DOI 10.37882/2223–2982.2025.11–3.26

# ПРАКТИКО-ОРИЕНТИРОВАННЫЕ КЕЙСЫ, ОБУЧАЮЩИЕ РАБОТЕ С БОЛЬШИМИ ДАННЫМИ И КУЛЬТУРЕ КИБЕРБЕЗОПАСНОСТИ

## PRACTICE-ORIENTED CASES THAT TEACH WORKING WITH BIG DATA AND CYBERSECURITY CULTURE

***O. Liseikina***
***I. Kutlikova***
***O. Kishkinova***

*Summary:* There is a paradoxical situation in the modern digital economy: despite the growing demand for specialists in the field of big data and cybersecurity, traditional educational approaches are not effective enough to train competent personnel. The relevance of the research is due to the need to bridge the gap between students' theoretical training and the practical requirements of the industry, where big data skills and cybersecurity culture are becoming interrelated competencies. The purpose of this research is to develop and theoretically substantiate a system of practice-oriented cases aimed at simultaneously developing competencies for working with big data and a cybersecurity culture. As a result of the research, four author's cases have been developed and described, adapted for use in the pedagogical practice of higher educational institutions. The discussion of the results of the implementation of the developed cases allows us to identify several significant patterns. Firstly, an integrated approach to learning how to work with big data and cybersecurity culture contributes to a more holistic understanding of modern IT systems in which these aspects are inextricably linked. Secondly, the practice-oriented nature of the cases, their proximity to real professional situations, increases students' motivation and promotes deeper learning of the material. An important aspect is also the gradual complication of cases, which allows students to consistently build up competencies, moving from solving relatively simple tasks to complex complex problems. The proposed approach contributes not only to the acquisition of technical knowledge, but also to the development of analytical thinking, an understanding of the ethical aspects of working with data, and the formation of sustainable behavioral patterns in the field of cybersecurity.

*Keywords:* practice-oriented learning, big data, cybersecurity culture, pedagogical cases, teaching methods.

***Лисейкина Ольга Витальевна***
*Старший преподаватель, Московская государственная академия ветеринарной медицины и биотехнологии имени К.И. Скрябина*
*ofoxi73@bk.ru*
***Кутликова Ирина Вениаминовна***
*Старший преподаватель, Московская государственная академия ветеринарной медицины и биотехнологии имени К.И. Скрябина*
*ivk-b@yandex.ru*
***Кишкинова Ольга Алексеевна***
*Старший преподаватель, Московская государственная академия ветеринарной медицины и биотехнологии имени К.И. Скрябина*
*olga.19672015@yandex.ru*

*Аннотация:* В современной цифровой экономике наблюдается парадоксальная ситуация: несмотря на растущий спрос на специалистов в области больших данных и кибербезопасности, традиционные образовательные подходы оказываются недостаточно эффективными для подготовки компетентных кадров. Актуальность исследования обусловлена необходимостью преодоления разрыва между теоретической подготовкой студентов и практическими требованиями индустрии, где навыки работы с большими данными и культура кибербезопасности становятся взаимосвязанными компетенциями. Целью данного исследования является разработка и теоретическое обоснование системы практико-ориентированных кейсов, направленных на одновременное формирование компетенций работы с большими данными и культуры кибербезопасности. В результате исследования разработаны и описаны четыре авторских кейса, адаптированных для применения в педагогической практике высших учебных заведений. Обсуждение результатов внедрения разработанных кейсов позволяет выявить несколько значимых закономерностей. Во-первых, интегрированный подход к обучению работе с большими данными и культуре кибербезопасности способствует формированию более целостного понимания современных ИТ-систем, в которых эти аспекты неразрывно связаны. Во-вторых, практико-ориентированный характер кейсов, их приближенность к реальным профессиональным ситуациям повышает мотивацию студентов и способствует более глубокому усвоению материала. Важным аспектом является также постепенное усложнение кейсов, которое позволяет студентам последовательно наращивать компетенции, переходя от решения относительно простых задач к сложным комплексным проблемам. Предложенный подход способствует не только приобретению технических знаний, но и развитию аналитического мышления, пониманию этических аспектов работы с данными и формированию устойчивых поведенческих паттернов в области кибербезопасности.

