

Полицейская деятельность

Правильная ссылка на статью:

Темняков Д.А., Миронов В.Л. Дидактические особенности реализации в образовательных организациях МВД России профессионально-ориентированных дисциплин, связанных с противодействием преступлениям, совершенным с использованием информационно-коммуникационных технологий // Полицейская деятельность. 2024. № 1. DOI: 10.7256/2454-0692.2024.1.69918 EDN: YSUVNT URL: https://nbpublish.com/library_read_article.php?id=69918

Дидактические особенности реализации в образовательных организациях МВД России профессионально-ориентированных дисциплин, связанных с противодействием преступлениям, совершенным с использованием информационно-коммуникационных технологий

Темняков Дмитрий Александрович

кандидат педагогических наук

заместитель начальника кафедры организации деятельности подразделений по обеспечению безопасности дорожного движения московского областного филиала Московского университета МВД России имени В.Я. Кикотя

143100, Россия, Московская область, пос. Старотеряево, Старотеряево, 1

✉ Dima-terjewo@rambler.ru



Миронов Вадим Леонидович

старший преподаватель, кафедра оперативно-разыскной деятельности ОВД и применения информационных технологий, Московский областной филиал Московского университета МВД России имени В.Я. Кикотя

143100, Россия, Московская область, пос. Новотеряево, ул. Николая Григорьева, 5, кв. 17

✉ v.miro@mail.ru



[Статья из рубрики "Профессиональная подготовка сотрудников полиции"](#)

DOI:

10.7256/2454-0692.2024.1.69918

EDN:

YSUVNT

Дата направления статьи в редакцию:

20-02-2024

Аннотация: Предметом исследования являются особенности обучения информационно-

коммуникационным технологиям в образовательных организациях высшего образования. Объектом исследования выступает реализация профессионально-ориентированных дисциплин, связанных с противодействием преступлениям, совершенным с использованием информационно-коммуникационных технологий в образовательных организациях высшего образования системы МВД России. Авторы подробно рассматривают внедрение информационных и коммуникационных технологий в образовательный процесс их эффективность в решении прикладных задач по улучшению учебного процесса, повышению активности обучающихся через их вовлечение в различные виды деятельности и стимулирование образовательной активности. Особое внимание авторы уделяют использованию информационно-коммуникационных технологий в педагогическом процессе учебных организаций системы МВД России. Авторами раскрываются проблемы реализации профессионально-ориентированных дисциплин, связанных с противодействием преступлениям, совершенным с использованием информационно-коммуникационных технологий. Методы исследования: в процессе исследования применялись диалектический метод научного познания, а также комплекс общенаучных и специальных методов изучения теоретических основ педагогики, творческое осмысление проблем использования информационно-коммуникационных технологий в учебном процессе. Внедрение научных выводов и рекомендаций в практику преподавания профессионально-ориентированных дисциплин. Основными выводами проведенного исследования являются предложенные авторами пути решения проблем реализации профессионально-ориентированных дисциплин. Рассмотрены основные дидактические вопросы «Кто должен быть обучен?», «Чему нужно учить?», «Каким образом следует проводить обучение?» и «Кто будет осуществлять обучение?» профессионально-ориентированного обучения, связанного с противодействием преступлениям, совершенным с использованием информационно-коммуникационных технологий. Особым вкладом авторов в исследование темы является предложенная ими методика обучения слушателей и курсантов вузов МВД России противодействию преступлениям, совершенным с использованием информационно-коммуникационных технологий. Авторы, отмечают, что обучение должно осуществляться с использованием междисциплинарного подхода, включая элементы юриспруденции, информационных технологий, психологии, социологии и других соответствующих областей знаний. Новизна исследования заключается в раскрытии основных дидактических принципов реализации профессионально-ориентированного обучения, связанного с противодействием преступлениям, совершенным с использованием информационно-коммуникационных технологий.

Ключевые слова:

информационно-коммуникационные технологии, юридическое образование, профессионально-ориентированные дисциплины, дидактическое обеспечение, методическое обеспечение, квалификация преподавателя, образовательный процесс, технология обучения, проблемы обучения, специалитет

Информационно-коммуникационные технологии позволяют собирать, обрабатывать, хранить, распространять и отображать информацию различного типа, а также обеспечивают взаимодействие между людьми с помощью электронных коммуникационных средств.

На юридических специальностях в вузах МВД России уже более двадцати лет изучаются

основы информационно-коммуникационных технологий (ИКТ) в рамках различных дисциплин, таких как «Информатика и математика», «Информатика и информационные технологии в профессиональной деятельности», «Информационно-коммуникационные технологии в профессиональной служебной деятельности» и других. Важно отметить, что эти дисциплины изучаются на первом курсе, когда обучающиеся еще не имеют четкого представления о своей будущей профессиональной деятельности. Поэтому изучение соответствующих тем ограничивается рассмотрением общих понятий в области телекоммуникаций и формированием базовых навыков работы с компьютерными сетями [3, с. 336]. Это помогает курсантам понять роль и значение ИКТ только в рамках профессиональной деятельности органов внутренних дел.

