ISSN 0234-0453 • ИНФОРМАТИКА И ОБРАЗОВАНИЕ • 2024 • Том 39 № 2

DOI: 10.32517/0234-0453-2024-39-2-34-47

ИСПОЛЬЗОВАНИЕ КЕЙС-МЕТОДА ДЛЯ ОБУЧЕНИЯ СТУДЕНТОВ НАПРАВЛЕНИЯ ПОДГОТОВКИ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ» РАЗВЕДКЕ ПО ОТКРЫТЫМ ИСТОЧНИКАМ

Д. М. Назаров[1], **Р. А. Симбирцев**[1,2] ✉, **Д. П. Салалайко**[1,2]

[1] ***Уральский государственный экономический университет, Екатеринбург, Россия***

[2] ***АО «Точка», Екатеринбург, Россия***

✉ *rsimbirtsev@mail.ru*

Аннотация

В современном мире информация является одним из самых ценных ресурсов, а умение ее обрабатывать приобретает особую значимость в процессе подготовки специалистов различного профиля, в том числе и специалистов в области информационной безопасности. OSINT (*англ.* Open Source Intelligence — разведка по открытым источникам) — это технология сбора и анализа информации о человеке, организации, событии или явлении по открытым источникам. Этот мощный инструмент эффективной обработки открытых данных представляет особый интерес для формирования профессиональных компетенций студентов, обучающихся по направлению подготовки 10.03.01 «Информационная безопасность».

Авторы статьи исследуют и апробируют принципы кейс-метода как эффективной методики обучения студентов технологиям OSINT. Кейс-метод (*англ.* Case Method), или метод ситуационного анализа, предполагает решение реальных проблемных ситуаций и разбор практических примеров для глубокого осмысления и усвоения материала. В статье подробно представлены конкретные кейсы по OSINT, которые можно использовать для обучения студентов направления подготовки «Информационная безопасность». Данные задачи способствуют развитию критического мышления, формированию аналитических навыков и способности применять полученные знания на практике.

Особое значение в статье придается обратной связи как критически важному элементу обучения, позволяющему настраивать и адаптировать учебный процесс в соответствии с потребностями и уровнем освоения технологий OSINT студентами. Помимо этого, авторы подчеркивают важность мультидисциплинарного подхода в обучении OSINT, включающего в себя изучение не только технических аспектов темы, но также правовых и этических норм.

Анализ принципов кейс-метода и конкретные кейсы, представленные в статье, будут полезны преподавателям, разрабатывающим курсы по обучению технологиям OSINT, а также специалистам, заинтересованным в современных методах и подходах к обучению в области информационной безопасности.

Ключевые слова: методика преподавания, информационная безопасность, OSINT, кейс-метод, обратная связь, индуктивный метод, дедуктивный метод.

Для цитирования:

Назаров Д. М., Симбирцев Р. А., Салалайко Д. П. Использование кейс-метода для обучения студентов направления подготовки «Информационная безопасность» разведке по открытым источникам. *Информатика и образование*. 2024;39(2):34–47. DOI: 10.32517/0234-0453-2024-39-2-34-47.

USING THE CASE METHOD FOR TEACHING INFORMATION SECURITY STUDENTS IN OPEN SOURCE INTELLIGENCE

D. M. Nazarov[1], **R. A. Simbirtsev**[1,2] ✉, **D. P. Salalayko**[1,2]

[1] ***Ural State University of Economics, Ekaterinburg, Russia***

[2] ***JSC "Tochka", Ekaterinburg, Russia***

✉ *rsimbirtsev@mail.ru*

Abstract

In today's world, information is one of the most valuable resources, and the ability to process it becomes especially important in the process of training specialists of various profiles, including specialists in the field of information security. OSINT (Open Source Intelligence) is a technology for collecting and analyzing information about a person, organization, event or phenomenon from open sources. This powerful tool for the effective processing of open data is of particular interest for the formation of vocational competencies of students studying in the direction of training 10.03.01 "Information Security".

The authors of the article explore and test the principles of the case method as an effective method of teaching OSINT technologies. The case method, or the method of situational analysis, involves solving real-life problem situations and practical examples for deep

ISSN 0234-0453 • INFORMATICS AND EDUCATION • 2024 • Volume 39 No 2

understanding and mastering of the material. The article presents in detail specific cases on OSINT that can be used to teach students of "Information Security". These tasks contribute to the development of critical thinking, the formation of analytical skills, and the ability to apply the acquired knowledge in practice.

The article emphasizes the importance of feedback as a critical element of learning, which allows to customize and adapt the learning process according to students' needs and level of mastery of OSINT technologies. In addition, the authors emphasize the importance of the multidisciplinary approach in OSINT training, including not only the study of technical aspects but also legal and ethical norms.

The analysis of case method principles and case studies presented in the article will be useful for instructors developing OSINT training courses, as well as for specialists interested in modern methods and approaches to training in the field of information security.

Keywords: teaching methods, information security, OSINT, case method, feedback, inductive method, deductive method.

For citation:

Nazarov D. M., Simbirtsev R. A., Salalayko D. P. Using the case method for teaching information security students in open source intelligence. *Informatics and Education.* 2024;39(2):34–47. (In Russian.) DOI: 10.32517/0234-0453-2024-39-2-34-47.

1. Введение

Не будет преувеличением сказать, что все концепции обучения можно рассмотреть через противопоставление индуктивного и дедуктивного методов. Они принципиально различаются направлениями мыслительного процесса обучающихся: индуктивный метод обучения предполагает постепенный переход от конкретных примеров к теоретическим обобщениям, движение по спирали вверх (в контексте российской педагогической науки — «от частного к общему»), в то время как дедуктивный метод обучения начинается с обсуждения общих принципов с постепенным переходом к конкретным случаям, движение по спирали вниз (в контексте российской педагогической науки — «от общего к частному»). Главное отличие между этими подходами состоит в том, что при применении индуктивного метода в образовательном процессе обучающиеся постепенно формируют теоретические представления изучаемого явления, а при применении дедуктивного метода проверяют базовые теоретические положения на практике, разбирая как общие, так и частные случаи.

Джон Дьюи (США), Жан Пиаже (Швейцария), Джером Брунер (США), Лев Выготский (СССР) внесли значительный вклад в развитие и популяризацию этих методов. Джером Брунер, например, разработал концепцию обучения через открытие, которая основывается на индуктивном методе обучения [1]. Американские психологи и педагоги во главе с Джоном Дьюи акцентировали внимание на «обучении посредством делания», на методе «проектов», который можно рассматривать как платформу для индуктивного метода обучения [2]. J. D. Bransford, A. L. Brown, R. R. Cocking предлагали фокусироваться на том, как именно люди учатся (и дети, и взрослые): «Отправной точкой является основной набор принципов обучения, тогда выбор стратегий обучения (конечно, опосредованный предметом, уровнем знаний и желаемым результатом) может быть целенаправленным» [3] и максимально широким, т. е. включающим любой частный инструмент дедуктивного и индуктивного методов. На основе этих концепций разработаны десятки конкретных технологий обучения, например, таких, как проектное обучение, кейс-метод, проблемное обучение и др. Каждая из этих концепций имеет свои сильные и слабые стороны, и выбор между ними зависит от конкретных образовательных целей, ситуаций и характеристик обучающихся. Часто на практике наиболее эффективным признается сочетание методов обучения.

В условиях постоянного развития информационных технологий и постепенного перехода к использованию цифровых платформ в самых разных сферах экономики и жизни повышается актуальность организации эффективного процесса обучения специалистов в области информационной безопасности. Однако выбор оптимального метода их обучения остается сложной задачей, поскольку сама сфера информационной безопасности — это многогранная область знаний, требующая глубокого теоретического понимания протекающих в ней процессов, развития практических навыков и в конечном итоге приобретения профессиональных компетенций.

OSINT (*англ.* Open Source Intelligence — разведка по открытым источникам) — это технология поиска, сбора информации о человеке, организации, событии или явлении из открытых источников и последующий ее анализ. Это мощный инструмент для эффективной обработки открытых данных, и потому он представляет особый интерес для формирования профессиональных компетенций студентов, обучающихся по направлению подготовки 10.03.01 «Информационная безопасность».

Цель статьи — сформулировать принципы эффективной методики обучения студентов направления подготовки 10.03.01 «Информационная безопасность» и продемонстрировать их апробацию на примере освоения студентами технологий OSINT.

