**УДК 336.7: 004.056**

# КИБЕРБЕЗОПАСНОСТЬ В УСЛОВИЯХ РАЗВИТИЯ ИНТЕРНЕТА ВЕЩЕЙ И ЭЛЕКТРОННОГО БАНКИНГА

***Ю.А. БАШКИРОВА***
***(Представлено: И.А. СТРОГАНОВА)***

*В данной статье раскрыта актуальность понятия кибербезопасности в Интернет-пространстве и особенно в кредитно-финансовой сфере, также представлены факторы, повышающие уровень воздействия кибератак, предложены направления совершенствования кибербезопасности в условиях применения Системы электронного банкинга и Интернета вещей.*

Развитие информационного общества 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.

Производители средств защиты вынуждены постоянно обороняться, то есть искать защиту в условиях жесткого лимита времени, поскольку самый большой вред исходит именно от атак «нулевого дня». В некоторых случаях защищаться приходится то того, о чем есть крайне поверхностное представление: отсутствуют данные о количестве подобных атак, которые уже направлялись на банки, о том, каким способом непосредственно производилось заражение программного обеспечения, как действовали злоумышленники в определенных ситуациях и т.п. [1].

Кибербезопасность организаций кредитно-финансовой 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.

К факторам, повышающим уровень воздействия кибератак, относятся [2]:

– отсутствие отлаженного правового и организационно-технического обеспечения законных интересов граждан, государства и общества в области кибербезопасности (в том числе в условиях применения Системы электронного банкинга);

– высокая латентность киберпреступлений и недостаточное осознание органами государственной власти возможных политических, экономических, моральных и юридических последствий компьютерных преступлений;

– слабая координация действий правоохранительных органов, суда и прокуратуры в борьбе с киберпреступлениями, неподготовленность их кадрового состава к эффективному предупреждению, выявлению и расследованию таких действий;

– несовершенство системы единого учета правонарушений, совершаемых с использованием средств информатизации;

– существенное отставание отечественной индустрии средств и технологий информатизации и кибербезопасности от мирового уровня;

– ограниченные возможности бюджетного финансирования научно-исследовательских, опытно-конструкторских работ по созданию правовой, организационной и технической баз кибербезопасности.

Безопасность всего пространства Интернета вещей должна задаваться на уровне создания архитектуры (тем более для организаций кредитно-финансовой сферы). Иными словами, необходимо обеспечить защиту от любых вредоносных действий еще при разработке протоколов и устройств Интернета вещей. Поэтому эффективные решения по безопасности должны быть найдены на этапе развертывания всей инфраструктуры банковских сервисов.

Учитывая тот факт, что кредитно-финансовая сфера становится одной из самых привлекательных зон интересов киберпреступников (о чем свидетельствует значительный рост числа киберпреступлений и целевых атак на банки), а также оптимизацию финансовых решений в условиях Интернета вещей, необходимо оперативно принять меры по обеспечению повышенного уровня кибербезопасности (особое внимание должно быть обращено на Систему электронного банкинга) [3].

Пожалуй, единственный способ защитить все устройства, объединенные Интернет-сетью, – это надежная защита единого центра управления Интернетом вещей.

Учитывая, что финансовый и банковский сектора наиболее восприимчивы к внедрению новейших достижений в области ИКТ, приведем три основных направления совершенствования кибербезопасности в условиях применения Системы электронного банкинга и Интернета вещей:

Таблица 1. – Направления совершенствования кибербезопасности в условиях применения Системы электронного банкинга и Интернета вещей

| Направления совершенствования кибербезопасности в условиях применения Системы электронного банкинга и Интернета вещей | | | |
|---|---|---|---|
| | Цель | Что надо сделать регулятору | Что должны сделать банки |
| Нормативно-правовое регулирование в области кибербезопасности | Повысить роль регулятора в вопросах кибербезопасности Системы электронного банкинга и Интернета вещей | Создать орган (отдельное подразделение в структуре Национального Банка Республики Беларусь), в функции которого будет входить постоянный мониторинг кибератак на банки и оперативное реагирование на них (в том числе совместно с правоохранительными органами). Для этого необходимо разработать и внедрить регламенты взаимодействия при передаче сведений о кибератаках. Подготовить и выпустить рекомендации для банков по обеспечению кибербаезопасности в применении Системы электронного банкинга и Интернета вещей | Организовать выполнение регламентов взаимодействия при оперативной передаче сведений о кибератаках регулятору. Выполнять рекомендации регулятора по обеспечению кибербезопасности |
| Надежность аппаратно-программного обеспечения Системы электронного банкинга | Повысить надежность аппаратно-программного обеспечения, в том числе их защищенность от кибератак | Установить требования по надежности и защищенности аппаратно-программного обеспечения Системы электронного банкинга и организовать взаимодействие по данному вопросу с разработчиками Системы электронного банкинга и провайдерами услуг | Внедрять аппаратно-программное обеспечение Системы электронного банкинга, соответствующее требованиям по надежности и защищенности. Повысить качество заключаемых договоров с разработчиками аппаратно-программного обеспечения и провайдерами услуг |
| Финансовая грамотность населения и уровень профессиональной подготовки персонала банков в условиях применения Системы электронного банкинга и Интернета вещей | Повысить уровень финансовой грамотности населения и персонала банков по вопросам обеспечения кибербезопасности в условиях применения Системы электронного банкинга | Разработать и довести до банков рекомендации по повышению уровня финансовой грамотности клиентов и персонала по вопросам обеспечения кибербезопасности. Разработать программу и методику проведения киберучений для Национального банка Республики Беларусь и для коммерческих банков | Организовать доведение информации до клиентов банков (через web-сайт, смс-сообщения) о различных мошеннических схемах с использованием Системы электронного банкинга. Постоянно проводить переподготовку персонала по вопросам кибербезопасности |

Источник: составлено автором на основе [4].

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.

Таким образом, 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, а также всегда готовый прийти на помощь своим клиентам, оказавшимся в трудной ситуации.

## ЛИТЕРАТУРА

1. Грень, И.В. Компьютерная преступность. – Минск: Новое знание, 2007. – 413 с.
2. Конявский, В.А., Лопаткин, С.В. Компьютерная преступность. В 2-х т. Т. 1. – М.: РФК-Имидж Лаб, 2006. – 560 с.
3. Ревенков, П.В., Дудка, А.Б., Сычев, А.М., Пеленицын А.М. Электронный банкинг: сопутствующие риски и особенности безопасного функционирования: Практ. Пособие. – М.: ИД «Регламент», 2009. – 248 с.
4. Фролов, Д.В., Поспелов, А.Л., Ревенков, П.В. Обеспечение информационной безопасности в условиях ДБО // Аналитический банковский журнал. 2014. № 6 (219). С. 76–81.