ИКТ способствуют решению следующих задач:

1. Реализации информационных и информационно-деятельностных моделей в обучении
2. Активизации познавательной деятельности учащихся (курсантов и слушателей).
3. Внедрению современных методов контроля, оценки мониторинга учебных достижений учащихся (курсантов и слушателей).

Внедрение информационных и коммуникационных технологий в образовательный процесс позволяет решать прикладные задачи по улучшению учебного процесса, повышению активности обучающихся через их вовлечение в различные виды деятельности и стимулированию образовательной активности.

Использование информационно-коммуникационных технологий (ИКТ) в педагогическом процессе юридического вуза может значительно обогатить и улучшить образовательный опыт курсантов. Вот некоторые способы, применения ИКТ в образовательной среде учебных учреждений МВД России:

1. Электронные учебники и материалы: Преподаватели могут использовать электронные учебники, статьи, журналы и другие материалы, доступные через интернет, чтобы предоставить курсантам и слушателям актуальную информацию о правовых вопросах. Это также позволяет курсантам получать доступ к материалам любое время и из любого места.
2. Видео-лекции и вебинары: Преподаватели могут записывать видео-лекции или проводить вебинары, чтобы представить сложные концепции и объяснить юридические принципы. Это позволяет курсантам и слушателям просматривать лекции в своем собственном темпе и повторять материал при необходимости.
3. Онлайн-форумы и дискуссии: ИКТ позволяют создавать виртуальные форумы платформы для обсуждения юридических вопросов. Курсанты и слушатели могут активно участвовать в дискуссиях, задавать вопросы и делиться своими мыслями и мнениями с другими обучающимися и преподавателями.
4. Компьютерные программы и симуляции: Существуют специализированные компьютерные программы и симуляции, которые помогают курсантам и слушателям развивать навыки анализа правовых случаев, проводить исследования и решать юридические проблемы. Это позволяет курсантам и слушателям получить практический опыт и применить теоретические знания на практике.
5. Электронная система управления обучением (LMS): LMS позволяет преподавателям организовывать курсы, предоставлять материалы, задания и тесты, а также отслеживать

прогресс обучающихся. Курсанты и слушатели могут загружать свои работы, общаться с преподавателями и получать обратную связь.

6. Исследовательские проекты и онлайн-ресурсы: Курсанты и слушатели могут использовать ИКТ для проведения исследований, доступа к правовым базам данных, судебным решениям и другим онлайн-ресурсам. Это помогает им развивать навыки поиска информации, анализа и критического мышления.

Важно отметить, что успешное использование ИКТ в педагогическом процессе требует соответствующей подготовки преподавателей и доступности необходимой инфраструктуры, такой как компьютеры, интернет-соединение и программное обеспечение. Также необходимо учитывать вопросы безопасности и конфиденциальности при использовании ИКТ в юридическом образовании.

Использование информационно-коммуникационных технологий в педагогическом процессе учебных организаций системы МВД России имеет множество преимуществ. Оно позволяет курсантам и слушателям получать более широкий доступ к актуальным материалам, развивать навыки самостоятельного изучения и исследования, а также общаться и сотрудничать с преподавателями и студентами других вузов. Это способствует более глубокому пониманию юридических концепций и развитию практических навыков.

Однако, не следует забывать о значимости личного взаимодействия общения в процессе обучения. Виртуальные форматы не всегда могут полностью заменить классические методы преподавания, поэтому важно находить баланс между использованием ИКТ и традиционными подходами.

В настоящее время (2023–2024 г.г.) вузы МВД России находятся на этапе подготовки к реализации целого ряда новых дисциплин, которые так или иначе связаны с практическим применением отдельных видов ИКТ в деятельности органов внутренних дел по раскрытию и расследованию преступлений. Вот лишь некоторые из них:

- «Организация противодействия преступлениям в сфере незаконного оборота наркотиков, совершаемых с использованием информационно-телекоммуникационных технологий»;
- «Получение оперативно значимой информации в информационно-телекоммуникационных сетях»;
- «Киберпреступность в финансово-кредитной сфере»;
- «Информационно-техническое обеспечение выявления и раскрытия преступлений, совершаемых с использованием информационно-телекоммуникационных технологий»;
- «Расследование преступлений, совершенных с использованием информационно-телекоммуникационных технологий»;
- «Практикум по проведению отдельных следственных действий по преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий».