2. Принципы кейс-метода в обучении студентов

На протяжении многих столетий высшее образование опиралось на дедуктивный метод обучения, в котором преподаватель выступал как источник абсолютного, объективного знания, транслируемого обучающимся в основном через лекционные занятия. Задача студентов была ассимилировать эти знания, выступая при этом пассивными получателями информации, и закрепить их на практике [3]. С развитием информационных технологий и появлением технических средств обработки информации традиционное восприятие учебного процесса в рамках дедуктивного подхода подверглось переосмыслению. Превалирующая концепция дедуктивного метода

обучения стала меняться на индуктивную, которая, в свою очередь, исходит из предпосылки, что знания не просто передаются от преподавателя к школьнику или студенту, а усваиваются ими активно, исходя из уже имеющихся знаний и опыта (в том числе полученных из открытых источников — книг, журналов, средств массовой информации, соцсетей и т. д.). Таким образом, новая информация проходит сквозь фильтр индивидуального восприятия обучающегося, опираясь на его предыдущие знания, а также опыт и убеждения. Если новые данные согласуются с уже сформированными внутренними структурами, они интегрируются в систему убеждений студента. Если же они противоречат существующим знаниям или убеждениям, то могут быть лишь временными и будут использованы, например, только для сдачи экзамена. Таким образом, роль преподавателя трансформируется: теперь его задача не только в передаче знаний, но и в стимулировании активного участия обучающихся в образовательном процессе, а также в поддержке обучающихся в процессе связывания новой информации с уже имеющимися знаниями и опытом.

В современном образовании все больше делается акцент на применении индуктивного метода обучения в различных направлениях и областях знаний, от гуманитарных до технических наук. Особое внимание уделяется созданию условий, при которых студенты могут взаимодействовать, обмениваться знаниями и навыками для решения различных задач профессиональной деятельности. Поэтому важнейшей методикой обучения студентов в мировом масштабе стал метод ситуационного анализа, или кейс-метод (*англ.* Case Method), который заключается в разборе и решении проблемных ситуаций (задач, кейсов), характерных для профессиональной деятельности в рамках изучаемой дисциплины.

Монография M. A. Lundeberg, B. B. Levin, H. L. Harrington «Who learns what from cases and how? The research base for teaching and learning with cases» [4], вышедшая в1999 году, представляет собой фундаментальное исследование эффективности использования кейс-метода в образовании. Авторы анализируют, как именно студенты усваивают информацию, работая с ситуационными задачами (кейсами), какие факторы влияют на успех такого типа обучения и какие педагогические подходы наиболее эффективны при работе с кейсами.

L. E. Lynn в своем руководстве «Teaching and learning with cases: A guidebook» [5] предлагает практические рекомендации по применению кейс-метода в обучении, при этом подчеркивая важность правильного создания кейсов. Кейс должен представлять из себя хорошо структурированный и вместе с тем реалистичный сценарий, который стимулирует аналитическое мышление и развивает творческий потенциал студентов.

Согласно этим исследованиям, обучение на основе кейсов (при условии правильного применения этого метода) способствует глубокому пониманию материала и улучшает критическое мышление студентов, позволяя им достичь наилучших результатов. При использовании кейс-метода должен быть установлен оптимальный баланс между теорией и практикой, чтобы эффективно вовлекать студентов в учебный процесс и мотивировать их на решение практических задач.

Обучение на основе кейсов представляет собой пример практического подхода к образованию, который позволяет студентам применять теоретические знания в процессе анализа реальных или вымышленных ситуаций. Этот метод применяется во многих сферах и помогает студентам освоить способы анализа сложных ситуаций, а также развить навыки принятия решений, отмечают **О. Б. Симонова, Т. Е. Исаева в статье «Методика применения педагогических кейсов в обучении студентов технических вузов (эмпирическое исследование)»** [6].

G. Kardos, C. O. Smith в работе «On writing engineering cases» [7] предлагают методы создания кейсов, которые максимально приближены к реальным инженерным задачам и потому помогают студентам развивать не только практические навыки, но и критическое мышление.

Н. В. Никуличева в статье «Обучение студентов педагогических специальностей магистратуры методике преподавания предмета в условиях дистанционного обучения» [8] подчеркивает важность адаптации кейс-метода в условиях онлайн-обучения. **В. И. Шармаев, Я. А. Андреева, К. А. Василевский в работе «Обеспечение информационной безопасности с помощью разведки по открытым источникам (OSINT)»** [9] на основе практических примеров анализируют, как использование открытых источников может способствовать предотвращению угроз и улучшению обеспечения безопасности данных.

Обзор статей, посвященных разведке по открытым источникам, показывает не только тематическую, но и педагогическую актуальность этого инструмента. Например, **М. Е. Сидорова и А. Р. Кузьмин в статье «Разведка по открытым источникам данных и ее применение для решения задач кибербезопасности»** [10] систематизируют методы OSINT для защиты от киберугроз. **А. Г. Качалов и М. М. Лантаев в работе «Подготовка специалистов по работе с открытыми данными в сети Интернет (OSINT) в гражданских и ведомственных вузах»** [11] приходят к выводу, что необходимо усилить качество подготовки специалистов OSINT в указанных вузах, в том числе «увеличить количество дисциплин по работе в сети Интернет и с открытыми данными, что отвечает потребностям государства в обеспечении безопасности национальных интересов России от внешних и внутренних угроз».

Исходя из анализа литературы по использованию кейс-метода в педагогике, сформулируем принципы эффективного обучения студентов и с опорой на эти принципы определим содержательные аспекты их применения на занятиях по технологиям OSINT (табл. 1).

ISSN 0234-0453 • INFORMATICS AND EDUCATION • 2024 • Volume 39 No 2

Таблица 1 / Table 1

Принципы кейс-метода и его использование на занятиях по технологиям OSINT

The principles of the case method and its use in OSINT technology classes

№ п/п	Принцип	Характеристика	Применение на занятиях по технологиям OSINT
1	Интерактивность и критическое мышление	Вовлечение студентов в решение практических задач. Развитие способности анализировать, оценивать и синтезировать информацию из различных источников	Разработка интерактивных заданий, в том числе игровых сценариев. Организация групповых проектов и совместных исследований, способствующих обмену знаниями между студентами для развития командных навыков и совместного решения проблем
2	Использование реальных бизнес-задач	Содержанием занятий становятся кейсы, основанные на реальных событиях, проблемах, задачах	Решение кейсов из реальной практики OSINT, например, в области кибербезопасности
3	Мультидисциплинарный подход	Интеграция знаний из различных дисциплин	Создание междисциплинарных кейсов, сочетающих технические аспекты OSINT с вопросами из сферы юриспруденции, права, этики. Освещение вопросов этики и законности при сборе и использовании открытой информации
4	Постепенное усложнение и обновление материала	Последовательное усложнение кейсов. Обучение работе с разнообразными типами источников информации, включая социальные сети, публичные базы данных и другие. Постоянное обновление учебных материалов	Постепенное усложнение учебных модулей: от базовых принципов OSINT до продвинутых методов и технологий. Обучение студентов работе с различными источниками данных, в том числе с использованием специализированного программного обеспечения. Постоянное обновление учебных материалов для отражения последних тенденций и технологий в сфере OSINT
5	Обратная связь	Постоянная реализация обратной связи для корректировки и улучшения учебного процесса и качества обучения	Создание системы обратной связи со студентами, включая работу над ошибками и обсуждение результатов решений кейсов по технологиям OSINT

Сформулированные принципы кейс-метода обеспечивают всестороннее и глубокое понимание технологий OSINT, а также создают уникальную среду для обучения, в которой теория эффективно сочетается с практикой. Важнейшей составляющей этой методики мы считаем принцип обратной связи, который подчеркивает необходимость активного участия студентов в процессе обучения и способствует развитию у обучающихся способности анализировать, оценивать и синтезировать информацию. Методика обучения, основанная на описанных принципах, обеспечивает студентам не только теоретические знания, но и практические навыки, необходимые для решения реальных задач в области OSINT.

3. Использование кейс-метода на занятиях по разведке по открытым источникам

Занятия по изучению технологий OSINT начинаются с освоения теоретического материала. В вводной части кейса преподаватель сообщает необходимую информацию: определение термина [12], историю его возникновения [13], принципы работы (например, важность установления четких правил использования OSINT для минимизации возможных злоупотреблений и нарушений конфиденциальности [14]) и инструменты [14–16]. Педагог помогает развести схожие технологии поиска информации в интернете: OSINT, пентест[1] и нетсталкинг[2] [15], — и обращает внимание на новые подходы и инструменты, которые усиливают эффективность использования OSINT для защиты информации [16].

Среди инструментов OSINT студентам предлагается освоить технику поисковых запросов Google Dorks, а также сервисы, представленные в таблице 2.

Начало работы с технологиями OSINT — освоение Google Dorks. Студенты знакомятся с основами данной техники — операторами расширенного поиска,

[1] Пентест (*англ.* pentest — тест на проникновение) — это проверка защищенности компьютерной системы или сети, при которой моделируется реальная атака злоумышленника.

[2] Нетсталкинг (сложное слово, образовавшееся в русском языке из заимствованных из английского языка самостоятельных слов: net — сеть и stalking — преследование) — это сбор, хранение и анализ малодоступных, малоизвестных и малопосещаемых объектов интернета.

