УДК 004.056

АНАЛИЗ И СНИЖЕНИЕ ОБМАНА МОШЕННИКАМИ В ИНТЕРНЕТЕ: МЕТОДЫ, ТЕХНОЛОГИИ И СТРАТЕГИИ ПРОТИВОДЕЙСТВИЯ

Коновалов К.А., студент гр. ЭПб-241, 1 курс

Научный руководитель: Андреев В.А., старший преподаватель кафедры ЭГПП КузГТУ

Кузбасский государственный технический университет

имени Т.Ф. Горбачева, г. Кемерово

Аннотация: Интернет-мошенничество представляет собой глобальную проблему, постоянно эволюционирующую и наносящую значительный ущерб пользователям и организациям. В данной статье проводится всесторонний анализ современных методов онлайн-мошенничества, включая фишинг, мошенничество с использованием социальных сетей, обман при онлайн-покупках, инвестиционное мошенничество и другие. Рассматриваются технические, психологические и социальные факторы, способствующие успеху мошеннических схем. Предлагаются эффективные стратегии и технологии для обнаружения, предотвращения и снижения рисков интернет-мошенничества, включая использование искусственного интеллекта, анализ данных, усиление безопасности онлайн-транзакций и повышение осведомленности пользователей.

Ключевые слова: интернет-мошенничество, киберпреступность, фишинг, социальная инженерия, онлайн-торговля, инвестиционное мошенничество, искусственный интеллект, машинное обучение, анализ данных, кибербезопасность, осведомленность пользователей, защита данных.

Интернет, являясь неотъемлемой частью современной жизни, предоставляет огромные возможности для коммуникации, торговли и развлечений. Однако, с ростом онлайн-активности, увеличивается и количество киберпреступлений, в частности, интернет-мошенничества. Мошенники постоянно совершенствуют свои методы, используя новые технологии и приемы социальной инженерии для обмана пользователей и получения финансовой выгоды. Данная статья посвящена глубокому анализу проблемы интернет-мошенничества, изучению его различных проявлений,

выявлению ключевых факторов, способствующих успеху мошеннических схем, и разработке эффективных стратегий противодействия.

Интернет-мошенничество принимает различные формы, каждая из которых имеет свои особенности и механизмы:

1. Фишинг (Phishing): Мошенники выдают себя за доверенные лица (банки, платежные системы, социальные сети), отправляя поддельные электронные письма, сообщения или создавая поддельные веб-сайты для кражи личных данных (логины, пароли, данные банковских карт).
2. Мошенничество в социальных сетях: Использование поддельных профилей, взлом учетных записей, распространение ложной информации, фишинговые ссылки, продажа несуществующих товаров или услуг, вымогательство.
3. Мошенничество при онлайн-покупках и продажах: Обман при покупке товаров (недоставка, подделки), обман при продаже товаров (получение оплаты без отправки товара), использование поддельных платежных реквизитов.
4. Инвестиционное мошенничество: Предложение инвестиций в высокодоходные проекты (криптовалюты, акции, форекс), которые на самом деле являются финансовыми пирамидами или схемами Понци.
5. Романтическое мошенничество: Знакомство с жертвами через онлайн-платформы знакомств с целью получения денег, подарков или другой финансовой выгоды.
6. Мошенничество с использованием онлайн-объявлений: Размещение ложных объявлений о продаже товаров или оказании услуг по заниженным ценам, требуя предоплату.
7. Подделка официальных сайтов и ресурсов: Создание копий сайтов государственных органов, банков, почтовых служб и других, с целью кражи конфиденциальной информации.
8. Мошенничество с использованием вредоносного ПО: Установка на устройства жертв вредоносных программ (вирусы, трояны, шпионское ПО) для кражи данных, блокировки доступа или вымогательства денег.
9. Мошенничество с использованием криптовалют: Поддельные ICO, схемы Pump and Dump, скам-проекты, а также кража криптовалюты.

Эффективность интернет-мошенничества обусловлена сочетанием технических, психологических и социальных факторов. Использование уязвимостей в программном обеспечении, слабых паролей, отсутствие многофакторной аутентификации.

Использование методов социальной инженерии (доверие, страх, жадность, срочность, любопытство) для манипулирования жертвами.

Отсутствие знаний о распространенных мошеннических схемах, низкий уровень компьютерной грамотности, игнорирование предупреждений.

Быстрое распространение мошеннических схем через социальные сети, электронную почту и другие онлайн-каналы.

Возможность оставаться анонимным, используя VPN, прокси-серверы и поддельные учетные записи.

Возможность охвата широкой аудитории по всему миру, увеличивая шансы на успех.

Сложная экономическая ситуация, финансовые трудности, которые делают людей более уязвимыми к мошенническим предложениям.

