

© Н.А. Боробов, А.С. Зуфарова

Научная статья  
УДК 37.01:007**ФОРМИРОВАНИЕ ИНФОРМАЦИОННОЙ ГРАМОТНОСТИ ОБУЧАЮЩИХСЯ КАК  
ФАКТОР ПРОТИВОДЕЙСТВИЯ КИБЕРПРЕСТУПНОСТИ НА ОСНОВЕ  
АВТОМАТИЗИРОВАННОГО ВЫЯВЛЕНИЯ ФЕЙКОВЫХ АККАУНТОВ В  
СОЦИАЛЬНОЙ СЕТИ ВКОНТАКТЕ**

Н.А. Боробов, А.С. Зуфарова

**Боробов Никита Андреевич,**  
студент, Тихоокеанский государственный  
университет, Хабаровск, Россия.  
2020102113@togudv.ru**Зуфарова Анна Сергеевна,**  
старший преподаватель кафедры математических  
методов защиты информации и компьютерной  
безопасности, Тихоокеанский государственный  
университет, Хабаровск, Россия.  
006694@togudv.ru

**Аннотация.** В условиях роста активности киберпреступников, использующих поддельные учетные записи для распространения вредоносного контента и осуществления кибератак, применение современных технологий для защиты и обучения пользователей приобретает особую значимость. В статье рассматривается проблема противодействия киберпреступности в образовательной среде через формирование цифровой и информационной грамотности обучающихся. Обосновывается необходимость интеграции педагогических и технологических решений, направленных на выявление фейковых аккаунтов в социальной сети «ВКонтакте». Одним из ключевых методов противодействия этой угрозе является использование автоматизированных систем обнаружения поддельных учетных записей. Автоматизированная система осуществляет анализ поведенческих паттернов учетных записей и выявляют признаки их подозрительности. В основе их работы лежат различные алгоритмы и методики. В данной статье речь пойдет о реализации автоматизированной обучающей онлайн-платформы для выявления фейковых аккаунтов в социальной сети/мессенджере ВКонтакте средствами OSINT. В работе описана основная информация о продукте, о механизмах его работы и о преимуществах данного решения. Показаны результаты социального опроса. Рассмотрена актуальная проблема формирования цифровой и информационной грамотности среди обучающихся как важного аспекта противодействия современным видам киберпреступности. Рассматриваются методы и подходы, применяемые в образовательном процессе для повышения уровня цифровой грамотности учащихся, особое внимание уделено вопросу автоматизированного выявления фейковых аккаунтов в популярной российской социальной сети ВКонтакте. Показано, что интегрированная методика обучения, объединяющая классические педагогические приемы и современные цифровые технологии, позволяет подготовить молодое поколение к безопасному взаимодействию в виртуальном пространстве и уменьшить риски вовлечения в противоправные действия.

**Ключевые слова:** *фейковые аккаунты, ВКонтакте, обучение, социальная сеть, информационная безопасность, онлайн-платформы.*

**Библиографическая ссылка:** *Боробов Н.А., Zufarova A.S. Формирование информационной грамотности обучающихся как фактор противодействия киберпреступности на основе автоматизированного выявления фейковых аккаунтов в социальной сети ВКонтакте // ЦИТИСЭ. 2026. № 1. С. 740-755.*

Research Full Article

UDC 37.01:007

**DEVELOPING DIGITAL AND INFORMATION LITERACY IN STUDENTS AS A  
FACTOR IN COUNTERING CYBERCRIME BASED ON THE AUTOMATED  
IDENTIFICATION OF FAKE ACCOUNTS ON THE VKONTAKTE SOCIAL NETWORK**

N.A. Borobov, A.S. Zufarova

**Nikita A. Borobov**

Student, Pacific State University, Khabarovsk,  
Russian Federation.  
2020102113@togudv.ru

**Anna S. Zufarova,**

Senior Lecturer at the Department Mathematical  
Methods of Information Security and Computer  
Security, Pacific State University, Khabarovsk,  
Russian Federation.  
006694@pnu.edu.ru

**Abstract.** *With cybercriminals using fake accounts to distribute malicious content and carry out cyberattacks on the rise, the use of modern technologies for user protection and training is becoming increasingly important. This article examines the problem of combating cybercrime in the educational environment by developing students' digital and information literacy. It also substantiates the need to integrate pedagogical and technological solutions aimed at identifying fake accounts on the VKontakte social network. One key method for countering this threat is the use of automated account detection systems. Automated systems analyze account behavior patterns and identify suspicious signs. They rely on various algorithms and methodologies. This article discusses the implementation of an automated online training platform for identifying fake accounts on the VKontakte social network/messenger using OSINT. The paper provides basic information about the product, its operating mechanisms, and the advantages of this solution. The results of a social survey are also presented. This article examines the pressing issue of developing digital and information literacy among students as an important aspect of countering modern forms of cybercrime. It explores methods and approaches used in the educational process to improve students' digital literacy, with particular attention paid to the automated detection of fake accounts on the popular Russian social network VKontakte. It demonstrates that an integrated teaching methodology, combining classical pedagogical techniques and modern digital technologies, helps prepare the younger generation for safe interaction in the virtual space and reduces the risk of involvement in illegal activities.*

**Keywords:** *Fake accounts, VKontakte, training, social network, information security, online platforms.*

**For citation:** Borobov, N. A., & Zufarova, A. S. (2026). Formation of information literacy of students as a factor in countering cybercrime based on automated detection of fake accounts on the social network VKontakte. *CITISE, 1*, 740–755. (In Russian).

### **Введение.**

Цифровая эпоха ставит перед обществом новые вызовы, связанные с растущим уровнем преступлений в информационно-коммуникационной среде. Один из наиболее острых аспектов современной киберпреступности — распространение фейковых аккаунтов в социальных сетях, используемых злоумышленниками для мошенничества, шантажа, дезинформации и иных противоправных деяний [1]. Особенно актуальной эта проблема становится в молодежной среде, где школьники и студенты активно пользуются социальными сетями, такими как ВКонтакте. Проблема усугубляется отсутствием достаточной цифровой и информационной грамотности среди подростков и молодежи, что делает их легкой мишенью для преступников [12]. Чтобы противостоять этому, необходимы комплексные меры, направленные на воспитание культуры безопасного поведения в интернете и активное внедрение современных технических решений для автоматического выявления фейковых профилей.