ISSN 0234-0453 • ИНФОРМАТИКА И ОБРАЗОВАНИЕ • 2024 • Том 39 № 2

Таблица 2 / Table 2

Инструменты OSINT
OSINT tools

№ п/п	Сервис	Адрес в интернете	Описание
1	Shademap	https://shademap.app	Предлагает интерактивную карту теней строений в городах
2	Skylens	https://skylens.io/	Определяет геолокацию постов в социальных сетях
3	Snoop Project	https://github.com/snooppr/snoop	Осуществляет поиск в социальных сетях по никнеймам
4	Search4faces	https://search4faces.com/	Ищет по фотографии людей в социальных сетях («ВКонтакте», «Одноклассники» и др.) и публичных персон по базам данных («Википедия», IMDB и др.)
5	Social Mapper	https://github.com/Greenwolf/social_mapper	Ищет связи профилей в социальных сетях во всем интернете, используя распознавание лиц
6	PimEyes	https://pimeyes.com	Ищет по фотографии людей во всей сети Интернет
7	ImageSearch	https://www.image-search.org/ru	Ищет изображения в интернете (по картинке, по ключевым словам, по голосовому вводу и др.)[1]
8	RevEye Reverse Image Search	https://chromewebstore.google.com/detail/reveye-reverse-image-sear/keaaclcjhehbbapnphnmpiklalfhelgf	Помогает найти первоисточник фотографии
9	Kamerka-GUI	https://www.kamerka.io/	Собирает информацию об устройствах, подключенных к интернету вещей, и отображает их на карте
10	Geowifi	https://github.com/GONZOsint/geowifi	Ищет геолокационные данные WiFi по идентификаторам BSSID и SSID в различных публичных базах данных
11	Web.archive	https://web.archive.org/	Позволяет просмотреть неработающую или удаленную веб-страницу

необходимыми для обнаружения скрытой информации, располагающейся на общедоступных серверах:

- filetype:xls intext:"контактные данные" — поиск конкретных файлов: этот запрос поможет найти таблицы Excel, содержащие контактные данные;
- site:example.com intext:"годовой отчет" — поиск на определенном сайте: позволяет найти годовые отчеты, опубликованные на конкретном веб-сайте;
- "email@example.com" -site:example.com — поиск по электронной почте: ищет упоминания конкретного электронного адреса, который может быть использован для деанонимизации личности, за пределами официального сайта;
- site:vk.ru intext:"имя фамилия" "город проживания" — поиск в социальных сетях: этот запрос поможет найти профиль человека в социальной сети «ВКонтакте» по имени и месту проживания;
- filetype:pdf site:competitor.com intitle:"отчет" — поиск документов конкурентов: ищет PDF-файлы с отчетами на сайте конкурента.

Процесс обучения строится на принципе мультидисциплинарности — со студентами обсуждаются последствия получения доступа к частной или конфиденциальной информации без разрешения правообладателя: необходимо всегда убеждаться в том, что ваш поиск соответствует юридическим и этическим нормам.

Далее студенты решают кейсы (ситуационные задачи) различного уровня сложности на применение технологий OSINT.

[1] Для поиска по изображению студенты осваивают многообразие имеющихся на данный момент инструментов: Google Images, Яндекс Картинки, TinEye, Bing Image Search, Getty Images или даже поиск через соцсеть Pinterest и сервис для определения плагиата Dupli Checker и др.

ISSN 0234-0453 • INFORMATICS AND EDUCATION • 2024 • Volume 39 No 2

Кейс 1.

Условие. Известно, что некий подозреваемый в киберпреступлении искал сотрудников на сайте сервиса по поиску работы HeadHunter. Он создавал объявления о вакансиях от имени компании, расположенной в городе Москве.

Задание. Необходимо собрать о подозреваемом как можно больше информации.

Решение. Чтобы получить информацию о данном подозреваемом, составим расширенный запрос, ограничивающий поиск только по сайту сервиса HeadHunter — https://hh.ru. Будем искать в заголовках вакансий теги «Кибербезопасность, Москва», поскольку нам необходимо найти вакансию, связанную с кибербезопасностью в городе Москве: intitle:Кибербезопасность, Москва site:hh.ru. Результат поиска представлен на рисунке 1.

Можем заметить, что найдено всего 216 результатов — это гораздо меньше, чем если бы мы искали вакансию простым поисковым запросом «Кибербезопасность, Москва» (рис. 2).

При обычном поиске мы получаем 1 030 000 результатов, а это в 4769 раз больше, чем результаты расширенного поиска [17].

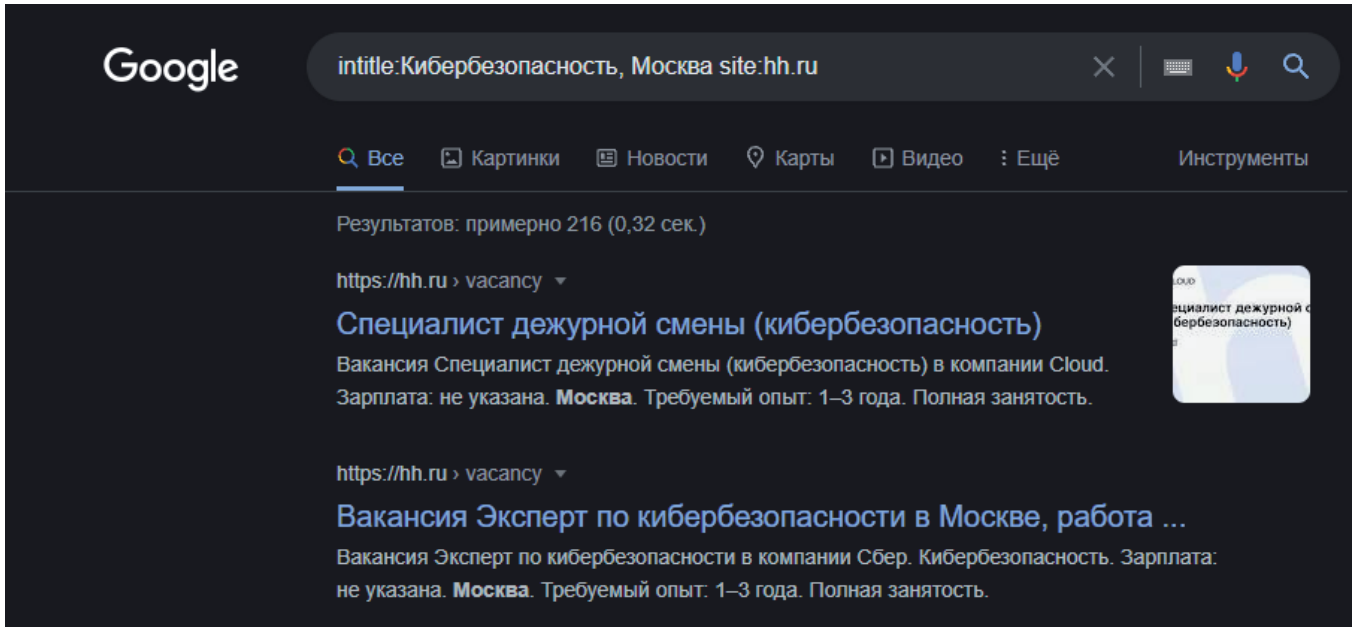


Рис. 1. Результат расширенного поиска
Fig. 1. The result of the extended search

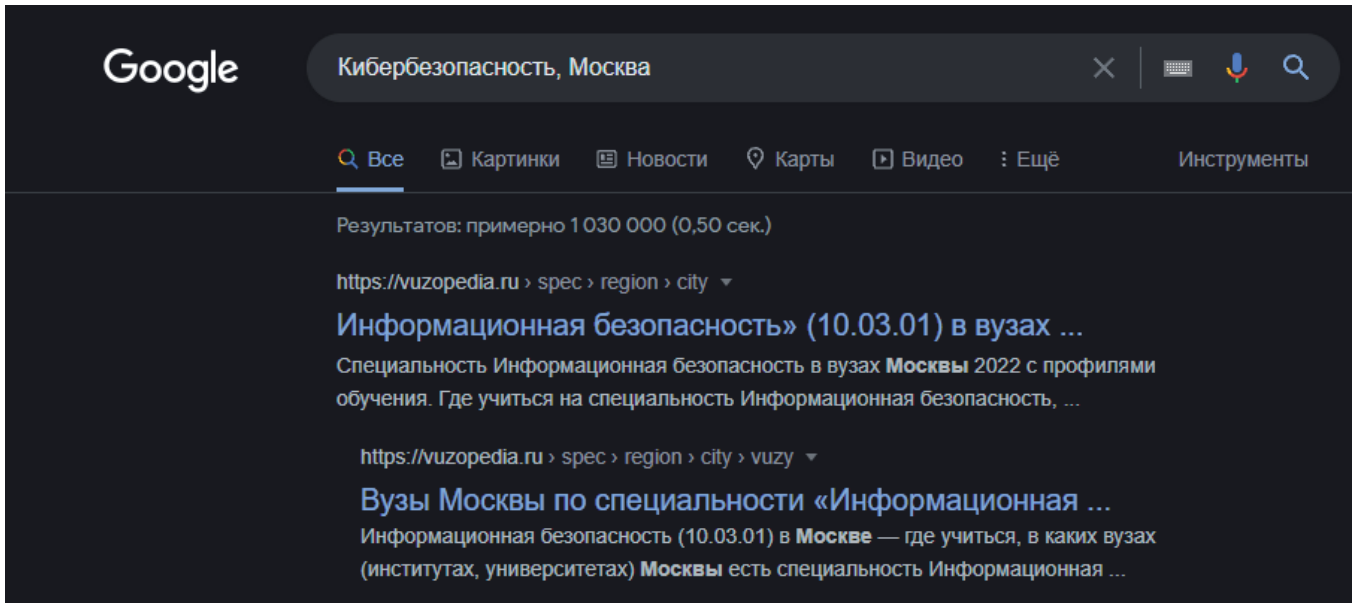


Рис. 2. Результат обычного поиска
Fig. 2. The result of the regular search

Кейс 2.