Современные технологии предлагают широкий спектр инструментов для борьбы с интернет-мошенничеством:

1. Использование систем обнаружения и предотвращения вторжений (IDS/IPS). Обнаружение и блокировка вредоносного трафика, попыток фишинга и других атак.
2. Анализ веб-сайтов и электронной почты. Проверка веб-сайтов на предмет подозрительности, выявление фишинговых ссылок и вредоносных вложений.
3. Использование систем многофакторной аутентификации (MFA). Добавление дополнительного уровня защиты, требующего ввода кода, отправленного на мобильный телефон или сгенерированного приложением.
4. Применение антивирусного ПО и антишпионских программ. Защита устройств от вредоносного ПО, кражи данных и других угроз.
5. Анализ поведения пользователей. Отслеживание подозрительной активности пользователей (необычные транзакции, попытки входа в систему с неизвестных устройств).
6. Разработка и использование систем искусственного интеллекта (ИИ) и машинного обучения (МО):
   a) Обнаружение фишинговых атак и спама.
   b) Выявление аномалий в транзакциях и подозрительной активности.
   c) Анализ текста и изображений для выявления мошеннических схем.
   d) Автоматическая классификация и блокировка мошеннических ресурсов.
7. Блокчейн и децентрализованные технологии. Использование блокчейна для обеспечения безопасности транзакций и защиты данных.
8. Технологии обработки естественного языка (NLP). Анализ текста, для обнаружения признаков мошенничества в онлайн-коммуникациях.
9. Оценка репутации (Reputation Management). Использование инструментов для анализа репутации продавцов, сайтов, пользователей, для повышения безопасности онлайн-транзакций.
10. Использование систем анализа трафика (Traffic Analysis). Для выявления вредоносных активностей и предотвращения кибер-атак.

Повышение осведомленности пользователей является ключевым фактором в борьбе с интернет-мошенничеством.

Проведение образовательных программ, направленных на повышение киберграмотности населения, обучение распознаванию мошеннических схем и правилам безопасного поведения в интернете. Организация информационных кампаний в СМИ, социальных сетях и других каналах коммуникации, рассказывающих о распространенных видах мошенничества и методах защиты.

Разработка и предоставление инструментов, позволяющих пользователям проверять подлинность веб-сайтов, электронных писем и других ресурсов. Использование интерактивных инструментов, таких как симуляторы фишинга, для обучения пользователей распознаванию мошеннических атак.

Создание онлайн-сообществ и форумов, где пользователи могут делиться информацией о мошеннических схемах и обсуждать методы защиты.

Создание и распространение практических руководств, содержащих советы по безопасной работе в интернете, настройке безопасности устройств и защите личной информации. Включение курсов кибербезопасности в учебные программы школ, колледжей и университетов. Поддержка этичных подходов к онлайн-поведению и соблюдению прав пользователей.

Эффективная борьба с интернет-мошенничеством требует активного участия государства и разработки соответствующего законодательства:

1. Ужесточение ответственности за киберпреступления: Введение более строгих наказаний за совершение мошеннических действий в интернете.
2. Регулирование деятельности онлайн-платформ: Обязывание онлайн-платформ (социальные сети, маркетплейсы) принимать меры по выявлению и предотвращению мошенничества, а также обеспечивать безопасность пользователей.
3. Разработка законов о защите данных и приватности: Принятие законов, обеспечивающих защиту личной информации пользователей и контроль над ее обработкой.
4. Международное сотрудничество: Укрепление сотрудничества с международными организациями и правоохранительными органами для борьбы с трансграничной киберпреступностью.
5. Создание специализированных подразделений по борьбе с киберпреступностью: Формирование специализированных подразделений в правоохранительных органах, занимающихся расследованием киберпреступлений и защитой пользователей.
6. Регулярный пересмотр законодательства: Адаптация законодательства к постоянно меняющимся методам интернет-мошенничества и развитию технологий.

Интернет-мошенничество представляет собой серьезную и постоянно растущую угрозу. Эффективная борьба с этим явлением требует комплексного подхода, сочетающего технические средства, социальные и психологические меры, а также нормативное регулирование. Реализация предлагаемых стратегий, направленных на повышение осведомленности пользователей, укрепление кибербезопасности и усовершенствование механизмов обнаружения и предотвращения мошенничества, является ключевым фактором для защиты пользователей и организаций от финансовых потерь и репутационного ущерба. Непрерывное совершенствование технологий, адаптация законодательства и развитие культуры кибербезопасности являются необходимыми условиями для обеспечения безопасного и надежного онлайн-пространства.

Список литературы

1. Конституция Российской Федерации : принята всенар. голосованием 12 дек. 1993 г. [с учетом поправок, внесенных Законами Рос. Федерации о поправках к Конституции Рос. Федерации от 30 дек. 2008 г. № 6-ФКЗ, от 30 дек. 2008 г. № 7-ФКЗ, от 5 февр. 2014 г. № 2-ФКЗ, от 21 июля 2014 г. № 11- ФКЗ] // Собрание законодательства Российской Федерации. — 2014. — № 31. — Ст. 4398.

2. Кодекс Российской Федерации об административных правонарушениях : Федер. закон от 30 дек. 2001 г. № 195-ФЗ : принят Гос. Думой 20 дек. 2001 г. : одобрен Советом Федерации 26 дек. 2001 г. : [ред. от 2 авг. 2019 г.] // Собрание законодательства Российской Федерации. — 2002. — № 1, ч. 1. — Ст. 1.

3. Об установлении ограничения на публикацию информации о залогодержателе движимого имущества в информационнотелекоммуникационной сети «Интернет» : постановление Правительства Рос. Федерации от 31 авг. 2019 г. № 1119 // Собрание законодательства Российской Федерации. — 2019. — № 36. — Ст. 5025.

4. Буянов, Д. С. Информационная безопасность в социальных сетях / Д. С. Буянов. — Текст : непосредственный // Молодой ученый. — 2018. — № 39 (225). — С. 14-16. — URL: https://moluch.ru/archive/225/52820/ (дата обращения: 01.04.2025).

5. Актуальные вопросы информационной безопасности и защиты информации : сборник научных статей / под ред. проф. Е.В. Стельмашонок, доц. И.Н. Васильевой. – СПб. : Изд-во СПбГЭУ, 2021. – 82 с. ISBN 978-5-7310-5338-9