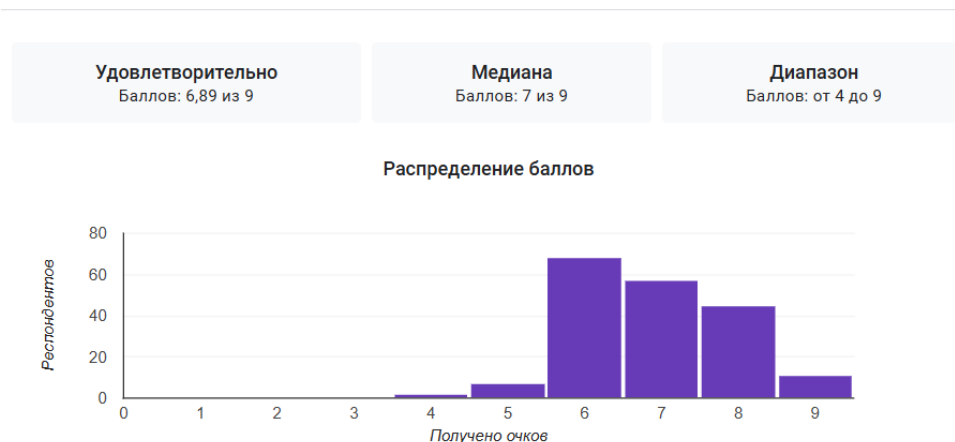
Современные мессенджеры стали не только удобным инструментом для общения, но и платформой для введения бизнеса, распространения информации и организации сообществ. Киберпреступники активно используют социальные сети и мессенджеры для проведения атак, включая фишинг, мошенничество и распространители вредоносного ПО. Фейковые аккаунты играют ключевую роль в таких операциях, позволяя преступникам маскироваться под доверенные лица или организации. По данным лаборатории Касперского, к 2025 году доля фейковых аккаунтов в интернете составляет от 5 до 15 %, что свидетельствует о масштабности проблемы и необходимости её системного решения [2].

Для эффективного противодействия таким угрозам необходим комплексный подход, включающий разработку автоматизированных систем распознавания фейков. Особую сложность представляет выявление фейковых аккаунтов во ВКонтакте, где сохраняется возможность анонимного взаимодействия, а традиционные методы проверки ограничены. Создание и распространение таких аккаунтов несёт угрозу как для обычных пользователей, так и для бизнеса и сообществ, включая риски финансовых потерь, утечки личных данных, манипуляций с репутацией и распространения недостоверной информации.

### **Социальный опрос, анализ данных.**

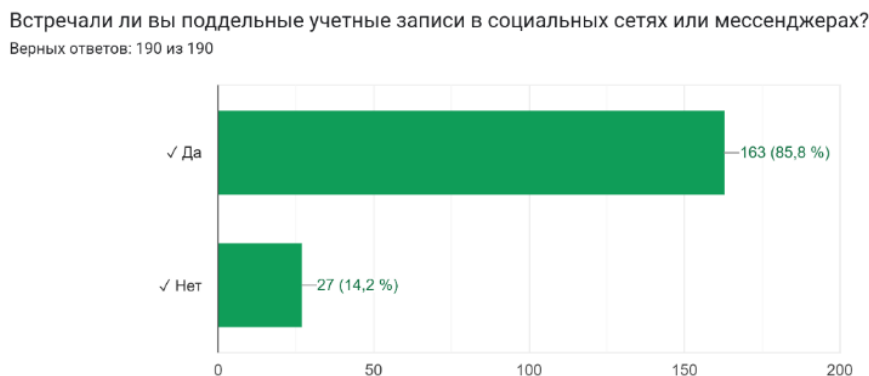
Проведение социального опроса имеет свою ценность. Ведь по средствам статистики появляется возможность сделать выводы об информационной грамотности населения в сфере поддельных аккаунтов, а также подтвердить актуальность темы.

В опросе приняли участие 191 человек, в возрасте от 15 до 60 лет. Опрашиваемым предлагался ряд вопросов. Анализ ответов опрошенных был начат с статистической столбчатой диаграммы распределения баллов. Средним значением оказалось 7 баллов из 9, что свидетельствует об осведомленности граждан с данной проблемой. Статистика приведена ниже на рисунке 1.

 Статистика


**Рисунок 1** – Диаграмма распределения баллов

Более 85-ти процентов опрошенных встречали фейковые аккаунты в социальных сетях, согласно диаграмме на рисунке 2.



**Рисунок 2** – Статистика взаимодействия опрошенных с фейковыми аккаунтами

А также, более 80-ти процентов пользователей могут отличить фейковый аккаунт от рядового. Но почти 20 процентов опрошенных имеют с этим сложности. А вот на практические вопросы большинство пользователей не смогли ответить верно. Хотя пользователи осведомлены о данной проблеме и теоретически имеют представление о фейковых аккаунтах и мошенничестве, соответственно, на практике возникают сложности, и многие пользователи остаются уязвимыми и могут стать непосредственной жертвой данных аккаунтов.

На вопрос «Какие бы советы могли дать другим пользователям, чтобы избежать потерь?» было дано большое количество ответов, которые показывают, что пользователи на собственном опыте или опыте близких людей, знакомых, сделали выводы и владеют необходимой информацией в теории, а кто-то и на практике, для противостояния подобным учетным записям в сети.

Большинство пользователи рекомендовали «Быть внимательными», «Не доверять подозрительным аккаунтам в сети», в том числе «Минимизировать общение с подобными аккаунтами».

С теоретическими познаниями у опрошенных все хорошо, а вот на очередные практические вопросы большинство пользователей не смогли ответить верно или ответили

частично верно. На вопрос, «Вам в мессенджере пишет человек, который представляется вашим директором» с дополнительными вводными данными, большинство ответили верно «Свяжитесь с директором через его старый аккаунт или по телефону». Но, силами пользователя, который распознал, что данный аккаунт фейковый могли быть предприняты дополнительные меры, например «Сообщить о возможном фейковом аккаунте в службу поддержки мессенджера». Это бы позволило проверить или даже заблокировать аккаунт на более высоком уровне, а значит предотвратить мошеннические действия данного аккаунта в отношении других пользователей. Пример заданного вопроса, представлен на рисунке 3.



**Рисунок 3** – Статистика распознавания признаков фейкового аккаунта пользователями

Проведенный опрос дал возможность оценить осведомленность граждан и их способность противостоять фейковым учетным записям. Данный опрос подтверждает актуальность выбранной мной темы. Хотя большинство пользователей теоретически подкованы информацией, на практике могут совершить и, к сожалению, совершают ошибки и теряют драгоценную информацию, денежные средства и аккаунты.

