Министерство образования Российской Федерации

Негосударственное образовательное частное учреждение высшего образования «Московский финансово-промышленный университет «Синергия»

По дисциплине «Цифровая экономика»

Отчет по лабораторному практикуму №3

Тема «Цифровая безопасность»

ФИО: Шилова Татьяна Константиновна

Группа: ЗБПО-201фзк

Москва 2023

Оглавление

Цель лабораторной работы-изучить и определить направления развития кибербезопасности.

Задачи лабораторной работы:
1.Как меняется ландшафт киберрисков в настоящее время?
2.Выявите сферы применения сервисов по защите от киберрисков.
3.Приведите аргументы в пользу утверждения, что защита от цифровых рисков — это инвестиции, а не затраты.
4.Выявите возможности защиты от цифровых рисков.
5.Определите ключевые направления развития кибербезопасности.
6.Сравните рассмотренные продукты защиты от цифровых рисков на основе принципа «цена-функциональность».
7.Основные типы компьютерных атак в кредитно-финансовой сфере РФ в 2019–2020гг.: перечислите и опишите.

Объект исследование - информационная экономика

Предмет исследования – деятельность киберрискков.

Глоссарий терминов:

Интернет- Всемирная информационная компьютерная сеть, связывающая между собой как пользователей компьютерных сетей, так и пользователей индивидуальных компьютеров для обмена информацией.

Информационная безопасность — практика предотвращения несанкционированного доступа, использования, раскрытия, искажения, изменения, исследования, записи или уничтожения информации. Это универсальное понятие применяется вне зависимости от формы, которую могут принимать данные.

Правово́е регули́рование — процесс целенаправленного воздействия государства на общественные отношения при помощи специальных юридических средств и методов, которые направлены на их стабилизацию и упорядочивание.

Введение

В настоящем обзоре приводятся сведения об основных типах атак в кредитно-финансовой сфере, зафиксированных в 2019 и 2020 годах. Если в 2019 году Банк России наблюдал продолжение трансформации угроз в кредитно-финансовой сфере, то в 2020 году ландшафт угроз определяла эпидемия новой коронавирусной инфекции. В силу своей неожиданности она фактически стала «черным лебедем», кардинально и негативно изменившим все стороны социальной и экономической жизни, включая обеспечение информационной безопасности финансовых организаций и их клиентов. Основную роль сыграл перевод деловой, социальной, а также повседневной бытовой экономической активности в дистанционный формат.

И если финансовые организации были относительно неплохо подготовлены к негативным - мнениям, то их клиенты – как физические, так и юридические лица – столкнулись с таким ростом числа атак и их разнообразием впервые. Атаки с использованием методов социальной инженерии на клиентов банков – держателей банковских карт и счетов – показали значительный количественный рост и прогресс в качестве воздействия. Добавление в схемы введения в полученных из различных источников персональных данных, а также применение более узконаправленных, кастомизированных приемов социальной инженерии в рассматриваемый период многократно повысило эффективность и доходность, казалось бы, уже давно известного, так называемого телефонного мошенничества.

