УДК 336.71

Л.К. Голенда, К.Ю. Мяделец, Е.С. Хаританович
Белорусский государственный экономический университет
Минск, Республика Беларусь

ВРЕДОНОСНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ И БЕЗОПАСНОСТЬ БАНКОВСКИХ УСЛУГ В СОВРЕМЕННЫХ УСЛОВИЯХ

Аннотация. *В статье рассматриваются порождаемые цифровой экономикой проблемы и пути реализации киберпреступлений. Целью статьи является определение приоритетов развития информационной безопасности, направлений и перспектив ее совершенствования.*

L.K. Golenda, K.Y. Myadelets, E.S. Kharitanovich
Belarus State Economic University
Minsk, Republic of Belarus

HARMFUL SOFTWARE AND SECURITY OF BANKING SERVICES IN MODERN CONDITIONS

Abstract. *The article examines the challenges posed by the digital economy and the ways of implementing cybercrime. The purpose of the article is to determine the priorities for the development of information security, directions and prospects for its improvement.*

На сегодняшний день для многих кредитных организаций характерно стремление к трансформации в высокотехнологичные, способные соответствовать новым вызовам экономики корпорации путем использования разработок программного обеспечения (ПО), системной интеграции, консалтинга для финансовой сферы.

Цифровая трансформация наряду с преимуществами, такими как рост качества, скорости, доступности банковских услуг, несет в себе недостаток в виде роста числа кибератак. Такие риски требуют оперативного и своевременного мониторинга, обнаружения и оперативного реагирования [1].

Большинство пользователей банковских услуг ощутили на себе всю отрицательную сторону развития информационных технологий, конкретно – вредоносных программ. Сейчас, когда большая часть информации хранится на электронных носителях, особенно важно повышать уровень безопасности и сохранности этой информации от

влияния всевозможных угроз.

Из-за ограничений, связанных с эпидемиологической ситуацией, 2020 год отличился повышенной частотой атак со стороны адаптировавшихся к глобальным переменам киберпреступников, которые наживаются на уязвимостях, связанных с удаленной работой и растущей популярностью покупок в интернете.

В сложившихся условиях особую актуальность приобретает вопрос борьбы с вредоносными программами.

На основаниях аналитических данных облачной инфраструктуры Kaspersky Security Network, предназначенной для интеллектуальной обработки потоков данных, связанных с киберугрозами, была проанализирована активность финансовых угроз.

Под финансовыми вредоносными программами в данном исследовании понимаются несколько типов вредоносного ПО: зловреды, атакующие пользователей финансовых сервисов; вредоносные программы, пытающиеся получить доступ к финансовым организациям и их инфраструктуре.

По результатам исследования наиболее распространенными путями реализации киберпреступлений являются фишинг, использование вредоносных программ для персональных компьютеров (ПК) и мобильных приложений.

Финансовый фишинг — один из главных инструментов хищения денег, применяемых киберпреступниками, с помощью которого они получают доступ к персональным данным в последующем продавая или монетизируя их иными способами. Фишинг не требует крупных вложений и серьезных технических знаний.

Как показывает статистика, 13,2% пользователей антивирусных программных продуктов Kaspersky в 2020 году подверглись фишинговым атакам, из которых 37,2% пришлось на финансовые. Устойчивой тенденции изменения данного показателя в анализируемом периоде не наблюдается (рис. 1).

Следует отметить, что под «финансовым фишингом» понимается не только банковский фишинг, но и другие типы атак. К ним относятся атаки на пользователей платежных систем, в том числе маскировка под PayPal, Visa, MasterCard, American Express и другие широко известные сервисы. Кроме того, мошенники могут выдавать себя за интернет-магазины и онлайн-аукционы вроде Amazon, Apple Store, Steam, E-bay и других.

