СОВЕРШЕНСТВОВАНИЕ КИБЕРБЕЗОПАСНОСТИ В УСЛОВИЯХ РАЗВИТИЯ ЭЛЕКТРОННОГО БАНКИНГА

IMPROVING CYBERSECURITY IN THE CONTEXT OF THE DEVELOPMENT OF ELECTRONIC BANKING

Юлия БАШКИРОВА
Email: 17fk.bashkirava.y@pdu.by,
Научный координатор: **Ирина СТРОГАНОВА**
i.stroganova@psu.by
Учреждение образования «Полоцкий государственный университет»
Новополоцк, Республика Беларусь

Abstract. *This article reveals the relevance of the concept of cybersecurity in the Internet space, and especially in the credit and financial sphere, also presents the factors that increase the impact of cyber-attacks, suggests ways to improve cybersecurity in the context of using the Electronic Banking System and the Internet of Things.*

Keywords: information security, cybersecurity, cyberspace, cybercrime.
JEL classification: 0330

Введение

Финансовые технологии за последние годы значительно трансформировали финансовую сферу. В настоящее время наблюдается резкий рост инцидентов в области информационной безопасности, которые имеют широкое распространение и приобретают угрожающий характер. Многие из подобных атак затрагивают широкий круг частных, корпоративных, а также государственных интересов.

Методы исследования

Статистические методы исследования, общенаучные методы исследования, а также методы функционального анализа.

Основное содержание

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.

Также стоит отметить, что одними из наиболее опасных кибератак, на которые бесспорно реагировать и пытаться их предотвратить, работая на опережение, являются инсайдерские угрозы.

Инсайдерские угрозы — это вредоносные для организации угрозы, которые исходят от людей внутри организации, таких как работники, бывшие работники, подрядчики или деловые партнеры, у которых есть информация о методах безопасности внутри организации, данных и компьютерных системах.

За последние два года количество инсайдерских угроз выросло на 47%, указывая на все возрастающую важность данной проблемы. Это опасность, от которой не застрахована ни одна организация, а руководители прекрасно знают, что 2/3 компаний считают внутренние угрозы более серьезной проблемой, чем внешние.

В данном контексте финансовые организации особенно уязвимы – они являются естественной целью, в первую очередь из-за того, что типы данных, которые они собирают – финансовые и личные – дорого ценятся на рынке при перепродаже. Учитывая это, неудивительно, что в финансовых компаниях фиксируется больше нарушений безопасности, исходящих изнутри, чем в организациях из любого другого сектора рынка,

Почти каждый сотрудник может нести угрозу – все, что для этого требуется, это доступ к конфиденциальной информации или просто доступ к офису компании, независимо от того, работает ли человек в данной организации или нет. Например, бывшие сотрудники, внешние консультанты, члены совета директоров или текущие сотрудники.

В зависимости от намерений субъекта и обстоятельств происшествия, можно выделить 3 основных типа таких угроз (таблица 2):

Таблица 2. Типы инсайдерских угроз в зависимости от намерений субъекта и обстоятельств происшествия

Тип угроз	Описание
Ненамеренная инсайдерская угроза	Случайные внутренние угрозы появляются в результате небрежного, а иногда и безрассудного поведения, помогая злоумышленникам достигать своих целей. Напрмер: сотрудник, который кликает на фишинговое электронное письмо, неосознанно помогая распространить вредоносный код по сети. Или менеджер, который устанавливает несанкционированное ПО или использует Shadow IT. Это может быть человек, который использует дату своего рождения в качестве пароля, или тот, кто записывает свои данные для аутентификации в корпоративной сети на клочке бумаги под клавиатурой.
Намеренный взлом	Сотрудники, имеющие злой умысел, с другой стороны, не являются безрассудными, небрежными или недостаточно информированными. Они точно знают, что делают, и у них есть мотив для взлома сети и кражи данных. Например, недовольный специалист или тот, кому платят за использование своего служебного положения для предоставления доступа к сети. Некоторые могут находиться в трудной финансовой ситуации, или работать на конкурентов, ожидая больше вознаграждения и карьерных перспектив.
Угрозы, исходящие от удаленных сотрудников	Это более свежая категория инсайдерских угроз. Уже несколько десятилетий у многих людей есть возможность работать из дома, но вместе с резким ростом количества удаленных сотрудников растут и риски для безопасности. Помимо подключения к корпоративной сети через потенциально небезопасную домашнюю или общедоступную сеть, эти работники могут также использовать личные устройства, которые не были приобретены, настроены и защищены IT-специалистами компании, тем самым еще сильнее усугубляя проблему. Также существует опасность, что люди, имеющие доступ к дому такого сотрудника или его сожители, могут получить доступ и к рабочим устройствам.

