УДК 336.719.2

# НОРМАТИВНО-ПРАВОВОЕ ЗАКРЕПЛЕНИЕ АНТИВИРУСНОГО ОБЕСПЕЧЕНИЯ БАНКОВСКОГО ТЕРМИНАЛЬНОГО ОБОРУДОВАНИЯ

***С.Ю. Воробьёв[1], Г.В. Мишнев[2]***
***[1]Закрытое акционерное общество «Банк роста и развития бизнеса»***
***[2]Генеральная прокуратура Республики Беларусь***

Одними из наиболее существенных угроз национальной безопасности государства являются угрозы в экономической и информационной сферах. Противоправная деятельность злоумышленников в киберпространстве, направленная в отношении информационной инфраструктуры банков, которая основывается на использовании современных информационных систем и технологий, может привести к дестабилизации финансовой и денежно-кредитной систем страны со всеми вытекающими негативными последствиями.

Банковский сектор является одной из приоритетных целей злоумышленников[1]. При этом необходимо учитывать, что банковская отрасль является одной из самых зарегулированных с точки зрения безопасности, в каждом банке функционирует собственная служба безопасности (в том числе информационной), многие сертифицируют свои процессы в соответствии с требованиями международных стандартов в сфере информационной безопасности таких как PCI DSS, ISO 27001, Программа безопасности пользователей SWIFT и т.д. Применение в информационных системах

банковских учреждений защитных мероприятий по тщательному отбору персонала, поддержанию здорового климата в коллективе, ролевой модели доступа пользователей, антивирусному программному обеспечению, DLP-систем и SIEM-систем, брандмауэров, разработки локальных актов по вопросам информационной безопасности в совокупности существенно снижает вероятность успешной реализации таргетированной кибератаки злоумышленников.

Вместе с тем в банковской деятельности широко применяются банкоматы, информационные платежные терминалы самообслуживания, электронные депозитарные машины (т.н. терминальное оборудование). Одновременно за последние несколько лет произошла эволюция от физических атак на терминальное оборудование до атак с применением средств высоких технологий.

Появление специального вредоносного программного обеспечения (далее - ВПО) для терминального оборудования (в первую очередь для банкоматов) предоставило киберзлоумышленникам изящную и неприметную альтернативу физическому взлому[2].

Для логического завершения кибератаки на банкомат необходимо находиться рядом с последним для изъятия наличных денежных средств. Как правило, для непосредственного обналичивания денег с атакованного банкомата злоумышленники привлекают «мулов» - пособников, которые по команде вводят уникальный сессионный ключ либо используют специальную карту для авторизации несанкционированной транзакции, после чего изымают наличность.

Однако, до финальной стадии необходимо осуществить внедрение вредоносного программного обеспечения в компьютер банкомата, что производится получением физического доступа к USB-портам либо оптическому привода последнего, либо удаленным внедрение ВПО, посредством предварительной компрометации внутренней информационной сети банка, получением и дальнейшее распространение зловреда на сеть банкоматов.

Удаленные атаки на сеть банкоматов через Интернет даже более опасны. Преступники могут создать виртуальный процессинговый центр или даже взломать настоящий. Например, именно это проделали члены банды Carbanak, чтобы украсть миллиард долларов: они проникли в ключевые компьютеры в банковских сетях и использовали их, чтобы напрямую командовать банкоматами[3].

Необходимо отметить, что в технических нормативных правовых актах, регулирующих сферу информационной безопасности в банковской отрасли Республики Беларусь (СТБ 34.101.41-2013 и ТТП ИБ 1.1-2020), отсутствует прямое нормативное предписание на обеспечение антивирусной защиты терминального оборудования (обязательной антивирусной защите подлежат только сервера и рабочие станции), что также увеличивает риск заражения терминального оборудования в случае атак с использованием ВПО.

Так, согласно абз.1 п. 7.5.1 СТБ 34.101.41-2013 *«На всех автоматизированных рабочих местах и серверах автоматизированной банковской системы, если иное не предусмотрено технологическим процессом, должны применяться средства антивирусной защиты, сертифицированные в национальной системе сертификации либо имеющие положительное заключение государственной экспертизы»*[4]. Таким образом, прямое требование по установке антивирусного программного обеспечения на терминальное оборудование в вышеуказанном СТБ отсутствует (установка антивируса фактически осуществляется банками–владельцами терминального оборудования «инициативно»). Абз.1 п. 7.5.1 ТТП ИБ 1.1-2020 фактически дублирует требование стандарта «*на всех автоматизированных рабочих местах и серверах автоматизированной банковской системы, если иное не предусмотрено технологическим процессом, должны применяться средства антивирусной защиты»*[5].

На основании вышеизложенного представляется целесообразным в данных СТБ и ТТП дополнить абз. 1 п.7.5.1 словами «а также терминальном оборудовании» изложив его в следующей редакции: «*На всех автоматизированных рабочих местах и серверах автоматизированной банковской системы, если иное не предусмотрено технологическим процессом, а также терминальном оборудовании (банкоматах, платежно-справочных терминалах самообслуживания, электронных депозитарных машинах) должны применяться средства антивирусной защиты*».

Вместе с тем для придания стандартам информационной безопасности статуса технических нормативных правовых актов, обязательных для соблюдения всеми субъектами банковской сферы, требуется внесение изменений в Банковский кодекс Ресублики Беларусь[6].

Вышеуказанные изменения закрепят необходимость обязательного применения средств антивирусной защиты и, как следствие, повысят эффективность мероприятий по обеспечению и под-

держанию кибербезопасности в банковской сфере, позволят предотвратить и (или) снизить ущерб от киберинцидентов, повысят стабильность функционирования как отдельных банков, и, как следствие, стабильность функционирования всей банковской сферы государства в целом.

**Список использованных источников**


1. Кибербезопасность в условиях электронного банкинга: Практическое пособие / Под ред. П.В. Ревенкова. – М.: Прометей, 2020. – 522 с.

2. Торчиков, В. 10 лет изящного взлома. Как развивалось вредоносное ПО для банкоматов / В. Торчиков // Журн. «Системы безопасности». – 2019. – № 5. – С. 32-36.

3. 7 причин, почему злоумышленникам так легко взламывать банкоматы [Электронный ресурс] // Блог Касперского. Режим доступа : https://www.kaspersky.ru/blog/atm-jackpotting-explained/10890/. – Дата доступа : 19.02.2022.

4. Информационные технологии и безопасность. Обеспечение информационной безопасности банков Республики Беларусь. Общие положения = Інфармацыйныя тэхналогіі і бяспека. Забеспячэнне інфармацыйнай бяспекі банкаў Рэспублікі Беларусь. Агульныя палажэнні : СТБ 34.101.41-2013. – Введ. впервые. – Минск : Белорус. гос. ин-т стандартизации и сертификации, 2013. – 40 с.

5. Технические требования и правила информационной безопасности в банковской деятельности [Электронный ресурс] // Официальный сайт Национального банка Республики Беларусь. Режим доступа : https://www.nbrb.by/legislation/informationsecurity. – Дата доступа : 16.02.2022.

6. Концепция обеспечения кибербезопасности в банковской сфере [Электронный ресурс] // Официальный сайт Национального банка Республики Беларусь. Режим доступа Технические требования и правила информационной безопасности в банковской деятельности [Электронный ресурс] // Официальный сайт Национального банка Республики Беларусь. Режим доступа : https://www.nbrb.by/legislation/informationsecurity. – Дата доступа : 16.02.2022.