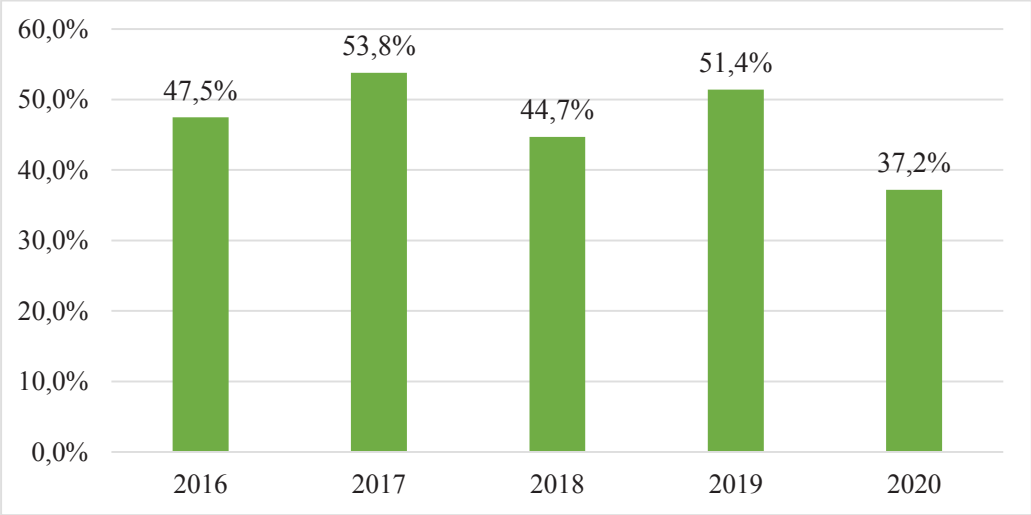

Рис. 1 – Доля финансовых фишинговых атак от общего числа фишинговых атак
Примечание – Источник: собственная разработка на основе [2].

На банковский сектор в 2020 году пришлось 10,7% фишинговых атак, что на 17 п.п. меньше по сравнению с 2019 годом. Доля фишинга, связанного с интернет-магазинами, наоборот, практически утроилась: с 7,57% в 2019 году до 18,12% в 2020 году. Эти изменения можно связать с ограничениями из-за пандемии: проводя много времени дома, люди чаще интересуются онлайн-покупками и цифровыми развлечениями. Очевидно, рост спроса со стороны пользователей привел к росту «предложения» со стороны киберпреступников.

Задачей банковских вредоносных программ для ПК является похищение учетных данных для входа в системы интернет-банкинга или в платежные системы, а также перехват одноразовых паролей.

После всплеска активности вредоносных программ в октябре 2016 года, когда они затронули 1 494 236 пользователей, наблюдается постепенное снижение числа пользователей, атакованных банковскими вредоносными программами. И 2020 год не стал исключением. Количество атакованных пользователей сократилось с 773 943 в 2019 году до 625 364 в 2020 году — почти на 20% (рис. 2).

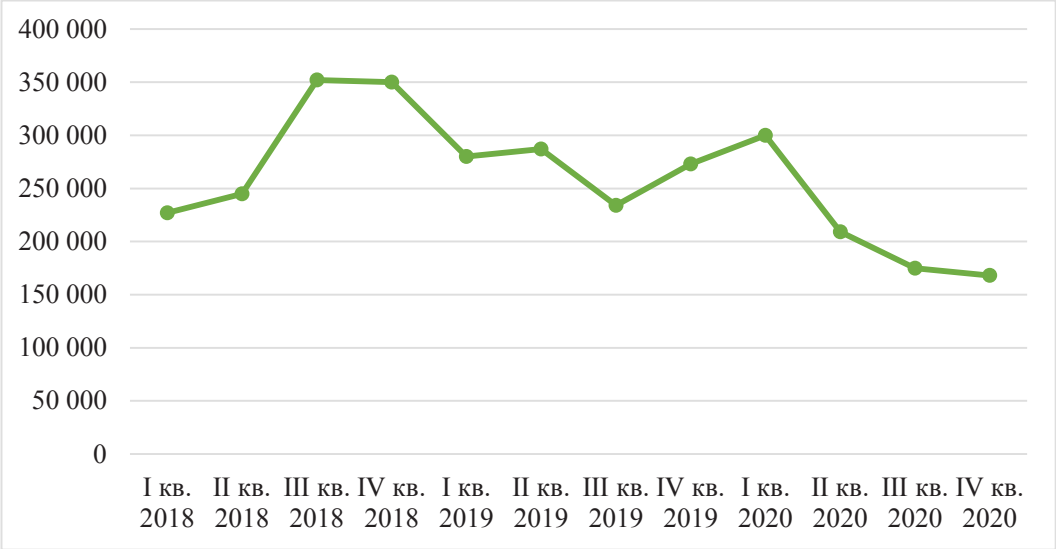

Рис. 2 – Изменение числа уникальных пользователей, атакованных банковскими вредоносными программами

(Примечание – Источник: собственная разработка на основе [2])

При этом 36% пострадавших от банковских вредоносных программ — корпоративные пользователи, это на 1 п.п. больше, чем в прошлом году. В целом компании стали более уязвимыми в 2020 году. Спешный переход на дистанционную работу ослабил корпоративную безопасность. Слабые знания о безопасности в интернете, использование ноутбуков со стандартными настройками и уязвимые подключения для удаленного доступа — все это создало благоприятную почву для самых разных атак.

Наиболее распространенной банковской вредоносной программой является Zbot (22,2% атакованных пользователей), второе место занимает CliptoShuffler (15,3%), а замыкает тройку лидеров Emotet (14,5%).

Уже хорошо известной угрозой являются банковские вредоносные программы для мобильных устройств на базе Android, цель функционирования которых практически ничем не отличается от целей соответствующих программ для ПК. В последнее время наблюдается снижение числа атакованных пользователей дистанционных банковских услуг (рис. 3).