*Ключевые слова:* практико-ориентированное обучение, большие данные, культура кибербезопасности, педагогические кейсы, методы обучения.

## Введение

Актуальность интеграции обучения работе с большими данными и культуре кибербезопасности в современном образовательном процессе невозможно переоценить. Цифровая трансформация всех сфер общественной жизни привела к тому, что ежедневно генерируется свыше 2,5 квинтиллионов байтов данных, а сложность и изощренность кибератак постоянно возрастает, с 86% данных утечек, связанных с компроме-

тацией учетных данных [8]. В таких условиях подготовка специалистов, способных не только обрабатывать и анализировать большие данные, но и обеспечивать их защиту, становится стратегической задачей системы высшего образования. Однако, как показывают исследования, традиционные методы обучения, основанные на пассивном усвоении информации, оказываются малоэффективными для формирования практических навыков и поведенческих паттернов в области кибербезопасности. Метаанализ, проведенный в 2024 году Лейденским университетом, продемонстрировал, что хотя обучение значительно улучшает знания (размер эффекта $d \approx 1,02$), оно оказывает лишь незначительное влияние на реальное поведение ($d \approx 0,36$) [10]. Этот разрыв между знанием и действием указывает на необходимость разработки новых педагогических подходов, способных преодолеть указанные противоречия.

Целью данного исследования является разработка и теоретическое обоснование системы практико-ориентированных кейсов, направленных на одновременное формирование компетенций работы с большими данными и культуры кибербезопасности. В отличие от существующих подходов, предлагаемые кейсы построены по принципу интеграции двух областей знаний, что отражает реальные профессиональные вызовы, с которыми сталкиваются современные специалисты.

## Материалы и методы исследования

Методологической основой исследования служит практико-ориентированный подход в образовании, который трактуется как организация учебного процесса, направленная на формирование у будущих специалистов готовности решать профессиональные задачи через погружение в контекст, максимально приближенный к реальной практике [2, 5]. В контексте данного исследования практико-ориентированные кейс-ситуации понимаются как проблемные задания, включающие описание ситуации и вопросы к ней, направленные на применение знаний в области больших данных и кибербезопасности, развитие аналитического и критического мышления и формирование готовности решать профессиональные задачи.

Для разработки кейсов использовался комплекс методов исследования: анализ профессиональной литературы и реальных инцидентов в области больших данных и кибербезопасности. Изучались отчеты о крупных утечках данных, случаи внедрения машинного обучения для защиты информации в банковской сфере, а также практики компаний, успешно использующих технологию больших данных. Это позволило обеспечить аутентичность разрабатываемых кейсов и их соответствие реальным вызовам, с которыми сталкиваются специалисты. Также использован контекстно-ориентированный подход, предполагающий, что обучение должно происходить в условиях, максимально приближенных к реальной профессиональной деятельности. Каждый кейс содержит не только технические задачи, но и учитывает организационный контекст, этические дилеммы и ограничения ресурсов, с которыми сталкиваются специалисты в повседневной работе.

Разработанные кейсы предназначены для использования в образовательном процессе высших учебных заведений при подготовке специалистов в области информационных технологий, анализа данных, а также в программах повышения квалификации работающих специалистов. Внедрение кейсов предполагает сочетание индивидуальной и групповой работы, проведение дискуссий и презентаций решений, что способствует развитию не только профессиональных, но и коммуникативных компетенций студентов.

## Результаты и обсуждения

В последние годы наблюдается многократное возрастание угроз в современном киберпространстве, их ярко выраженная агрессивная направленность на внешнюю и внутреннюю безопасность Российской Федерации, значительный рост киберпреступлений [3]. Разнообразие киберугроз требует от предприятий разработки и внедрения комплексных стратегий по кибербезопасности для защиты своих данных и инфраструктуры.

В результате исследования были разработаны четыре практико-ориентированных кейса, каждый из которых направлен на формирование комплекса компетенций в области больших данных и кибербезопасности. Кейсы построены по принципу постепенного усложнения и увеличения степени самостоятельности студентов при их выполнении.

