К. Ю. Мяделец
Научный руководитель — доцент Л. С. Ефремова
БГЭУ (Минск)

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ БАНКОВСКОГО СЕКТОРА РЕСПУБЛИКИ БЕЛАРУСЬ И ПУТИ ЕЕ ПОВЫШЕНИЯ

Драйвером инноваций в банковском секторе выступает спрос потребителей, и с целью его удовлетворения банки Республики Беларусь направляют свои ресурсы на приобретение и развитие решений цифровой экономики, которые наряду с такими преимуществами, как рост качества и доступности банковских услуг, несут в себе и угрозы информационной безопасности, вероятность реализации которых с каждым годом неуклонно повышается.

Подтверждение тому — статистика зарегистрированных атак мошенников на пользователей банковских услуг и банковскую инфраструктуру. Так, если в 2015 г. в Республике Беларусь их число составляло 2,4 тыс., то в 2021 г. уже насчитывалось свыше 26 тыс. что равнозначно 30 % всех совершенных преступлений в стране за год [1].

С целью выявления подверженности отдельных банков Республики Беларусь угрозам нарушения информационной безопасности нами было проведено исследование на основе анализа утечек электронных адресов, производительности, доступности и надежности шифрования их сайтов и риска кибersквоттинга. В результате исследования определено, что 15 кредитных учреждений имеют адекватный уровень информационной безопасности. Наиболее высоким уровнем безопасности характеризуется лишь один банк — ОАО «Статусбанк», использующее в качестве инструмента обеспечения безопасности SIEM-систему – программно-аппаратный комплекс автоматизированной системы обнаружения вторжений, атак и вредоносной активности в сети. Слабый уровень имеют 7 банков. Помимо таких распространенных проблем, как низкая производительность сайтов и надежность их шифрования, отмечаются и факты утечек электронных адресов. В ОАО «АСБ Беларусбанк» отмечено за три года максимальное число случаев — 7.

Банки Республики Беларусь уже активно используют передовой мировой опыт обеспечения безопасности в виде формирования необходимого законодательства и повышения уровня финансовой грамотности клиентов, но при этом актуальным остается высокий уровень киберриска, поэтому считаем необходимым повсеместное внедрение в банках механизмов искусственного интеллекта, например специализированной платформы на уровне сети. Ключевыми компонентами данной платформы должны стать динамический анализ и эмуляция угроз, передовые технологии обнаружения, ретроспективный анализ, репутационная база угроз банковского сектора государства и анализатор целевых атак. Система обнаружения мошенничества должна быть построена на основе больших данных, которые помогут отслеживать необычные изменения привычных моделей пове-

дения пользователей с применением механизмов машинного обучения, поведенческого анализа и корреляции событий.

Данная платформа уже оправдала себя в компаниях Англии и Нидерландов. Основным барьером для применения подобной технологии, по словам системных администраторов банков Республики Беларусь, является высокая стоимость приобретения и обслуживания подобных механизмов. Однако согласно оценке разработчика iTechArt Group, комплексное решение обойдется в сумму около 40 тыс. долл. США, что является незначительной величиной по сравнению с ежегодным ущербом от реализации мошеннических атак, который оценивается в 0,5 % ВВП.

Таким образом, эффективное противостояние банками атакам мошенников возможно только с помощью решений, которые находятся как минимум на ранг выше по уровню технологичности, чем методы преступников, тем более в настоящее время в Республике Беларусь есть возможность повышения информационной безопасности банков с использованием новейших технологий.

Источник

1. Число зарегистрированных преступлений и уровень преступности в Республике Беларусь [Электронный ресурс] // Национальный статистический комитет Республики Беларусь. — Режим доступа: https://www.belstat.gov.by/ofitsialnaya-statistika/solialnaya-sfera/pravonarusheniya/grafiki_diagrams/uroven-prestupnosti-po-respublike-belarus/. — Дата доступа: 29.03.2022.