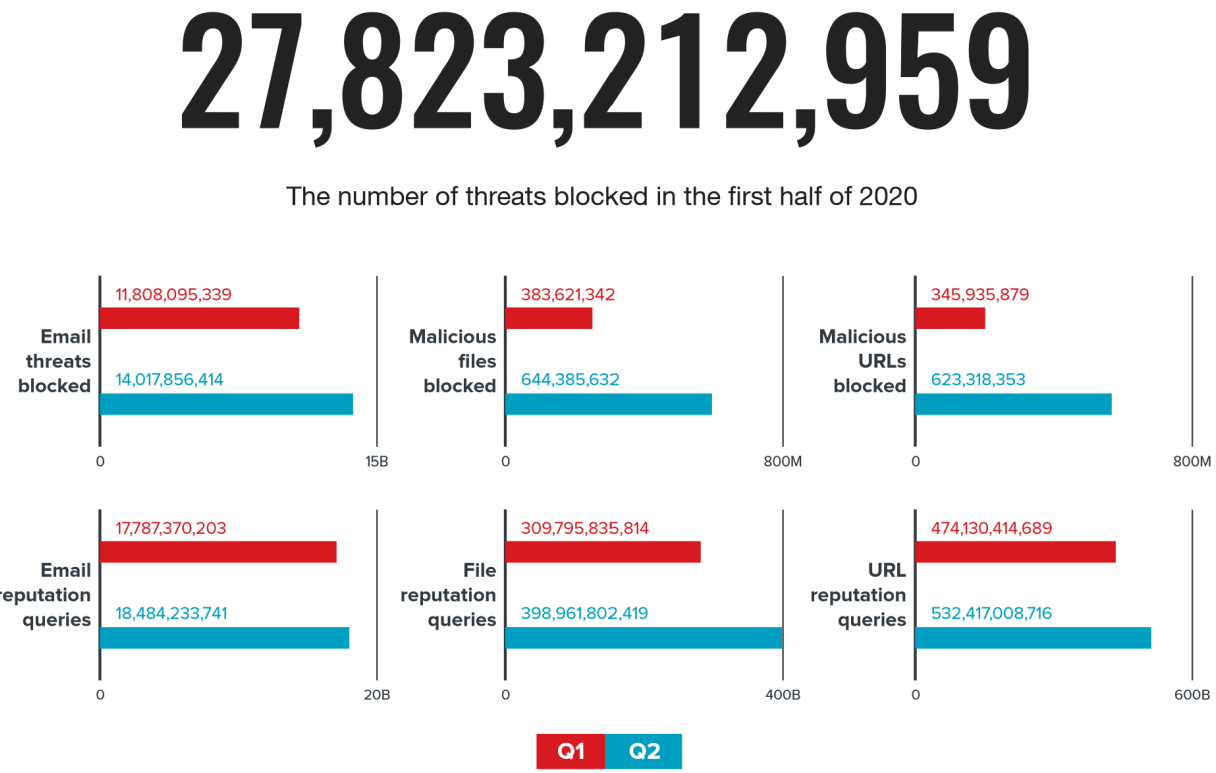
Спрос на конфиденциальные данные клиентов, используемые для преодоления порога недоверия клиентов банков, привел к резкому увеличению рынка незаконно полученных баз данных финансовых организаций и услуг по «пробиву» счетов клиентов.

Другой важной тенденцией года стало продолжение многолетнего снижения количества наиболее опасных целевых атак на информационную инфраструктуру финансовых организаций, вплоть до их почти полного прекращения. Массовые рассылки вредоносных программ типа Cobalt Strike и Silence, привлекавших особое внимание индустрии информационной безопастности в прошлые годы, по спискам адресов сотрудников почти прекратились. Редкие взломы привели к весьма

незначительному по сравнению с прошлыми годами ущербу. Также почти полностью прекратились атаки на устройства банковского самообслуживания. При этом имеющиеся в распоряжении Банка России данные позволяют сделать предположение о появлении как минимум одной группы атакующих, сосредоточившихся на квалифицированном взломе финансовых мобильных приложений.

1.Как меняется ландшафт киберрисков в настоящее время?

Давая прогнозы на 2020 год, можно не предвидеть, как обрушившая мировую экономику новая реальность повлияет на нашу жизнь. Однако сейчас можно подвести итоги первого полугодия и показать, как изменился ландшафт киберрисков за это время.



Количество угроз, заблокированных Trend Micro Smart Protection Network за первое полугодие 2020 года. Источник здесь и далее: Trend Micro.

В первом полугодии 2020 года защитные решения Trend Micro заблокировали более 27 млрд мошеннических писем, содержащих вредоносные вложения и фишинговый ссылки. Во втором квартале наблюдался значительный рост числа вредоносных сообщений по сравнению с началом года.