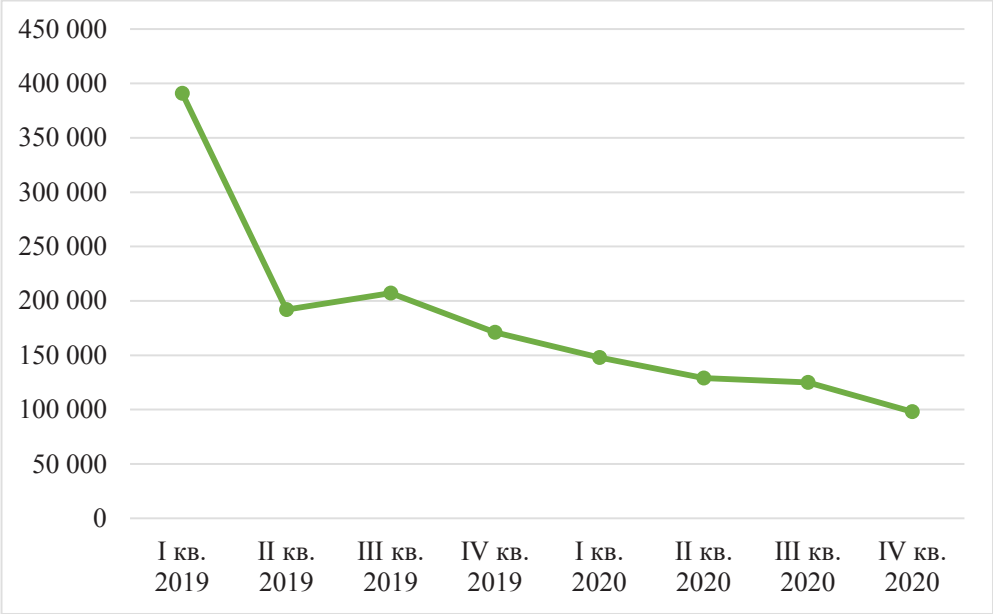

Рис. 3 – Изменение числа пользователей, атакованных банковскими вредоносными программами для Android

(Примечание – Источник: собственная разработка на основе [2])

В результате исследования выявлено, что киберпреступники способны адаптироваться к новым реалиям и переменам в мире, продолжая развивать вредоносные программы и методы обхода защитных алгоритмов. Однако общая статистика во всех проанализированных нами областях (вредоносные программы для ПК и мобильных устройств, а также фишинг) показывает нисходящую тенденцию, что внушает оптимизм.

Актуальность вопросов противодействия вредоносным ПО и повышения информационной безопасности раскрывается в Государственной программе «Цифровое развитие Беларуси» на 2021 – 2025 годы [3], задачами которой в отношении банковского сектора являются создание благоприятных условий для обеспечения и сопровождения процессов цифрового развития; совершенствование системы информационной безопасности, обеспечивающей правовое и безопасное использование внедряемых решений.

Решение поставленных задач предполагается выполнить в том числе путем реализации в рамках подпрограммы «Информационная безопасность и «цифровое доверие» мероприятий по созданию инфраструктуры мобильной и иных способов идентификации на базе единой системы идентификации физических и юридических лиц.

В дополнение к предусмотренным Государственной программой мероприятиям с целью предотвращения реализации кибератак считаем необходимым пользователям банковских программных продуктов соблюдать следующие рекомендации:

1. установка приложений только из надежных источников, таких как официальные веб-сайты;
2. проверка разрешений и прав доступа, запрашиваемых приложением, и отказ в их предоставлении, если они фактически не требуются для работы приложения;
3. установка надежного защитного решения, способного обезопасить от широкого спектра финансовых киберугроз.

Для корпоративных пользователей рекомендуется организация обучения основам кибербезопасности сотрудников; проведение вебинаров, направленных на повышение финансовой и компьютерной грамотности; по возможности установка актуальных обновлений и исправлений для всех используемых программ.

Список использованных источников

1. Бозиева З.А. Роль цифровизации в развитии финансового сектора // Вестник КЭУ, № 2(47), Бишкек,2019.
2. Официальный сайт Kaspersky Lab. [Электронный ресурс]. – Режим доступа: https://www.kaspersky.com/. – Дата доступа: 19.10.2021.
3. Государственная программа «Цифровое развитие Беларуси» на 2021 – 2025 годы: постановление Совета Министров Респ. Беларусь, 2 февр. 2021 г., № 66 // Национальный правовой Интернет-портал Республики Беларусь. – Режим доступа: https://pravo.by/upload/docs/op/C22100066_1612472400.pdf. – Дата доступа: 22.10.2021.

УДК 339.37:004(476)

Л.К. Голенда, А. В. Грань, М. А. Шульга
Белорусский государственный экономический университет
Минск, Республика Беларусь

РОЗНИЧНАЯ ТОРГОВЛЯ В РЕСПУБЛИКЕ БЕЛАРУСЬ В УСЛОВИЯХ ЦИФРОВОЙ ТРАНСФОРМАЦИИ