Реализация профессионально-ориентированных дисциплин, связанных с противодействием преступлениям, совершенным с использованием информационно-коммуникационных технологий (ИКТ), может столкнуться с несколькими проблемами некоторые из них:

1. Быстрое развитие технологий: ИКТ постоянно развиваются, и новые виды преступлений, связанных с использованием ИКТ, появляются на регулярной основе. Это создает вызов для образовательных программ, так как они должны быть постоянно обновлены, чтобы отражать последние тенденции и методы преступников.
2. Недостаток квалифицированных преподавателей: Преподаватели, обладающие достаточными знаниями и опытом в области противодействия преступлениям, совершенным с использованием ИКТ, на современном этапе это редкий специалист. Что может затруднить обеспечение высококачественного обучения в данной области.
3. Обновление учебных материалов: Учебные материалы, используемые для обучения профессионально-ориентированных дисциплин, должны быть актуальными и соответствовать современным методам преступников. Однако обновление материалов может быть сложным и требовать постоянного мониторинга изменений в ИКТ применяемых для совершения противоправных действий.
4. Необходимость доступа к специализированному программному обеспечению: Для эффективного обучения курсантам и слушателям может потребоваться доступ к специализированному программному обеспечению и инструментам, используемым в борьбе с преступлениями, совершаемыми с использованием информационно-коммуникационных технологий. Это может потребовать дополнительных финансовых затрат на приобретение и поддержку такого программного обеспечения.
5. Сложность практической работы: Противодействие преступлениям, совершенным с использованием информационно-коммуникационных технологий требует не только теоретических знаний, но и практических навыков. Обучение слушателей и курсантов практическим аспектам противодействия ИКТ-преступлениям может быть сложным из-за необходимости доступа к реальным информационным средам и данным, что ограничивает проведение практических занятий.
6. Законодательные и этические вопросы: Противодействие преступлениям, совершенным с использованием информационно-коммуникационных технологий может подразумевать работу с информацией конфиденциального характера, а также требовать знания законодательства и этических норм. Обучение слушателей и курсантов в этой области должно учитывать эти аспекты и помогать им развивать соответствующие навыки и осознанность [\[1, с. 53\]](#).

Это лишь несколько проблем, с которыми может столкнуться реализация профессионально-ориентированных дисциплин, связанных с противодействием преступлениям, совершенным с использованием информационно-коммуникационных технологий. Однако, с помощью постоянного обновления программ, привлечения квалифицированных преподавателей, актуализации учебных материалов, обеспечения доступа к специализированному программному обеспечению разработки практических упражнений, эти проблемы могут быть преодолены, а слушатели и курсанты могут получить качественное образование в этой области.

Появление новых дисциплин отражает современные изменения в структуре преступности, объектах преступного посягательства и способах совершения преступлений.

Предстоящая реализация этих дисциплин сопряжена, на наш взгляд, с рядом проблем, обусловленных интеграцией в них не только юридических, экономических, психологических (что свойственно гуманитарному образованию), но и технических аспектов.

Для выявления и определения путей решения проблем реализации указанных профессионально-ориентированных дисциплин, мы можем задать следующие вопросы: «Кто должен быть обучен?», «Чему нужно учить?», «Каким образом следует проводить обучение?» и «Кто будет осуществлять обучение?».

Первый вопрос: «Кого нужно обучать?». Существует определенная сложность в изучении информационно-технических дисциплин для значительной части слушателей и курсантов, имеющих гуманитарный тип мышления, и осваивающих программы юридических специальностей. Несмотря на то, что современная молодежь начинает использовать различные электронные устройства с раннего возраста, их знания о теории функционирования компьютеров и компьютерных сетей практически не изменились за последнее десятилетие. Кроме того, уровень знаний слушателей и курсантов в области информатики, полученные ими в школе, значительно различаются, а случаи формального преподавания этой дисциплины не являются исключением.

Одновременно активное использование информационно-коммуникационных технологий в деятельности правоохранительных органов приводит к необходимости для слушателей и курсантов имеющих гуманитарный тип мышления дополнительного изучения и понимания технических аспектов современных информационных процессов. Однако такое «погружение» представляет серьезные сложности для многих из них.

Возможно, что данная проблема может быть решена в значительной степени при изучении указанных профессионально-ориентированных дисциплин, что позволит создать практически непрерывную цепочку изучения информационно-коммуникационных технологий: от основных теоретических знаний до их практического применения в профессиональной деятельности, но это потребует и дополнительного времени на данные курсы, что в рамках основных профессиональных образовательных программ обучения не представляется возможным.

Второй вопрос: «Чему необходимо обучать?». Ответ на этот вопрос напрямую связан с формированием требований образовательной организации к результатам освоения программы специалитета (бакалавриата) в виде определенного набора компетенций. При решении этой задачи необходимо не только сбалансировать достижение общекультурных и профессиональных компетенций внутри одной специальности (в основном юридической), но и определить необходимый уровень знаний и навыков в области информационно-технических дисциплин [\[4, с. 67\]](#).

