УДК 336.719.2

С. Ю. Воробьёв
начальник сектора информационной безопасности ЗАО «РРБ-Банк»
Г. В. Мишнев
заместитель начальника отдела
Генеральной прокуратуры Республики Беларусь

НОРМАТИВНО-ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ЗАЩИТЫ БАНКОВСКОГО ТЕРМИНАЛЬНОГО ОБОРУДОВАНИЯ ОТ ВРЕДОНОСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Одними из наиболее существенных угроз национальной безопасности государства являются угрозы в экономической и информационной сферах. Противоправная деятельность злоумышленников в киберпространстве, направленная на информационную инфраструктуру банков, которая основывается на использовании современных информационных систем и технологий, может привести к дестабилизации финансовой и денежно-кредитной систем государства.

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, эксплуатации антивирусного программного обеспечения, а также DLP-систем и SIEM-систем, брандмауэров, разработке 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 (так называеиое терминальное оборудование). Одновременно за последние несколько лет произошла эволюция от физических атак на терминальное оборудование до атак с применением средств высоких технологий.

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 [1].

Однако до финальной стадии необходимо осуществить внедрение вредоносного программного обеспечения (далее — ВПО) в компьютер банкомата, что производится получением физического доступа к USB-портам либо оптическому приводу последнего либо удаленным внедрением ВПО, посредством предварительной компрометации внутренней информационной сети банка, получением и дальнейшим распространением зловреда на сеть банкоматов.

Вышеуказанные инциденты с терминальным оборудованием крайне негативно сказываются на репутации кредитно-финансовых учреждений [2].

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 серверы 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»* [3]. 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»). Абзац 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»* [4].

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».

Вышеуказанные изменения закрепят необходимость обязательного применения средств антивирусной защиты и, как следствие, повысят безопасность при использовании операций с банковскими платежными картами и наличными денежными средствами.

Список основных источников

1. Торчиков, В. 10 лет изящного взлома. Как развивалось вредоносное ПО для банкоматов / В. Торчиков // Системы безопасности. — 2019. — № 5. — С. 32–36. Вернуться к статье

2. Защита банкоматов и платежных терминалов от вредоносных программ и инсайдеров [Электронный ресурс] // Издание Anti-Malware.ru – Независимый информационно-аналитический центр по информационной безопасности. — Режим доступа : https://www.anti-malware.ru/node/2354. — Дата доступа: 21.12.2021. Перейти к источнику Вернуться к статье

3. 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. Вернуться к статье

4. 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: 21.12.2021. Перейти к источнику Вернуться к статье