МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Тихоокеанский государственный университет»

ВОПРОСЫ КИБЕРБЕЗОПАСНОСТИ И ПРОФИЛАКТИКА МОШЕННИЧЕСТВА. СОВРЕМЕННЫЕ ВЫЗОВЫ И РЕШЕНИЯ.

Материалы конкурса научно-практических работ и проектов студентов (курсантов) высших учебных заведений (в том числе филиалов) Дальневосточного федерального округа по вопросам кибербезопасности и профилактики мошенничества, совершенного с применением методов социальной инженерии на финансовом рынке Российской Федерации, 2025 год

Хабаровск 2025

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Тихоокеанский государственный университет»

ВОПРОСЫ КИБЕРБЕЗОПАСНОСТИ И ПРОФИЛАКТИКА МОШЕННИЧЕСТВА. СОВРЕМЕННЫЕ ВЫЗОВЫ И РЕШЕНИЯ.

Материалы конкурса научно-практических работ и проектов студентов (курсантов) высших учебных заведений (в том числе филиалов) Дальневосточного федерального округа по вопросам кибербезопасности и профилактики мошенничества, совершенного с применением методов социальной инженерии на финансовом рынке Российской Федерации, 2025 год

Хабаровск
Издательство ТОГУ
2025

ISBN 978-5-7389-4073-6

УДК 004.056:336.76:343.72
ББК Я431+Х401.114я431
В748

В748 **Вопросы кибербезопасности и профилактика мошенничества. Современные вызовы и решения**: материалы конкурса науч.-практ. работ студ. (курсант.), 2025 г. / Министерство науки и высшего образования Российской Федерации, Тихоокеанский государственный университет ; редколлегия: А. С. Соловьева (ответственный редактор) [и др.]. – Хабаровск : Издательство ТОГУ, 2025. – Текст : электронный. – 233, [1] с. – URL: https://togudv.ru/ru/library/elektronnye-izdaniya/collections/. – Дата публикации: 17.06.2025. – ISBN 978-5-7389-4073-6

В сборнике представлены материалы конкурса научно-практических работ и проектов студентов (курсантов) высших учебных заведений (в том числе филиалов) Дальневосточного федерального округа по вопросам кибербезопасности и профилактики мошенничества, совершенного с применением методов социальной инженерии на финансовом рынке Российской Федерации, проводимого Дальневосточным главным управлением Центрального банка Российской Федерации.

Излагаются материалы исследований по вопросам нормативно-правового регулирования в сфере противодействия кибермошенничеству; противодействия киберпреступности в условиях развития цифрового общества и искусственного интеллекта; психологии телефонных мошенников и их жертв.

Рекомендуется для широкого круга лиц: преподавателей и студентов вузов.

Авторы опубликованных статей несут ответственность за подбор и точность приведенных фактов, цитат, статистических данных и прочих сведений, а также за то, что материалы не содержат сведений, не подлежащих открытой публикации.

УДК 004.056:336.76:343.72
ББК Я431+Х401.114я431

Является самостоятельным электронным изданием.

Минимальные системные требования: 1) браузер GoogleChrome; 2) скорость подключения к сети Интернет – 1 Мбит/с и выше.

ISBN 978-5-7389-4073-6

Time. 2024. № 5. URL: https://cyberleninka.ru/article/n/kiberprestupleniya-v-sovremennoy-rossii (дата обращения: 06.05.2025).

4. Гончарова С. В., Полунина Е. Н. Киберпреступления и преступления по телефону // Балтийский гуманитарный журнал. 2020. № 3. URL: https://cyberleninka.ru/article/n/kiberprestupleniya-i-prestupleniya-po-telefonu (дата обращения: 06.06.2025).

5. Хачатурова С. С. Киберпреступления в информационном обществе // Проблемы Науки. 2016. № 11. URL: https://cyberleninka.ru/article/n/kiberprestupleniya-v-informatsionnom-obschestve (дата обращения: 06.06.2025).

УДК 37.025.7:004.056

Вертинова Анна Александровна,
канд. экон. наук, доцент, кафедра экономики и управления,
Владивостокский государственный университет,
г. Владивосток

Литвиненко Элеонора Дмитриевна,
студент 2 курса, группа БЭУ-23ФЭ1,
факультет «Экономика»,
Владивостокский государственный университет,
г. Владивосток

Критическое мышление как инструмент борьбы с кибермошенничеством: теоретические основы и эмпирический анализ

Аннотация: в статье рассматриваются теоретические аспекты критического мышления в качестве инструмента профилактики кибермошенничества, основные теВхники социальной инженерии. В практической части проведен эмпирический анализ на основании предложенного автором тестирования, также разработаны рекомендации по развитию критического мышления в контексте цифровой среды.

