Библиографические ссылки

1. О компании «Гомсельмаш» : сайт. URL: https://www.gomselmash.by/o-kompanii/ (дата обращения: 07.05.2021).
2. О компании «МТЗ» : сайт. URL: http://www.belarus-tractor.com/company/ (дата обращения: 07.05.2021).
3. Модель Зайцевоq для оценки риска банкротства предприятия : сайт. URL: https://afdanalyse.ru/load/1/ocenka_verojatnosti_bankrotstva_predprijatija_model_o_p_zajcevoj/3-1-0-77 (дата обращения: 08.05.2021).
4. Бухгалтерскиǐ баланс ОАО «Гомсельмаш» : сайт. URL: http://maz.by/en/about/branches/zavod-mogilevtransmas-oao-maz-upravlausaa-kompania-holdinga-belavtomaz-g-mogilev (дата обращения: 08.05.2021).
5. Бухгалтерскиǐ баланс ОАО «МТЗ» : сайт. URL: http://www.belarus-tractor.com/company/financial-and-economic-activity.php (дата обращения: 09.05.2021).

УДК 336.719.2

МЕРЫ КИБЕРЗАЩИТЫ БАНКОВСКОЙ ОТРАСЛИ

С. Ю. Воробьёв[1)], Д. А. Жук[2)], Т. В. Русак[3)], В. А. Шкред[4)]

[1)] *Главный специалист управления внутреннего аудита, ОАО «Белагропромбанк», г. Минск, Республика Беларусь, e-mail: stogovo@list.ru*

[2)] *Инженер-программист ООО «ГлокСофт», г. Минск, Республика Беларусь, e-mail: dmitriy_zhuk_95@mail.ru*

[3)] *старший преподаватель, Белорусский государственный университет информатики и радиоэлектроники, г. Минск, Республика Беларусь, e-mail: rusaktv@gmail.com*

[4)] *оперуполномоченный, Борисовское РУВД, г. Борисов, Республика Беларусь, e-mail: vlad.shkred@yandex.by*

В статье рассматривается интерес злоумышленников к банковской отрасли Республики Беларусь, акцентируется внимание на роли Национального Банка Республики Беларусь по вниманию к вопросам обеспечения кибербезопасности в банковской сфере, перечислены основные виды киберугроз, совершаемых с использованием высоких технологий. Даны рекомендации, выполнение которых позволит успешно противодействовать цифровым атакам киберпреступников.

Ключевые слова: банк; банковская сфера; киберпреступность; информационные технологии; информационная безопасность.

BANKING INDUSTRY CYBER PROTECTION MEASURES

S. Yu. Vorobiev[1)], D. A. Zhuk[2)], T. V. Rusak[3)], V. A. Shkred[4)]

[1)] *Chief Internal Audit Officer, OJSC «Belagroprombank», Minsk, Republic of Belarus, e-mail: stogovo@list.ru*

[2)] *Software Engineer «GlokSoft» LLC, Minsk, Republic of Belarus, e-mail: dmitriy_zhuk_95@mail.ru*

[3)] *Senior Lecturer, Belarusian State University of Informatics and Radio Electronics, Minsk, Republic of Belarus, e-mail: rusaktv@gmail.com*

[4)] *Borisov District Department of Internal Affairs, Borisov, Borisov, Republic of Belarus, e-mail: vlad.shkred@yandex.by*

The article examines the interest of cybercriminals in the banking industry of the Republic of Belarus, focuses on the role of the National Bank of the Republic of Belarus in paying attention to the issues of ensuring cybersecurity in the banking sector, lists the main types of cyber threats committed using high technologies. Recommendations are given, the implementation of which will allow successfully countering digital attacks by cybercriminals.

Keywords: bank; banking sector; cybercrime; Information Technology; Information Security.

