УДК 330.341.11

Игнатьева В.А., студентка ЭОб-221
Курусканова С.А., студентка ЭОб-221
Научный руководитель: Шутько Л.Г., к.э.н., доцент
Кузбасский государственный технический университет
имени Т.Ф. Горбачева, г. Кемерово

Ignateva V.A., student, group EOb-221, 4th year
Kuruskanova S.A., student, group EOb-221, 4th year
Shutko L.G., PhD in Economics, Associate Professor
T.F. Gorbachev Kuzbass State Technical University

МАРКЕТПЛЕЙС: КИБЕРБЕЗОПАСНОСТЬ ПОЛЬЗОВАТЕЛЕЙ, АНАЛИЗ ОСНОВНЫХ УГРОЗ И СПОСОБОВ ЗАЩИТЫ

MARKETPLACE: CYBERSECURITY OF USERS, ANALYSIS OF MAIN THREATS AND PROTECTION METHODS

Современный рынок онлайн-торговли развивается стремительными темпами. Маркетплейсы стали неотъемлемой частью жизни миллионов пользователей: они позволяют приобретать товары из любой точки мира, сравнивать предложения, читать отзывы и получать удобную доставку. Однако вместе с ростом количества онлайн-покупок растёт и число киберпреступлений.

По данным аналитических центров, более половины случаев мошенничества с банковскими картами связано именно с интернет-платежами. Особенно уязвимыми оказываются пользователи маркетплейсов, где большое количество участников и высокая скорость оборота средств создают благоприятную почву для злоумышленников. Мошенничество в сфере онлайн-доставки, фишинг и взлом аккаунтов – всё это делает кибербезопасность пользователей ключевым вопросом современной электронной коммерции [1].

Целью данной работы является выявление основных киберугроз, с которыми сталкиваются пользователи маркетплейсов, а также определение эффективных мер защиты, предпринимаемых как самими пользователями, так и платформами и государственными структурами.

Одной из наиболее распространённых угроз для пользователей маркетплейсов являются фишинговые атаки. Злоумышленники создают поддельные сайты или страницы, внешне полностью копирующие дизайн популярных платформ, например Wildberries, Ozon или AliExpress.

Пользователь получает сообщение о "скидке", "блокировке аккаунта" или "подтверждении оплаты" и переходит по ссылке, где вводит свои данные – логин, пароль, номер карты. В результате информация оказывается у мошенников.

По аналогии с системой интернет-платежей, надёжную защиту обеспечивают SSL-сертификаты и многоуровневое шифрование, однако при посещении фальшивых страниц эти механизмы отсутствуют, что и становится уязвимостью.

Вторая по распространённости угроза – мошенничество, связанное с оплатой и доставкой товаров. Пользователь может получить сообщение о необходимости доплаты за транспортировку или разблокировку посылки. Оплата совершается на поддельные счета, а товар, разумеется, не поступает.

Такие схемы часто используют подставные сайты и фейковые службы доставки. Аналогичные случаи описывались в сфере интернет-платежей: более 8% всех мошеннических действий связано с оплатой услуг доставки. Для защиты необходима проверка реквизитов и использование только официальных платёжных шлюзов, сертифицированных по стандарту PCI DSS.

Взлом личных кабинетов покупателей и продавцов – еще одна серьёзная угроза. После получения доступа злоумышленники могут менять адрес доставки, оформлять возвраты, получать бонусы и даже выводить деньги с привязанных карт.

Причиной часто становится слабый пароль, повторное использование комбинаций или отсутствие двухфакторной аутентификации. Кроме того, взломы аккаунтов часто происходят после фишинговых рассылок, когда пользователь сам сообщает данные.

Согласно исследованиям в сфере интернет-платежей, более половины преступлений совершается через онлайн-ресурсы. Это подтверждает необходимость многофакторной защиты, включая подтверждение входа по SMS или через специальные приложения.

Особую опасность представляют мошеннические продавцы, регистрирующиеся на маркетплейсах для одноразовых продаж. Они размещают привлекательные предложения, принимают оплату и исчезают.

Проблема усугубляется тем, что пользователи доверяют интерфейсу маркетплейса, считая, что все продавцы проверены. Однако проверка не всегда достаточна: некоторые площадки не требуют полной верификации документов.

Подобная угроза близка по механизму к классическому мошенничеству в сфере интернет-платежей и требует как технических, так и организационно-правовых мер контроля – лицензирования, сертификации и постоянного мониторинга активности продавцов.

Основной уровень безопасности формируется самими пользователями. Чтобы минимизировать риски, необходимо:

1. Использовать уникальные и сложные пароли, не дублируя их на
разных сайтах.
2. Проверять адрес сайта перед оплатой (должен начинаться с https:// и содержать корректное доменное имя).
3. Не переходить по ссылкам из подозрительных сообщений.
4. При вводе платёжных данных использовать виртуальную клавиатуру, чтобы исключить возможность перехвата информации.

Такие меры соответствуют принципам цифровой гигиены и доказали эффективность в снижении числа успешных атак.

Покупки и расчёты следует совершать только через официальные мобильные приложения или веб-сайты маркетплейсов.

Использование сторонних ресурсов увеличивает риск утечки персональных данных. Также важно устанавливать обновления приложений, поскольку они часто содержат исправления уязвимостей [2].

Кроме того, маркетплейсы активно внедряют системы авторизации по биометрии, SMS-подтверждение транзакций и уведомления в реальном времени, что позволяет оперативно реагировать на попытки несанкционированного входа.