#### **Основная часть.**

Фейковые аккаунты создаются для трех основных целей. Фейки часто используются для мошенничества. Это может быть как классический фишинг, так и социальный инжиниринг. В последнем случае через фейк к вам входят в доверие, чтобы потом обмануть. Так могут делать и в соцсетях, и, например, в дейтинг-сервисах. Количество преступлений в сфере онлайн-знакомств растет с каждым годом.

Отдельная опасная категория – груминг. В этом случае взрослые выдают себя за ровесников детей, чтобы вступать с ними в контакт. Они ведут доверительное общение, постепенно склоняют к встрече или просят отправить интимные фото и видео [4].

Навязать мнение или услуги. Существуют так называемые ботофермы — большие сети фейков, которые работают как единый организм. Их применяют для накрутки лайков, подписчиков, просмотров, комментариев и голосов в онлайн-опросах. А еще их активно используют в информационных войнах, чтобы создать иллюзию популярности того или иного мнения, распространить фейковые новости, настроить общественность против оппонентов или проголосовать на выборах за определенного кандидата [5]. Ботов можно узнать по общему сценарию коммуникации, который в народе еще называют «методичкой».

Их нередко используют для продвижения. Вы наверняка видели назойливые аккаунты вроде «НАТАЛЬЯ ПРОДАЖИ НА МАРКЕТПЛЕЙСАХ», которые спамят в комментариях в телеграм-каналах под видом органичных реплик. А в англоязычном «Твиттере» под вирусными твитами полно порноботов.

Кроме того, фейковые аккаунты имитируют лояльных клиентов — они пишут восторженные отзывы и советуют друзьям товары и услуги. Они могут быть частью схем с конкурсами: создаются десятки профилей, чтобы выиграть приз или продвинуть пост. Настоящие пользователи верят, что бренд популярен, и интересуются им.

Сохранить анонимность. Фейковые аккаунты могут использоваться и в более нейтральных целях — например, чтобы обезопасить себя. Некоторые создают отдельные анонимные профили, чтобы читать новости, комментировать или вести блог, не боясь общественного осуждения и угроз для своей карьеры. А кто-то не хочет оставлять большой цифровой след [6].

Часто за фейковыми аккаунтами скрываются боты, в том числе созданные злоумышленниками. Они могут преследовать разные цели, например: создание эффекта мнимой популярности человека или движения; политические манипуляции (выборы, митинги); манипулирование финансовыми рынками; попытки заставить других замолчать; распространение спама и фишинга [7].

Боты, как и обычные пользователи, могут ставить лайки, репостить и комментировать публикации в социальных сетях. Особенно опасны боты, которые умело маскируются под реальных пользователей и принимают активное участие в обсуждениях.

Однако не все боты — обманщики: некоторые служат благим целям и не скрывают, что они боты. Равно как и не все фейковые аккаунты — боты: за некоторыми стоит человек. Например, некоторые пользователи создают подставные или дополнительные учетные записи специально, чтобы критиковать других или хвалить себя.

Боты, которые используются для накрутки просмотров и твитов, обычно входят в состав ботнета, или бот-сети. Все они действуют по одному алгоритму, выбирая одинаковые темы или хештеги. Бот-тролли используются злоумышленниками, чтобы сеять хаос и недоверие. Они не только пытаются привести к расколу в сообществе, но и внушают участникам, что правды нигде не найти [8].

Для эффективного противодействия киберпреступности необходимо использовать не только обучение цифровой гигиене, но и современные технологии, в том числе для выявления фейковых аккаунтов в мессенджерах [15]. Это особенно важно, учитывая, что злоумышленники часто используют поддельные аккаунты для распространения вредоносного контента, фишинга и других видов киберпреступлений. Одним из способов борьбы с фейковыми аккаунтами является использование автоматизированных систем, которые могут анализировать поведение аккаунтов и выявлять подозрительные признаки. Такие системы могут использовать различные алгоритмы и методы.

Параллельно с разработкой технических решений необходимо усиливать воспитательную работу с молодежью. Школы и университеты должны уделять больше внимания вопросам цифровой грамотности, развивая компетенции обучающихся в понимании особенностей функционирования социальных сетей и принципов безопасного поведения в виртуальной среде [3]. Педагогическим коллективам необходимо вести активную профилактику, формируя правильное представление о киберугрозах и прививая навыки разумного потребления информации. Родителей также необходимо привлекать к участию в формировании грамотности детей и подростков [3; 4].

Нами был разработан продукт для автоматизации выявления фейковых аккаунтов под названием «Phantom» (рисунок 4). Он поможет в обучении учащихся на уроке информатики, информационной безопасности или на дополнительных уроках по цифровой гигиене [13]. Продукт представлен для пользователя в виде удобной web конфигурации с возможностью использования поддержки 24/7.

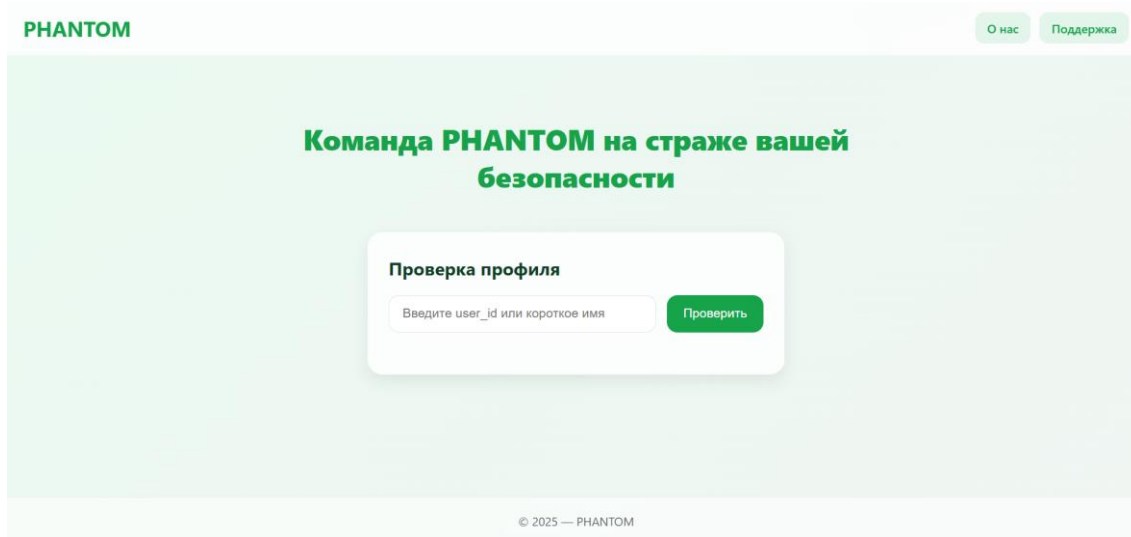


Рисунок 4 - Основная страница сайта

Цель обучающей платформы — это повышение уровня цифровой грамотности учащихся, молодежи пользователей ВКонтакте. А также формирование навыков быстрого и точного выявления фейковых аккаунтов. Ознакомление с основными правилами безопасного поведения в социальных сетях и предоставление рекомендаций по профилактике киберпреступности. Основными потребителями платформы могут стать: школьники и студенты, активные пользователи социальных сетей; родители и учителя, стремящиеся следить за безопасностью своих детей и подопечных, а также специалисты сферы кибербезопасности, желающие расширить свои профессиональные компетенции [9].