Для правонарушителей в цифровой среде существенный интерес представляет банковская сфера, осуществляющая ежедневно огромное количество транзакций и оборот огромного количества денежных средств. Возможность баснословных прибылей в случае успеха и достаточно невысокий уровень риска быть обнаруженными благоприятствуют росту киберпреступлений. Злоумышленники, как хамелеоны, приспосабливаются к изменениям обстановки в сфере информационной безопасности, тщательно отслеживают появление новых уязвимостей в программном обеспечении и появление брешей в информационных системах банков и финансовых организаций.

Так, банковская система Республики Беларусь по-прежнему остается в поле зрения злоумышленников и международных преступных группировок. В последние несколько лет постоянно выявлялись факты мошенничества с использованием электронных платежных средств, имели места хакерские атаки на банки Республики Беларусь, в результате которых злоумышленниками похищались значительные денежные средства. Сотрудниками правоохранительных органов на территории республики Беларусь задерживались участники международных преступных группировок Cobalt, Andromeda и др. [1].

Национальный Банк Республики Беларусь (далее – Национальный банк) поддерживает и стимулирует обновление имеющихся и применение банками страны новых технических средств, систем и технологий обработки информа-

ции. Серьезное внимание уделяется регулированию вопросов обеспечения кибербезопасности банковской отрасли. В Национальном банке создан центр мониторинга и реагирования на компьютерные угрозы в банковской сфере Республики Беларусь (FinCERTby), основной задачей которого является организация, координация и осуществление оперативного взаимодействия Национального банка с банками и иными организациями по вопросам противодействия кибератакам.

Анализ мировой практики показывает, что на мировом уровне можно выделить следующие наиболее характерные для банковской сферы виды киберугроз:

- воздействие через аппаратные уязвимости – уязвимости, присутствующие в микропроцессорах разных производителей, открывающие новые возможности для злоумышленников, неустранимые при помощи программных обновлений;
- компьютерный шпионаж – направлен на долговременное присутствие в сетях объектов критической информационной инфраструктуры с целью саботажа и шпионажа за деятельностью кредитно-финансовых организаций;
- целенаправленные кибератаки – целенаправленное воздействие программных и (или) программно-аппаратных средств на объекты информационной инфраструктуры, сети электросвязи банка, используемые для организации взаимодействия таких объектов, в целях проникновения в сеть конкретных банков и изолированные финансовые системы для вывода денежных средств;
- клиенто-ориентированные кибератаки – целенаправленное воздействие программных и (или) программно-аппаратных средств на объекты информационной инфраструктуры, сети электросвязи банка, используемые для организации взаимодействия таких объектов, в целях хищения денежных средств конкретных клиентов или групп клиентов банка [2].

Выбор целей киберпреступников обусловлен технической подготовкой, имеющимся в наличии инструментарием и знаниями о внутренних процессах банка [3]. При этом, как правило, основным фактором целевой атаки на финансовую организацию является слабая защита ИТ-инфраструктуры.

Также необходимо упомянуть и такой деятельности злоумышленников, как социальная инженерия – одну из главных угроз кибербезопасности. Социальная инженерия – это методы психологической манипуляции человеком, направленные на то, чтобы заставить жертву выполнить определенные действия в пользу атакующего [4]. Необходимо помнить, что работник организации, как пользователь, является одним из звеньев информационной системы организации, так как обладает определенными привилегиями, осуществляет различные операции в процессе выполнения трудовых операций. Необходимо помнить, что работник организации, как пользователь, является одним из звеньев информационной системы организации, так как обладает определенными привилегиями, осуществляет различные операции в процессе выполнения трудовых операций. Также необходимо отчетливо представлять, что степень защищенности информационной системы в организации измеряется защищенностью ее самого слабого звена [5]. Потенциально этим звеном как раз и может является пользователь (например, разочарованный заработной платой системный администратор или повздоривший с руководителем работник отдела кадров). Необходимо придер-

живаться корректного увольнения работников, так как данная процедура, как правило, сопровождается выплеском негативных эмоций, что может привести к реализации угроз информационной безопасности.

