числе учитывая в сложившихся обстоятельствах влияния структурного кризиса в глобальном масштабе необходимость комплексного применения инструментов общегосударственной экономической, денежно-кредитной, фискальной и валютной политики для успешного решения данных проблем.

Библиографические ссылки

1. НБ РБ. Общая характеристика подходов к реализации денежно-кредитной политики : сайт. URL: https://www.nbrb.by/mp/target/general-character (дата обращения: 16.02.2022).

2. TradingView. Interest Rates (white) vs Inflation (red) : сайт. 10.02.2022. URL: https://www.facebook.com/tradingview/photos/a.802024629816535/5156766831008938/ (дата обращения: 18.02.2022).

3. Аседова Н. Торги на Мосбирже сегодня не проводятся, инвесторы будут следить за внешним фоном : сайт // Группа Финам. 04.11.2021. URL: https://www.finam.ru/analysis/newsitem/torgi-na-mosbirzhe-segodnya-ne-provodyatsya-investory-budut-sledit-za-vneshnim-fonom-20211104-092334/ (дата обращения: 18.02.2022).

4. Волкова О. Рекорды глобального долга: решения и риски : сайт // ЭКОНС. Экономический разговор. 16.09.2021. URL: https://econs.online/articles/ekonomika/rekordy-globalnogo-dolga-resheniya-i-riski/ (дата обращения: 18.02.2022).

5. Волкова, Е. Развитие глобального банковского сектора: новые точки роста в Евразии : сайт // Информационно-аналитический и научно-практический журнал Национального банка Республики Беларусь «Банкаўскі веснік». 2022. № 1 (702). С. 35–45. URL: https://www.nbrb.by/bv/articles/10943.pdf (дата обращения: 18.02.2022).

УДК 336.719.2

НОРМАТИВНЫЕ МЕРЫ ЗАЩИТЫ БАНКОВСКОГО ТЕРМИНАЛЬНОГО ОБОРУДОВАНИЯ ОТ ВОЗДЕЙСТВИЯ ЦИФРОВЫХ УГРОЗ

С. Ю. Воробьёв[1)], Г. В. Мишнев[2)]

[1)] *начальник сектора информационной безопасности, ЗАО «РРБ-Банк», г. Минск, Республика Беларусь, e-mail: vorobyovsy@rrbbank.by*

[2)] *заместитель начальника отдела, Генеральная прокуратура Республики Беларусь, г. Минск, Республика Беларусь, e-mail: g.mishnev2015@gmail.com*

В статье описываются стабильность кредитно-финансовой сферы как составной части национальной безопасности государства, угрозы банковским учреждениям при помощи средств цифровизации. Обосновываются целесообразность применения антивирусного программного обеспечения на терминальном оборудовании (банкоматах, инфокиосках и пр.), необходимость внесения изменений и дополнений в действующие нормативные (технические) правовые акты.

Ключевые слова: банк; банкомат; информационная безопасность; антивирус; вредоносное программное обеспечение.

REGULATORY MEASURES TO PROTECT BANK TERMINAL EQUIPMENT FROM DIGITAL THREATS

S. Yu. Vorobyov[1)], G. V. Mishnev[2)]

[1)] *head of information security sector, RRB-Bank CJSC, Minsk, Republic of Belarus, e-mail: vorobyovsy@rrbbank.by*

[2)] *deputy head of department, General prosecutor's office of the Republic of Belarus, Minsk, Republic of Belarus, e-mail: g.mishnev2015@gmail.com*

The article describes the stability of the credit and financial sector, as an integral part of the national security of the state, the threat to banking institutions with the help of digitalization tools. The expediency of using anti-virus software on terminal equipment (ATMs, info kiosks, etc.), the need to make changes and additions to the current regulatory (technical) legal acts are substantiated.

Keywords: bank; ATM; information security; antivirus; malware.

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 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 (т. н. терминальное оборудование). Одновременно, за последние несколько лет произошла эволюция от физических атак на терминальное оборудование до атак с применением средств высоких технологий, в т. ч. вредоносного программного обеспечения (далее – ВПО).

Создатели вредоносных программ (т. н. «кодеры») являются элитой современного преступного мира. Создание, доработка и модификация банковских вредоносных программ требует не только изучения языков программирования, но и глубокого знания операционных систем, прикладных программ и программ дистанционного банковского обслуживания, на которое и оказывается основное вредоносное воздействие [1].

Внедрение ВПО в компьютер банкомата осуществляется путем получения физического доступа к USB-портам либо оптическому приводу последнего, либо удаленным внедрение ВПО, посредством предварительной компрометации внутренней информационной сети банка, получением и дальнейшим распространением зловреда на сеть банкоматов.

Данные 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 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» [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»). 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» [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*».

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 Республики Беларусь [5].

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

Библиографические ссылки

1. Кибербезопасность в условиях электронного банкинга / А. А. Бердюгин [и др.] ; под ред. П. В. Ревенкова. М. : Прометей, 2020. 522 с.

2. Защита банкоматов и платежных терминалов от вредоносных программ и инсайдеров : сайт // Издание Anti-Malware.ru – Независимый информационно-аналитический центр по информационной безопасности. URL: https://www.anti-malware.ru/node/2354 (дата обращения: 16.01.2022).

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.

4. Технические требования и правила информационной безопасности в банковской деятельности : сайт // Официальный сайт Национального банка Республики Беларусь. URL: https://www.nbrb.by/legislation/informationsecurity (дата обращения: 16.01.2022).

5. Концепция обеспечения кибербезопасности в банковской сфере ; Технические требования и правила информационной безопасности в банковской деятельности : сайт // Официальный сайт Национального банка Республики Беларусь. URL : https://www.nbrb.by/legislation/informationsecurity (дата обращения: 16.01.2022).