**Буй Тхи Тхао Хыонг**

4 курс, Финансовый факультет

РЭУ им. Г.В. Плеханова

**Научный руководитель: Донцова Людмила Васильевна**

д. э. н., профессор

Базовая кафедра Финансового контроля, анализа и аудита  
Главного контрольного управления города Москва

РЭУ им. Г.В. Плеханова

КИБЕРБЕЗОПАСНОСТЬ В ФИНАНСОВОМ СЕКТОРЕ: БЛОКЧЕЙН

Аннотация: киберпреступность (или кибер-атака) является актуальной проблемой во всем мире. В частности, индустрия банковских и финансовых услуг стала целью крупных кибератак. В данной статье рассмотрены основные угрозы и потенциальные решения для кибербезопасности в секторе банковских и финансовых услуг.

**Ключевые слова:** кибератак, кибербезопасность, сектор банковских и финансовых услуг, блокчейн, Интернет вещей.

**CYBERSECURITY IN THE FINANCIAL SECTOR: BLOCKCHAIN**

**Abstract:** cybercrime (or cyber-attack) is a pressing problem worldwide. In particular, the banking and financial services industry has become the target of large cyber attacks. This article discusses the main threats and potential solutions for cybersecurity in the banking and financial services sector.

**Keywords:** cyber attack, cyber security, banking and financial services sector, blockchain, Internet of Things.

Кибератака - это преднамеренная эксплуатация компьютерных систем, технологических предприятий и сетей. Хакеры (киберпреступники) используют вредоносный код и программное обеспечение для изменения компьютерного кода, логики или данных, что приводит к разрушительным последствиям, которые могут поставить под угрозу данные и привести к киберпреступлениям, таким как финансовая информация, медицинские данные, кража личных данных или проникновение в систему.

Сектор банковских, финансовых услуг и страхования является одной из наиболее важных областей, подверженных кибератакам. Сектор банковских и финансовых услуг подвергается почти в три раза большему количеству кибератак, чем любая другая отрасль. В банках лежат деньги. Кроме того, банки также располагают данными миллионов пользователей. Таким образом, для киберпреступников атакующие банки предлагают множество способов получения прибыли за счет вымогательства, кражи и мошенничества. Все больше и больше организаций, оказывающих финансовые услуги, постоянно находятся в состоянии атаки, в результате чего ИТ-отделы и службы безопасности испытывают трудности с возможностью сбора, распространения и интерпретации вредоносных событий.

**Рост кибератак в мире Интернета вещей (англ. Internet Of Things - IoT)**

С увеличением количества устройств, подключенных к IoT, увеличивается риск кибератак. Благодаря IoT датчики собирают, обмениваются информацией, анализируют ее и обрабатывают информацию, предлагая новые способы создания стоимости для компаний, работающих в сфере технологий, средств массовой информации и телекоммуникаций. Но это также создает новые возможности для компрометации всей этой информации. Мало того, что через IoT распространяется больше данных среди большего числа участников, но и делятся более конфиденциальными данными. В результате риски экспоненциально возрастают.

**Основные угрозы кибербезопасности в банковском и финансовом секторе**

- Незашифрованные данные. Большинство нарушений данных происходит из-за неправильного шифрования и кражи данных, которые сразу же становятся доступными после кражи.

- Новая технология автоматизации без безопасности. Камеры видеонаблюдения, подключенные устройства и игрушки могут быть превращены в боты, если они не защищены.

- Незащищенные сторонние сервисы. Интернет является универсальным соединителем, поэтому незащищенные сторонние сервисы могут открыть доступ к данным для злоумышленников.

- Небезопасный мобильный банкинг. В последнее время, когда популярность мобильного банкинга возросла, он дал возможность экспертам-хакерам получить доступ к его данным из-за менее сложных систем безопасности на мобильных устройствах.

- Постоянно меняющийся ландшафт угроз - За последние несколько лет ландшафт киберугроз изменился. Количество нарушений, затрагивающих финансовый сектор, привело к росту мошеннических действий.

- Ложные срабатывания. Одной из главных проблем банков в системах мониторинга противодействия отмыванию денег является «ложные срабатывания».

- Большое нарушение. Огромные объемы ценных финансовых данных находятся под растущим давлением, чтобы защитить данные клиентов от хакеров и мошенников.

- Новые формы взлома. В настоящее время хакеры не только удаляют данные о потребителях, но и изменяют или удерживают их в качестве заложников для дальнейшего использования.