Самым популярным типом вредоносных вложений в первом полугодии 2020 г. стали PDF-файлы — на их долю приходилось более 50% рассылок. Вторым по популярности типом вложений были HTML-файлы. Около шести процентов писем содержали XLS-вложения, немного менее популярными были JavaScript-файлы, исполняемые файлы и документы MS Word.

Характерной чертой 2020 года стал рост популярности шифровальщиков-вымогателей. По сравнению с 2019 годом их количество увеличилось на 45% — с января по июнь текущего года было обнаружено 68 новых семейств этой разновидности вредоносного ПО.

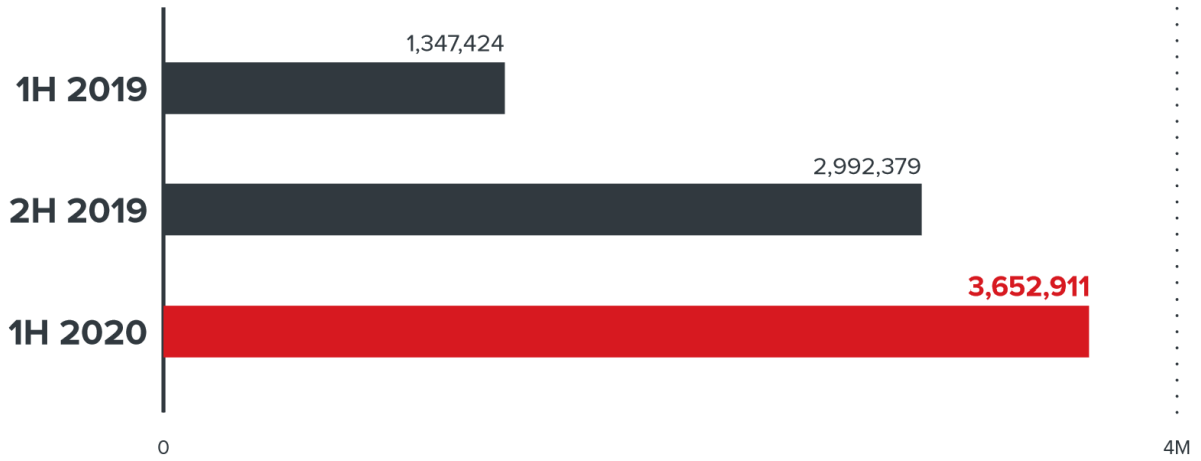


Рисунок 1 Количество выявленных за полгода образцов мобильных вредоносной

Самой популярной целью для BEC-атак был генеральный директор (CEO) компании. На долю этой категории сотрудников приходится 30% всех инцидентов

Любопытно что писем «от CEO» стало меньше: в 2019 году доля таких писем составляла 41%. Возможно, мошенники экспериментируют с другими должностями, чтобы оценить их эффективность.

Закономерно, что самими востребованными остаются люди, связанные с финансами, например, финансовые менеджеры и директора по финансам.

2.Выявите сферы

Ландшафт угроз постоянно расширяется, а это означает, что группы по кибербезопасности все интенсивнее вынуждены работать над защитой организаций. Мы собрали наглядные примеры для демонстрации сферы применения сервисов по защите от рисков.

- **Обнаружение фишинга**

Фишинг — коварная проблема, и злоумышленники обожают его, потому что он эффективен. DRP включает в себя упреждающие меры, выявляющие и пресекающие атаки до того, как причинят вред. Отслеживая различные ключевые фишинговые показатели — зарегистрированные домены, изменения в записях MX и репутацию DNS, решение определяет вредоносные домены и быстро уничтожает сайты-подделки.