В контексте обучения информационно-техническим дисциплинам для слушателей и курсантов юридических специальностей, следует уделить особое внимание следующим аспектам:

1. Основы компьютерных наук: слушатели и курсанты образовательных учреждений МВД России должны овладеть базовыми понятиями и принципами функционирования компьютеров, операционных систем, компьютерных сетей и интернета. Это включает в себя понимание аппаратной и программной составляющих компьютера, принципы работы с операционными системами, базовые навыки работы с сетевыми протоколами и сервисами.
2. Информационная безопасность: в связи с активным использованием информационных технологий в правоохранительной деятельности, слушатели и курсанты должны быть осведомлены об основных принципах и методах защиты информации, предотвращении киберпреступлений и обеспечении конфиденциальности данных. Это включает в себя

знание о типичных угрозах информационной безопасности, методах аутентификации и шифрования, а также основных принципах защиты компьютерных сетей.

3. Программное обеспечение: слушатели и курсанты должны иметь представление о различных программных инструментах приложениях, которые могут быть полезными в их профессиональной деятельности. Это может включать знание о текстовых редакторах, электронных таблицах, базах данных, специализированных программных продуктах для юридической работы и других инструментах, используемых в правовой сфере.

4. Информационные ресурсы и поиск информации: слушатели и курсанты должны быть обучены навыкам эффективного поиска и анализа информации в сети интернет, использованию электронных библиотек и баз данных для получения актуальных юридических материалов и научных исследований.

Третий вопрос: «Каким образом следует проводить обучение?». Для эффективного обучения информационно-техническим дисциплинам студентов юридических специальностей существует несколько подходов:

1. Интеграция в основную программу обучения: информационно-технические дисциплины могут быть включены в основную программу обучения юридических специальностей. Это позволит слушателям и курсантам получить необходимые знания и навыки параллельно с изучением юридических предметов. Такой подход поможет обучающимся увидеть связь между информационными технологиями и правовой сферой.

2. Специализированные курсы и тренинги: можно организовать отдельные курсы или тренинги, посвященные информационно-техническим аспектам для слушателей и курсантов. Это позволит более глубоко и систематически изучить соответствующие темы и приобрести необходимые навыки.

3. Практические занятия и проекты: активное использование практических заданий, проектов и кейсов поможет слушателям и курсантам применить полученные знания на практике. Например, они могут разрабатывать политики информационной безопасности, создавать веб-сайты или анализировать юридическую информацию с использованием специализированных программных инструментов.

4. Обратная связь и оценка: важно предоставить слушателям и курсантам обратную связь по результатам их работы и оценивать их достижения. Это поможет стимулировать активное участие обучающихся в учебном процессе, что в свою очередь позволит им повысить свои навыки в информационно-технической области.

5. Постоянное обновление материалов: учитывая быстрое развитие информационных технологий, необходимо постоянно обновлять учебные материалы и следить за последними тенденциями в данной области. Это позволит слушателям и курсантам быть в курсе новых технологий и методов работы.

В целом, комбинация этих подходов может обеспечить эффективное обучение информационно-техническим дисциплинам для слушателей и курсантов учебных заведений системы МВД России и подготовить их к успешной работе в современной правовой сфере.

Вопрос третий: «какова методика обучения?». Для успешной реализации вновь вводимых дисциплин, связанных с противодействием преступлениям, совершаемым с использованием информационно-коммуникационных технологий (ИКТ), необходимо разработать соответствующее дидактическое и методическое обеспечение. Вот

несколько шагов, которые могут помочь в этом процессе:

1. Исследование актуального уровня развития ИКТ: Проведите анализ современных технологий, трендов и инструментов, используемых в сфере киберпреступности. Изучите последние случаи нарушений безопасности, типичные угрозы и методы атак. Это позволит вам понять основные проблемы вызовы, с которыми сталкиваются специалисты по кибербезопасности.
2. Разработка учебных программ: На основе полученных знаний создайте учебные программы для вновь вводимых дисциплин. Определите цели и задачи каждого курса, определите ключевые темы и компетенции, которые слушатели и курсанты должны приобрести. Учтите актуальные методики и инструменты, используемые в кибербезопасности [\[5, с. 114\]](#).
3. Создание учебных материалов: Разработайте учебники, лекции, практические задания и другие материалы, необходимые для обучения слушателей и курсантов. Уделите особое внимание практическим аспектам, таким как анализ случаев, симуляции атак и защиты, разработка политик безопасности и т.д. Используйте современные примеры и реальные случаи из мира кибербезопасности.
4. Применение современных методик обучения: Включите в свои программы активное и интерактивное обучение, такие как групповые проекты, дискуссии, ролевые игры и практические занятия. Используйте онлайн-ресурсы, вебинары и тренинги для расширения возможностей обучения.
5. Сотрудничество с индустрией: Установите партнерство с организациями и компаниями, работающими в сфере кибербезопасности. Пригласите экспертов для проведения лекций, мастер-классов практических занятий. Организуйте стажировки и практику для обучающихся, чтобы они могли применить свои знания на практике.
6. Оценка и обновление программы: Регулярно оценивайте эффективность программы и получайте обратную связь от обучающихся и преподавателей. Внесите необходимые коррективы и обновления в программу на основе полученных данных. Следите за изменениями в сфере киберпреступности и обновляйте учебные материалы и методики соответствующим образом.
7. Проведение практических тренировок: Организуйте практические тренировки, где слушатели и курсанты смогут применить свои знания и навыки в реальных сценариях. Это может включать симуляции атак, разработку и тестирование систем безопасности, анализ инцидентов и другие практические задания. Обеспечьте доступ к необходимому программному обеспечению и инструментам для проведения таких тренировок.
8. Создание сообщества и обмен опытом: Поддерживайте активное сообщество обучающихся и преподавателей, интересующихся кибербезопасностью. Организуйте конференции, семинары и форумы, где они могут делиться своим опытом, исследованиями и лучшими практиками. Содействуйте участию слушателей и курсантов в ИТ-соревнованиях и хакатонах по кибербезопасности.
9. Внедрение системы оценки: Разработайте систему оценки, которая позволит оценить достижения слушателей и курсантов в области кибербезопасности. Включите различные формы оценки, такие как тесты, проекты, лабораторные работы практические задания. Обратите внимание на развитие навыков решения проблем, критического мышления и коммуникации.

Важно помнить, что разработка дидактического и методического обеспечения для дисциплин по кибербезопасности требует постоянного обновления и адаптации к изменяющейся противоправной среде. Следите за последними тенденциями и новыми технологиями в области кибербезопасности и вносите соответствующие изменения в свою программу обучения.

Вопрос четвертый: «кто учит?» тесно связан со вторым и, особенно, с третьим вопросами.

Усиление роли информационно-коммуникационных технологий (ИКТ) в образовательном процессе способствует развитию информационно-коммуникационной компетенции преподавательского состава. Умение использовать ИКТ для решения профессиональных задач и проблем в педагогической деятельности способствует осуществлению личностно-ориентированной парадигмы образования.

Эффективность использования информационных продуктов зависит не только от умения применять информационные и коммуникационные технологии, но и от качества знаний педагогических методов. Поэтому одной из основных задач внедрения ИКТ в образовательный процесс является развитие технологической компетентности преподавательского состава.

Развитие информационно-коммуникационной компетенции преподавательского состава имеет ряд преимуществ. Во-первых, использование ИКТ позволяет преподавателям эффективно организовывать учебный процесс, делая его более интерактивным и привлекательным для обучающихся. С помощью ИКТ преподаватели могут предоставлять доступ к разнообразным информационным ресурсам, проводить онлайн-консультации и обратную связь, создавать интерактивные задания и тесты. Во-вторых, развитие информационно-коммуникационной компетенции способствует повышению профессиональной компетентности преподавателей. Они могут использовать ИКТ для поиска актуальной информации, анализа данных, разработки учебных материалов и методик, а также для самообразования и профессионального развития.

Кроме того, использование ИКТ в педагогической деятельности способствует осуществлению личностно-ориентированной парадигмы образования. Интерактивные образовательные технологии позволяют учитывать индивидуальные потребности и особенности каждого учащегося, создавать условия для его саморазвития и самореализации [\[2, с. 86\]](#).

Однако успешное использование ИКТ в образовательном процессе требует не только наличия соответствующей технической базы, но и развития соответствующих компетенций у преподавателей. Поэтому важными задачами являются проведение систематического обучения и поддержка преподавателей в освоении ИКТ, а также создание условий для их творческого применения в педагогической практике.

В свою очередь необходимо отметить, что преподаватели вновь вводимых дисциплин, с одной стороны, должны быть специалистами в соответствующих предметных областях (уголовный процесс, предварительное расследование, криминалистика, оперативно-розыскная деятельность и др.). С другой стороны, знать основы функционирования компьютерных сетей, уметь использовать сетевые технологии для получения требуемой информации, владеть навыками работы со специализированным программным обеспечением. Преподаватель новых дисциплин может быть как юристом, получившим дополнительную квалификацию в сфере информационно-коммуникационных технологий

(ИКТ), так и айтишником, который углубился в юридические науки. Возможно, это зависит от конкретного образовательного учреждения, где преподаватель работает. В обоих случаях преподаватель обладает уникальным сочетанием знаний в области юриспруденции и информационных технологий, что позволяет ему эффективно преподавать новые дисциплины, связанные с развитием ИКТ и их правовыми аспектами.

