям регуляторов

Data Leak Prevention (DLP) и Системы контроля доступа



DATA LEAK PREVENTION (DLP)

— Не все компании оказались готовы к работе своих сотрудников в режиме онлайн – многим пришлось в спешке организовывать удаленный доступ к корпоративным системам, что негативно сказалось на рисках утечки конфиденциальной информации. Сотрудники почувствовали себя свободными от контроля со стороны руководства и коллег из информационной безопасности и решили использовать закрытую информацию по своему усмотрению.

— **DLP-технологии** – комплекс ИТ-решений, способный перехватывать утечки конфиденциальной информации во внешнюю среду и осуществлять анализ и мониторинг внутрикорпоративных потоков информации в формате 24/7 с учетом заданных политик безопасности.

— DLP нацелена на защиту конфиденциальной информации, клиентских и персональных данных, выявление фактов хищения и мошенничества, нецелевого использования ресурсов, фактов коррупции и саботажа, внутреннего мошенничества и нелояльных компании сотрудников.

— С помощью технологии можно контролировать и блокировать использование электронной почты (включая отправку, получение писем и вложений); общение на форумах, блогах, в социальных сетях и мессенджерах; осуществление снимков экрана; анализировать и предотвращать подозрительные операции с данными, направляемыми на USB-накопители, внешние устройства и принтеры; а также установить контроль за сетевыми каналами и данными буфер-обмена.

КПМГ сотрудничает с ведущими поставщиками DLP-решений и помогает Клиентам проанализировать специфику бизнеса и оценить необходимость использования DLP, выявить сценарии мошенничества и определить оптимальные настройки системы. Мы оказываем поддержку при внедрении и пилотировании DLP-систем, проводим независимый мониторинг инцидентов и внедряем процесс реагирования и эскалации критичных кейсов.

СИСТЕМЫ КОНТРОЛЯ ДОСТУПА

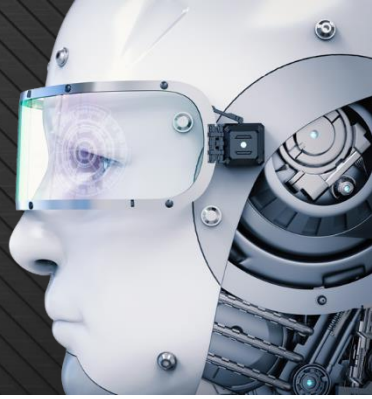
— В условиях пандемии огромное количество компаний и их сотрудников перешли на работу в дистанционном режиме. При этом сотрудники подключаются к корпоративной сети из дома, что повышает риски информационной безопасности. С помощью машинного обучения и технологии распознавания лиц на базе решения **KPMG Smart Observer**, можно организовать мощную систему контроля и управления доступом.

— Решение **KPMG Smart Observer** работает очень просто: на корпоративный ноутбук сотрудника, оснащенный веб-камерой, устанавливается программа, которая требует биометрической аутентификации пользователя по лицу при начале работы, а также отслеживает действия сотрудника после прохождения проверки. Сделанные веб-камерой фотографии лица отправляются на сервер, где сравниваются с эталоном при помощи методов машинного обучения. Также может быть реализована возможность постоянного мониторинга фотографии в фоновом режиме без отправки фотографии на сервер.

— Если алгоритмы не распознали лицо, информация может передаваться в службу безопасности для ручной проверки и определения мероприятий по отношению к компьютеру и сотруднику.

Биометрическая аутентификация сотрудников позволяет минимизировать неавторизованный доступ к корпоративным сетям и базам данных, тем самым снижает риски хищения чувствительной информации и финансовых потерь. КПМГ регулярно взаимодействует и обменивается опытом с лучшими на рынке решениями по использованию биометрической идентификации и аутентификации и продолжает развивать свой продукт KPMG Smart Observer.