- **Приоритизация уязвимостей**

Вручную соотносить данные об угрозах с уязвимостями собственной организации уже нереально. Слишком много используемых технологий, слишком много данных. DRP — это автоматизированный сбор уязвимостей, использующий данные отовсюду. Далее происходит структурирование этих массивов в реальном времени, позволяющие увидеть, что представляет наибольший риск.

- **Видимость в даркнете**

Злоумышленники умны и анонимны, но все же видимы. DRP следит за их деятельностью во всех уголках Интернета — как они разведывают цели, используют подозрительные инструменты и сотрудничают с другими хакерами. Продвинутое DRP решение понимает, как думают киберпреступники и как развиваются угрозы, предоставляя вам шанс для прокатных действий. Между прочим, мониторинг и отслеживание веб-активности в даркнете — ключевая часть того, как обычно угрозы обнаруживаются и смягчаются.

- **Защита бренда**

Вы потратили уйму времени и денег, создавая и строя свой бренд. Увы, хакеры тоже знают, насколько он ценен. DRP решение призвано сканировать внешние источники в поисках злонамеренного использования вашего бренда в мошеннических

целях. Оно следит за вашими доменами, IP-адресами, мобильными приложениями и страницами в социальных сетях, чтобы выявить злоумышленников. А в случае обнаружения подозрительной активности мгновенно рассылает оповещения в рамках всей вашей организации, в отделы маркетинга, соблюдения нормативных требований, ИТ-отдел и службу безопасности.

- **Обнаружение мошенничества**

У вас установлены все виды защиты периметра — брандмауэры, шлюзы, IDS/IPS и системы обнаружения вредоносного ПО, и возможно, вы даже предприняли шаги по интеграции и укреплению этих систем. Это круто! Проблема в том, что хакеры все равно обходят эту защиту, используя вместо этого мошенничество. Поэтому DRP решение должно следить за попытками создания фишинговых сайтов или продажи утекших учетных данных, информации о банковских счетах ваших клиентов и сотрудников. Мгновенные оповещения в реальном времени помогают предотвратить такие действия до их совершения, экономя организациям миллионные затраты каждый год.

- **Идентификация вредоносных мобильных приложений**

Мобильные устройства и приложения расширяют охват аудитории. Но злоумышленники, возможно, уже создали мошеннические мобильные приложениями, за которыми ваша маркетинговая команда, скорее всего, не следит и не знает. DRP должно проверять различные магазины приложений — как легальные, так и пиратские, чтобы обнаруживать подозрительные приложения и инициировать их закрытие. Это возможно, если у решения существуют партнерские отношения с магазинами приложений.

- **Защита руководства**

В прошлом руководители нуждались только в физической безопасности. В офисах для этого установлена сигнализация, охрана, иногда за высшим руководством закреплены телохранители. Теперь высшие чины сталкиваются с серьезными угрозами в сфере кибербезопасности. Так же, как и инвесторы, члены советов директоров и консультанты. DRP-программа должна сканировать онлайн-источники, чтобы

находить и пресекать попытки подделать или скомпрометировать их личность и данные.

3.Приведите аргументы в пользу утверждения, что защита от цифровых рисков — это инвестиции, а не затраты.

По оценке Accenture мировой рынок услуг в сфере кибербезопасности будет расти на 13% в год и достигнет объема в $94 млрд к 2025 г. Об этом компания сообщила 4 февраля 2022 года. Главными направлениями развития станут кибербезопасность как сервис и автоматизация операций ИБ, особое внимание будет уделено защите критической инфраструктуры и приложений.

По мнению Accenture, рост расходов на кибербезопасность обусловлен различными факторами, в частности постоянным увеличением объема вредоносного ПО. Непрерывно эволюционируют методы злоумышленников. Услуги хакеров становятся более доступны и часто используются как средство конкурентной борьбы или легкого заработка, что привело к формированию модели Cybercrime-as-a-Service (киберпреступление как услуга).