Современные платформы внедряют комплексные системы защиты:

1. Шифрование данных по международным стандартам ISO/IEC 27001:2013.
2. Собственные антифрод-сервисы, анализирующие подозрительные операции.
3. Верификацию продавцов и покупателей.
4. Использование систем рейтинга и отзывов, снижающих риск мошенничества.

Государство, в свою очередь, усиливает нормативную базу в сфере цифровой безопасности, разрабатывает программы по борьбе с кибермошенничеством и поддерживает инициативы по просвещению пользователей. Регулятор, как отмечает Л.Г. Шутько, «должен оценивать возможности новых игроков рынков компаний-цифровых гигантов оказывать влияние на общие условия обращения товара на товарных рынках» [4. с.238]. Комплексный подход – сочетание технических, правовых и организационных мер – является наиболее эффективным инструментом противодействия угрозам [5]. Кибербезопасность пользователей маркетплейсов – одно из ключевых направлений развития электронной коммерции. Итак, проведенный анализ показывает, что большинство угроз связано с человеческим фактором – неосторожностью и недостаточной цифровой грамотностью. В то же время совершенствование технологий защиты, сертификация платёжных систем, активная работа

маркетплейсов и государства создают основу для безопасного онлайн-опыта. Повышение уровня цифровой культуры и внимательность при совершении операций остаются важнейшими условиями безопасности в интернет-среде. Только совместными усилиями пользователей, платформ и регулирующих органов можно обеспечить надёжную защиту в условиях стремительно растущего цифрового рынка.

Список литературы

1. Белова, К. Д. Кибермошенничество на маркетплейсах: основные проблемы и методы регулирования / К. Д. Белова, Д. А. Москвин. – Текст : электронный // Научно-образовательный потенциал молодежи в решении актуальных проблем XXI века : Сборник XII международной студенческой научной конференции, Ачинск, 25 апреля 2024 года. – Ачинск:, 2024. – С. 238-243. – URL: https://www.elibrary.ru/item.asp?id=67360719 (дата обращения: 25.10.2025).

2. Ташева, Г. Р. Кибербезопасность: вызовы и решения / Г. Р. Ташева. – Текст : электронный // Право и управление. – 2023. – №11. – URL: https://cyberleninka.ru/article/n/kiberbezopasnost-vyzovy-i-resheniya (дата обращения: 25.10.2025).

3. Душин, С. Д. Цифровизация розничной торговли: угроза или возможность для локальных рынков? / С. Д. Душин. – Текст : электронный // Вестник экономического научного общества студентов и аспирантов : Сборник материалов XXIII Межвузовской студенческой научно-практической конференции «LECTIO IBI – 2025», Санкт-Петербург, 22 мая 2025 года. – Санкт-Петербург, 2025. – С. 93-99. – URL: https://www.elibrary.ru/item.asp?id=82764609 (дата обращения: 25.10.2025).

4. Шутько, Л. Г. Актуальная проконкурентная политика государства как фактор социально-экономического развития / Л. Г. Шутько // Конкуренция и монополия : Сборник материалов Всероссийской научно-практической конференции школьников, студентов, магистрантов, аспирантов, научно-педагогических работников и специалистов в области антимонопольного регулирования, Кемерово, 11–12 декабря 2018 года / Под общей редакцией В. Г. Михайлова; Кузбасский государственный технический университет имени Т.Ф. Горбачева. – Кемерово: Кузбасский государственный технический университет имени Т.Ф. Горбачева, 2018. – С. 238-243.

5. Павлов, Е. Н. Методика расследования мошенничества, совершаемого на маркетплейсах. Постановка проблемы / Е. Н. Павлов. – Текст : электронный // Право и государство: теория и практика. – 2024. – №9 (237). – URL: https://cyberleninka.ru/article/n/metodika-rassledovaniya-

moshennichestva-sovershaemogo-na-marketpleysah-postanovka-problemy (дата обращения: 25.10.2025).

References

1. Belova, K. D., & Moskvin, D. A. (2024). Cyber fraud on marketplaces: main problems and regulation methods. In Scientific and Educational Potential of Youth in Solving Urgent Problems of the 21st Century: Proceedings of the XII International Student Scientific Conference, Achinsk, April 25, 2024 (pp. 238–243). Achinsk. URL: https://www.elibrary.ru/item.asp?id=67360719

2. Tasheeva, G. R. (2023). Cybersecurity: Challenges and Solutions. Law and Governance, (11). URL: https://cyberleninka.ru/article/n/kiberbezopasnost-vyzovy-i-resheniya

3. Dushin, S. D. (2025). Digitalization of retail trade: a threat or an opportunity for local markets? In Bulletin of the Economic Scientific Society of Students and Postgraduates: Proceedings of the XXIII Interuniversity Student Scientific and Practical Conference "LECTIO IBI – 2025", Saint Petersburg, May 22, 2025 (pp. 93–99). Saint Petersburg. URL: https://www.elibrary.ru/item.asp?id=82764609

4. Shutko, L. G. (2018). Current pro-competitive state policy as a factor of socio-economic development. In Competition and Monopoly: Proceedings of the All-Russian Scientific and Practical Conference for School Students, Students, Master's Students, Postgraduates, Academic and Teaching Staff, and Specialists in Antimonopoly Regulation, Kemerovo, December 11–12, 2018 / Edited by V. G. Mikhailov. Kemerovo: T. F. Gorbachev Kuzbass State Technical University (pp. 238–243).

5. Pavlov, E. N. (2024). Methodology for investigating fraud committed on marketplaces: problem statement. Law and State: Theory and Practice, 9(237). URL: https://cyberleninka.ru/article/n/metodika-rassledovaniya-moshennichestva-sovershaemogo-na-marketpleysah-postanovka-problemy