Кибератаки как источник угроз безопасности систем электронного банкинга

Юсеф Рагид,
аспирант института экономики и управления НИУ «БелГУ»,
Белгород, Россия

Ваганова Оксана Валерьевна,
зав. кафедрой инновационной экономики
и финансов, профессор, доктор экономических наук,
профессор кафедры инновационной
экономики и финансов НИУ «БелГУ»,
Белгород, Россия

Талимова Лязат Азимовна,
заведующая кафедрой «Банковское дело», доктор экономических наук, профессор
Карагандинского экономического университета
Казпотребсоюза, Караганда, Россия

Аннотация

В настоящее время расширение использования Интернета и создание систем передовых технологий приводит к широкому и международному увеличению использования электронного банкинга. Однако на технологию электронного банкинга может повлиять ряд случаев кибератак. В данной статье дается четкое определение термина электронного банкинга. Также будут всесторонне рассмотрены типы кибератак и даны их характеристики. В заключении автор предоставит рекомендации и предложения для развития и усиления аспекта безопасности электронного банкинга.

Ключевые слова: Электронный банкинг, атаки, безопасность, безопасность электронного банкинга.

Cyber attacks as a source of threats to the security of electronic banking systems

Yousef Ragheed,
postgraduate student of the Institute of Economics and Management of the National Research University "BelSU",
Belgorod, Russia

Scientific supervisor: **Oksana V. Vaganova,**
Head of the Department of Innovative Economics and Finance, Professor, Doctor of Economics,
Professor of the Department of Innovative Economics and Finance of the National Research University "BelSU",
Belgorod, Russia

Lyazat A. Talimova,
Head of the Department of Banking, Doctor of Economics, Professor of Karaganda University of Economics
Kazpotrebsoyuza, Karaganda, Russia

Abstract

At the moment, the increased usage of the Internet and the development of advanced technological systems are leading to a growth in the use of electronic banking on a national and

worldwide scale. However, e-banking technology is vulnerable to a variety of cyber threats. This article defines the word "e-banking" in detail. It will also outline the various types of cyberattacks and their features in detail. Finally, it will include recommendations and ideas for the advancement and improvement of electronic banking security.
Keywords: Electronic banking, attacks, security, security of electronic banking.

За последние несколько лет, благодаря впечатляющему технологическому скачку, количество электронных услуг значительно увеличилось. Таким образом, мы за очень короткое время перешли от эры почтовых сообщений к эре цифровых технологий. Электронный банкинг - одна из основных услуг, сделавших жизнь простой и легкой; пользователь может получить множество услуг в любое время в любом месте.

Исследования показывают, что электронный банкинг имеет многомерные преимущества как для частных лиц, так и для компаний, но он не лишен некоторых проблем и проблем, связанных с безопасностью и интересами клиентов [Рокало И.А, 2017]. Поскольку безопасность считается одной из основных забот как больших, так и малых организаций, электронные банковские системы также сталкиваются с кибератаками, как и любая другая система, подключенная к Интернету.

В этой статье основное внимание будет уделено аспекту безопасности технологии «электронного банкинга» в контексте научных исследований. Первая часть представит электронный банкинг в общем виде. Он определяет этот расплывчатый термин, представляет свои услуги, а также перечисляет преимущества и риски, связанные с этой технологией. Вторая часть будет посвящена анализу предыдущих работ с целью определения их ограничений, проблем и проблем. Наконец, третья часть будет посвящена типам атак, а также рекомендациям и предложениям по развитию и усилению безопасности.

«Э-банкинг» или «электронный банкинг» - нечеткий термин; его можно определить по-разному. Проще говоря, это может означать предоставление банком информации или услуг своим клиентам через компьютер, телевизор или мобильный телефон.

Определение «э-банкинга», сокращение от электронного банкинга, сильно варьируется от одного автора к другому. Иногда авторы ссылаются на отдельные аспекты, иногда на одно и то же или частично пересекаются [Ваганова О. В., Юсеф Р. 2019], ниже приведены некоторые определения:

- Электронный банкинг: относится к предоставлению розничных и мелких банковских продуктов, и услуг через электронные каналы. Такие продукты и услуги могут включать в себя прием депозитов, кредитование, управление счетами, предоставление финансовых консультаций, электронную оплату счетов и предоставление других электронных платежных продуктов и услуг, таких как электронные деньги [Вуколов А.С., Белугин И.С., Василенко О.А. 2017].
- Электронный банкинг: форма банковского обслуживания, при которой учетная запись ведется через Интернет, а не в отделении банка [Nagar, N, Ghai, E. 2019].