Кейс 1 - Анализ инцидента утечки данных через аномальную активность привилегированных пользователей. Цель кейса - формирование навыков выявления аномалий в поведении пользователей через анализ логов доступа к большим данным. Студентам предлагается ретроспективно проанализировать структурированный набор данных, содержащий записи доступа к корпоративному хранилищу данных, и идентифицировать подозрительную активность, указывающую на возможную утечку информации. Этот кейс основан на реальных практиках банковского сектора, где машинное обучение используется для мониторинга аномальной активности пользователей [1].

Содержание кейса включает структурированный набор данных с записями входов пользователей за три месяца, содержащий информацию о времени доступа, объеме скачанных данных, IP-адресах и уровне приви-

легий пользователей. В данные искусственно внедрены паттерны, характерные для инсайдерских угроз: несанкционированные доступы в нерабочее время, аномально большие объемы скачивания и доступы с необычных географических локаций. Студенты должны использовать методы анализа больших данных (агрегация, кластеризация, выявление аномалий) для идентификации подозрительной активности и предложить систему правил для автоматического обнаружения подобных инцидентов в будущем.

Образовательный потенциал кейса заключается в формировании понимания взаимосвязи между методами анализа больших данных и задачами кибербезопасности. Студенты не только осваивают технические навыки работы с записями, но и развивают критическое мышление, учась отличать реальные угрозы от ложных срабатываний, что является одной из главных проблем в современных системах безопасности [4, 7].

Кейс 2 - Разработка системы обнаружения фишинговых атак с применением машинного обучения. Цель кейса – освоение принципов создания систем машинного обучения для задач кибербезопасности на основе больших данных. Студенты получают набор данных, содержащий характеристики электронных писем (метаданные, содержание, заголовки) с разметкой «фишинг» / «не фишинг», на основе которого необходимо разработать и обучить классификационную модель.

Содержание кейса предполагает выполнение полного цикла работы с данными: предобработку и очистку, разработка функциональных возможностей, выбор и обучение модели, оценку ее эффективности. Особое внимание уделяется проблеме интерпретируемости результатов - студенты должны не только достичь высокой точности классификации, но и объяснить, какие признаки наиболее значимы для обнаружения фишинговых писем. Этот аспект особенно важен, поскольку одной из проблем ML-моделей в безопасности является их характер «черного ящика» [1].

Образовательный потенциал кейса связан с формированием целостного представления о возможностях и ограничениях машинного обучения в кибербезопасности. Студенты сталкиваются с типичными вызовами аналитиков больших данных: несбалансированностью классов, проблемой переобучения, необходимостью обработки неструктурированных текстовых данных. При этом они осваивают не только технические аспекты, но и учатся оценивать риски, связанные с развертыванием таких систем в реальной корпоративной среде.

Кейс 3 – Проектирование системы мониторинга и защиты больших данных в распределенной инфраструктуре. Цель кейса – формирование навыков проектирования комплексных систем защиты больших данных в распределенных средах, таких как Hadoop или Spark кластеры. В отличие от предыдущих кейсов, фокус смещается с анализа данных на проектирование архитектуры безопасности. Содержание кейса представляет собой описание бизнес-ситуации: компания разворачивает распределенную инфраструктуру для обработки больших данных, содержащих конфиденциальную информацию, и нуждается в разработке комплексной системы защиты. Студенты должны предложить архитектуру безопасности, включающую аутентификацию, авторизацию, шифрование данных при остановке и в движении, мониторинг подозрительной активности и систему оповещения об инцидентах. При этом необходимо учитывать требования производительности - предлагаемые решения не должны существенно замедлять обработку данных [9].

Образовательный потенциал кейса заключается в развитии системного мышления и понимания взаимосвязи различных аспектов защиты больших данных. Студенты знакомятся с новыми технологиями для управления доступом, для управления метаданными и отслеживания данных, а также методами шифрования и токенизации. Кроме того, кейс поднимает важные вопросы соответствия требованиям регуляторов, что является неотъемлемой частью современной культуры кибербезопасности.