Условие. У нас есть фотография преподавателя Уральского государственного экономического университета, представленная на официальном сайте вуза.

Задание. Необходимо найти схожие фотографии в профилях в социальной сети «ВКонтакте».

Решение. Для поиска похожих фотографий в социальных сетях будем использовать сервис Search4faces, который благодаря работе нейронных сетей может с легкостью находить схожие портреты. Результатом поиска является ссылка на профиль найденного человека в социальной сети «ВКонтакте».

1. Переходим на https://search4faces.com/, выбираем «Поиск по фотографиям профиля “ВКонтакте”» и нажимаем кнопку «Перейти» (рис. 3).

Рис. 3. Вкладка с поиском профиля по фотографиям в сервисе Search4faces

Fig. 3. The tab with profile search by photos in the Search4faces

2. На открывшейся странице вставляем фотографию преподавателя и нажимаем кнопку «Загрузить». После загрузки сервис автоматически обрезает ее для более корректного поиска фотографии с лицом человека и выдает список с похожими снимками в профилях социальной сети «ВКонтакте». На каждом экземпляре выдачи указано процентное соотношение сходства фотографий (рис. 4).
3. Переходим на профиль страницы «ВКонтакте» с самым высоким процентом совпадения. Таким образом, мы нашли страницу нашей поисковой цели в социальной сети «ВКонтакте» (рис. 5). Она принадлежит тому же преподавателю Уральского государственного экономического университета.

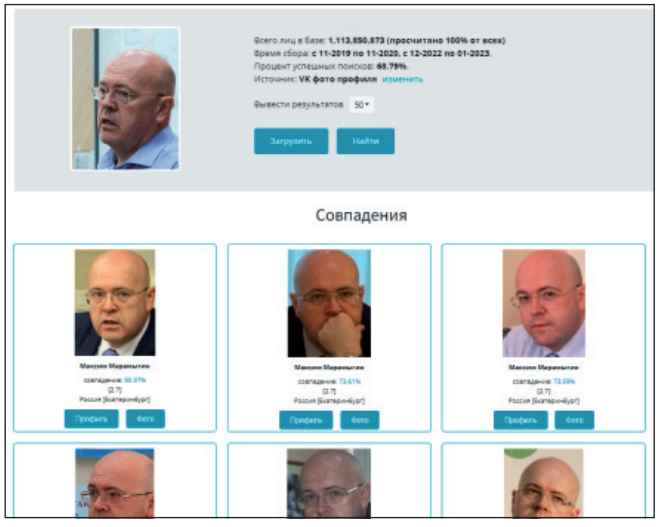


Рис. 4. Найденные совпадения фотографий по разным профилям социальной сети «ВКонтакте»

Fig. 4. Found matches of VK profiles based on photos

Кейс 3.

Условие. Представим, что в социальной сети мы нашли четыре фотографии с отдыха интересующего нас человека (рис. 6).

Задание. По имеющимся фотографиям необходимо определить, в каком городе отдыхал этот человек, в каком отеле, а затем установить адрес данного отеля.

Решение. Для поиска информации по фотографиям мы будем использовать инструмент Яндекс Картинки, а в качестве метода применим обратный поиск изображений[1].

1. Последовательно загрузим имеющиеся фотографии в сервис Яндекс Картинки (рис. 7).
2. Для начала попробуем найти город, где отдыхал наш объект. Выберем область поиска, двигая рамки на странице с загруженной фотографией (это будет фотография 2), и нажмем кнопку «Готово» (рис. 8).
3. Сервис показывает варианты мест, на которые наша фотография похожа, в следующем виде (рис. 9):
   - теги — «Екатеринбург», «центр», «здание», «Москва», «центр Екатеринбурга»;
   - похожие фотографии;
   - сайты, а в нашем случае это сайты с объявлениями об аренде жилья.
4. Проанализировав найденные похожие изображения, можно предположить, что исходная фотография представляет город Екатеринбург, а точнее — объект, расположенный по адресу: улица Малышева, д. 42а.
5. Для того чтобы подтвердить или опровергнуть наше предположение, необходимо использовать оставшиеся три интерьерные фотографии. На фотографии 4 больше индивидуальных деталей стилистики отеля, чем на фотографиях 1 и 3, поэтому искать будем по ней.
   Передвинем рамки на фотографию 4 и зададим область нового поиска (рис. 10).
6. В качестве похожих изображений сервис Яндекс Картинки предлагает нам фотографии отеля Radius.

[1] Обратный поиск изображений — это инструмент поиска информации по введенному (загруженному пользователем) изображению.

ISSN 0234-0453 • INFORMATICS AND EDUCATION • 2024 • Volume 39 No 2

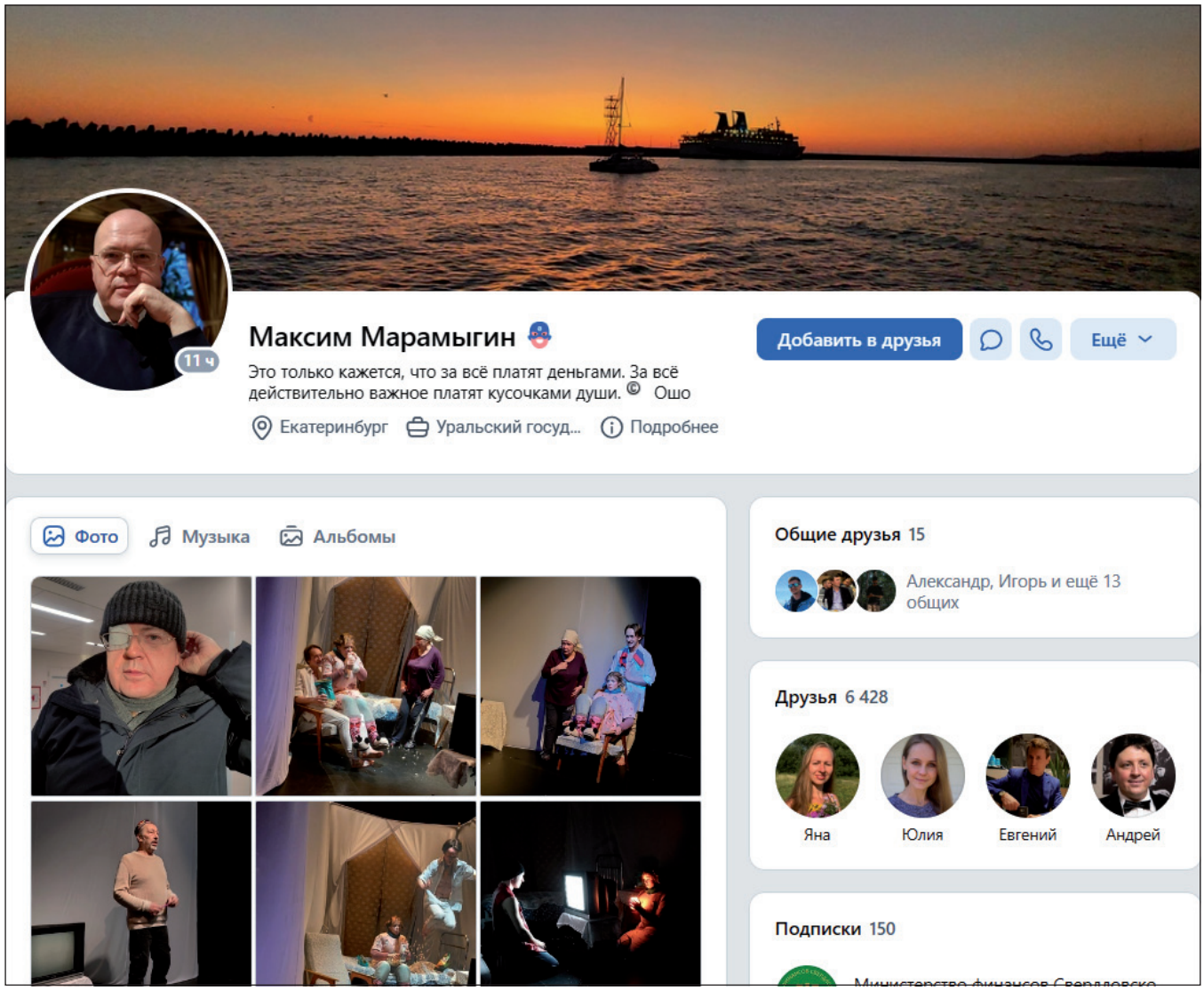


Рис. 5. Найденная страница поисковой цели в социальной сети «ВКонтакте»
Fig. 5. The found page of search target in the social network VK