Борьба с инсайдерскими угрозами



ПРОБЛЕМАТИКА

— Инсайдерские угрозы включают риски мошенничества и кражи конфиденциальной информации, исходящие от текущих и бывших сотрудников компании, подрядчиков или деловых партнеров, которые могут обладать сведениями о подходах к обеспечению безопасности внутри организации.

— Сотрудники компании имеют доступ к информационным системам и зачастую проинформированы о применяемых методах защиты данных, что позволяет им эффективно обходить контроли безопасности. Организовать защиту от внутренних угроз затруднительно.

ЗРЕЛОСТЬ УПРАВЛЕНИЯ ИНСАЙДЕРСКИМИ РИСКАМИ

Основные области анализа уровня зрелости компании с точки зрения инсайдерских рисков:

— **Модель (методы, политики) управления рисками** – все подразделения организации должным образом скоординированы с точки зрения инициатив, направленных на снижение инсайдерских угроз, оценки связанных рисков

— **Защита и безопасность данных** – меры, принимаемые до того, как произошел инсайдерский инцидент, для снижения вероятности и влияния таких инцидентов

— **Выявление** – практики и инструменты для детектирования инцидентов в режиме реального времени

— **Реагирование** – подходы к анализу и пересмотру практик после того, как произошел инцидент (восстановление, расследование и создание новых элементов защиты и возможностей обнаружения)

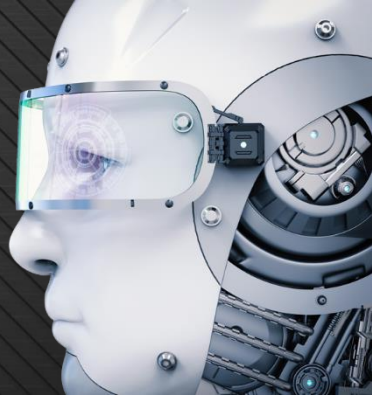
— **Обучение** – тренинги по инсайдерским рискам и создание корпоративной культуры

ПЛАТФОРМА KPMG INSIDER THREAT PREVENTION

Эффективная стратегия защиты от инсайдерских рисков должна затрагивать все функции компании (безопасность, ИТ, идентификация и контроли, подразделения и владельцы данных, HR, LGRC, закупки и внешние контрагенты, SDLC) и все источники угроз, включая ранее неизвестные и скрытые. КПМГ разработала фреймворк **Insider Threat Assessment**, отвечающий этим требованиям, и апробировала его в десятках компаний. Основные уровни и модули платформы защиты от инсайдерских угроз на примере **KPMG Insider Threat Prevention Platform:**

— Пересмотр рабочих процессов
— Визуализация рисков
— Поведенческая аналитика
— Машинное обучение
— Сокращение ложноположительных исходов
— Автоматический перевод
— Поиск по лексикону
— Обработка правил и обогащение данных
— Индексация, speech-to-text, фонетика
— Данные о связях между объектами

Обучение навыкам информационной безопасности



ПРОБЛЕМАТИКА

— Даже при высоком уровне автоматизации процессов управления рисками в ряде случаев именно сотрудники компании становятся последним рубежом защиты. Сотрудники должны обладать соответствующими компетенциями для предотвращения, идентификации и реагирования на инциденты безопасности и мошеннические операции. **Комплексные программы обучения** помогают сотрудникам систематизировать и развить имеющиеся знания и навыки.