Данное решение основывается на сборе публичных данных пользователя и их анализе. Основной функционал реализован на языке программирования Python с использованием микрофреймворка Flask. Frontend реализован на языке гипертекстовой разметки html с применением каскадных таблиц стилей css и интерпретируемого языка программирования js. В реализации функционала использовался сторонний API от ВКонтакте. Это необходимо для легального сбора данных о пользователях. Для ознакомления, на рисунке 5 представлена схема архитектуры ПС.



Рисунок 5 - Схема архитектуры ПС Phantom

Далее были рассмотрены механизмы сбора данных и их анализа в удобном табличном формате. Необходимые данные собираются по средствам взаимодействия реализованных нами функций и API ВКонтакте. На данный момент происходит сбор следующих данных: ID, статус

онлайн/не онлайн, город, страна, пол, день рождения, семейное положение, подписчики, статус пользователя, работа / учеба, группы, возраст друзей пользователя. Также реализован сбор фотографии профиля для дальнейшего анализа. Для ознакомления, на рисунке 6 представлена визуальная схема взаимодействия компонентов ПС.



**Рисунок 6** - Схема взаимодействия компонентов ПС

Фейковые аккаунты во ВКонтакте, создаваемые как людьми, так и автоматизированными ботами, часто обладают характерными признаками, позволяющими их выявлять. Рассмотрим основные из них [10; 11].

1. Имя и username: неестественные или странные комбинации: случайные наборы букв и цифр, чрезмерно длинные или слишком «идеальные» имена; несоответствие имени и активности: имя указывает на взрослого человека, а контент аккаунта явно детский или наоборот; массовое повторение username: фейковые аккаунты часто используют похожие или идентичные схемы имен.

2. Фотография профиля: стоковые или украденные изображения: фото знаменитостей, моделей, генеративные изображения или взятые из интернета; отсутствие фотографии или слишком нейтральный аватар (например, просто цветной фон, символ); частая смена фото — признак автоматизированного управления аккаунтом.

3. Активность и поведение: минимум личного контента: отсутствие постов, комментариев или публикаций на стене; шаблонные действия: одинаковые комментарии, лайки или репосты на разных страницах; массовые сообщения и ссылки: отправка однотипных сообщений незнакомым пользователям.

4. Связи и сеть контактов: подозрительные друзья и подписчики: многие из них сами имеют признаки фейковых аккаунтов; отсутствие реальных взаимодействий: нет совместных фото, отметок «Мне нравится» или диалогов с живыми пользователями.

5. Технические признаки: недавнее создание аккаунта с высокой активностью; использование однотипных ссылок, шаблонных описаний или одинаковых биографий.

Первичная проверка имени, username и фотографии позволяет быстро выявлять подозрительные профили, а комплексная оценка активности и связей повышает точность идентификации фейковых аккаунтов.

Ниже представлена проверка пользователя по id. Можно увидеть основную информацию об учетной записи. Цветная шкала фейковости свидетельствует о том, что вероятность фейковости данного аккаунта равна 5%, что очень низко. А значит аккаунт, с

высокой вероятностью принадлежит обычному пользователю. Так же показан результат большого процента, фейкового аккаунта. Ознакомиться с выводом результатов можно на рисунке 7. Представлено два аккаунта. Один подозрение не фейковый аккаунт, а другой обычного пользователя.

**Проверка профиля**

id417711419

**Nikita Borobov** (@id417711419)

ID: 417711419    Онлайн: Нет

Город: Khabarovsk    Страна: Россия

Пол: Мужской    День рождения: 27.1.2003

Семейное положение: Не указано

Подписчики: 443    Статус:

Работа / учеба: Nikita Borobov - Идеальный мужской фотограф

Группы: 102

club157369801   club10362317   club60114472

club38583067   club18954214

*Первые 5 групп из списка\**

**Риск фейковости: Низкий (5/100)**

Обоснование:

- Отсутствует статус

**Возрастной анализ друзей:** Возраст друзей примерно соответствует возрасту пользователя (**Низкий**)

Из кэша: Нет

**Nikita Kruglov** (@id212358407)

ID: 212358407    Онлайн: Нет    Город: —

Страна: —    Пол: Мужской

День рождения: Не указан

Семейное положение: Не указано

Подписчики: 286    Статус:

Работа / учеба: —    Группы: 0

**Риск фейковости: Средний (57/100)**

Обоснование:

- Нет фотографии профиля
- Не указана дата рождения
- Не указан город и страна
- Отсутствует статус
- Не указано образование
- Не указана работа или деятельность

**Возрастной анализ друзей:** Нет данных (**Неизвестно**)

Из кэша: Нет

**Рисунок 7 -.** Результат проверки профиля по id

Помимо общей информации со страницы пользователя происходит сбор данных о количестве групп пользователя и реализована возможность сравнивать возраст пользователя с возрастом друзей. Последнее может свидетельствовать об аномалии. Далее для обучения учащихся в определении фейкового аккаунта, можно использовать другие функции нашего приложения для обучения пользователей.

Рассмотрим работу онлайн-платформу «Phantom». Пользователь заходит на стартовую страницу приложения и после ввода id, пользователь нажимает кнопку «Проверить». Если id или username не указаны в поле, то выводится соответствующее уведомление, представленное на рисунке 8.

**Проверка профиля**

Введите user\_id или короткое имя

**!** Вы пропустили это поле.

**Рисунок 8 –** Обработка данных в поле для ввода

После ввода id, нажимая кнопку проверки необходимо подождать, пока сервер обратиться в ВКонтакте и запросит данные, занимает до 15 секунд. Далее в виде дашборда отображается основная информация о пользователе с фотографией слева, справа граф друзей по населенным пунктам. Ознакомиться можно на рисунке 9.