Ключевые слова: критическое мышление, кибермошенничество, социальная инженерия, киберугроза.

В современном обществе цифровые технологии стали неотъемлемой частью всех аспектов человеческой деятельности, и их интеграция в повседневную жизнь происходит с высокой скоростью. Это вызвано развитием информационно-коммуникационных технологий и ростом объемов, обрабатываемых данных. Адаптация к новым условиям требует от людей освоения новых инструментов и изменения привычек, что является сложным процессом. Важно отметить, что время, необходимое для адаптации, часто превышает темпы развития цифрового пространства, что может привести к социальным и экономическим последствиям, включая увеличение цифрового неравенства и снижение удовлетворенности пользователей. цифровые технологии стали неотъемлемой частью практически всех аспектов человеческой деятельности.

С развитием цифрового пространства и стремительным внедрением информационных технологий в различные сферы жизнедеятельности общества наблюдается не только значительное улучшение качества жизни и эффективности бизнес-процессов, но и формирование новых рисков, связанных с киберугрозами. В условиях глобальной цифровизации, когда доступ к информации и коммуникационным ресурсам становится все более простым и удобным, кибермошенничество приобретает угрожающий масштаб, представляя собой одну из наиболее актуальных проблем современности.

Недостаточная осведомленность пользователей о потенциальных угрозах и методах защиты информации способствует распространению киберпреступлений. Таким образом, кибермошенничество не только затрагивает индивидуальные интересы граждан, но и подрывает доверие к цифровым платформам и услугам, что может иметь серьезные последствия для экономики в целом.

Анализ научных источников, касающихся профилактики кибермошенничества, показал, что важнейшим инструментом является критическое мышление, однако единой методики его оценки нет. В данной статье предложена методика оценки критического мышления для профилактики кибермошенничества.

Одним из ключевых аспектов к успешной адаптации в условиях цифровизации является развитие критического мышления, которое помогает пользователям эффективно анализировать информацию, различать надежные источники от мошеннических и принимать обоснованные решения. В условиях киберугроз, таких как кибермошенничество, критическое мышление становится важным инструментом профилактики, позволяя людям не только защитить себя, но и активно участвовать в формировании безопасной цифровой среды.

Критическое мышление представляет собой способность человека обрабатывать поступающую информацию на предмет обоснованности, правдивости, адекватности.

Разберем каждую из характеристик в соответствии со словарем С.И. Ожегова [5].

Обоснованный – подтвержденный фактами, серьезными доводами, убедительный.

Правда – то, что существует в действительности, соответствует реальному положению вещей.

Адекватный – вполне соответствующий, совпадающий.

Веретенникова А.В. в своей статье приводит мнение Б. Бейера касательно отрицательного эффекта слова «критическое» относительно «мышления». Ученый подчеркивает, что многие люди переносят негативный оттенок слова «критическое» на всю концепцию критического мышления, предполагая, что оно состоит из резкой критики, негативизма и поиска ошибок. Чтобы избежать этого, ученый предлагает заменить термин «критическое мышление» «оценочным мышлением» [1]. Однако, на наш взгляд, критика является составляющей оценки, то есть существование одного невозможно без другого. Тогда, негативное восприятие слова «критическое» является признаком неразвитого критического

мышления, так как оценивается на уровне эмоций и чувств, а не фактов.

Критическое мышление является сложным процессом обработки информации, который состоит из элементов, представленных на рисунке 1.

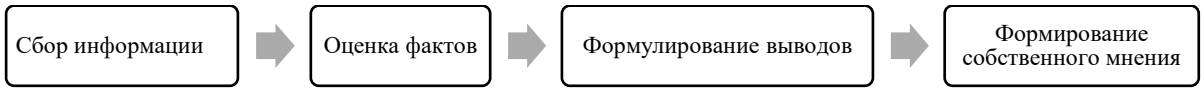

Рис. 1. Элементы критического мышления

Особенностью этих элементов является то, что их развитие происходит благодаря критическому мышлению [2].

Сбор информации, подразумевает под собой сохранение фокуса на первоначальной теме и интеграции информации из различных источников.