ХАРАКТЕРИСТИКИ ПРОГРАММЫ ОБУЧЕНИЯ

— **Вовлеченность сотрудников** – использование лучших практик визуализации и геймификации контента для быстрого обучения

— **Персонализированные тренинги** – учет роли и задач конкретных сотрудников, информирование об основных целях обучения, ожидаемых результатах и критериях оценки

— **Мотивация для повторения материала** – новые знания базируются на ранее полученных

— **Микро-обучение** – подача знаний порциями с помощью коротких модулей по 3-5 минут

— **Разбор реальных случаев** – конкретные примеры и инциденты

— **Имитация настоящих инцидентов** – геймификация и эксперименты для проверки готовности к практическому использованию полученных знаний, проверка реакции на инциденты безопасности

— **Доступность** – поддержка различных платформ (включая мобильные устройства), методы обучения, нацеленные на разные категории сотрудников и виды навыков

— **Совершенствование навыков** – подведение итогов, систематизация знаний, разработка вспомогательных чек-листов, консультации и оперативная обратная связь

— **Социальное обучение и создание культуры информационной безопасности**

— **Мотивация** для самостоятельной передачи знаний и навыков между сотрудниками (обмен опытом)

КЛЮЧЕВЫЕ АСПЕКТЫ

— Риски и инциденты информационной безопасности

— Инсайдерские угрозы

— Признаки взлома и оповещения об инцидентах

— Антифишинг и безопасный веб браузинг

— Безопасность мобильных устройств

— Безопасность удаленной работы

— Пароли и физический доступ

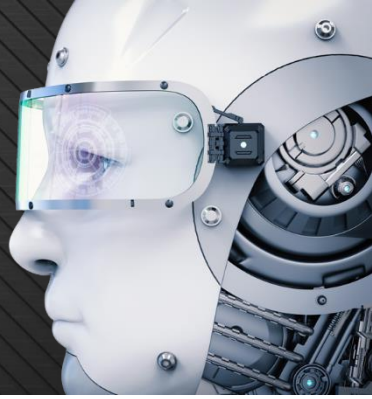
— Использование социальных сетей

— Безопасность внешних носителей и облачных сервисов

— Социальная инженерия

— Защита персональных данных (GDPR и пр.)

Наша команда



НАША КОМАНДА

Группа перспективных технологий КПМГ состоит из высококвалифицированных сертифицированных специалистов, обладающих экспертными знаниями и большим опытом в области расследования и противодействия мошенничеству в различных сферах ведения бизнеса: финансовой, страховой, ритейле, телекоммуникационной, нефтегазовой и ряде других.

Мы обладаем большим опытом реализации комплексных проектов в сфере противодействия мошенничеству и организации процессов внутреннего контроля, управления рисками и минимизации потерь.

Oz Forensics – наш технологический партнер, обладающий более чем десятилетним опытом разработки программного обеспечения по выявлению и предотвращению цифрового мошенничества.

Команда **OzForensics** имеет собственную лабораторию по разработке программного обеспечения для анализа изображений и сканов, а также биометрической идентификации и аутентификации пользователей.

WhyHappen – технологический партнер КПМГ, разработчик автоматизированных решений для автоматизации процессов управления рисками мошенничества и выявления подозрительных операций в различных бизнес-процессах.

Команда **WhyHappen** включает специалистов-практиков в области аудита, информационной и экономической безопасности, а также разработчиков и специалистов по анализу больших данных.

ЧТО МЫ ДЕЛАЕМ

Проверка подлинности цифровых фотографий и документов

Биометрическая идентификация и аутентификация пользователей систем

Анализ транзакций на предмет аномалий и рисков мошенничества

Противодействие мошенничеству в трейдинге

Реализация комплексных проектов по управлению рисками и антифроду

Сопровождение при внедрении DLP-решений

Дарья Максимова

Директор

Руководитель Группы разработки
цифровых решений

T:+7 (495) 937 44 77 доб. 10241
E: dmaximova@kpmg.ru

Лилия Шароватова

Старший менеджер

Руководитель Группы
противодействия мошенничеству

T:+7 (495) 937 44 77 доб. 11342
E: lsharovatova@kpmg.ru

Андрей Мананков

Старший консультант

Перспективные технологии
в риск-консалтинге

T:+7 (495) 937 44 77 доб. 14597
E: amanankov@kpmg.ru

kpmg.ru