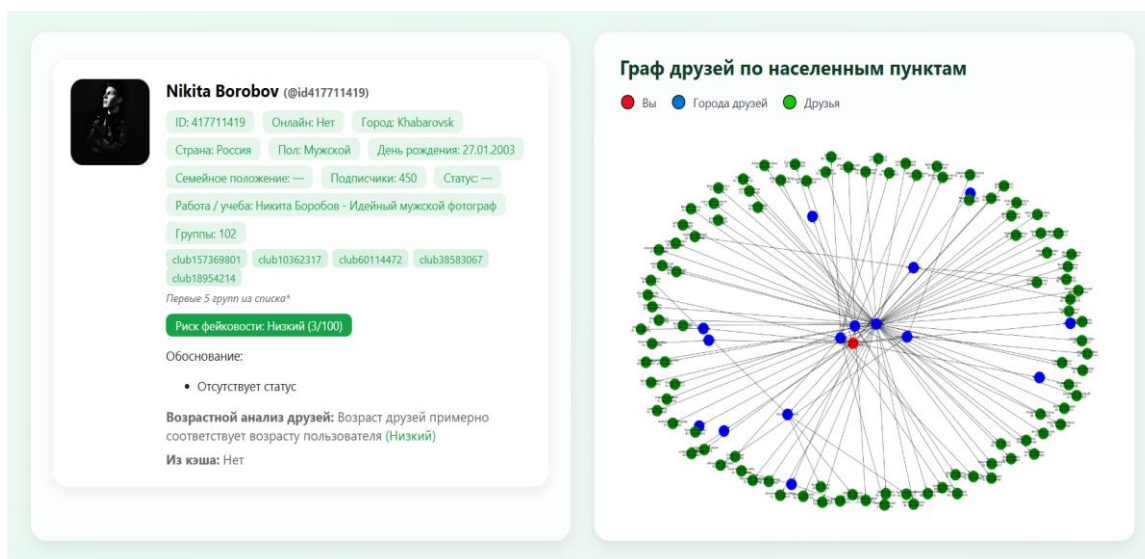


Рисунок 9 – Дашборд с данными пользователя и анализом + граф

Граф отображает красным цветом пользователя, которого мы проверяем с указанием имени, фамилии и id. Синим цветом указаны города, где проживают друзья и зеленым сами друзья с именем, фамилией и id. Граф является ориентированным. Для удобства восприятия отображается выборка из 100 первых друзей. Этих данных может быть достаточно, чтобы сделать первые выводы. Ознакомиться с данными графа можно на рисунках 10 и 11.

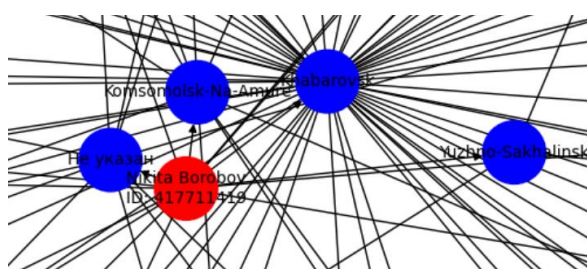


Рисунок 10 – Граф с информацией проверяемого пользователя и городами

Граф друзей по населенным пунктам

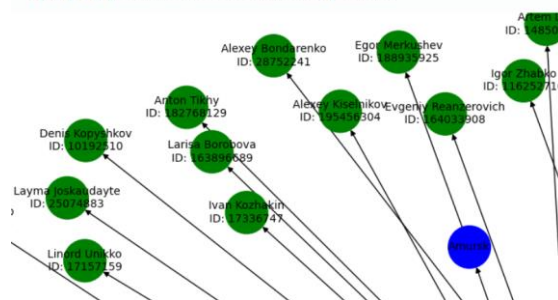


Рисунок 11 – Граф с информацией друзей пользователя и городами

Далее обратимся к модулю с анализом изображения. На рисунках 12-14 представлены критерии проверки, их значения и информация об анализе. Ниже указано значение риска возможной генерации фото нейросетью. Хотелось бы заметить отработку функции «Цветовой баланс». Фотография действительно черно-белая, соответствующий комментарий указан в выводе. По итогам проверки отклонений по профилю не было выявлено. Риски фейковости низкие.