- Электронный банкинг: ПС-банкинг, Веб-банкинг, Интернет-банкинг, домашний банкинг и т. Д. Различные термины относятся к «Электронному банкингу». Благодаря сети у вас есть возможность управлять своей учетной записью из дома [Лямин Л.В. 2015].

Тот факт, что существует множество определений, не является совпадением, но он восходит к истории электронных банковских услуг с момента его запуска в 1981 году в Соединенных Штатах с первой услугой, а также благодаря ее развитию и появлению в Европе, можно объяснить множественность определения этого термина.

Услуги, предлагаемые электронным банкингом клиентам, представляют собой просто сочетание услуг традиционного банка и технологий / автоматизации, которые намного превосходят услуги, предлагаемые традиционным банком.

У электронного банкинга много преимуществ: как для клиента, так и для электронного банка. Поскольку есть преимущества, с этой технологией также связаны риски и проблемы. Можно выделить два типа рисков электронного банкинга: общие и прикладные риски. Общие риски могут включать доступ к физическому оборудованию, логический доступ к системам и информационным технологиям. Риски приложений могут быть результатом ошибочной ситуации, например, информация о приложении недоступна в реальном времени из-за сбоя системы [Ваганова О. В., Юсеф Р. 2019]. В таблице ниже в общих чертах представлены преимущества и риски этой технологии:

Последний риск (операционный риск) очень важен для нашей статьи и означает риск прямых или косвенных убытков в результате неадекватных процессов или сбоев для людей и систем или внешних событий. Этот вид риска связан с:

- Системы обслуживания, проектирования и внедрения,
- Неправильное использование товаров и услуг покупателем,
- Риск безопасности: при отсутствии соответствующей проверки безопасности не только хакеры могут нанести ущерб банку, раскрывая личные данные клиентов, но и третьи лица могут разрушить информационную систему, внедрив вредоносные вирусы. Помимо внешних атак, банки подвержены мошенничеству [Revenkov P.V, Berdyugin A.A. 2016].

Помимо преимуществ, банковская отрасль столкнулась с киберугрозами из-за подключения к Интернету. Основная проблема для сектора электронного банкинга — это интенсивное использование приложений информационных технологий, связанных с электронным банкингом. Это приводит к угрозам электронной безопасности, кибератакам на профиль клиентов, хищениям, мошенничеству с точки зрения сообщений с данными, конфиденциальности клиентов, защищающих от краж, тайне финансовых транзакций.

В нескольких статистических отчетах приводятся примеры размеров и последствий нарушений безопасности в электронных банковских услугах. Согласно исследованию SANS 2019 года, которое измеряет состояние риска и

безопасности в финансовом секторе, отрасль финансовых услуг наводнена программами-вымогателями и хакерскими атаками, число которых растет в геометрической прогрессии [Filkins.B, 2019].

Таблица 1 - Преимущества и риски электронного банкинга

Преимущества	Риски
• Для клиента: - сокращение его времени на выполнение различных операций со счетом, - Экономя деньги, - Имея доступ к своим услугам в любое время, когда он хотел бы, помимо доступности услуг через Интернет. • Для банка: - Имея снижение затрат и увеличение рентабельности, - Меньше бумажной работы, поскольку административные задачи компьютеризированы - Доступ к услуге будет в любое время, потребность в персонале и инвестициях для развития инфраструктуры значительно сокращается из-за отсутствия физических агентств.	• Общие риски • Риски приложений • Риск кредита • Рыночные риски • Стратегический риск • Риск репутации • Правовой риск • Операционный риск

Согласно Symantec в своем последнем отчете, выпущенном в 2020 году; В 2019 году было обнаружено более 430 миллионов новых уникальных вредоносных программ, что на 36% больше, чем в предыдущем году. Исследователи Symantec обнаружили новый фишинговый троян для Android, который побуждает пользователей вводить свою банковскую информацию, создавая поддельную страницу входа в легитимные банковские приложения. Такие угрозы, как «Dridex», используют исключительно рассылку спама по электронной почте и включают настоящие названия компаний в адрес отправителя и тело электронного письма [Symantec, 2020].

Другое исследование показывает, что 60% менеджеров банков согласны с тем, что кража личных данных в Интернете была выявлена их банками. В то время как атака через вредоносный код и атака отказа в обслуживании согласились 54% руководителей. Фактически, атаки Wikileaks на основные сайты электронной коммерции подогрели интерес мошенников. Случаи взлома, а также мошенничества с кредитными картами или банкоматами также были выявлены или зарегистрированы в банках. Изощренность фишинговых и спуфинговых атак также определяется и подтверждается 76% руководителей банка. Фишинг, фальсификация, взлом и кража личных данных в Интернете являются одними из основных проблем для банков [Bamrara A., 2015].