Рис. 6. Имеющиеся исходные фотографии
Fig. 6. Available original photos

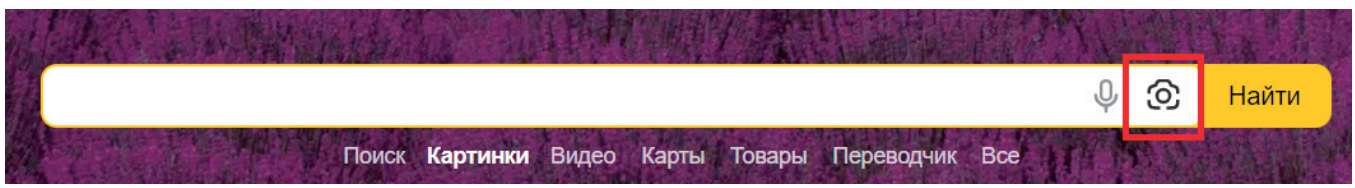


Рис. 7. Значок поиска по изображению в сервисе Яндекс Картинки
Fig. 7. The image search icon in Yandex Images

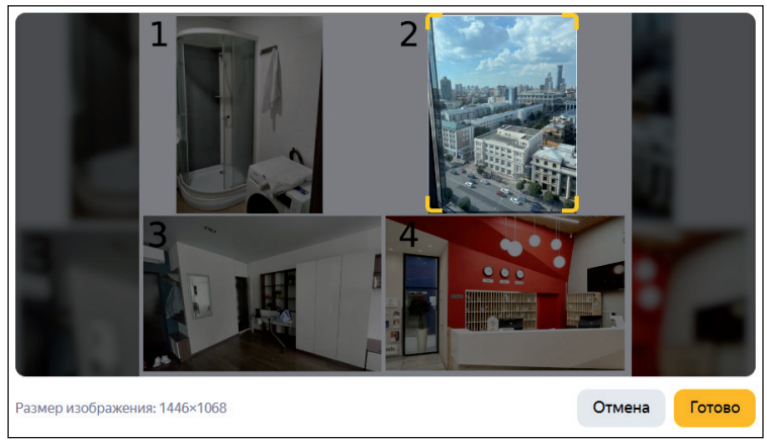


Рис. 8. Определение области поиска
Fig. 8. Defining the search area

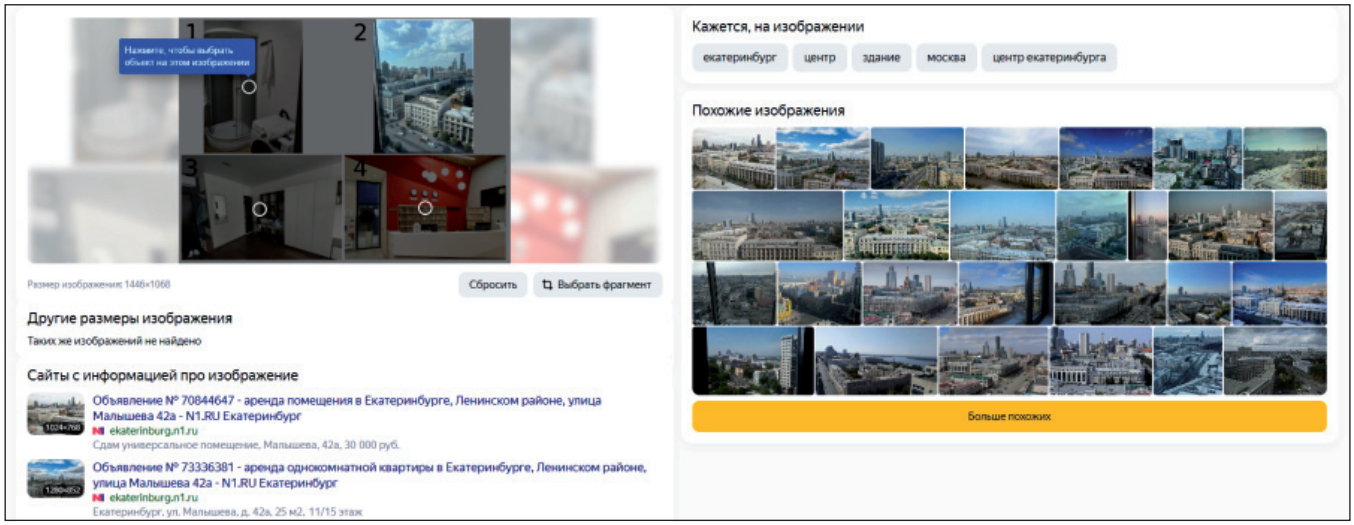


Рис. 9. Результат поиска в сервисе Яндекс Картинки
Fig. 9. The search result in the Yandex Images

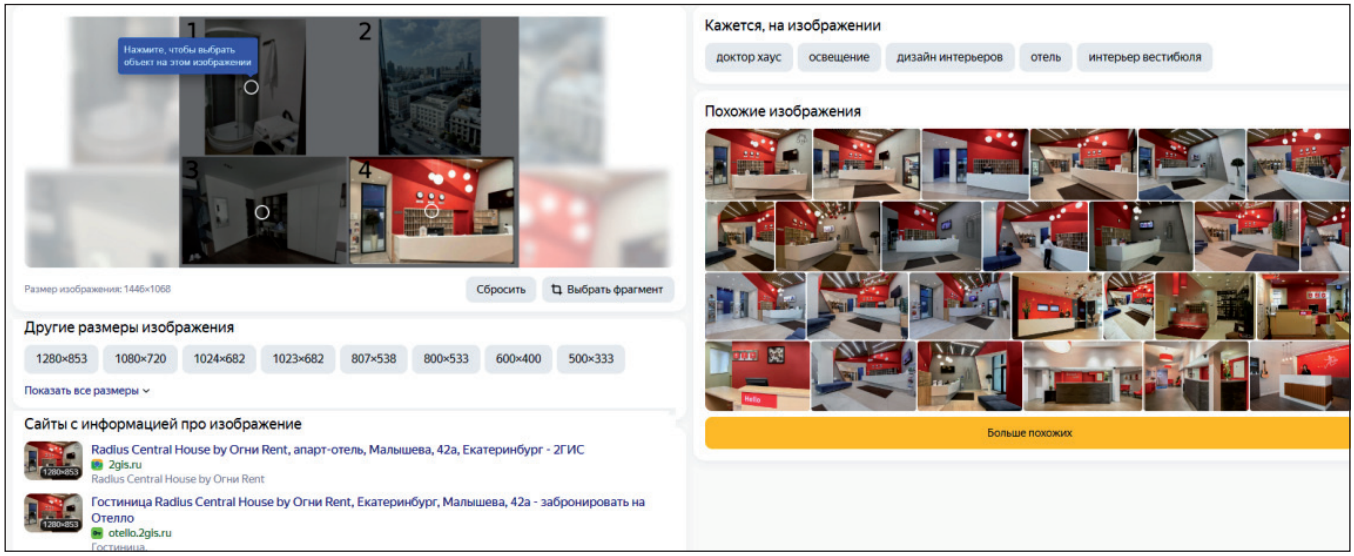


Рис. 10. Поиск схожих изображений по четвертой фотографии
Fig. 10. Searching for images similar to the fourth photo