Зависимость бизнес-экосистем от стабильной работы цифровой инфраструктуры делает компании крайне уязвимыми перед ИБ-угрозами. Эффективность атак при этом растет, так как киберпреступники вооружаются цифровыми технологиями, включая ML/AI-решения.

Цифровая защита от рисков — упреждающая оборонительная стратегия. Она позволяет противостоять угрозам, избегать ненужных затрат, повышать эффективность и возмещать убытки. Именно по этим четырем областям DRP предлагает возврат инвестиций. Рассмотрим детальнее.

ROI 1: Избегание рисков

Как и большинство других элементов стратегии кибербезопасности, инвестиции в решение должны рассматриваться в контексте нежелательных расходов, которые может повлечь за собой взлом системы безопасности. Но это только одна часть преимущества. Одним из наиболее ценных аспектов DRP является визуализация

собственного «цифрового следа» организации — важнейшего элемента для защиты бизнеса и репутации.

ROI 2: Снижение затрат

DRP решения автоматизируют многие задачи, связанные с выявлением, мониторингом цифровых угроз. Самостоятельные действия на местах по киберзащите покрывают такие задачи лишь частично по сравнению со специально разработанными, постоянно обновляемыми решениями. Лучшие DRP сервисы охватывают также Shadow IT (т.е. неавторизованные домены, приложения или устройства, создаваемые или используемые без уведомления ИТ-отдела) и Forgotten IT (например, старые целевые страницы веб-сайтов и архивированный контент), обеспечивая дополнительные возможности снижения затрат.

ROI 3: Повышение эффективности

Автоматизация, присущая цифровым решениям по защите от рисков быстрее и проще выявляет уязвимые места, повышая эффективность процесса. Идентификация и устранение Shadow и Forgotten IT дополнительно оптимизирует цифровое пространство предприятия, экономя ресурсы.

ROI 4: Получение дохода

Успешные кибератаки, фишинговые письма и поддельные сайты организации оказывают непосредственное негативное влияние на доходы, и, конечно, отрицательно влияют на репутацию. Цифровые решения по защите от рисков помогают снизить и эти риски, помогая максимально быстро выявлять и устранять незаконные или угрожающие действия.

4.Выявите возможности защиты от цифровых рисков.

1. Используйте оригинальные пароли для каждого сервиса

Если у вас один пароль для почты, соцсетей, рабочих аккаунтов и других учетных записей, достаточно одной утечки, чтобы злоумышленники взломали все. Установите менеджер паролей с функцией их создания, к примеру, 1Password. Не храните ключевые комбинации на листочках или в записных книжках. Масштабируйте эту практику на всю компанию: поручите сотрудникам ИТ-службы следить за регулярностью обновления паролей среди работников. Хорошим тоном считается смена ключевых комбинаций раз в три месяца.

2. Передавайте данные только по защищенным каналам

Даже надежный пароль могут перехватить злоумышленники. Это в особенности применимо к публичным беспроводным сетям в аэропортах, кафе или бизнес-центрах. Используйте VPN-соединение, когда работаете с деловыми документами, общаетесь с партнерами или авторизуетесь в личных аккаунтах. То же самое можно развернуть в рамках компании: обязуйте сотрудников подключаться к серверам организации по защищенным каналам, чтобы избежать утечек данных. Однако помните, что сведения, которые вы передаете через VPN-соединение, может просмотреть провайдер, поэтому пользуйтесь услугами доверенных компаний.

3. Учитесь и учите киберграмотности.

Освойте основы кибергигиены, чтобы не стать жертвой преступников. Инвестируйте в повышение киберграмотности, в частности, в тренинги по противодействию фишингу и охране чувствительных данных. Привлеките к этому процессу не только высшее руководство, но и сотрудников на всех уровнях: никто не знает, где именно будут атаковать злоумышленники. Подобные меры окупаются: по

нашим данным, регулярные тренинги повышают устойчивость сотрудников к фишингу в девять раз.