Чтобы предложить модели безопасности и радикальные решения, необходимо сначала понять и определить методы атак и существующие уязвимости, на которых они основаны. В ходе поиска была предпринята попытка

классифицировать различные виды атак на электронный банкинг по-разному. Основные угрозы безопасности или атаки платформ электронного банкинга: отказ в обслуживании, незаконное использование, раскрытие информации и отказ от авторства [Сиротский А.А. 2013]. Другие исследователи представили классификацию текущих атак на системы онлайн-банкинга. Другое исследование предложило иерархию причин, которая включала три основные категории; законный доступ, контроль устройств и кража собственности [Закиров М.Р. 2014]. Существует модель (Модель атакующего оружия), которая представляет основные и эффективные атаки, объясняет, как использовать унаследованные уязвимости (социальная инженерия и фишинговые атаки) и берет под контроль программное обеспечение (вредоносное программное обеспечение) и кражу личных данных законного пользователя (поддельные страницы). веб-сайтов и вредоносного ПО).

С другой стороны, цель атакующего может измениться. Злоумышленник может попытаться использовать уязвимости, характерные для операционных систем, где он может снова попытаться не авторизовать вход на веб-сайт, что приведет к отказу в обслуживании клиентов [30]. Вот исчерпывающий список типов атак:

Таблица 2 - Типы атак на электронный банкинг

Тип атаки	характеристика
1	2
отказ в обслуживании «DOS атаки»	Атака типа «отказ в обслуживании» — это кибератака, при которой злоумышленник пытается сделать машину или сетевой ресурс недоступными для предполагаемых пользователей, временно или на неопределенный срок прерывая работу хоста, подключенного к Интернету. Отказ в обслуживании обычно достигается путем переполнения целевой машины или ресурса избыточными запросами в попытке перегрузить системы и предотвратить выполнение некоторых или всех законных запросов.
Атака программ-вымогателей	Это вредоносное ПО использует страх людей перед раскрытием своей личной информации, потерей важных данных или необратимым повреждением оборудования. Программы-вымогатели — это компьютерные вредоносные программы, которые незаметно устанавливаются на устройство жертвы и осуществляют криптовирусную атаку-вымогательство со стороны криптовирусологии, которая удерживает в заложниках данные жертвы.
Атака «Man-In-The Middle»	нацелена на фактические данные, которые передаются между конечными точками, а также на конфиденциальность и целостность самих данных, общий сценарий включает две конечные точки (жертвы) и третью сторону (злоумышленник). Злоумышленник имеет доступ к каналу связи между двумя конечными точками и может манипулировать их сообщениями. В результате злоумышленник убедил обе жертвы, что они используют защищенные каналы, но на самом деле он имеет доступ ко всем зашифрованным сообщениям.

Продолжение табл. 2

1	2
Фишинг	представляет собой кражу личных данных в Интернете, при которой делается попытка украсть конфиденциальную информацию, такую как имя пользователя, пароль и данные онлайн-банкинга, у жертв. Это тип семантической атаки, при которой злоумышленники пытаются обмануть и украсть деньги у законных пользователей Интернета, отправляя электронные письма, а не используя ошибки в компьютерном программном обеспечении. Злоумышленник создает мошеннический веб-сайт, который имеет внешний вид законного веб-сайта. В фишинговых письмах используются различные тактики, чтобы обманом заставить людей раскрыть свою конфиденциальную информацию, такую как имена пользователей, пароли, номера государственного страхования и номера кредитных / дебетовых карт.
Фарминг	Фарминг-атаки - изощренная версия фишинговых атак. Злоумышленник внедряет троянов и / или червей на компьютеры пользователей или DNS-сервер, что вызывает различные типы атак (изменение файла хостов пользователей, отравление кеша DNS, захват домена, подмена статического домена и т. Д.). перенаправлять веб-пользователей на поддельную страницу, чтобы получить информацию об их конфиденциальности, пароли учетных записей или другую важную информацию. Ужасная опасность фарминг-атаки заключается в том, что даже если пользователи тщательно проверяют URL-адрес перед посещением веб-сайта, они не могут найти никаких исключений.
Вишинг	Голосовой фишинг — это преступная практика использования социальной инженерии через телефонную систему для получения доступа к частной личной и финансовой информации от общественности с целью получения финансового вознаграждения. Голосовой фишинг обычно используется для кражи номеров кредитных карт или другой информации, используемой в схемах кражи личных данных у людей.
Спуфинг	Когда злоумышленник притворяется законным передатчиком для распространения ложных сообщений или законным приемником для кражи конфиденциальной информации
Раскрытие информации	Распространение информации среди всех, кто не имеет доступа к этой информации. Эти действия по угрозе могут вызвать несанкционированное раскрытие: раскрытие, перехват, вывод, вторжение.
Атака отказа	Атака отказа происходит, когда приложение или система не принимает элементы управления для правильного отслеживания и регистрации действий пользователей, что позволяет злонамеренно манипулировать или подделывать идентификацию новых действий. Эта атака может использоваться для изменения исходной информации о действиях, выполняемых злоумышленником, с целью записи неверных данных в файлы журналов. Его использование может быть расширено до общей обработки данных от имени других, аналогично подделке почтовых сообщений. Отказ относится к отказу от участия в общении полностью или частично.