Кейс 4 – Этический хакинг и защита от атак на модели машинного обучения. Цель кейса – формирование понимания уязвимостей моделей машинного обучения и методов защиты от атак на системы искусственного интеллекта. Этот кейс представляет наибольшую сложность и предназначен для студентов, уже обладающих базовыми знаниями в области больших данных и машинного обучения.

Содержание кейса включает две взаимосвязанные задачи: во-первых, студенты выступают в роли этических хакеров, пытаясь обойти созданную ранее модель обнаружения фишинговых атак через методы машинного обучения; во-вторых, они должны разработать механизмы защиты, повышающие устойчивость модели к таким атакам. Этот кейс отражает современный тренд, когда злоумышленники также используют алгоритмы машинного обучения для создания вредоносных программ, анализа пользовательского поведения и поиска уязвимостей [1].

Образовательный потенциал кейса связан с формированием продвинутых компетенций в области безопасности искусственного интеллекта - одной из самых актуальных и быстроразвивающихся областей кибербезопасности. Студенты не только углубляют понимание ограничений ML-моделей, но и развивают прогностическое мышление, учась находить возможные векторы

атак и разрабатывать превентивные меры защиты.

Далее в таблице представим сравнительную характеристику разработанных практико-ориентированных кейсов, обучающих работе с большими данными и культуре кибербезопасности. (Таб. 1.)

Обсуждение результатов внедрения разработанных кейсов позволяет выявить несколько значимых закономерностей. Во-первых, интегрированный подход к обучению работе с большими данными и культуре кибербезопасности способствует формированию более целостного понимания современных ИТ-систем, в которых эти аспекты неразрывно связаны. Во-вторых, практико-ориентированный характер кейсов, их приближенность к реальным профессиональным ситуациям повышает мотивацию студентов и способствует более глубокому усвоению материала. Это подтверждается результатами мета-анализа, показавшего, что увлекательное и релевантное обучение, где пользователи видят непосредственную связь со своей работой и сталкиваются с реалистичными задачами, вызывает больший отклик [6].

Важным аспектом является также постепенное усложнение кейсов, которое позволяет студентам последовательно наращивать компетенции, переходя от решения относительно простых задач к сложным комплексным проблемам. Такой подход соответствует принципу «от простого к сложному» и создает условия для непрерывного профессионального роста. Кроме того, разнообразие типов кейсов (аналитические, проектные, исследовательские) способствует формированию разносторонних компетенций, необходимых современному специалисту.

Следует отметить, что эффективность применения разработанных кейсов в значительной степени зависит от методики их внедрения в образовательный процесс. Как показано в исследовании Лейденского университета, программы, выполненные формально для галочки (например, скучные обязательные презентации раз в год), практически не меняют поведения [10]. В связи с этим, использование кейсов должно сопровождаться активными методами обучения: дискуссиями, проектными сессиями, симуляциями реальных профессиональных ситуаций. Особую важность имеет создание «безопасной» образовательной среды, где студенты могут совершать ошибки и учиться на них без серьезных последствий — это особенно актуально для сферы кибербезопасности.

Внедрение разработанных практико-ориентированных кейсов в образовательный процесс высших учебных заведений будет способствовать подготовке специалистов нового поколения, обладающих не только техническими знаниями в области больших данных, но и сформированной культурой кибербезопасности, что является критически важным в условиях цифровой трансформации всех сфер общественной жизни.

## Выводы

Проведенное исследование позволило разработать и теоретически обосновать систему практико-ориентированных кейсов, направленных на интегративное обучение работе с большими данными и культуре кибербезопасности. На основе анализа профессиональной литературы и реальных кейсов были созданы четыре оригинальных кейса, охватывающих различные аспекты этой комплексной проблемы - от анализа аномальной активности пользователей до защиты моделей машинного обучения от атак. Интегрированный подход к обучению работе с большими данными и культуре кибербезопасности является методически обоснованным, поскольку отражает реальную взаимосвязь этих областей в профессиональной деятельности. Раздельное изучение этих дисциплин создает искусственный барьер, который препятствует формированию целостного понимания современных ИТ-систем.

Предложенная система кейсов, построенная на принципе постепенного усложнения задач, позволя-

Таблица 1.