Источник составлено автором на основе [5]

Удаленные пользователи, работающие изолированно, с большей вероятностью станут жертвами атак с применением методов социальной инженерии, ведь они не могут просто пододвинутся на стуле к коллеге и спросить легитимны ли запросы злоумышленников. В условиях домашнего офиса меньше контроля и ограничений, что, к сожалению, ведет к ослаблению бдительности.

В штаб-квартире компании, IT специалисты также сталкиваются с проблемами, вызванными удаленными сотрудниками. Внешние соединения создают больше логов трафика и данных о событиях, которые необходимо анализировать, в то время как ресурсы отнюдь не бесконечны. Атака может просто затеряться в информационном шуме.

Управление традиционными внутренними рисками, вероятно, уже является частью IT-стратегии любой финансовой организации. Поэтому для эффективности мер, обеспечивающих кибербезопасность, предлагаются направления по минимизации инсадерских угроз для финансово-банковской сферы (таблица 3):

Таблица 3 – Рекомендации по управлению рисками инсайдерских угроз

Рекомендации	Описание
Обезопасьте удаленные соединения	Шифрование данных в реальном времени имеет важное значение, поэтому следует использовать SSL и IPSec VPN вместе со строгой аутентификацией при подключении удаленных пользователей к сети и предоставлении им доступа к данным. Сюда также входит проверка зашифрованного трафика, поскольку туннели VPN могут быть так же легко, как и легальный трафик, использованы для передачи вредоносных программ и финансовых данных без обнаружения. Это потребует развертывания межсетевого экрана, производительность которого соответствует масштабу организации.
Шифруйте хранимые данные.	Все конфиденциальные данные, в том числе те, которые хранятся на устройствах сотрудников, должны быть зашифрованы. Если это невозможно, удаленным сотрудникам следует запретить хранить данные на личных устройствах.
Применяйте технологии контроля доступа.	IT-командам нужны все возможные ресурсы, способные обеспечивать видимость пользователей, устройств и приложений в сети, чтобы контролировать, кто и к каким приложениям имеет доступ. Автоматический контроль доступа – важный инструмент, который необходимо взять на вооружение.
Считайте безопасность конечных точек приоритетной	Атаки на конечные точки весьма распространены, что обуславливает необходимость регулярной оценки устройств на предмет наличия уязвимостей и сложных угроз. Важно использовать передовые решения безопасности, такие как EDR (endpoint detection and response – система обнаружения и реагирования на угрозы конечным точкам), обеспечивающая защиту от вредоносных программ и взломов в реальном времени. Эти решения также следует сочетать с целостной структурой безопасности, которая может автоматически обнаруживать, реагировать и управлять угрозами, тем самым защищая данные, сокращая время простоя системы и обеспечивая непрерывность бизнеса.
Отслеживайте необычную активность	Используйте технологии SIEM и SOAR для предупреждения об аномальных попытках входа в систему, необоснованной передаче больших объемов данных или других необычных сетевых событиях.
Обучайте удаленных сотрудников	Сотрудники должны знать и соблюдать политики безопасности, относящиеся к удаленной работе.

Источник: составлено автором на основе [5]

Таким образом, борьба с инсайдерскими угрозами жизненно важна для обеспечения непрерывности бизнес-процессов. Сегодня внутренние угрозы представляют беспрецедентную опасность для финансового сектора, особенно для тех организаций, которые перешли на удаленную работу для обеспечения непрерывности бизнеса. Хотя для защиты от внешних киберпреступников введены различные меры безопасности, традиционные методы не всегда учитывают угрозы, которые уже существуют внутри компании. Понимание специфики существующих внутренних угроз и выполнение рекомендаций, изложенных выше, поможет лучше защитить вашу сеть, клиентов и сотрудников от новых рисков, обусловленных стратегией удаленной работы.

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.

Библиографические ссылки

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. – 560с.
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. – 248с.
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.
5. Как устранить внутренние угрозы в финансовых организациях в условиях удаленной работы [Электронный ресурс]. – Режим доступа: https://www.klerk.ru/buh/articles/505467/. – Дата доступа: 10.10.2020