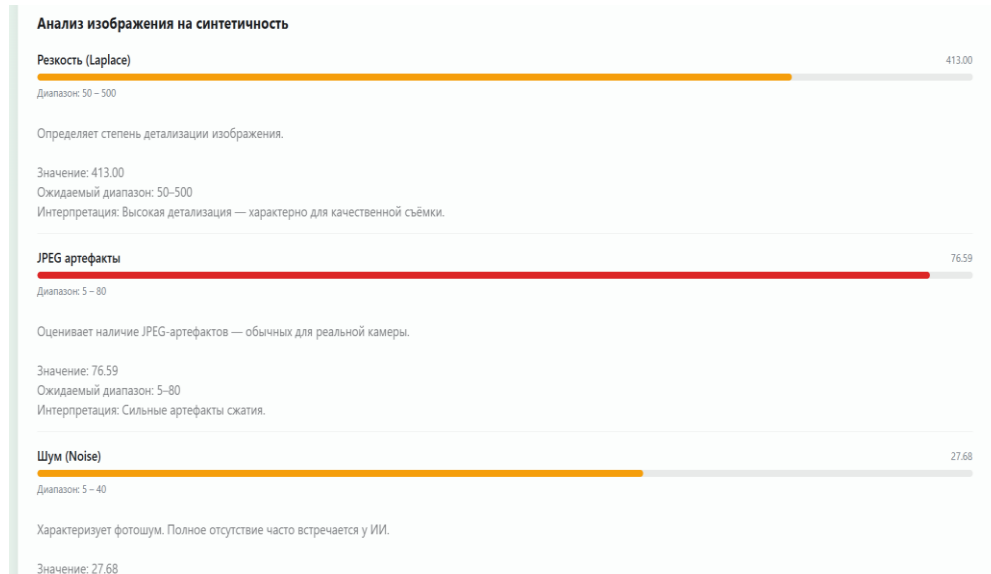


Рисунок 12 – Анализ изображения на возможную генерацию часть 1

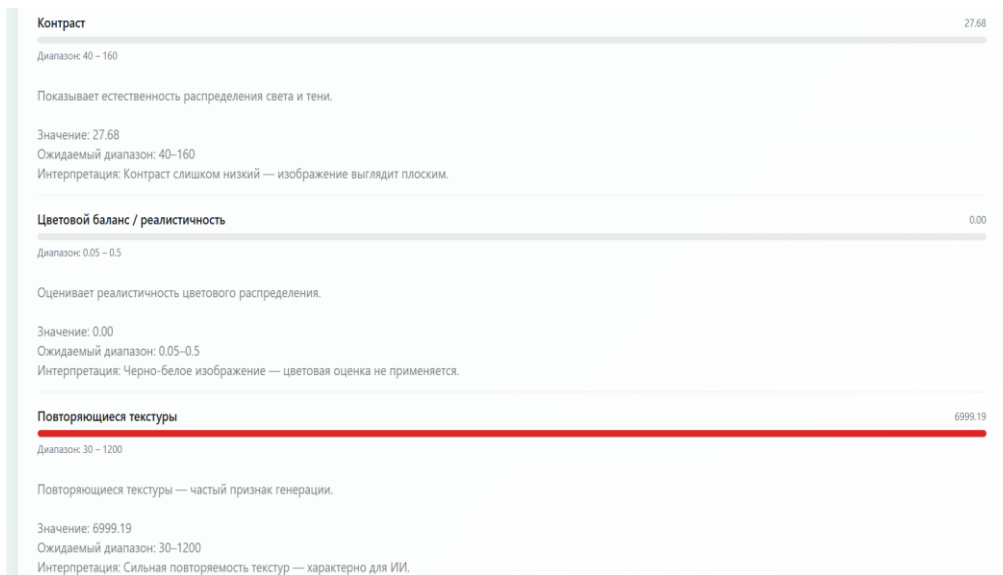


Рисунок 13 – Анализ изображения на возможную генерацию часть 2

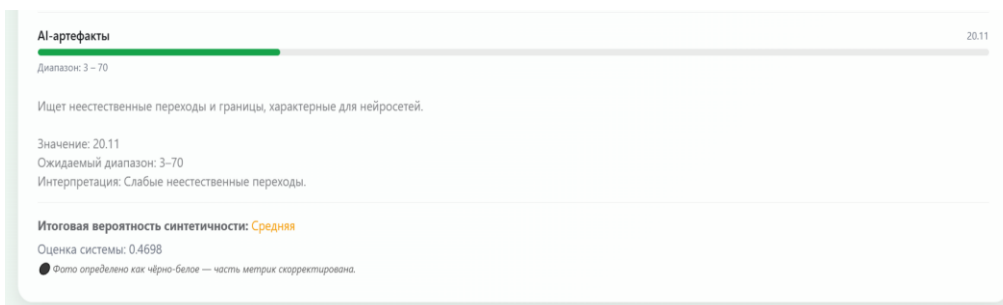


Рисунок 14 – Анализ изображения на возможную генерацию часть 3

Теперь проведем проверку профиля, который может быть фейковым, вызывает подозрения. Результат представлен на рисунке 15.

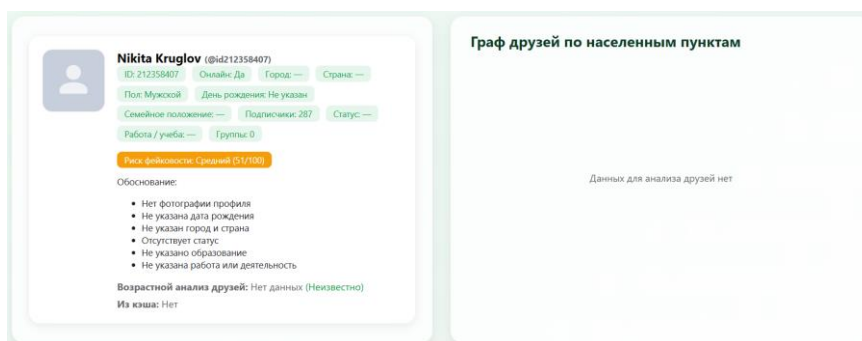


Рисунок 15 – Дашборд с данными пользователя и анализом

По результатам анализа представлен риск фейковости, отображенный оранжевым сигнальным цветом. Указана информация, которая отсутствует в профиле. Справа, в модуле построения графа выводится сообщение «Граф друзей недоступен». Это связано с тем, что пользователь закрыл доступ с данным своих друзей. Анализ изображения также не был выполнен в связи с тем, что фото профиля отсутствует. Ознакомиться с модулем и сообщением можно на рисунке 16.

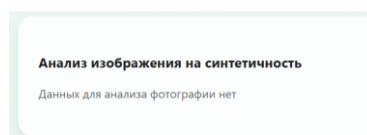


Рисунок 16 – Анализ изображения, при его отсутствии, на возможную генерацию

Далее был проверен профиль с подозрительной страницей. Данные профиля практически отсутствуют. С результатом анализа подозрительного аккаунта можно ознакомиться на рисунках 17-19.

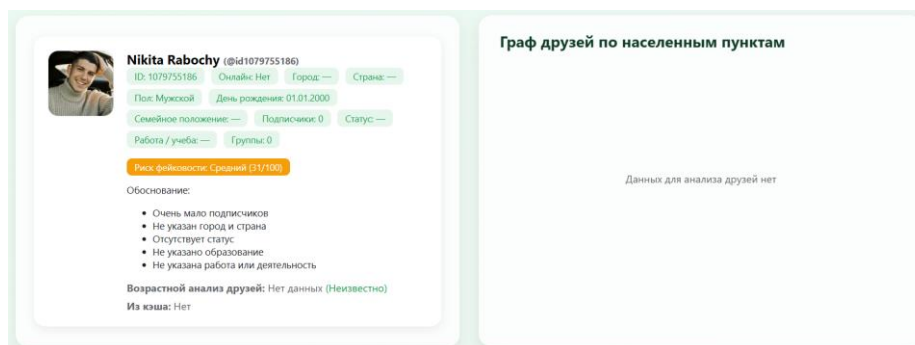
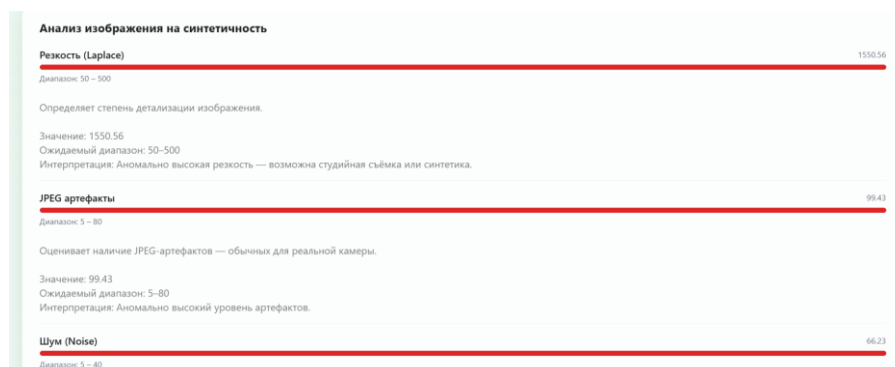
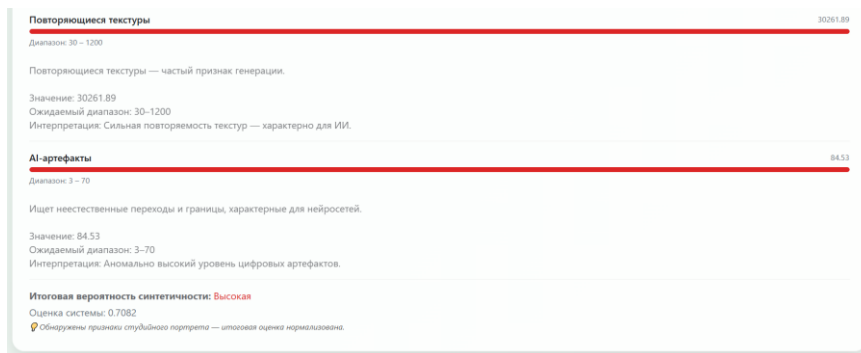