Повышение квалификации профессорско-преподавательского состава образовательных организаций МВД России, направленное на получение знаний об основах функционирования информационно-коммуникационных технологий (ИКТ) и приобретение умений и навыков использования конкретного инструментария для противодействия преступлениям, совершаемым с использованием ИКТ, является важной задачей в современном информационном обществе.

Для достижения этих целей можно применять различные подходы и методы повышения квалификации. Вот несколько возможных шагов:

1. Организация специализированных курсов и тренингов: МВД России может проводить специальные курсы и тренинги, которые позволят преподавателям и профессорам ознакомиться с основами функционирования ИКТ и научиться использовать конкретные инструменты для борьбы с киберпреступностью. Эти мероприятия могут включать лекции, практические занятия и обмен опытом.
2. Партнерство с ведущими учебными заведениями экспертами: МВД России может установить партнерские отношения с ведущими университетами и другими образовательными организациями, специализирующимися в области ИКТ и кибербезопасности. Это позволит преподавателям и профессорам получить доступ к актуальным знаниям и передовым методикам.
3. Создание специализированных учебных материалов: МВД России может разработать специальные учебные материалы, которые будут содержать информацию об основах функционирования ИКТ и конкретных инструментах для борьбы с киберпреступностью. Эти материалы могут быть представлены в виде электронных курсов, учебников или онлайн-ресурсов.
4. Организация стажировок и практических занятий: Для эффективного освоения навыков использования конкретного инструментария необходима практика. МВД России может организовывать стажировки и практические занятия, в рамках которых преподаватели и профессора смогут применять полученные знания и навыки на практике. Это может включать работу с реальными кейсами, участие в симуляциях и тренировках, а также сотрудничество с экспертами в области кибербезопасности.
5. Проведение исследовательских проектов: МВД России может поддерживать исследовательские проекты, связанные с противодействием киберпреступности и использованием ИКТ. Профессора и преподаватели могут участвовать в таких проектах, что позволит им расширить свои знания и опыт в данной области.
6. Организация конференций и семинаров: МВД России может организовывать конференции, семинары и другие мероприятия, на которых будут обсуждаться актуальные вопросы в области кибербезопасности и использования ИКТ. Это позволит преподавателям и профессорам быть в курсе последних тенденций и развития в данной области.

Важно также обеспечить постоянное обновление программ повышения квалификации,

чтобы они отражали последние изменения и новые вызовы в области ИКТ и кибербезопасности. Регулярное оценивание эффективности программ и получение обратной связи от участников также поможет оптимизировать процесс повышения квалификации.

Программы повышения квалификации необходимо дифференцировать для разных категорий преподавателей, исходя из совокупности преподаваемых ими дисциплин: сферы оперативно-розыскной деятельности, криминалистики, уголовного процесса и т.д. Дифференциация программ повышения квалификации для разных категорий преподавателей, исходя из совокупности преподаваемых ими дисциплин, является важным аспектом обеспечения эффективного профессионального развития педагогического персонала. Вот несколько примеров того, как можно дифференцировать такие программы:

1. Технические дисциплины: Преподаватели, которые специализируются на технических аспектах информационных технологий, могут получить программу повышения квалификации, фокусирующуюся на технических аспектах кибербезопасности, защите данных, сетевой безопасности и других связанных областях.
2. Правовые дисциплины: Преподаватели, преподающие правовые аспекты информационных технологий, могут получить программу повышения квалификации, ориентированную на законодательные и регуляторные аспекты кибербезопасности, киберпреступности, правовую ответственность и другие юридические аспекты.
3. Психологические и социальные дисциплины: Преподаватели, занимающиеся психологическими и социальными аспектами информационных технологий, могут получить программу повышения квалификации, которая фокусируется на понимании мотиваций преступников, социальных инженерных методах, психологических аспектах киберпреступности и предотвращении таких преступлений.
4. Общие программы: Для преподавателей, которые преподают широкий спектр дисциплин, может быть полезно предложить общую программу повышения квалификации, которая охватывает основные аспекты кибербезопасности, киберпреступности и защиты данных без глубокого углубления в конкретные области.

Важно учитывать потребности и интересы преподавателей при разработке программ повышения квалификации. Различные категории преподавателей могут иметь разные потребности и уровни экспертизы в области информационной безопасности, поэтому дифференциация программ может помочь им получить релевантные знания и навыки [\[6, с. 429\]](#).

