А.А. Боровик
Научный руководитель — О.В. Мартысевич
БГЭУ (Минск)

КИБЕРПРЕСТУПЛЕНИЯ В БАНКОВСКОЙ СФЕРЕ

Важной проблемой в функционировании банковской сферы является предотвращение огромных объемов хищений денежных средств.

Задачи работы — проведение классификации существующих киберпреступлений в банковской сфере и описание способов защиты от них.

Киберпреступления в банковской сфере — преступления, связанные с кредитно-денежными операциями, ценными бумагами и платежными расчетами в сфере информационных технологий для разных денежных форм (наличных и безналичных).

Отдельное внимание мошенников устремлено на социальные сети и мобильные устройства, так как их пользователи наименее информированы о киберугрозах.

В настоящее время существующие кибератаки в банковской сфере можно классифицировать следующим образом:

1. Банковские атаки. Злоумышленники обманом выведывают данные карточек или интернет-банка.

2. Телефонные атаки. Необходимые данные для злоумышленника узнаются с использованием телефона:

- через звонок из «службы безопасности банка»;
- СМС;
- мобильный банк;
- мошенничество с переводом денег на карту.

3. Атаки в соцсетях. Данные пытаются получить, используя соцсети:

- через помощь, при которой деньги идут злоумышленнику, а не на благотворительность;
- кражу личных данных;
- фейковые сайты.

4. Атаки при установке приложений. Предлагается установить приложение, выполняющее шпионские функции или работающее как вирус.

Для предотвращения киберпреступлений банки стремятся повысить финансовую грамотность и внимательность клиентов, используя для этого информационные рассылки, буклеты, соответствующие разделы на сайтах и т.д. Некоторые банки проводят круглосуточный мониторинг операций, которые совершаются при использовании карточек. При выявлении даже предположительно мошеннических операций карточка блокируется и клиенту направляется уведомление

http://edoc.bseu.by

о блокировке. Также в банках внедряют системы дистанционного банковского обслуживания физических лиц с системой фрод-мониторинга. Данная система дает возможность существенно сокращать денежные потери «невнимательных» клиентов за счет использования системы искусственного интеллекта, который позволяет построить профиль его поведения и проанализировать все операции. Физическим лицам и клиентам стоит соблюдать правила безопасности при использовании платежных карт и систем дистанционного банковского обслуживания: не передавать реквизиты карт и данные для доступа в интернет и мобильный банк третьим лицам, не вводить платежные реквизиты на сомнительных ресурсах. Государство должно выстроить многоуровневую систему кибербезопасности, в том числе на законодательном уровне, которая смогла бы защитить интересы граждан, государственные и частные организации.

Источники

1. *Савенков, А. Н.* Противодействие киберпреступности в финансово-кредитной сфере как вектор обеспечения глобальной безопасности / А. Н. Савенков // Государство и право. — 2017. — № 10. — С. 5–18.

2. *Тюнин, В. И.* Мошенничество в сфере компьютерной информации: сложности квалификации / В. И. Тюнин // Уголов. право. — 2017. — № 5. — С. 92–97.