ISSN 0234-0453 • INFORMATICS AND EDUCATION • 2024 • Volume 39 No 2

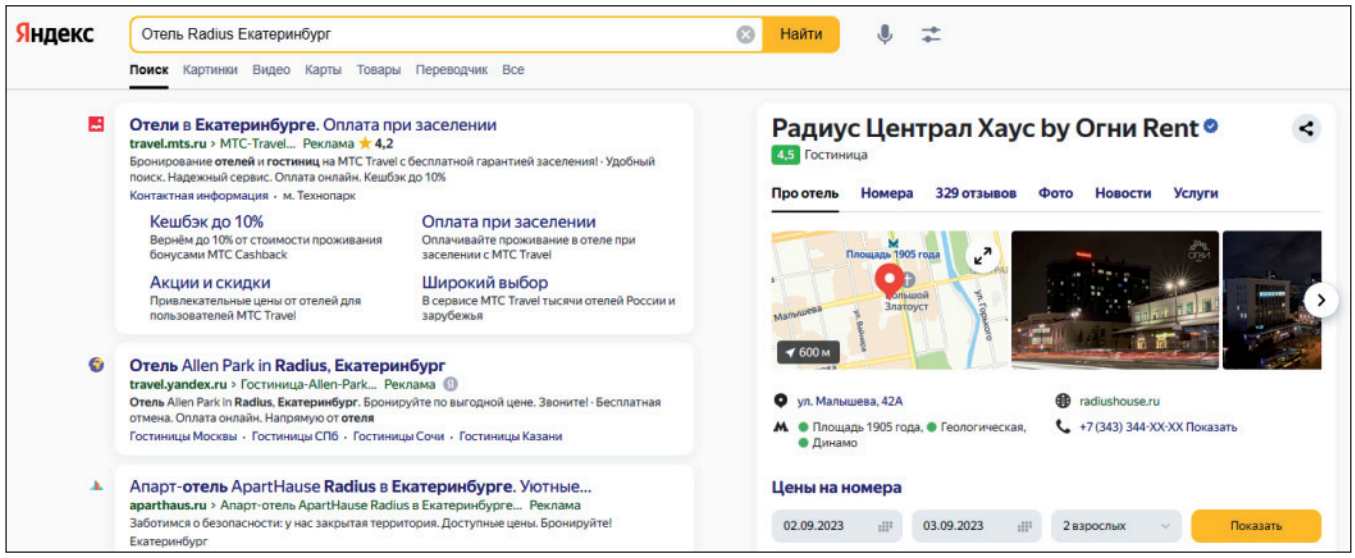


Рис. 11. Поиск отеля Radius в Екатеринбурге с помощью Яндекса
Fig. 11. Searching for the Radius hotel in Ekaterinburg using Yandex

7. В поисковой системе Яндекс выполним следующий запрос: «Отель Radius Екатеринбург» (рис. 11).

В поисковой выдаче мы видим, что действительно в Екатеринбурге есть данный отель и он находится по адресу: улица Малышева, д. 42а, — что совпадает с адресом, который мы получили как результат поиска по фотографии 2.

В качестве примеров упомянем еще несколько кейсов, использующихся на занятиях по обучению технологии разведки по открытым источникам.

Кейс 4.

Условие. В вашем распоряжении есть фото неизвестного.

Задание. Необходимо найти *официальную* страницу пользователя в социальной сети «ВКонтакте» по имеющейся фотографии (рис. 12) и деанонимизировать его.

Решение. Поиск ведется с использованием сервиса PimEyes.

Рис. 12. Фотография для выполнения задания по кейсу 4
Fig. 12. The photo for the case study assignment 4

Кейс 5.

Условие. В вашем распоряжении есть несколько фотографий одного ресторана (рис. 13).

Задание. Определите название ресторана и его местоположение (полный адрес).

Рис. 13. Фотографии для поиска ресторана
Fig. 13. Photos to identify the restaurant

Решение. Поиск ведется методом обратного поиска изображений (например, на сервисах ImageSearch, Dupli Checker, Google Images, TinEye и др.).

4. Анализ результатов решения кейсов студентами

Покажем реализацию принципа обратной связи в предложенной методике на конкретных примерах. После выполнения заданий студенческие работы под-

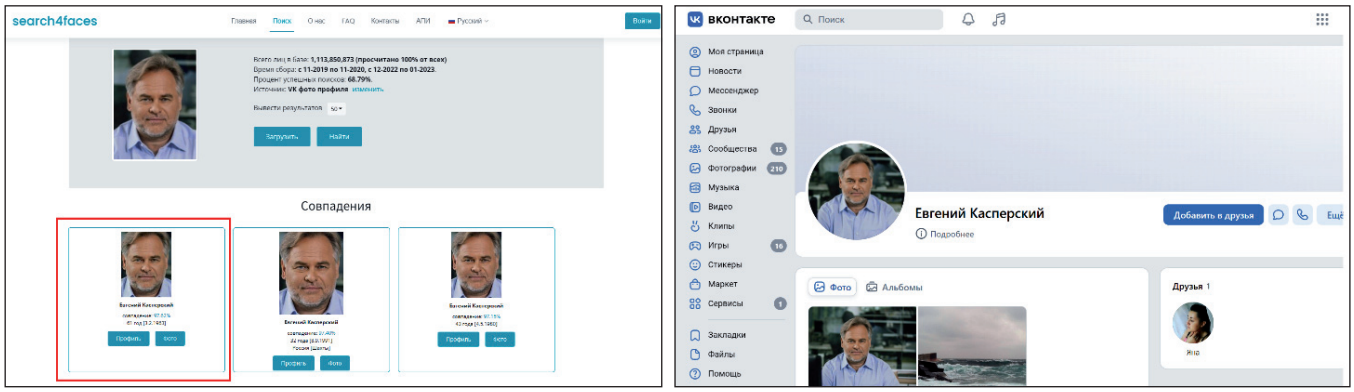


Рис. 14. Ошибка студентки при выполнении задания
Fig. 14. The student's mistake in completing an assignment

лежат тщательному анализу с целью оценки и обобщения результатов применения методики OSINT в учебном процессе. Сравним работы двух студентов.

Студентка О. при решении кейса 4 допустила ошибку: установив личность пользователя, которому принадлежит фотография, студентка не предоставила ссылку на его официальный профиль в социальной сети «ВКонтакте» и другие аргументы в качестве доказательства правильного ответа, выбрав один из фейковых аккаунтов. Верификацией официального профиля любого пользователя в данной соцсети служит галочка (в зависимости от условий верификации — серая или синяя) рядом с его именем (рис. 14). Преподаватель оценил работу *студентки О.* на 3 балла.

Студент В., выполняя тот же кейс 4 и получив результаты поиска по фотографии, заметил, что первый профиль «ВКонтакте» из предложенных поисковым сервисом не принадлежит реальному владельцу данной фотографии, так как на странице нет знака верификации (к тому же у этого пользователя мало друзей и т. п.). Поэтому студент решил, что данная страница не является официальным профилем пользователя (рис. 15), и продолжил поиск.

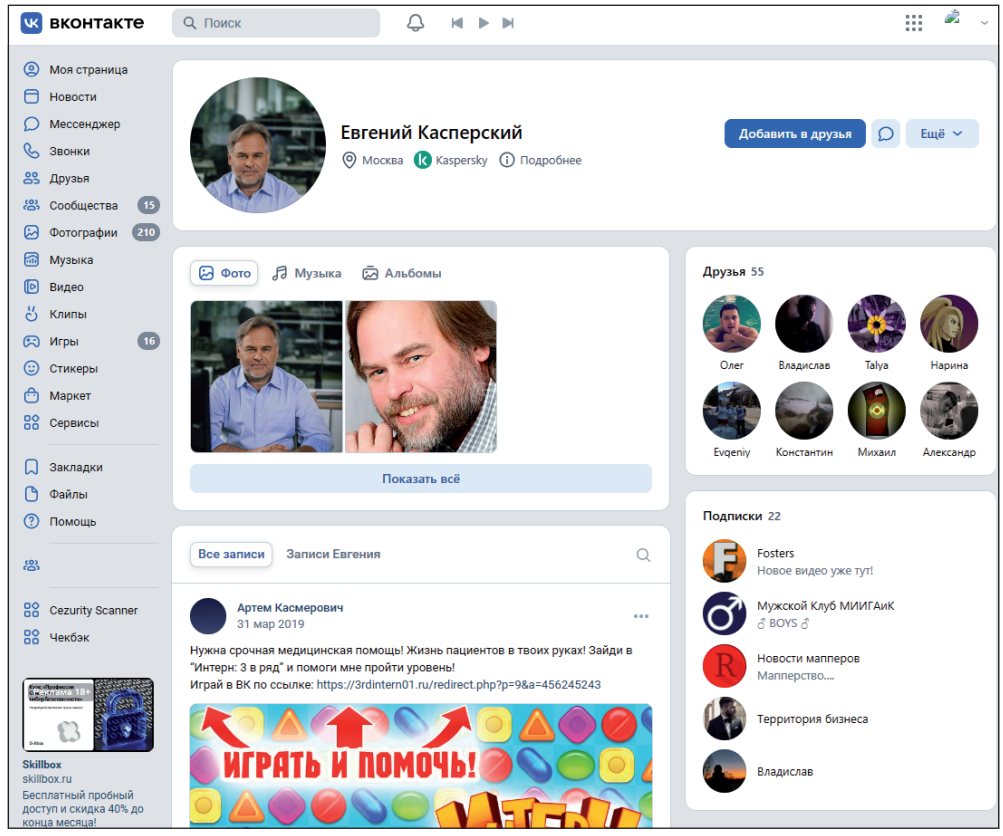


Рис. 15. Выявление студентом фейковой страницы пользователя
Fig. 15. The student's identification of a fake user page

