УДК 004.056.5

ПРИМЕНЕНИЕ ФРОД-МОНИТОРИНГА ДЛЯ ПРЕДОТВРАЩЕНИЯ МОШЕННИЧЕСКИХ ДЕЙСТВИЙ В БАНКОВСКОЙ СФЕРЕ

Воробьёв Станислав Юрьевич, начальник сектора информационной безопасности ЗАО «РРБ-Банк»
Vorobyov Stanislav Yurievich, Master of Science in Engineering, Head of the Information Security Sector, CJSC RRB-Bank, stogovo@list.ru
Мишнев Григорий Викторович, заместитель начальника отдела Генеральной прокуратуры Республики Беларусь
Mishnev Grigory Viktorovich, Deputy Head of the Department of the General Prosecutor's Office of the Republic of Belarus

Аннотация. В статье описано увеличение фактов противоправной деятельности, связанной с цифровизацией отраслей человеческой деятельности, акцентируется проблематика обеспечения безопасности электронных платежей, дается определения системы фрод-мониторинга

Ключевые слова: банк, мошенничество, цифровизация, мониторинг, фрод

В связи с процессами цифровизации всех отраслей человеческой деятельности в международной практике отмечается увеличение противоправной активности в киберпространстве, в частности, в отношении информационной инфраструктуры банков, основанной на использовании современных информационных систем и технологий предоставления цифровых финансовых услуг [1].

В настоящее время перед банками наиболее остро стоит проблема обеспечения безопасности функционирования электронных платежей как в сегменте юридических, так и физических лиц. В первую очередь, это связано с ростом регистрируемых фактов хищения денежных средств со счетов клиентов, увеличением сумм хищений, а также появлением новых сложных схем мошенничества.

На сегодняшний день чрезвычайно востребованным инструментом для выявления мошеннических операций в банковской деятельности является фрод-мониторинг [2].

В соответствии с Концепцией безопасного функционирования объектов банков, небанковских кредитно-финансовых организаций, открытого акционерного общества «Банк развития Республики Беларусь» система антифрода (фрод-мониторинга) – это система, предназначенная для оценки финансовых транзакций в глобальной компьютерной сети Интернет на предмет подозрительности с точки зрения мошенничества и предполагающей рекомендации по их дальнейшей обработке [3]. Так, например, ограничение на сумму платежа является примером системы фрод-мониторинга.

Используемые белорусскими банками системы фрод-мониторинга разнообразны по функциональным возможностям, стоимости, интегрированности в процес-

синговую систему банка. Для целей фрод-мониторинга может использоваться и система расходных лимитов и сложная дорогостоящая специализированная система.

Среди основных требований к системе фрод-мониторинга, как правило, выделяют следующие:

– соответствие требованиям VISA и MasterCard;

– обеспечение уровня безопасности операций, соответствующего политике управления рисками банка;

– сохранение простоты и удобства процедуры выполнения операции по картам итерминалам банка;

– использования больших массивов данных об операциях для определения стандартного поведения точек приема и карт;

– создание разных профилей поведения для разных точек приема карт (объектов торговой сети), разных категорий карт;

– удобство управления правилами и параметрами фрод-мониторинга;

– поддержка расследования подозрительных операций:

– взаимодействие (возможность интеграции) с системой управления претензионной работы банка, системами процессинга, банковской учетной системой;

–наличие инструментов, обеспечивающих надежность и безопасность, сертификатов по международным стандартам безопасности (напр., PA DSS) VISA и MasterCard [4].

Национальным банком Республики Беларусь (далее - Нацбанк) уделяется серьезное внимание вопросам управления киберриском и обеспечением кибербезопасности банков. Нацбанк поддерживает и стимулирует обновление имеющихся и использование банками новых технических средств, систем и технологий работы с информацией с учетом всесторонней оценки рисков, присущих такой деятельности. В 2016 г. последним разработаны и доведены до всех заинтересованных Рекомендации по безопасному использованию банковских платежных карточек – документ рекомендательного характера, выполнение которого позволит обеспечить максимальную сохранность денежных средств владельца карточки, а также снизить вероятные риски при совершении операций.

В настоящее время приоритетными задачами является создание нормативного правового «фундамента» применения систем фрод-мониторинга в банковском секторе государства, требуют совершенствования правовые аспекты информационного обмена об участниках схем хищений денежных средств в электронных платежных системах, целесообразно разработка, внедрение и организация работы общереспубликанской системы, в которой будет организовано накопление и распространение информации о фактах несанкционированного перевода денежных средств.

Список использованных источников

1. Концепция обеспечения кибербезопасности в банковской сфере [Электронный ресурс] : постановление Национального банка Респ. Беларусь, от 20 ноября 2019 г., № 466 // Официальный сайт Национального банка Республики Беларусь. – Режим доступа : https://https://www.nbrb.by/legislation/documents/koncepciya-kiberbezopasnosti.pdf. – Дата доступа : 17.09.2021.

2. Разина, О.М. Инновационные инструменты фрод-мониторинга в практике внутреннего аудита банка / О.М. Разина, Т.М. Костерина // Вопросы инновационной экономики. – 2015. – Том 5.– Вып. 4. – С. 257-266.

3. О Концепции безопасного функционирования объектов банков, небанковских кредитно-финансовых организаций, открытого акционерного общества «Банк развития Республики Беларусь» [Электронный ресурс] : постановление Национального банка Респ. Беларусь, от 23 марта 2021 г., № 69 // Официальный сайт Национального банка Республики Беларусь. – Режим доступа : https://www.nbrb.by/bv/arch/suppl_120.pdf. – Дата доступа : 17.09.2021.

4. Дурандина, А.П. Бизнес-модель фрод-мониторинга операций банковских карт / А.П. Дурандина// Ученые записки международного банковского института. – 2016. – № 18. – С. 127-136.