4. Готовьте руководства на любые случаи

Разработайте с сотрудниками сценарии поведения для ситуаций, связанных с повышенным риском, таких как срочные переводы крупных сумм и предоставление важных документов. Придумайте секретные слова для подтверждения подобных операций — мы помним, что преступники осваивают дипфейк-технологии, так что стандартного звонка с повтором указаний уже недостаточно. Отрабатывайте эти сценарии с коллегами и старайтесь следовать им сами.

5. Устанавливайте обновления

Этот совет относится ко всем устройствам и программам, которыми вы пользуетесь. В новых релизах разработчики зачастую закрывают уязвимости. Чем новее ПО в вашем компьютере, смартфоне, часах и даже автомобиле, тем ниже риск, что вы станете жертвой кибератаки. Представьте, сколько уязвимых точек в компании, которая насчитывает даже 20 компьютеров — и это не считая серверов, роутеров и другой техники. Обновление ПО в компании — лучшая профилактика взломов.

6. Не храните рабочие документы на личных устройствах

Посмотреть квартальные отчеты в дороге на ноутбуке — в целом здравая мысль, до тех пор, пока это корпоративный компьютер. Если загружаете рабочие данные на личный планшет или смартфон, не забывайте их удалять, иначе в случае кражи ворам достанется не только новенький гаджет, но и ваши коммерческие тайны. Для надежности установите пароль или разблокировку по биометрическим данным на всех устройствах. Еще есть способ усложнить злоумышленникам доступ к почтовому ящику на корпоративном уровне — попросите ИТ-департамент разрешить вход в рабочие email-аккаунты только тем, кто подключен через VPN-туннель. В условиях пандемии разделять офис и дом стало намного сложнее, но вы можете перевести бизнес-процессы в облачные сервисы: они защищены чуть лучше, чем персональные устройства сотрудников.

7. Проектируйте системы с оглядкой на безопасность

Любые ИТ-проекты — от настройки почтового сервера до цифровой трансформации, должны опираться на принцип security by design. Он заключается в том, что безопасность должна быть неотъемлемой частью системы и встраиваться во все ее компоненты. Соблюдение этого принципа требует четко выстроенных процессов и участия компетентных специалистов. Лучше обратиться к сторонним подрядчикам: их осведомленность о киберугрозах будет выше, чем у среднестатистического отдела КБ, а конечная стоимость услуг — ниже. При этом вы не перегрузите штатных сотрудников дополнительной работой. На рынке достаточно компаний, специализирующихся на подобных задачах, — они учтут особенности вашей ИТ-инфраструктуры и помогут построить цифровой бастион, чтобы дать отпор даже продвинутым атакам.

Forrester выделяет две основные задачи для любой организации, стремящейся снизить цифровые риски: во-первых, выявить, какие риски существуют, и, во-вторых, устранить их. Согласны с вами — на первый взгляд цели очевидны. Но на самом деле они предполагают определенную позицию касательно безопасности — более активную, чем реагирование на инциденты.

- **Отчет Forrester также определяет несколько важнейших качеств, присущих DRP решению:**

1.Возможности сбора и сканирования данных с широкого набора цифровых каналов.

2.Функции картирование, мониторинга и снижения цифровых рисков. Благодаря автоматизации.

3.Фокусировка на юз-кейсах и функциях безопасности.

Наиболее надежные решения — обширные примеры из практики клиентов и стратегическое партнерство, что делает их гибкими и способными к использованию в различных приложениях.

5.Определите ключевые направления развития кибербезопасности.

Виртуальный мир давно уже стал неотъемлемой частью современного общества. С другой стороны, правовые отношения, реализуемые в контексте «Всемирной паутины», продолжают требовать правового регулирования. Так, в существующем информационном пространстве одни из самых значимых этические проблемы, связанные с информационным неравенством, нарушениями неприкосновенности личной жизни, этикой поведения в сети.