Под оценкой фактов понимается объективный анализ и интерпретация собранных данных.

Формулирование выводов основывается на утверждениях, поддержанных эмпирическими данными и логическими аргументациями.

Формирование собственного мнения происходит исходя из следующих факторов [6]:

– учет опыта (личного и чужого);

– исследование вопроса (источники, литература, мотивы автора, тематические обсуждения);

– принцип «непредвзятости».

Принцип «непредвзятости» состоит из следующих элементов:

– игнорирование личных предубеждений;

– учитывание причин разнящегося мнения;

– сохранения спокойствия и уважения другого мнения;

– изменение личных взглядов, при разумности.

Основным документом, устанавливающим ответственность за кибермошенничество на территории Российской Федерации, является Уголовный Кодекс РФ [8]. Тем не менее, достаточный уровень осведомленности пользователей является ключевым фактором в противодействии кибермошенничеству.

Чаще всего киберпреступники используют основы социальной инженерии для совершения киберпреступлений. По данным Positive Technologies, социальная инженерия используется в 92% кибератак на физических лиц и в 37% кибератак на компании [7].

Социальная инженерия представляет собой метод манипуляции людьми с целью получения их конфиденциальной информации, доступа к ресурсам или других представляющих ценность объектов [10]. В дополнение к методам социальной инженерии злоумышленники часто эксплуатируют недостаток знаний у пользователей. Быстрые темпы развития технологий приводят к тому, что многие рядовые пользователи остаются неосведомленными о некоторых типах угроз, таких как скрытая загрузка вредоносного программного обеспечения. Не все осознают ценность своих персональных данных, например, номера телефона, что делает их уязвимыми и затрудняет защиту как собственных интересов, так и конфиденциальной информации. Атака на основе социальной

инженерии состоит из стадий представленных на рисунке 2.

Рис. 2. Стадии атаки с применением социальной инженерии

Подготовка – сбор информации о жертве или группе, к которой она принадлежит.

Проникновение – установление контакта и завоевание доверия.

Эксплуатация – поиск и использование уязвимости жертвы.

Исчезновение – прекращение общения с жертвой после достижения поставленной цели. Эти стадии могут содержаться как в одном письме на электронную почту, так и длиться на протяжении нескольких месяцев по переписке [10].

Основные техники социальной инженерии представлены на рисунке 3.

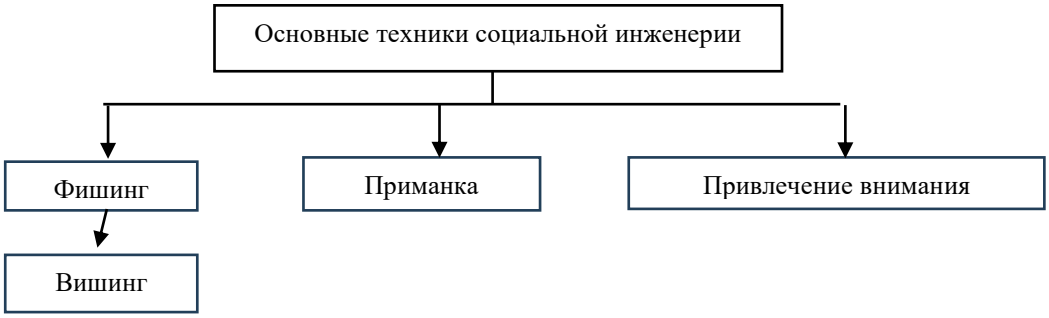

Рис. 3. Основные техники социальной инженерии

Подробнее рассмотрим, каждый из них.

Фишинг использует поддельные электронные письма, которые выглядят подлинными и якобы поступают из законных источников, таких как финансовые учреждения, сайты электронной коммерции и т.д. чтобы пользователи переходили на мошеннические веб-сайты по ссылкам, указанным в фишинговом письме. Мошеннические веб-сайты предназначены для имитации внешнего вида веб-страницы реальной компании [3].

Вишинг основан на социальной инженерии голосового канала связи и подразумевает мошеннические звонки от имени сотрудников технической поддержки, банков, страховых и телекоммуникационных компаний. Хакеры используют различные техники социального воздействия для получения данных карт, паролей и банковских счетов от неосведомленных пользователей [7].

Приманка – мошенники используют различные устройства, такие как флешки или power bank, в качестве приманок. Эти устройства заражены вирусами. Когда кто-то находит и подключает их к своему компьютеру, происходит заражение, что позволяет злоумышленникам получить доступ к данным на устройстве [7].