Сравнительная характеристика разработанных практико-ориентированных кейсов, обучающих работе с большими данными и культуре кибербезопасности.

| Название кейса | Основные формируемые компетенции | Уровень сложности |
|---|---|---|
| Анализ инцидента утечки данных через аномальную активность привилегированных пользователей | Анализ логов, выявление аномалий, интерпретация результатов | Базовый |
| Разработка системы обнаружения фишинговых атак с применением машинного обучения | Обработка естественного языка, разработка функциональных возможностей, классификация, валидация моделей | Средний |
| Проектирование системы мониторинга и защиты больших данных в распределенной инфраструктуре | Проектирование архитектуры безопасности, управление доступом, шифрование, мониторинг | Продвинутый |
| Этический хакинг и защита от атак на модели машинного обучения | Состязательное машинное обучение, методы повышения устойчивости моделей, тестирование на проникновение | Экспертный |

Источник: составлено автором

ет последовательно формировать профессиональные компетенции – от базовых навыков анализа данных до проектирования комплексных систем защиты. Такой подход соответствует дидактическому принципу доступности и обеспечивает возможность индивидуальной образовательной траектории. Практико-ориентированный характер кейсов, их приближенность к реальным профессиональным ситуациям повышает мотивацию студентов и способствует преодолению разрыва между знанием и действием – основной проблемы, выявленной в современных исследованиях эффективности обучения кибербезопасности. Эффективность применения разработанных кейсов в значительной степени зависит от методов их внедрения в образовательный процесс. Активные формы обучения, такие как дискуссии, проектные сессии и симуляции, значительно повышают образовательный эффект по сравнению с пассивным изучением материала.

ЛИТЕРАТУРА

1. Вичугова А.А. 5 причин, почему машинное обучение не заменит другие методы Cybersecurity и реальные примеры эффективного использования ML для защиты данных // Школа больших данных. 2025. - URL: https://bigdataschool.ru/blog/ml-cybersecurity-use-cases-and-perspectives/ (дата обращения: 12.11.2025).
2. Качалова Л.П., Светоносова Л.Г. Понятие, виды и характеристика практико-ориентированных кейс-ситуаций, используемых в подготовке будущих педагогов // Вестник Шадринского государственного педагогического университета. – 2021. – №4(52). – С. 73–75.
3. Ковалев О.Г., Семенова Н.В. Кибербезопасность современной России: теоретические и организационно-правовые аспекты // Столыпинский вестник. – 2021. - №3. – С. 14–19.
4. Количество кибератак на российский бизнес по итогам 2024 года выросло в четыре раза – подсчитали эксперты // Cyber Media. – URL: https://securitymedia.org/news/kolichestvo-kiberatak-na-rossiyskiy-biznes-po-itogam-2024-goda-vyroslo-v-chetyre-raza-podschitali- (дата обращения: 12.11.2025).
5. Копылова И.В. Кейс-метод в контексте практико-ориентированного обучения // Вестник науки. – 2025. – Т.5, ч.1. - №6. – С. 447–456.
6. Обучение по кибербезопасности - главное из исследований // Хабр. – 2025. URL: https://habr.com/ru/articles/958276/ (дата обращения: 12.11.2025).
7. Сафонова М.Ф., Ципляева С.А. Кибербезопасность: проблемы и решения // Естественно-гуманитарные исследования. – 2019. - №24(2). – С. 63–68.
8. Alani M.M. Big data in cybersecurity: a survey of applications and future trends // Reliable Intell Environ. – 2021. - № 7. – pp. 85–114. https://doi.org/10.1007/s40860-020-00120-3.
9. Aldorisio J Best Practices for Cybersecurity Auditing [a Step-by-Step Checklist] // Securityscorecard. – URL: https://securityscorecard.com/blog/best-practices-for-a-cybersecurity-audit (date of application: 12.11.2025).
10. Prümmer J., van Steen T., van den Berg B. Assessing the effect of cybersecurity training on End-users: A Meta-analysis // Computers & Security. – 2024. – V.150. – pp. 104206. Doi: https://doi.org/10.1016/j.cose.2024.104206.



Журнал «Современная наука: актуальные проблемы теории и практики»