- Игнорирование потенциального нарушения. Эта неспособность системы предупредить о потенциальном нарушении является основной частью современной стратегии кибербезопасности.

- Счета клиентов. Счета клиентов могут быть наиболее уязвимой точкой входа в банковские системы.

- Безжалостные противники. Угроза должна рассматриваться не как технологическая проблема, а скорее как организованная преступность. Они похожи на безжалостные операции, которые работают вне системы регулирования.

**Решения в кибербезопасности для сектора банковских и финансовых услуг**

- Коммуникация и интеллект. Кибербезопасность и мошенничество теперь сместили подход к целостному, и это привело к улучшению обмена информацией и обменом информацией. Это сводится не только к технологиям, но и к людям и процессам.

- Сценарий на основе тестирования. Структурные упражнения и тестирование на основе тестирования также являются одним из лучших способов защиты банковского и финансового сектора от киберугроз, особенно когда они проводятся во всей отрасли.

- Межотраслевое сотрудничество. Для того чтобы добиться прогресса в борьбе с сегодняшними киберугрозами, банкам необходимо прекратить хранить кибер-стратегию в строжайшем секрете только для сотрудников банков.

- Осведомленность о действии. Финансовый и банковский сектор стремится получить более действенные идеи не только для своих аналитиков по безопасности, но и для сотрудников бизнес-единицей.

- От охраны периметра до нескольких уровней. Банки нуждаются в изменении своей охраны периметра для углубленной многоуровневой защиты.

**Внедрение технологии** блокчейн **для кибербезопасности**

Хотя технология блокчейн изначально была изобретена для криптовалют (биткойнов), она может быть очень полезна для усиления кибербезопасности. Блокчейн может сократить расходы на инфраструктуру банков на 15-20 миллиардов долларов США в год к 2022 году. Благодаря своей распределенной природе блокчейны не обеспечивают «взломанного» входа или центральной точки отказа и, таким образом, обеспечивают большую безопасность по сравнению с различными существующими транзакционными структурами, управляемыми базой данных.

Применение технологии блокчейн в финансово-технологическом секторе и кибербезопасности:

- Решение проблемы отсутствия доверия между контрагентами на базовом уровне;

- Исключение вмешательства человека из процесса аутентификации;

- Обеспечение децентрализованного хранения;

- Криптографическая защита, которая защищает это хранение от несанкционированного изменения;

- Потенциал для улучшения всего: от повышения целостности данных и цифровых идентификаторов до обеспечения более безопасных устройств IoT для предотвращения распределенных атак на отказ в обслуживании;

- Обеспечение прослеживаемости всех транзакций;

- Синхронизированная сторонняя проверка на основе консенсуса по каждой записанной транзакции.

**Вывод**

Разрешенные блокчейны предоставляют уникальные возможности в управлении рисками кибербезопасности. Функции разрешенных блокчейнов предоставляют ряд возможностей для снижения рисков кибербезопасности и выявления, предотвращения и борьбы с типами кибератак, которые часто направлены на финансовые организации. Поскольку индустрия финансовых услуг исследует использование разрешенных блокчейнов для улучшения услуг и операций, участники отрасли должны признать и принять во внимание ряд возможностей кибербезопасности, а также риски и другие соображения, связанные с этой технологией.

**Список используемых источников**

1. Кибербезопасность – приоритет для банков в текущем году – [Электронный ресурс] – Режим доступа: <http://nbj.ru/publs/upgrade-modernizatsija-i-razvitie/2018/03/03/kiberbezopasnost-prioritet-dlja-bankov-v-tekuschem-godu/index.html>. 03.03.2018.
2. Кибербезопасность (2017–2018): цифры, факты, прогнозы – [Электронный ресурс] – Режим доступа: [https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/cybersecurity-2017-2018-rus.pdf](https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/cybersecurity-2017-2018-rus.pdf.%2020.08.2018). 20.08.2018.
3. Будущее кибербезопасности: технология блокчейна – [Электронный ресурс] – Режим доступа: <https://www.blockchain-council.org/blockchain/the-future-of-cyber-security-blockchain-technology/>. 25.09.2018.
4. Блокчейн, кибербезопасность и глобальные финансы – [Электронный ресурс] – Режим доступа: <https://www.huntonak.com/images/content/3/2/v2/32097/blockchain-cybersecurity-and-global-finance.pdf>. 21.10.2018.