Для успешного отражения банками кибератак необходимо выполнение последними следующих мер:

- создание информационной инфраструктуры, которая позволит должным образом обеспечить информационную безопасность;
- подразделение киберзащиты должно быть независимым от профильных ИТ-подразделений;
- использование соответствующих аппаратных, программных и программно-аппаратных комплексов средств защиты информации;
- мониторинг событий безопасности;
- постоянное повышение квалификации работников, отвечающих за информационную безопасность (целесообразно организовать работу по получению последними сертификатов международного образца в области обеспечения кибербезопасности, например, Certified Ethical Hacker, Certified Information Systems Security Professional и др.);
- обучение работников банков основам информационной безопасности;
- включение пункта, связанного с соблюдением требований локальных правовых актов банка в сфере информационной безопасности, в трудовой договор;
- поддержание здорового климата в коллективе (довольный работник с меньшей долей вероятности осознанно навредит организации, в которой работает);
- информирование и обучение клиентов банков финансовой и цифровой грамотности;
- разработка пакета нормативной документации, регламентирующей сферу информационной безопасности в банке;
- установление процедур обеспечения конфиденциальности информации;
- создание команды по расследованию инцидентов информационной безопасности из числа наиболее подготовленных сотрудников;
- стандартизация бизнес-процессов;
- скрупулезный подбор персонала в банковские организации с учетом их профессиональных, нравственных и моральных качеств;
- регламентация порядка управления проектами по разработке, приобретению, внедрению новых и (или) обновлению имеющихся объектов информационной инфраструктуры;
- создание дублирующих и резервных объектов информационной инфраструктуры;
- внедрение в эксплуатацию автономных систем электропитания;
- взаимодействие и обмен информацией о кибератаках между банками, правоохранительными органами и организациями, осуществляющими помощь в борьбе с угрозами цифрового пространства;
- разработка и ввод в действие планов обеспечения непрерывности деятельности (в международной практике приемлемым считается восстановление безопасного функционирования банка в течение двух часов с момента его прекращения).

Создание современной и надежной системы информационной безопасности и соблюдение требований норм последней всеми участниками информационного обмена является залогом доверия не только к конкретной кредитно-финансовой организации, но и ко всей банковской системе государства.

Библиографические ссылки

1. Плешкевич В. М. О ходе реализации стратегического проекта Национального банка «Созданием системы мониторинга и противодействия компьютерным атакам в кредитно-финансовой сфере (FinCERT)» // Банковский вестник. 2019. № 10 (663). С. 15–16.

2. Концепция обеспечения кибербезопасности в банковской сфере: постановление Правления Национального банка Республики Беларусь, 20 ноября 2019 г., № 466 // Национальный правовой Интернет-портал Республики Беларусь: сайт. URL: http://www.pravo.by/novosti/obshchestvenno-politicheskie-i-v-oblasti-prava/2019/october/41392/ (дата обращения: 26.04.2021).

3. Панков А. Атака на банки // Веснік сувязі. 2018. № 4 (150). С. 40–45.

4. Скабцов Н. В. Аудит безопасности информационных систем. СПб.: Питер, 2018. 272 с.

5. Олифер В., Олифер Н. Компьютерные сети. Принципы, технологии, протоколы: учебник для вузов. 5-е изд. СПб.: Питер, 2017. 992 с.

УДК 338(470+571)

СТРУКТУРНО-ИНВЕСТИЦИОННАЯ ПЕРЕСТРОЙКА ПРОМЫШЛЕННОСТИ И РОЛЬ ГОСУДАРСТВА В ЕЕ РЕАЛИЗАЦИИ

А. Н. Гайшун

аспирант, экономический факультет, Белорусский государственный университет, г. Минск, Республика Беларусь, e-mail: ashutova@gsu.by

Рассмотрен опыт структурно-инвестиционной перестройки промышленности Республики Беларусь, выявлена роль государства в ее реализации.

Ключевые слова: структурная перестройка; структурная политика; промышленная политика; промышленный комплекс Республики Беларусь.