НУЛЕВОЕ ДОВЕРИЕ КАК СПОСОБ ПОВЫШЕНИЯ БЕЗОПАСНОСТИ УДАЛЁННОГО ВЗАИМОДЕЙСТВИЯ КЛИЕНТА С БАНКОМ

Овчаренко Д. Р.
Научный руководитель – д.т.н., проф. Антипов И.Е.
Харьковский национальный университет радиоэлектроники
(61166, Харьков, пр. Науки, 14, кафедра КРиСТЗИ
(057) 702 14 30) e-mail: diana.naidonova@nure.ua

Today it is impossible to imagine any area of business without the use of information technologies. But the number of cybercrimes is also growing rapidly. Such crimes are extremely dangerous for financial institutions, so banks try to secure their systems as much as possible from cybercriminals. This work presents an effective way to protect Internet banking from intruders - the principle of Zero Trust. Singly this method does not guarantee full safety, but as an additional measure it is a very effective protective measure.

Все последние годы с ростом уровня цифровизации бизнеса растёт и ущерб от киберпреступлений. По данным Cybersecurity Ventures, потери бизнеса от киберпреступности к 2021 году могут составить $6 триллионов [1]. Киберугрозы в первую очередь опасны финансовым учреждениям, как филиалам, так и их онлайн помощникам в виде интернет-банков. В настоящее время удаленное использование банковских услуг является очень распространённым. Банки, безусловно, прилагают усилия по обеспечению безопасности своих клиентов и их средств, но, зачастую, злоумышленники оказываются «на шаг впереди» в части изобретения и реализации различных мошеннических схем [2].

Доклад посвящён организационным и техническим мерам, основанным на так называемом принципе нулевого доверия (Zero Trust).

При строгом следовании принципам нулевого доверия можно рассчитывать на защищённость банков и клиентов как от уже налаженных, так и от новых мошеннических схем. Эти принципы уже частично реализованы в работе как зарубежных, так украинских банков. Например, давно являются обязательным использование:

- SSL-сертификатов;
- cookies-файлов;
- двухфакторной аутентификации;
- мобильной аутентификации.

В работе произведен анализ угроз, характерных для вышеназванных мер, из-за которых их использование ещё не гарантирует безопасность. Их краткий перечень приведён в таблице. Предложен комплекс организационных и технических мер, направленных на предотвращение совершения злоумышленниками мошеннических действий как на стороне клиента и самого банка.

Метод	Что обеспечивает	Уязвимости	Дополнительные меры
SSL-сертификаты	Целостность данных, невозможность стороннего вмешательства; шифрование, повышенное доверие пользователей к сайту.	Отсутствие обязательной проверки сертификата со стороны пользователя	SSL-pining
Cookies-файлы	Сохранение личных данных; автоматическая авторизация.	Хищение и перехват cookies-файлов злоумышленником	Удаление cookies-файлов после окончания работы
Двухфакторная/многофакторная аутентификация	Общее повышение безопасности за счёт нескольких этапов авторизации, в том числе с использованием технических средств	Обусловлены уязвимостями соответствующих технических средств	Оотдельные для каждого из технических средств

Названные в таблице, но не уточнённые уязвимости технических средств и дополнительные меры по повышению безопасности для них будут рассмотрены в докладе

Также в докладе будут рассмотрены конкретные приёмы, используемые злоумышленниками: подмена номера, фейковые sms «от банка», звонки от «службы безопасности банка» и др., и показана эффективность принципа нулевого доверия для противодействия им.

Метод Zero Trust в настоящее время не формализован в виде свода конкретных правил и рекомендаций. В основном он пока он представляет собой ряд правил, которые во многом каждый понимает по-своему. Тем не менее, выработка общих мер и принципов необходима, и потому работа в данном направлении является достаточно перспективной.

Следует отметить, что отдельные крупные компании (Cisco, Google) уже пытаются внедрять принцип Zero Trust в своей работе, в том числе рекомендуя их своим партнёрам.

Список используемых источников

1. Рынок кибербезопасности 2021-2025: угрозы и инвестиционные возможности // [Электронный ресурс.] Режим доступа: https://megatrends.su/блог/cybersecurity/

2. Нулевое доверие – единственный верный подход для борьбы с новыми угрозами ИБ// [Электронный ресурс.] Режим доступа:

https://www.securitylab.ru/blog/company/PandaSecurityRus/346416.php