Информационная безопасность уже международное понятие. Под ним подразумевают комплекс специальных технических и организационных мер, которыенаправ-лены на обеспечение защиты данных, целостности информации и ее доступности, специальные правила для управляемости массивов данных и информации. Структур-иные элементы информационной безопасности на международном и внутригосударственное уровняхвключают:

- защиту сведений, содержащих государственную или коммерческую тайну;
- защиту серверов государственных учреждений и систем жизнеобеспечения;
- защиту безопасности данных как набора аппаратных и программных средств, которые обеспечивают сохранность информацию неавторизированного доступа, затруднения доступа, разрушения и перепрограммирование;
- реализацию системы мер, направленных на защиту от целенаправленного информационного воздействия на субъект нападения, его психологическое состояние или имидж на международной арене

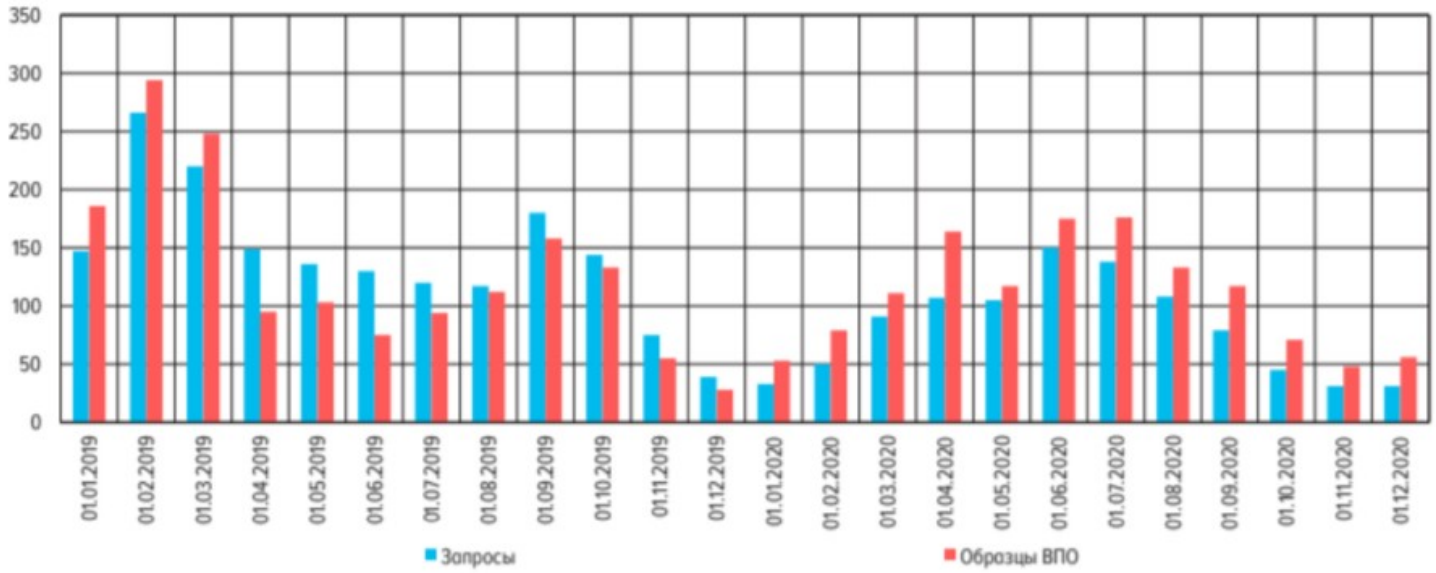
6.Сравните рассмотренные продукты защиты от цифровых рисков на основе принципа «цена-функциональность».

