О. А. Касевич
Научный руководитель — магистр экономических наук И. А. Строганова
ПГУ (Новополоцк)

СОВЕРШЕНСТВОВАНИЕ СИСТЕМЫ КИБЕРБЕЗОПАСНОСТИ В УСЛОВИЯХ ЦИФРОВОЙ ТРАНСФОРМАЦИИ

Развитие цифровой экономики предполагает внедрение информационных технологий во все сферы жизни, но это означает и появление новых угроз безопасности — от утечек информации до кибертерроризма. На ранних стадиях развития сетей связи вопросы безопасности не были главными из-за небольшого количества пользователей и наличия в основном локальных сетей, в которых подразумевается доверие всех пользователей друг другу. С развитием технологий и разрастанием сетей связи выросло и значение обеспечения безопасности [1].

Кибербезопасность организаций финансово-банковской сферы должна базироваться на готовности подразделений безопасности противостоять новым кибератакам, понимании всего спектра угроз в отношении организации в целом и распределения приоритетов между активами организации и их защитой [2].

Пожалуй, единственный способ защитить все устройства, объединенные интернет-сетью, — это надежная защита единого центра управления интернетом вещей. Приведем основные направления совершенствования кибербезопасности в таблице.

Направления совершенствования кибербезопасности

	Нормативно-правовое регулирование в области кибербезопасности	Надежность аппаратно-программного обеспечения системы электронного банкинга	Финансовая грамотность населения и уровень профессиональной подготовки персонала
1	2	3	4
Цель	Повысить роль регулятора в вопросах кибербезопасности системы электронного банкинга и интернета вещей	Повысить надежность аппаратно-программного обеспечения, в т.ч. их защищенность от кибератак	Повысить уровень финансовой грамотности населения и персонала банков по вопросам обеспечения кибербезопасности
Что сделать регулятору	Создать орган с функцией постоянного мониторинга кибератак на банки и оперативного реагирования на них. Разработать и внедрить регламенты взаимодействия при передаче сведений о кибератаках	Установить требования по надежности и защищенности системы электронного банкинга и организовать взаимодействие по данному вопросу с разработчиками и провайдерами услуг	Разработать рекомендации по повышению уровня финансовой грамотности клиентов и персонала по вопросам обеспечения кибербезопасности. Разработать программу и методику проведения киберучений для Национального и коммерческих банков

Окончание

1	2	3	4
Что сделать банкам	Организовать выполнение регламентов взаимодействия при оперативной передаче сведений о кибератаках регулятору. Выполнять рекомендации регулятора по обеспечению кибербезопасности	Внедрять аппаратно-программное обеспечение системы электронного банкинга, соответствующее требованиям по надежности и защищенности	Организовать доведение информации до клиентов банков о различных мошеннических схемах с использованием системы электронного банкинга. Постоянно проводить переподготовку персонала по вопросам кибербезопасности

Источник: собственная разработка на основе [3].

Перечисленные направления представляют далеко не полный перечень мероприятий, которые необходимо выполнить в рамках обеспечения кибербезопасности в условиях применения интернета вещей. Ведь в реальной практике каждое направление будет содержать гораздо больше задач, направленных на достижение цели. В перспективе нужно стремиться создать *не только систему надзора* в виртуальном пространстве, но и поднять культуру поведения в нем всех участников информационного обмена. Финансовые институты должны использовать защищенные программные продукты, иметь квалифицированный обслуживающий персонал, способный оперативно и грамотно реагировать на кибератаки и всегда готовый прийти на помощь своим клиентам, оказавшимся в трудной ситуации.

Источники

1. *Грень, И. В.* Компьютерная преступность / И. В. Грень. — Минск : Новое знание, 2007. — 413 с.

2. *Конявский, В. А.* Компьютерная преступность : в 2 т. / В. А. Конявский, С. В. Лопаткин. — М. : РФК-Имидж Лаб, 2006. — Т. 1. — 560 с.

3. *Фролов, Д. В.* Обеспечение информационной безопасности в условиях ДБО / Д. В. Фролов, А. Л. Поспелов, П. В. Ребенков // Аналитический банковский журн. — 2014. — № 6 (219). — С. 76–81.