Асанов Гирей Айдерович
студент
Научный руководитель
Иваненко Ирина Анатольевна
доцент
ГБОУВО РК «Крымский инженерно-педагогический
университет им. Февзи Якубова»
г. Симферополь, Республика Крым

ПОТЕНЦИАЛЬНЫЕ УГРОЗЫ БЕЗОПАСНОСТИ В ИНТЕРНЕТЕ, ВКЛЮЧАЯ СЕГМЕНТ ЭЛЕКТРОННОЙ КОММЕРЦИИ

Аннотация*: статья посвящена анализу основных угроз безопасности в интернете, с особым акцентом на электронную коммерцию. Рассматриваются распространенные типы атак, их последствия и методы противодействия. Автор подчеркивает необходимость комплексного подхода к обеспечению безопасности, включающего технологические решения, организационные меры и повышение осведомленности пользователей. В заключение делается вывод о важности превентивных мер для снижения рисков и обеспечения надежной работы интернет-магазинов.*

Ключевые слова*: мошенничество, электронная коммерция, фишинг, конфиденциальность, мобильные устройства, угрозы безопасности, защита данных, интернет-безопасность, вредоносное ПО, кредитные карты.*

В современном мире Интернет стал неотъемлемой частью нашей жизни и проникает во все сферы деятельности: от коммуникаций и образования до бизнеса и менеджмента. Однако по мере того, как глобальная сеть открывает новые возможности, возрастают и риски безопасности. Потенциальные угрозы в Интернете чрезвычайно разнообразны и постоянно развиваются, требуя постоянного внимания и эффективных мер защиты со стороны пользователей, организаций и государств. Проблема безопасности особенно остро стоит в сфере электронной коммерции, где циркулируют огромные денежные потоки и обрабатываются конфиденциальные данные миллионов клиентов. Недостаточная защита

может привести к значительным финансовым потерям, репутационному ущербу и потере доверия потребителей [5].

Цель этой статьи – изучить основные потенциальные угрозы безопасности в Интернете, уделив особое внимание особенностям электронной коммерции. Мы проанализируем наиболее распространенные типы атак, их возможные последствия и существующие контрмеры. Особое внимание уделяется рискам, связанным с потерей персональных данных, мошенничеством, фишингом и другими угрозами, имеющими отношение к онлайн-торговле.

В целом, интернет-безопасность, и особенно в электронной коммерции, является сложной задачей, требующей многоуровневого подхода, включающего технологические решения, организационные действия и осведомленность пользователей [3].

В Интернете существует множество потенциальных угроз безопасности, особенно в области электронной коммерции. Вот некоторые из них.

1. Мошенничество с кредитными картами. Мошенники могут использовать украденные данные кредитных карт для покупок, что приводит к финансовым потерям для покупателей и продавцов.

2. Фишинг. Атаки фишинга направлены на получение личной информации пользователей через поддельные веб-сайты или электронные письма, которые выглядят как официальные.

3. Разрешения на доступ. Некоторые сайты могут запрашивать избыточные разрешения на доступ к личным данным, что создает риск утечки информации [1].

4. Вредоносное ПО. Вредоносные программы могут захватывать данные с компьютера пользователя, красть пароли или другую конфиденциальную информацию.

5. Угрозы безопасности на мобильных устройствах. Мобильные приложения для электронных платежей могут быть подвержены атакам, если не защищены должным образом.

6. Неправомерный доступ. Хакеры могут использовать уязвимости в системах безопасности для получения несанкционированного доступа к данным пользователей.

7. Атаки «человека посередине». Злоумышленники могут перехватывать данные во время передачи между пользователем и сайтом.

8. Недостаточная защита данных. Многие компании не обеспечивают должный уровень безопасности данных клиентов, что может приводить к утечкам [4].

9. Защита конфиденциальности. Сбор и использование личной информации без согласия пользователя могут привести к утечкам данных и нарушениям конфиденциальности.

10. Спам и реклама. Нежелательные сообщения и реклама могут вводить в заблуждение пользователей и приводить к злоупотреблениям.

Для обеспечения безопасности в электронной коммерции важно соблюдать осторожность, использовать надежные пароли, обновлять программное обеспечение и быть осведомленным о возможных угрозах [2].

Таким образом, безопасность в Интернете требует комплексного подхода, особенно в сфере электронной коммерции, где на кону стоят большие суммы денег и доверие клиентов. Внимательное отношение к угрозам и превентивные меры помогут снизить риски и обеспечить надежную работу интернет-магазинов.

Список литературы

1. Дубень А.К. Опыт международного сотрудничества в сфере информационной безопасности: проблемы и перспективы / А.К. Дубень // Международное право и международные организации. – 2023. – №3. – С. 13–19. – DOI 10.7256/2454-0633.2023.3.43422. – EDN SLNHHW

2. Жарова А.К. Защита информации ограниченного доступа, получаемой по цифровым каналам передачи информации о совершаемых коррупционных правонарушениях / А.К. Жарова // Государственная власть и местное самоуправление. – 2023. – №.9. – С. 37–41. – DOI 10.18572/1813-1247-2023-9-37-41. – EDN FGGGDH

3. Назаров А.Н. Информационная безопасность в сетях общего пользования: учебно-методическое пособие / А.Н. Назаров, Е.Г. Андрианова. – М.: РТУ МИРЭА, 2023. – 52 с. – ISBN 978-5-7339-1751-1 [Электронный ресурс]. – Режим доступа: https://e.lanbook.com/book/368963 (дата обращения: 18.05.2025).

4. Основы информационной безопасности: учебное пособие / составитель С.П. Середкин. – Иркутск: ИрГУПС, 2024. – 80 с [Электронный ресурс]. – Режим доступа: https://e.lanbook.com/book/458102 (дата обращения: 18.05.2025).

5. Фот Ю.Д. Методы защиты информации: учеб. пособие / Ю.Д. Фот, Н.П. Мошуров. – Оренбург: ОГУ, 2019. – 230 с. – EDN YRTUVO