Кроме того, можно рассмотреть и такой вариант подходов к дифференциации программ повышения квалификации, преподавателей образовательных организаций системы МВД России:

1. Уровень сложности: Программы могут быть разделены на разные уровни сложности, чтобы соответствовать потребностям преподавателей с разным уровнем знаний и опыта области информационной безопасности. Например, можно предложить программы для начинающих, продвинутых и экспертов.
2. Специализация: Программы могут быть специализированы на конкретных аспектах информационной безопасности, таких как кибератаки, защита персональных данных, безопасность сетей и т.д. Это позволит преподавателям сосредоточиться на конкретных

областях своего интереса и экспертизы.

3. Формат обучения: Различные преподаватели могут предпочитать разные форматы обучения. Некоторые могут предпочитать очные семинары и тренинги, в то время как другие предпочитают онлайн-курсы или самостоятельное обучение. Предоставление разных форматов обучения может удовлетворить разнообразные потребности преподавателей.

4. Продолжительность программы: Программы повышения квалификации могут иметь разную продолжительность, чтобы соответствовать доступному времени и ресурсам преподавателей. Например, можно предложить короткие интенсивные программы или более длительные программы с более глубоким изучением материала.

В целом, дифференциация программ повышения квалификации в области противодействия преступлениям, совершенным с использованием информационно-коммуникационных технологий, позволяет учитывать разнообразные потребности и интересы преподавателей, а также обеспечивает более эффективное и релевантное обучение.

В заключении хотелось бы отметить, что методика обучения слушателей и курсантов вузов МВД России противодействию преступлениям, совершенным с использованием информационно-коммуникационных технологий, может включать следующие основные аспекты:

1. Осведомление о современных угрозах: Обучение должно начинаться с предоставления слушателям и курсантам полной информации о различных видах преступлений, связанных с использованием информационно-коммуникационных технологий. Это может включать киберпреступления, мошенничество в сети Интернет, нарушение авторских прав, кибершпионаж и другие.

2. Законодательство и нормативные акты: Обучение должно включать изучение соответствующего законодательства и нормативных актов, регулирующих противодействие преступлениям, связанным с информационно-коммуникационными технологиями. Слушатели и курсанты должны быть ознакомлены с правовыми аспектами и последствиями таких преступлений.

3. Технические аспекты: Обучение должно включать изучение основных технических аспектов, связанных с информационной безопасностью. Это может включать обучение по защите компьютерных систем, сетей и данных, распознаванию и анализу угроз, использованию специализированного программного обеспечения и т.д.

4. Практические навыки: Обучение должно предоставлять практические навыки, необходимые для противодействия преступлениям, связанным с информационно-коммуникационными технологиями. Это может включать тренировки по реагированию на инциденты, проведение расследований, сбор и анализ цифровых доказательств и другие практические упражнения.

5. Сотрудничество и координация: Обучение должно подчеркивать важность сотрудничества и координации между различными службами и организациями, занимающимися противодействием киберпреступности. Это может включать обучение по взаимодействию с правоохранительными органами, специалистами по информационной безопасности, представителями судебной системы и другими заинтересованными сторонами.

6. Этические аспекты: Обучение должно включать обсуждение этических аспектов противодействия преступлениям, связанным с информационно-коммуникационными технологиями. Слушатели и курсанты должны быть ознакомлены с принципами конфиденциальности, защиты личных данных, этическими нормами использования информации другими соответствующими вопросами.
7. Обновление знаний: Обучение должно поощрять постоянное обновление знаний и навыков в области противодействия преступлениям, связанным с информационно-коммуникационными технологиями. Слушатели и курсанты должны быть осведомлены о последних трендах и развитии в области киберпреступности, новых угрозах и методах защиты.
8. Проверка компетенций: Обучение должно включать проверку компетенций слушателей и курсантов в области противодействия преступлениям, связанным с информационно-коммуникационными технологиями. Это может быть осуществлено через проведение экзаменов, практических заданий, симуляций и других форм проверки знаний и навыков.
9. Система отзывов и улучшений: Обучение должно предусматривать систему обратной связи, включая возможность слушателей и курсантов оценивать эффективность методики и предлагать улучшения. Это позволит постоянно совершенствовать программу обучения и адаптировать ее к изменяющимся потребностям и требованиям.
10. Междисциплинарный подход: Обучение должно осуществляться с использованием междисциплинарного подхода, включая элементы юриспруденции, информационных технологий, психологии, социологии и других соответствующих областей знаний. Это поможет слушателям и курсантам получить всестороннее понимание проблемы и развить комплексный подход к противодействию преступлениям, связанным с информационно-коммуникационными технологиями.