Окончание табл. 2

1	2
Атака социальной инженерии	Авторы определяют социальную инженерию как «науку об использовании социального взаимодействия в качестве средства убедить человека или организацию выполнить конкретный запрос злоумышленника, где либо социальное взаимодействие, либо убеждение, либо запрос затрагивают объект, связанный с компьютером.». Существует множество моделей и таксономий, касающихся атак социальной инженерии. Наиболее известной моделью является цикл атак социальной инженерии Кевина Митника, описанный в его книге «Искусство обмана: управление человеческим элементом безопасности».
Сканеры портов	В этом типе атаки злоумышленник использует различные методы для кражи конфиденциальной информации, отправляя различные типы сигналов в систему для извлечения сообщения и получения подтверждения, чтобы обеспечить детализацию канала связи. Основное внимание уделяется сбору важной информации, относящейся к аппаратному и программному обеспечению, используемому системой, для заблаговременного планирования атак, которые могут быть выполнены на такой системе
Взлом пароля	Состоит из того, что злоумышленник пробует множество паролей или кодовых фраз в надежде в конечном итоге правильно угадать. Злоумышленник систематически проверяет все возможные пароли и парольные фразы, пока не будет найден правильный. Более распространенные методы взлома паролей, такие как словарные атаки, проверка шаблонов, подстановка списка слов и т. Д.
Трояны	Троянские атаки предназначены для нарушения нормальной работы схемы, что может иметь катастрофические последствия для критически важных приложений во многих различных областях. Они также могут стремиться к утечке секретной информации изнутри микросхемы через скрытые каналы или влиять на надежность ИС (интегральной схемы) посредством нежелательных изменений процесса, которые вызывают износ устройства / межсоединения и долгосрочные проблемы с надежностью.

Источник: составлено автором.

Электронный банкинг осуществляется посредством серии транзакций в различных средах между конечным пользователем и системой. Эти транзакции всегда уязвимы для хакерских атак. В результате из перечисленных выше угроз стало важным разработать и разработать модели эффективной безопасности, чтобы обеспечить безопасный доступ в сети.

Без упоминания традиционных решений и методов [Дьякова О.Н. 2015] и на основе отчетов и прогнозов нескольких известных организаций рекомендуется множество действий. это следует учитывать при реализации политик безопасности или разработке новых технологических и практических решений. Более того, эти организации начали формировать партнерские отношения, что является обязательным условием для непрерывного роста перед этими рисками.

Согласно прогнозному исследованию, проведенному Symantec и получившему несколько результатов, мы обнаружили, что количество вредоносных программ без файлов будет увеличиваться, злоупотребление Secure Sockets Layer приведет к увеличению количества фишинговых сайтов, использующих HTTPS. Что касается McAfee, то машинное обучение атак социальной инженерии ускоряется, и обмен информацией об угрозе делает большой прогресс [Symantec, 2020].

Наконец, для «Gartner», всегда известного своей способностью ставить проценты рядом с прогнозами; до 2018 года более 50% производителей устройств «Интернета вещей» не смогут справиться с угрозами, возникающими из-за слабых практик аутентификации. Это предсказание весьма показательно и было рекомендовано; Стимулируйте отрасль к стандартам аутентификации, но компании должны идентифицировать риски аутентификации, устанавливать требования к удостоверению личности и использовать меры высокой безопасности. К 2021 году использование паролей и токенов в приложениях со средней степенью риска снизится на 55% за счет внедрения технологий распознавания. Чтобы решить эту проблему, компаниям следует искать продукты, ориентированные на создание постоянной доверительной среды с хорошим пользовательским интерфейсом, с использованием биометрических и аналитических ресурсов.