Рисунок 17 – Дашборд с данными пользователя и анализом + граф



**Рисунок 18** – Анализ изображения на возможную генерацию часть 1**Рисунок 19** – Анализ изображения на возможную генерацию часть 2

По результатам анализа представлен риск фейковости, отображенный оранжевым сигнальным цветом. Указана информация, которая отсутствует в профиле. Справа, в модуле построения графа выводится сообщение «Данных для анализа друзей нет». Это связано с тем, что пользователь либо закрыл доступ к данным своих друзей, либо друзей вовсе нет.

Анализ изображения показал риск синтетичности «Высокий», это связано с тем, что по результатам анализа были выявлены сильные отклонения от диапазонов (повторяющиеся текстуры и AI-артефакты), сформированных для каждой метрики. А изображение действительно было сгенерировано ИИ.

Такую практическую работу можно осуществить на любом уроке информатике. Обучающее благодаря такой платформе, научатся механизмам выявления фейковых аккаунтов. Освоение теории сопровождается практическими заданиями, направленными на отработку навыков выявления фейковых аккаунтов [8].

Обучающие поймут, что основными факторами, свидетельствующими о сомнительном профиле, выступают: низкая активность или полное отсутствие публикаций, несоответствие аватара и имени профилю, отсутствие значимых связей и взаимных подписок, большое количество рекламы и призывов к действию, наличие массовой рассылки однотипных сообщений. Участники осваивают эти признаки и практикуются в обнаружении фиктивных профилей, постепенно улучшая свои навыки.

В современном обучении важной составляющей успеха является визуализация материала. Графические образы воспринимаются мозгом быстрее и эффективнее, чем обычный текст, что делает их незаменимым инструментом в передаче сложной информации. Графические объекты обладают рядом преимуществ: способствуют быстрому восприятию информации, улучшают запоминание материала, помогают установить ассоциации и связи между элементами, повышают интерес и мотивацию к изучению предмета. Такой подход существенно повысит вовлеченность участников, улучшит восприятие материала и увеличит процент усвоения знаний [9]. В нашей обучающей платформе представлена хорошая визуализация данных: графы, картинки, графики, соблюдена цветовая гамма.

Рассмотрим основные преимущества нашей обучающей онлайн-платформы «Phantom» по выявлению фейковых аккаунтов

Наглядность и интерактивность нашей онлайн-платформы. Пользователи получают возможность лично попробовать себя в роли эксперта по безопасности, непосредственно взаимодействуя с интерфейсами и профилями, созданными разработчиками. Это позволяет ощутить реальность происходящего и глубже погрузиться в суть вопроса.

Практичность и прикладной характер, предлагают не просто теорию, а реальные практики, близкие к повседневным жизненным ситуациям. Обучающийся учится не просто читать теоретические материалы, а реально сталкивается с подобными ситуациями, решая

поставленную задачу. Наша платформа обеспечивает, быстрое и эффективное обучение. За короткий промежуток времени можно пройти обучение, проверив свои навыки на большом количестве примеров. Такая практика способствует быстрой адаптации и закреплению знаний.

Доступность и удобство онлайн-платформы. Заниматься можно в любое удобное время и в любом месте, имея доступ к Интернету. Работа с нашей обучающей платформой развивает навыки критического мышления, позволяя анализировать профили и находить признаки мошенничества. Это важный элемент цифровой грамотности, полезный не только в рамках изучения конкретной темы, но и в повседневной жизни.

#### **Заключение.**

Комплексное обучение по информационной безопасности, является основой будущего образования, нацеленного на гармоничное развитие человека и подготовку квалифицированного специалиста нового формата [13; 14]. Оно обеспечивает широкий кругозор, гибкость мышления и способность быстро адаптироваться к изменениям окружающей среды.

Такое обучение повышает заинтересованность учащихся, так как обучение связано с решением реальных задач. Происходит развитие компетенций, соответствующих современным профессиональным стандартам.

Обучающая онлайн-платформа «Phantom», по выявлению фейковых аккаунтов имеет значительные преимущества в учебном процессе. Она улучшает качество обучения, повышают интерес и мотивацию учащихся, содействуют быстрому освоению навыков и развитию уверенности в себе. Такие инструменты становятся важными компонентами современных образовательных систем, способствующих развитию цифровой грамотности и финансовой безопасности граждан.

Плюсы использования платформы в обучении: повышение цифровой грамотности обучающихся, ранняя диагностика рисков, простота использования и интеграция в уроки информатики.

Итак, платформа «Phantom» служит действенным инструментом в деле предупреждения детской киберпреступности и укрепления цифровой грамотности наших школьников.