ISSN 0234-0453 • INFORMATICS AND EDUCATION • 2024 • Volume 39 No 2

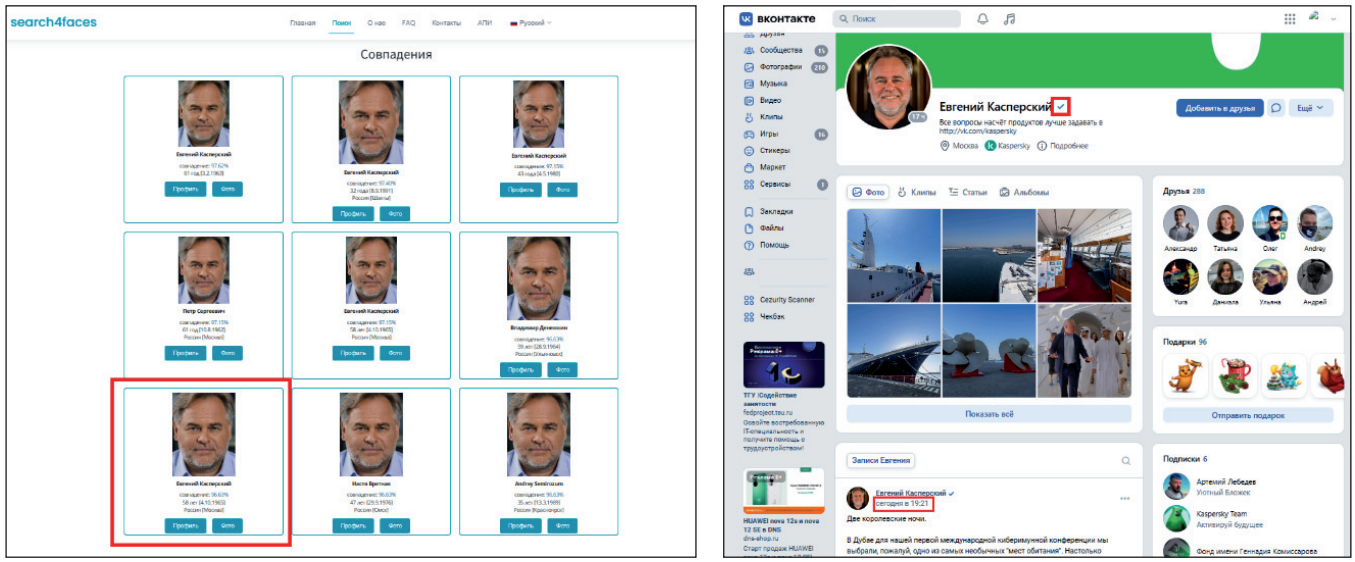
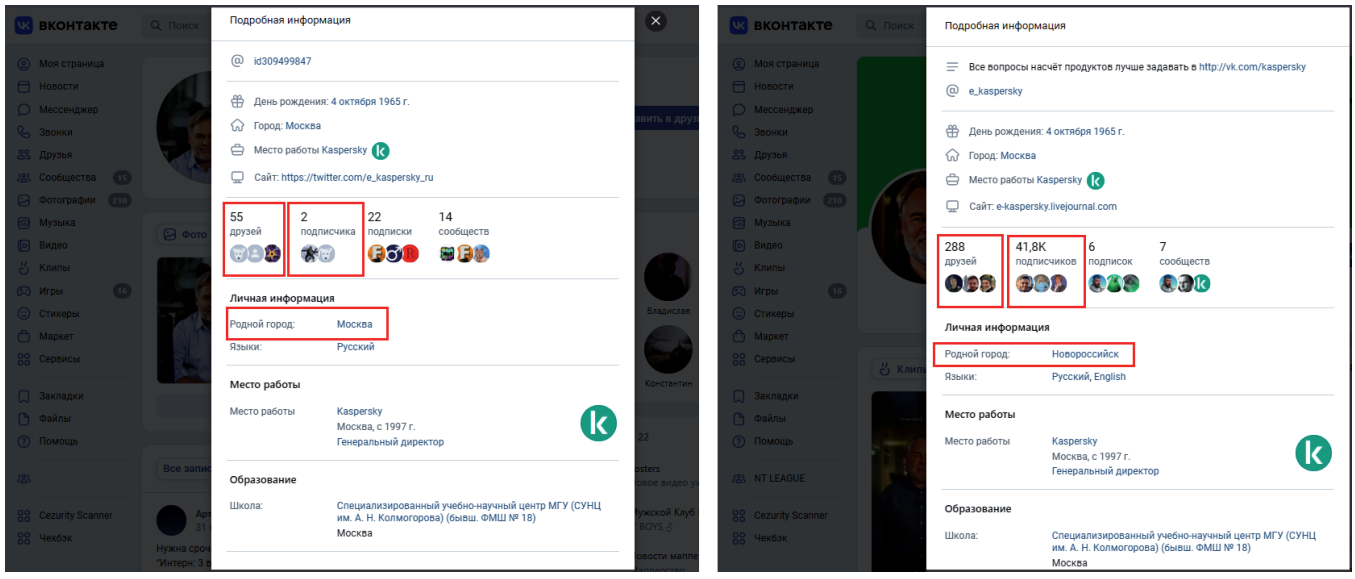


Рис. 16. Результат поисковой выдачи и официальная страница пользователя, найденная студентом
Fig. 16. The search result and the official user page found by a student

Он просмотрел следующие несколько профилей с высоким процентным совпадением изображений и нашел настоящую страницу искомого пользователя, официально подтвержденную синей галочкой (рис. 16).

Сравнив информацию на страницах первого из найденных профилей и верифицированного, студент еще раз убедился, что, несмотря на большой процент совпадения изображений, первый профиль в результатах поиска был фейковым: кроме уже упоминавшихся признаков, имеются фактологические ошибки и неточности (рис. 17). Преподаватель оценил работу *студента В.* на 5 баллов.

Работы с оценками преподавателя выдаются студентам. Те студенты, которые решили кейсы на «отлично», получают более слабые работы одногруппников с заданием найти ошибки. Это позволяет закрепить полученные ими навыки при решении ситуационной задачи и обратить внимание на типичные ошибки. Студентам, получившим балл ниже, чем «отлично», для анализа предлагаются работы отличников, чтобы разобраться в своих ошибках и выяснить правильный алгоритм работы. Затем организуется дискуссия: студенты размышляют над мнениями и комментариями друг друга, а пре-



а *б*

Рис. 17. Сравнение найденных профилей в социальной сети «ВКонтакте»:
а — фейковый профиль; б — официальный профиль
Fig. 17. The comparison of found profiles in the social network VK:
а — fake profile; б — official profile

подаватель помогает им подвести итоги и выделить ключевые идеи решения кейса.

Такой подход позволяет провести детальный анализ эффективности использования методики обучения технологиям OSINT в предложенных кейсах и выявить сильные и слабые стороны студенческих работ (типичные грубые и негрубые ошибки, недочеты). На основе подобного анализа преподаватель имеет возможность адаптировать методику обучения (усложнить или упростить кейсы, увеличить или уменьшить время на их выполнение и др.), что, безусловно, в дальнейшем позволит улучшить качество знаний студентов и повысить эффективность освоения профессиональных компетенций.

5. Заключение

Для организации эффективного процесса обучения специалистов в области информационной безопасности нами предложен индуктивный метод обучения и кейс-метод в качестве его инструмента. Важнейшими принципами выбранной методики обучения технологиям OSINT являются:

- мультидисциплинарный подход;
- постепенное усложнение кейсов, которые должны включать в себя изучение не только технических аспектов применения инструментов OSINT, но также правовых и этических норм и правил;
- обратная связь, которая подразумевает постоянное взаимодействие между преподавателями и студентами, с целью быстрой корректировки учебного процесса и его адаптации к определенному уровню освоения материала студентами.

В статье предлагается разработка специфических кейсов для обучения технологиям OSINT, направленных на решение реальных задач, с которыми специалисты в области информационной безопасности могут столкнуться в своей работе. Примененный подход облегчает понимание сложных инструментов и методов OSINT.

Основная цель предлагаемой методики — подготовить студентов к вызовам и проблемам, которые им придется преодолевать в профессиональной деятельности, и обеспечить высокий уровень профессиональной компетентности выпускников, обучавшихся по направлению подготовки «Информационная безопасность».

Список источников / References

1. *Bruner J. S.* The act of discovery. *Harvard Educational Review*. 1961;31(1):23–32.

2. *Dewey J.* How we think. New York, USA, Dover Publications; 1997. 240 p.

3. *Bransford J. D., Brown A. L., Cocking R. R.* How people learn: Brain, mind, experience, and school. Washington, D.C., USA, National Academy Press; 2000. 312 p.

4. *Lundeberg M. A., Levin B. B., Harrington H. L.* Who learns what from cases and how? The research base for teaching and learning with cases. Mahwah, N.J., USA, Lawrence Erlbaum Associates Inc.; 1999. 281 p.