Также к 2022 году большинство компаний и организаций будут основаны на блокчейне. Благодаря сервисной платформе блокчейн можно значительно сократить количество транзакций, а также их стоимость, а также сократить время транзакции. 42 крупнейших мировых финансовых гиганта, в том числе JP Morgan Chase, Citibank, Goldman Sachs Group, вложили огромные средства в платформу исследований, разработок и обслуживания блокчейн [Gartner, 2020].

Подводя итог, следует сказать, что для борьбы с этими атаками необходимо инициировать просвещение и повышение осведомленности потребителей, это действие должно осуществляться в сотрудничестве с правительством и другими частными организациями. Обучение должно быть организовано таким образом, чтобы пользователи понимали конфиденциальность данных, уровень конфиденциальности и механизмы, позволяющие обеспечить безопасность транзакции. Он также реализует модели безопасности «на месте» с технологией и отвечает требованиям и стандартам. Это говорит о том, что необходимо планировать сотрудничество с технологическими отраслями и банками.

С развитием, расширением передовых инструментов и инноваций постепенно проникают в нашу повседневную жизнь, требования цифровой безопасности выросли. Чтобы улучшить нашу кибернетическую защиту, отрасль должна сотрудничать. Банки должны рассматривать вопросы безопасности как главный аспект своих предложений по администрированию. Точно так же он стремится обеспечить безопасное управление онлайн-ситуациями в свете передовых методов безопасности. Безопасность и страхование данных, которыми обмениваются клиенты и банк, являются для всех счетов сложным стимулом в области электронного банкинга. Человек

посередине, фишинг и утечка данных, например, не могут быть полностью уничтожены, но их можно сдержать, вовремя определив их. Адекватность электронного банкинга основана на его конфиденциальности, целостности и невозможности отказа от авторства.

Список литературы

1. Bamrara A., Evaluating database security and cyber-attacks: A relational approach, J. Internet Bank. Commer., vol. 20, no. 2, p. 1, 2015.
2. Filkins.B, SANS 2019 State of OT/ICS Cybersecurity Survey. URL:https://www.sans.org/ reading-room/whitepapers/analyst (дата обращения: 11.08.2022).
3. Gartner, Predicts 2020: threat and vulnerability management, URL:https://www.gartner.com /en/insights /business-strategy-reset?type=Function&tag=Cross-Enterprise&utm_expid= .DFYKrZ3rQdaNV JRqa5cXgQ.1&utm_referrer=https%3A%2F% 2Fwww. gartner.com%2Fen (дата обращения: 15.08.2022).
4. Nagar, N & Ghai, E (2019). A Study of Bank Customer's Reliability towards Electronic Banking (E-Banking) Channel's!. International Journal of Management Studies. Vol.–VI, Issue – 1(1). P 34-40.
5. Revenkov P.V, Berdyugin A.A. The security of electronic banking: the service and the duty of the bank // Finance, and credit. – 2016. – № 8. – P. 22.
6. Symantec, Modern Endpoint Protection: Accruing Tangible Benefits of an Integrated EPP/EDR Solution Set. URL:https://www.broadcom.com/company/industry-analyst-report/modern-endpoint-protection (дата обращения: 14.08.2022).
7. Ваганова О. В., Юсеф Р. Эволюция и этапы становления электронного банкинга // Гуманитарные, социально-экономические и общественные науки. – 2019. – №. 11. – С. 276-279.
8. Вуколов А.С., Белугин И.С., Василенко О.А. Безопасность банковских электронных услуг//В книге: Проблемы экономической безопасности России в современных условиях//монография. Под редакцией Василенко О.А.. Домодедово, 2017. С. 90-95.
9. Дьякова О.Н. Содержание системы дистанционного банковского обслуживания // Современные проблемы науки и образования. 2015. № 1–1. С. 60–72.
10. Закиров М.Р. Исследование угроз нарушения безопасности в системах дистанционного банковского обслуживания // Информационное противодействие угрозам терроризма. 2014. № 22. С. 43–47.
11. Лямин Л.В. Применение технологий электронного банкинга: риск-ориентированный подход. – М.: КНОРУС, 2015. – 453 с.
12. Машевская О.В. Мтодика оценки инновационной деятельности промышленного предприятия// Вестник Самарского государственного университета. Серия: Экономика и управление. 2015. № 8 (130). С. 97-105.
13. Рокало И.А. Риски интернет-банкинга, особенности управления ими // Экономика и социум. – 2017. – № 9(40). – С. 23–29.
14. Сиротский А.А. Информационная безопасность личности и защита персональных данных в современной коммуникативной среде // Технологии техносферной безопасности: интернет-журнал. Вып. 4 (50). 2013. 8 с.