Библиография

1. Башлуева Н. Н. Подготовка курсантов вузов МВД РФ к педагогической профилактике информационной защищенности сотрудников органов внутренних дел как одного из факторов предупреждения преступлений в сфере информационных и телекоммуникационных технологий / Н. Н. Башлуева, Д. А. Темняков // Прикладная психология и педагогика. – 2018. – Т. 3, № 1. – С. 48-57.
2. Смирнова Л. Я. Этические основы профессиональной деятельности сотрудников органов внутренних дел : учебное пособие / Л. Я. Смирнова, Д. А. Темняков, А. П. Хаврак. – Москва : Московский университет Министерства внутренних дел Российской Федерации им. В.Я. Кикотя, 2018. – 128 с.
3. Темняков Д. А. Педагогический анализ мотивации к учебной деятельности курсантов Первого и второго курса Московского областного филиала Московского университета МВД России имени В.Я. Кикотя / Д. А. Темняков // Актуальные проблемы адаптации курсантов и слушателей образовательных организаций МВД России к условиям профессиональной деятельности: состояние и перспективы : Всероссийская научно-практическая конференция : сборник научных трудов, Москва, 31 марта 2022 года. – Москва: Московский университет МВД России имени В.Я. Кикотя, 2022. – С. 334-341.
4. Темняков Д. А. Использование педагогических принципов при адаптации иностранного опыта в учебный процесс образовательных организаций МВД России / Д. А. Темняков, Е. Д. Темнякова // Полицейская деятельность. – 2021. – № 3. – С. 65-74.

5. Темняков Д. А. Обучение слушателей и курсантов образовательных учреждений МВД России тактике и методам обеспечения личной профессиональной безопасности: специальность 13.00.01 "Общая педагогика, история педагогики и образования": диссертация на соискание ученой степени кандидата педагогических наук / Темняков Дмитрий Александрович. – Москва, 2002. – 266 с.
6. Темнышов А. А. Информационная защищенность сотрудников ГИБДД как один из факторов предупреждения преступлений в сфере информационных и телекоммуникационных технологий. *Управление деятельностью по обеспечению безопасности дорожного движения: состояние, проблемы, пути совершенствования*, 1(1), 425-432.

Результаты процедуры рецензирования статьи

В связи с политикой двойного слепого рецензирования личность рецензента не раскрывается.

Со списком рецензентов издательства можно ознакомиться [здесь](#).

Объектом исследования в представленной для рецензирования рукописи выступает обучение борьбе с киберпреступностью как педагогический процесс, предметом же – основные его структурно-содержательные аспекты. Актуальность исследования несомненна в условиях становления и развития цифрового мира с переносом всех традиционных социальных явлений в цифровую парадигму. Преступления в этом смысле не являются исключением.

С методологической точки зрения исследование имеет теоретический характер, элементы практической экспериментальной работы отсутствуют, а ведущим методом выступает описательный анализ, что в целом является достаточным для формата статьи. Подробное рассмотрение весьма узкоспециализированного профессионально-педагогического процесса содержит признаки элементов методической новизны.

Работа может вызвать интерес у весьма широкой аудитории не только педагогического и юридического, но и IT-круга.

Текст написан языком, удовлетворяющим нормам научного стиля, однако, отметим, что постулирование в нём доминирует над рассуждениями.

Представленный текст имеет характер методической разработки, методического отчёта, но не научного исследования.

Со структурной точки зрения отметим следующее.

Перечень литературы содержит лишь шесть источников, в то время как в научных работах в формате журнальной статьи традиционно принято десять и больше.

Текст статьи не разбит на содержательно взаимосвязанные части, что принято в научных работах.

В теоретической части (в начале исследования) отсутствует обзор авторов, рассматривавших схожую тематику, их определения, точки зрения, векторы исследования и пр..

В тексте отсутствует методологический блок с обоснованием инструментария исследования.

Выводы чрезвычайно растянуты. Желательно сократить их до 3-4 тезисов, отражающих основную суть исследования, в представленном виде выводы выглядят как отдельная содержательная часть.

Принципиальное содержательное замечание заключается в том, что 90 процентов тезисов работы подойдут не только для обучения борьбе с киберпреступностью, но и для любого качественно спроектированного учебного процесса. С учётом того, что название статьи начинается со слова «особенности» ожидается изложение на уровне большей

методической конкретики в плане особенных средств, приёмов, ситуаций и пр. обучения.

С языковой точки зрения в тексте почти не просматривается авторская точка зрения, что скорее минус для журнального жанра.

Рекомендуется также сократить название. Например, из него можно убрать слово «профессионально-ориентированных», потому что и так понятно, что речь идёт о профессиональной подготовке.

С содержательной точки зрения в тексте постулирование доминирует над анализом, так текст может органично вписаться в учебник или учебное пособие.

Представленная рукопись при высоком уровне актуальности и достаточно подробном рассмотрении специализированного педагогического процесса не полностью вписывается в формат научного исследования и может быть опубликована в рецензируемом журнале в порядке исключения по усмотрению редакции.