5. *Lynn L. E.* Teaching and learning with cases: A guidebook. New York, USA, Chatham House Publishers; 1999. 176 p.

6. *Симонова О. Б., Исаева Т. Е.* Методика применения педагогических кейсов в обучении студентов технических вузов (эмпирическое исследование). *Общество: социология, психология, педагогика*. 2022;(9(101)):114–122. EDN: SYICMN. DOI: 10.24158/spp.2022.9.16.

[*Simonova O. B., Isaeva T. E.* Application methodology of pedagogical cases in teaching technical universities students (empirical research). *Obshchestvo: Sotsiologiya, Psikhologiya, Pedagogika*. 2022;(9(101)):114–122. (In Russian.) EDN: SYICMN. DOI: 10.24158/spp.2022.9.16.]

7. *Kardos G., Smith C. O.* On writing engineering cases. *Proc. ASEE National Conf. on Engineering Case Studies*. Washington, D.C., USA, 1979;(1):67–68.

8. *Никуличева Н. В.* Обучение студентов педагогических специальностей магистратуры методике преподавания предмета в условиях дистанционного обучения. *Вестник МГПУ. Серия: Информатика и информатизация образования*. 2022;(1(59)):67–81. EDN: VXSJIK. DOI: 10.25688/2072-9014.2022.59.1.08.

[*Nikulicheva N. V.* Training of students of teacher's specialties of the master's degree in the methodology of teaching the subject in the conditions of distance learning. *MCU Journal of Informatics and Informatization of Education*. 2022;(1(59)):67–81. (In Russian.) EDN: VXSJIK. DOI: 10.25688/2072-9014.2022.59.1.08.]

9. *Шармаев В. И., Андреева Я. А., Василевский К. А.* Обеспечение информационной безопасности с помощью разведки по открытым источникам (OSINT). *Вопросы защиты информации*. 2022;(2(137)):45–50. EDN: KRYLPB. DOI: 10.52190/2073-2600_2022_2_45.

[*Sharmaev V. I., Andreeva Ya. A., Vasilevsky K. A.* Information security through open source intelligence (OSINT). *Information Security Questions*. 2022;(2(137)):45–50. (In Russian.) EDN: KRYLPB. DOI: 10.52190/2073-2600_2022_2_45.]

10. *Сидорова М. Е., Кузьмин А. Р.* Разведка по открытым источникам данных и ее применение для решения задач кибербезопасности. *Вестник Российского нового университета. Серия: Сложные системы: модели, анализ и управление*. 2023;(1):61–74. EDN: KKCSVG. DOI: 10.18137/RNU.V9187.23.01.P.61.

[*Sidorova M. E., Kuzmin A. R.* OSINT and its application for cyber security. *Vestnik of Russian New University. Series: Complex Systems: Models, Analysis, Management*. 2023;(1):61–74. (In Russian.) EDN: KKCSVG. DOI: 10.18137/RNU.V9187.23.01.P.61.]

11. *Качалов А. Г., Лантаев М. М.* Подготовка специалистов по работе с открытыми данными в сети Интернет (OSINT) в гражданских и ведомственных вузах. *Юридическая наука: история и современность*. 2021;(9):98–106. EDN: MXKJOE.

[*Kachalov A. G., Lantaev M. M.* Training specialists in open data in the Internet (OSINT) in civil and departmental universities. *Juridical Science: History and Modernity*. 2021;(9):98–106. (In Russian.) EDN: MXKJOE.]

12. *Ungureanu G. T.* Open source intelligence (OSINT). The way ahead. *Journal of Defense Resources Management*. 2021;12(1):177–200.

13. *Benes L.* OSINT, new technologies, education: Expanding opportunities and threats. A new paradigm. *Journal of Strategic Security*. 2013;6(3):22–37. DOI: 10.5038/1944-0472.6.3S.3.

14. *Böhm I., Lolagar S.* Open source intelligence. Introduction, legal, and ethical considerations. *International Cybersecurity Law Review*. 2021;2:317–337. DOI: 10.1365/s43439-021-00042-7.

15. *Дворянкин О. А.* OSINT, pentest и нетсталкинг — информационные технологии интернета. *Национальная ассоциация ученых*. 2022;(84–2):6–13. EDN: LQLPWZ.

[*Dvoryankin O. A.* OSINT, pentest and netstalking — Internet information technologies. *Natsional'naya Assotsiatsiya Uchenykh.* 2022;(84–2):6–13. (In Russian.) EDN: LQLPWZ.]

16. *Гурский С. М., Кочетков И. В.* OSINT: пути развития. *Методы и технические средства обеспечения безопасности информации. Сборник материалов 33-й научно-технической конференции имени Петра Дмитриевича Зегжды.* Санкт-Петербург: Санкт-Петербургский политехнический университет Петра Великого; 2023;(32):50–52. EDN: VTPSGU. Режим доступа: https://disk.yandex.ru/i/Vt-oDneOSPOAjQ

[*Gursky S. M., Kochetkov I. V.* OSINT: Ways of development. *Methods and Technical Means of Information Security. Proc. 33rd Scientific and Technical Conf. named after Petr Dmitrievich Zegzhda.* Saint Petersburg, Peter the Great St. Petersburg Polytechnic University; 2023;(32):50–52. (In Russian.) EDN: VTPSGU. Available at: https://disk.yandex.ru/i/Vt-oDneOSPOAjQ]

17. *Шкрадюк А. Д., Назаров Д. М.* Технология OSINT: обзор сервисов с открытым исходным кодом. *Безопасность информационного пространства: сборник научных трудов XXI Всероссийской научно-практической конференции студентов, аспирантов и молодых ученых.* Екатеринбург: Уральский государственный университет путей сообщения; 2022;(4(252)):112–144. EDN: PHRSMV.

[*Shkradyuk A. D., Nazarov D. M.* OSINT technology: Review of open source services. *Security of Information Space: Collection of Scientific Works of the 21th All-Russian Scientific and Practical Conf. of Students, Postgraduates and Young Scientists.* Ekaterinburg, Ural State University of Railway Transport; 2022;(4(252)):112–144. (In Russian.) EDN: PHRSMV.]

Информация об авторах

Назаров Дмитрий Михайлович, доктор экон. наук, доцент, зав. кафедрой бизнес-информатики, зав. кафедрой информационной безопасности, Институт цифровых технологий управления и информационной безопасности, Уральский государственный экономический университет, Екатеринбург, Россия; *ORCID:* https://orcid.org/0000-0002-5847-9718; *e-mail:* slup2005@mail.ru

Симбирцев Руслан Арзуевич, магистрант направления подготовки 09.04.03 «Прикладная информатика», профиль «Цифровая бизнес-аналитика», кафедра бизнес-информатики, Институт цифровых технологий управления и информационной безопасности, Уральский государственный экономический университет, Екатеринбург, Россия; аналитик данных службы безопасности, АО «Точка», Екатеринбург, Россия; *ORCID:* https://orcid.org/0009-0002-5245-6475; *e-mail:* rsimbirtsev@mail.ru

Салалайко Данил Павлович, магистрант направления подготовки 09.04.03 «Прикладная информатика», профиль «Цифровая бизнес-аналитика», кафедра бизнес-информатики, Институт цифровых технологий управления и информационной безопасности, Уральский государственный экономический университет, Екатеринбург, Россия; администратор информационной безопасности, АО «Точка», Екатеринбург, Россия; *ORCID:* https://orcid.org/0009-0000-2041-0515; *e-mail:* d_pavlovich@bk.ru

Information about the authors

Dmitry M. Nazarov, Doctor of Science (Economics), Docent, Head of the Department of Business Informatics, Head of the Department of Information Security, Institute of Digital Management Technologies and Information Security, Ural State University of Economics, Ekaterinburg, Russia; *ORCID*: https://orcid.org/0000-0002-5847-9718; *e-mail*: slup2005@mail.ru

Ruslan A. Simbirtsev, a master student of the educational program 09.04.03 "Applied Informatics", profile "Digital Business Analytics", Department of Information Security, Institute of Digital Management Technologies and Information Security, Ural State University of Economics, Ekaterinburg, Russia; Security Data Analyst, JSC "Tochka", Ekaterinburg, Russia; *ORCID*: https://orcid.org/0009-0002-5245-6475; *e-mail*: rsimbirtsev@mail.ru

Danil P. Salalayko, a master student of the educational program 09.04.03 "Applied Informatics", profile "Digital Business Analytics", Department of Information Security, Institute of Digital Management Technologies and Information Security, Ural State University of Economics, Ekaterinburg, Russia; Information Security Administrator, JSC "Tochka", Ekaterinburg, Russia; *ORCID*: https://orcid.org/0009-0000-2041-0515; *e-mail*: d_pavlovich@bk.ru

Поступила в редакцию / Received: 21.12.23.
Поступила после рецензирования / Revised: 29.01.24.
Принята к печати / Accepted: 30.01.24.