Характеристик	INTSIGHTS Threat Intelligenc	KASPERSKY Threat Inte.
IP-эдреса	• Есть	• Есть
URL-адреса	• Есть	• Есть
Угрозы категории TTP5	• Есть	• Есть
Индикаторы из социальных сетей	• Есть	
Номер карт	• Есть	• Есть
Код	• Есть	
Vulnerability Intelligence (CVE's)		

7.Основные типы компьютерных атак в кредитно-финансовой сфере РФ в 2019–2020гг.: перечислите и опишите.

Несомненно, новые технологии несут в себе все большие и большие возможности, скорость и комфорт, но в то же время это приносит новые угрозы. В связи с этим актуальными являются мониторинговые и аналитические исследования угроз в разных сферах экономической деятельности, в том числе банковской.

По статистике в 2020 г. мы наблюдаем сокращение попыток компьютерных атак более чем на 40% по сравнению с 2019 г.



Если рассматривать структуру сфер, в которых происходят вредоносные таки, то в 2020 г. на первом месте это шпионское ПО, причем увеличение атак составило практически до 45% доли всех операций, а за ним финансовое ПО с долей в 13%. Также, стоит отметить, что в 2020 г. заметно сократились массовые атаки. Связано это с тем, что механизмы Банка России быстрее начали реагировать на пресечение возможных вредоносных программ. Также, центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере, начал выпускать бюллетени, где прописана вся необходимая информация о самых опасных атаках, способах их обнаружения и противодействиями им.

Интересным фактом является и само расположение ресурсов в сети Интернет: все они находятся за пределами Российской Федерации, преимущественно в странах с

большим количеством веб-сервисов. Лидерами являются, как и в прошлые годы, США и Германия.

Если же рассматривать атаки на информационную инфраструктуру клиентов организаций кредитно-финансовой сферы РФ, то наиболее активной и опасной угрозой является группа злоумышленников, именуемых как RTM (Remote Transaction Manager). По статистике, за 2019–2020 гг. еженедельно происходило по 2–3 таких атаки, что показывает, насколько интенсивно данные группы людей захватывают информацию пользователей. Большинство случаев относится к фишинговым компаниям, в которых к сообщениям на электронную почту прикрепляется архив с вредоносными ссылками, так называемой «полезной» информацией.

На ряду с уже перечисленными атаками, остаются опасными и атаки на банкоматы. 44% случаев связаны с использованием всевозможных приспособлений для вскрытия дверцы банкомата для извлечения денежных средств. На кештреппинг приходится немного меньше: 32% всех случаев.

В связи с последними событиями, а именно с захватившей весь мир коронавирусной инфекцией, начало проявляться все больше случаев кибератак с использованием социальной инженерии. В 84% случаев мошенники использовали для атаки телефонную связь, а в остальных 16% – овладевали личными данными через СМС и сообщения в мессенджерах. На наш взгляд, пандемия оказалась рычагом для активизации мошенников. Так, за 2020 г. показатель количества заблокированных телефонных номеров превышает аналогичный показатель прошлого года на 86%. Анализ показал, что в 57% случаев мошенники представлялись сотрудниками службы безопасности или же сотрудниками той или иной кредитно-финансовой организации. Данное явление является следствием низкой финансовой грамотности населения.

Чаще всего атаки недобросовестных действий происходят с помощью методов социальной инженерии, далее посредством фишинговых рассылок по клиентам банков. По статистике 9 из 10 звонков относятся к теме угрозы накоплениям, либо операциям без согласия клиента.

8. Информационные источники

- https://lengu.ru/mag/ekonomika-novogo-mira/archive/58/514
- https://cyberleninka.ru/article/n/kiberbezopasnost-kak-osnovnoe-napravlenie-razvitiya-pravovyh-norm-v-usloviyah-tsifrovoy-ekonomiki-mezhdunarodnye-trendy/viewer
- https://www.cbr.ru/collection/collection/file/32122/attack_2019-2020.pdf
- https://www.tadviser.ru/index.php/Статья:Информационная_безопасность_(мировой_рынок)
- https://www.consultant.ru/law/consult/