#### **Список источников:**

1. Красовская Н.Р., Гуляев А.А. К вопросу о контроле фейков, дипфейков, фейковых аккаунтов в интернете // Вестник Удмуртского университета. Социология. Политология. Международные отношения. 2021. Т. 5, № 1. С. 96-99. URL: <https://www.elibrary.ru/twzysv>
2. Сафаров Ф. Г. Алгоритмы нахождения фейковых аккаунтов в социальных сетях с помощью нейронных сетей // Наука и инновация. Серия геологических и технических наук. 2024. № 4. С. 78-86. URL: <https://www.elibrary.ru/wvhfhw>
3. Зуфарова А.С., Кошелева, А. Д. Обучение сотрудников как ключевой фактор защиты от киберугроз: современные вызовы и решения // ЦИТИСЭ. 2025. № 1(43). С. 124-138. URL: <https://www.elibrary.ru/pwbawh>
4. Бочаров М.И., Симонова И.В. Методика обучения информационной безопасности старшеклассников: о содержании обучения информационной безопасности в школьном курсе информатики // Пространство и Время. 2014. № 3(17). С. 300-307. URL: <https://www.elibrary.ru/stqzab>
5. Ефимов С.А., Пронькин Н.Н. Роль сотрудников в обеспечении информационной безопасности: подходы к повышению осведомлённости // International Journal of Professional Science. 2024. № 6-2. С. 40-47. URL: <https://www.elibrary.ru/fgwhyv>

6. Захарова А.А. Методы обучения персонала в организации // Аллея науки. 2022. Т. 1, № 3 (66). С. 114-120. URL: <https://www.elibrary.ru/acjlnb>
7. Нечипуровский Д.И. Как построить многоуровневую защиту для борьбы с продвинутыми угрозами фишинга // Научный аспект. 2024. Т. 41, № 4. С. 5337-5342. URL: <https://www.elibrary.ru/jdtfvy>
8. Яковлева М.А. Лидерство в системе наставничества как эффективный инструмент адаптации персонала // Human Progress. 2021. Т. 7, № 1. URL: <https://www.elibrary.ru/mfmyrr>
9. Ченушкина С. В., Шмакова Л.Е. Роль визуализации в формировании компетентности в области кибербезопасности // Мир науки, культуры, образования. 2023. № 6(103). С. 229-233. URL: <https://www.elibrary.ru/wshgmi>
10. Коломеец М. В., Чечулин А.А. Метрики вредоносных социальных ботов // Труды учебных заведений связи. 2023. Т. 9, № 1. С. 94-104. URL: <https://www.elibrary.ru/hefhfr>
11. Коломеец М. В., Чечулин А. А. Подход к обнаружению вредоносных ботов в социальной сети ВКонтакте и оценка их параметров // Труды учебных заведений связи. 2024. Т. 10, № 2. С. 92-101. URL: <https://www.elibrary.ru/hefhfr>
12. Шайкова М. В. Защита несовершеннолетних в онлайн офлайн-пространстве: дилемма кибербуллинга // Виктимология. 2024. Т. 11, № 2. С. 267-277. URL: <https://www.elibrary.ru/xketur>
13. Дукальская И.В., Третьяков Е. Ю. Платформы информационной безопасности как основы экспериментального обучения // Вопросы педагогики. 2022. № 3-2. С. 233-236. URL: <https://www.elibrary.ru/eefczs>
14. Мадьярова Г. А. Особенности обучения информационной безопасности на основе применения цифровых технологий // Вестник Казахского национального педагогического университета имени Абая. Серия: Физико-математические науки. 2023. Т. 80, № 4(2022). URL: <https://www.elibrary.ru/nljfjb>
15. Синев С. Г. О совершенствовании обучения по образовательным программам в сфере информационной безопасности // Прикладная физика и математика. 2024. № 12. С. 60-68. URL: <https://www.elibrary.ru/psxusq>

## References:

1. Krasovskaya, N. R., & Gulyaev, A. A. (2021). On the issue of controlling fakes, deepfakes, and fake accounts on the Internet. *Bulletin of Udmurt University. Sociology. Political Science. International Relations*, 5(1), 96–99. (In Russian). <https://www.elibrary.ru/twzysv>
2. Safarov, F. G. (2024). Algorithms for finding fake accounts in social networks using neural networks. *Science and Innovation. Series of Geological and Technical Sciences*, 4, 78–86. (In Russian). <https://www.elibrary.ru/wvhfhw>
3. Zufarova, A. S., & Kosheleva, A. D. (2025). Employee training as a key factor in protecting against cyber threats: Modern challenges and solutions. *CITISE*, 1, 124–138. (In Russian). <https://www.elibrary.ru/pwbawh>
4. Bocharov, M. I., & Simonova, I. V. (2014). Methods of teaching information security to high school students: On the content of information security training in the school computer science course. *Space and Time*, 3, 300–307. (In Russian). <https://www.elibrary.ru/stqzab>
5. Efimov, S. A., & Pronkin, N. N. (2024). The role of employees in ensuring information security: Approaches to raising awareness. *International Journal of Professional Science*, 6-2, 40–47.
6. Zakharova, A. A. (2022). Personnel training methods in an organization. *Alley of Science*, 1(3), 114–120. (In Russian). <https://www.elibrary.ru/fgwhyv>
7. Nечипуровский, Д. И. (2024). How to build a multi-level defense to combat advanced phishing threats. *Scientific Aspect*, 41(4), 5337–5342. (In Russian). <https://www.elibrary.ru/jdtfvy>

8. Yakovleva, M. A. (2021). Leadership in the mentoring system as an effective tool for personnel adaptation. *Human Progress*, 7(1). (In Russian). <https://www.elibrary.ru/mfmyrr>
9. Chenushkina, S. V., & Shmakova, L. E. (2023). The role of visualization in the formation of competence in the field of cybersecurity. *The World of Science, Culture, Education*, 6, 229–233. (In Russian). <https://www.elibrary.ru/wshgmi>
10. Kolomeets, M. V., & Chechulin, A. A. (2023). Metrics of malicious social bots. *Proceedings of Educational Institutions of Communication*, 9(1), 94–104. (In Russian). <https://www.elibrary.ru/hefhfr>
11. Kolomeets, M. V., & Chechulin, A. A. (2024). Approach to detecting malicious bots in the VKontakte social network and assessing their parameters. *Proceedings of Educational Institutions of Communication*, 10(2), 92–101. (In Russian). <https://www.elibrary.ru/hefhfr>
12. Shaykova, M. V. (2024). Protecting minors online and offline: The cyberbullying dilemma. *Victimology*, 11(2), 267–277. (In Russian). <https://www.elibrary.ru/xketur>
13. Dukal'skaya, I. V., & Tretyakov, E. Yu. (2022). Information security platforms as a basis for experimental learning. *Questions of pedagogy*, 3-2, 233–236. (In Russian). <https://www.elibrary.ru/eefczs>
14. Madyarova, G. A. (2023). Features of information security training based on the use of digital technologies. *Bulletin of the Kazakh National Pedagogical University named after Abai. Series: Physical and Mathematical Sciences*, 80(4). (In Russian). <https://www.elibrary.ru/nljfjb>
15. Sinev, S. G. (2024). On improving training in educational programs in the field of information security. *Applied Physics and Mathematics*, 12, 60–68. (In Russian). <https://www.elibrary.ru/psxusq>

Submitted: 26 February 2026

Accepted: 26 March 2026

Published: 27 March 2026