Привлечение внимания – мошенники размещают в интернете материалы,

которые выглядят безобидно, например, простые тесты или опросы. Чтобы пройти тест или получить результаты, они просят предоставить личные данные, которые затем могут быть использованы для кибератак [7].

Критическое мышление играет ключевую роль в распознании и предотвращении киберугроз. Так как мошенники активно используют эмоциональные манипуляции, а критическое мышление в свою очередь подразумевает безэмоциональную оценку информации. Важно оценивать критическое мышление не отдельно, а непосредственно в контексте цифровой среды.

В предлагаемую методику входит:

– определение личного уровня критического мышления во время использования цифровых технологий;

– рекомендации по развитию критического мышления в условиях цифровой среды.

Для того чтобы оценить уровень критического мышления в контексте противодействия кибермошенникам, был разработан тест, который позволит понимать от чего отталкиваться, при развитии критического мышления. В тесте использовался метод сценарного анализа, подразумевающий под собой моделирование киберугроз и представлены варианты действия при этих сценариях. На основе результатов теста сформированы рекомендации по способам развития критического мышления как инструмента профилактики кибермошенничества [4].

Тестировании было проведено на фокус-группе, выбор участников которой основан на следующих критериях:

1) возраст от 16-60+;

2) слышали о понятии «критическое мышление»;

3) сталкивались с кибермошенничеством один раз и более;

В качестве респондентов были выбраны 70 экспертов следующих возрастных групп 16-21; 22-27; 28-35; 46-60; 60+. Максимально возможный балл за тестирование – 20 баллов.

Если тестируемый набрал от 1 до 4 баллов (1-2 верных ответа) – такой результат соответствует низкому уровню критического мышления.

Если тестируемый набрал от 5 до 8 баллов (2-4 верных ответа) – такой результат соответствует уровню критического мышления ниже среднего.

Если тестируемый набрал от 9 до 12 баллов (5-6 верных ответа) – такой результат соответствует среднему уровню критического мышления.

Если тестируемый набрал от 13 до 16 баллов (7-8 верных ответа) – такой результат соответствует высокому уровню критического мышления.

Если тестируемый набрал от 17 до 20 баллов (9-10 верных ответа) – такой результат соответствует очень высокому уровню критического мышления.

На основании результатов опроса была построена столбчатая диаграмма, представленная на рисунке 4.

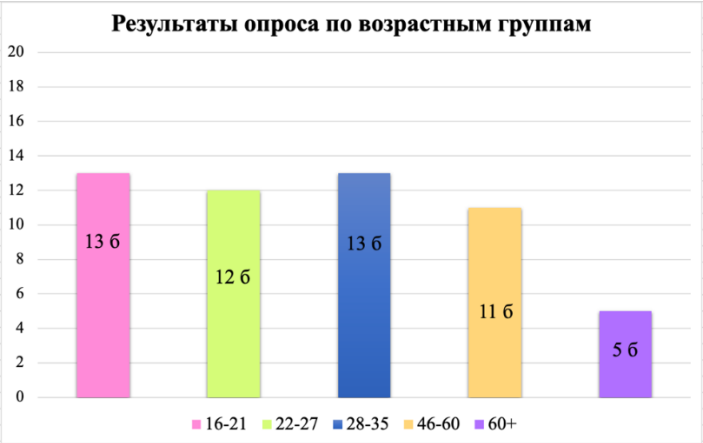

Рис. 4. Результаты опроса по возрастным группам

Таким образом наиболее высокий уровень критического мышления имеют возрастные группы 16-21 и 28-35. Наиболее низкий уровень критического мышления наблюдается у возрастной группы 60+.

Рекомендации по развитию критического мышления в контексте цифровой среды включают в себя:

– развитие цифровой грамотности (для низкого и ниже среднего уровней);

– постоянный мониторинг новых способов кибермошенничества (для среднего уровня);

– формирование собственного мнения (для низкого и ниже среднего уровней);

– кибергигиена (для всех уровней);

– участие в мероприятиях, направленных на профилактику кибермошенничества (для всех уровней);

– обучения методам распознавания манипуляций (для всех уровней).

Развитие цифровой грамотности: Обучение основам безопасного поведения в интернете, включая использование сложных паролей, распознавание фишинговых писем и защиту личной информации. Чем больше люди знают о цифровом мире, тем легче им будет критически оценивать информацию и избегать ловушек мошенников.

Мониторинг новых способов кибермошенничества: Разбор реальных примеров кибермошенничества, включая их механизмы и последствия. Это поможет людям лучше понять, как мошенники действуют, а также развить критическое отношение к подобным ситуациям.

Формирование собственного мнения: когда человек умеет формировать собственное мнение, он становится более критичным к информации, которую получает. Это позволяет ему задавать вопросы, проверять факты и не принимать все на веру, что особенно важно в условиях распространения ложной информации и манипуляций.

Соблюдение принципов кибергигиены [9] значительно снижает вероятность того, что пользователь станет жертвой кибермошенничества, делая его более защищенным в цифровом пространстве.

Участие в мероприятиях, направленных на профилактику кибермошенничества включает в себя не только посещение мероприятий на данную тематику, но и поощрение открытых дискуссий о киберугрозах и мошенничестве в семьях, на рабочих местах и в учебных заведениях. Это поможет людям делиться опытом и знаниями, а также развивать навыки критического анализа через

взаимодействие.

Обучения методам распознавания манипуляций: Обучение тому, как мошенники используют социальную инженерию для манипуляции людьми. Знание этих приемов поможет людям быть более настороженными и критически воспринимать информацию.

В результате исследования было установлено, что наиболее высокий уровень критического мышления в контексте цифровой среды имеют молодые люди в возрасте от 16 до 35 лет. Более низкие показатели имеют старшие возрастные группы в возрасте от 46 до 60+. Несмотря на это, показатели молодых возрастных групп, являются относительно высокими, так как, максимальное количество баллов за тестирование – 20 баллов. Таким образом, подтверждается актуальность развития критического мышления как инструмента профилактики кибермошенничества. Поскольку развитое критическое мышление является ключевым фактором в противодействии кибермошенничеству. Были разработаны и предложены рекомендации по развитию критического мышления непосредственно в контексте цифровой среды.

Библиографический список

1 Веретенникова А.Е. Критическое мышление поколения «Цифровых аборигенов» // Crede Experto: транспорт, общество, образование, язык. 2023. № 4. URL: https://cyberleninka.ru/article/n/kriticheskoe-myshlenie-pokoleniya-tsifrovyh-aborigenov/viewer (дата обращения: 12.02.2025).

2 Воронов А. Критическое мышление: что это, зачем нужно и как развить его у ребёнка? // iSmart – образовательная платформа. 2024. URL: https://www.ismart.org/library/kriticheskoe-myshlenie-chto-eto-zachem-nuzhno-i-kak-razvit-ego-u-rebyenka (дата обращения: 12.02.2025).

3 Завьялов А. Н. Интернет-мошенничество (фишинг): проблемы противодействия и предупреждения // Baikal Research Journal 2022. № 2. URL: https://cyberleninka.ru/article/n/internet-moshennichestvo-fishing-problemy-protivodeystviya-i-preduprezhdeniya/viewer (дата обращения: 21.02.2025).

4 Литвиненко Э.Д. Критическое мышление против кибермошенников // Конструктор тестов «Online Test Pad». URL: https://onlinetestpad.com/bhk5c6thopgsi (дата обращения: 25.02.2025).

5 Толковый словарь Ожегова. URL: https://slovarozhegova.ru (дата обращения: 10.02.2025).

6 Позднякова Е. И. Немного о формировании собственного мнения. С семинара по работе с психической травмой // b17.ru – сайт психологов 2019. № 1. URL: https://www.b17.ru/article/128083/ (дата обращения: 12.02.2025).

7 Социальная инженерия. Кибрарий. Интерактивный словарь // Сбербанк : сайт. URL: https://www.sberbank.ru/ru/person/kibrary/vocabulary/socialnaya_inzheneriya (дата обращения: 16.02.2025)

8 Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 28.02.2025) // Собрание законодательства РФ. 1996. № 25. Ст. 2954 ; 2025. № 9. Ст. 860.

9 Цифровая гигиена поможет обеспечить безопасность в сети // АО «Лабаротория Касперского». URL: https://www.kaspersky.ru/resource-center/preemptive-safety/cyber-hygiene-habits# (дата обращения: 23.02.2025).

10 Что такое социальная инженерия? // АО «Лабаротория Касперского». URL: https://www.kaspersky.ru/resource-center/definitions/what-is-social-engineering (дата обращения: 19.02.2025).