Педагогические подходы к обучению сотрудников органов внутренних дел основам противодействия кибертеррористическим угрозам в системе ведомственного дополнительного профессионального образования

Рустем Рафекович Садеков
Кандидат педагогических наук, доцент, доцент кафедры Психологии, педагогики и организации работы с кадрами
Академия управления МВД России
Москва, Россия
dotsentkaf.aumvd@yandex.ru
ORCID 0000-0002-2739-5490

Юлия Валерьевна Крохина
Старший преподаватель кафедры Огневой и физической подготовки
Международный межведомственный Центр подготовки и переподготовки специалистов по борьбе с терроризмом и экстремизмом Всероссийского института повышения квалификации сотрудников МВД России
Домодедово, Россия
i1lya@mail.ru
ORCID 0000-0002-0122-5418

Поступила в редакцию 09.03.2025
Принята 30.04.2025
Опубликована 30.05.2025

УДК 351.82:37.037.3
DOI 10.25726/g2468-7534-7315-v
EDN XNUPUU
ВАК 5.8.7. Методология и технология профессионального образования (педагогические науки)
OECD 05.03.HE. EDUCATION, SPECIAL

Аннотация

В представленной авторами статье рассматриваются педагогические подходы к обучению сотрудников органов внутренних дел Российской Федерации основам противодействия кибертеррористическим угрозам в системе ведомственного дополнительного профессионального образования. Проведены исследования в сфере теоретических основ обучения в области кибербезопасности, включая определение ключевых понятий и понимание их влияния на национальную безопасность. Обсуждаются различные педагогические подходы к обучению, включая традиционные методы и инновационные технологии, такие как виртуальные тренажеры и обучающие игры. Также рассматривается организация системы ведомственного дополнительного профессионального образования и партнерство с учебными заведениями и центрами кибербезопасности. Эффективное обучение сотрудников органов внутренних дел в области кибербезопасности считается ключевым фактором для обеспечения национальной безопасности и противодействия киберугрозам. Методология исследования носит комплексный характер и включает в себя: теоретический анализ, эмпирические методы, педагогический эксперимент, статистическую обработку данных, методы моделирования Основными выводы проведенного исследования посвящены оптимизации педагогических подходов к обучению сотрудников органов внутренних дел системы МВД России основам противодействия кибертеррористическим угрозам на базе учебных заведений ведомственного дополнительного профессионального образования. Исследование выявило необходимость внедрения в учебный процесс современных интерактивных методов, симуляций реальных кибератак, а также акцентирования на

практических навыках анализа и оперативного реагирования на возникающие вероятные угрозы. Авторами подчеркивается важность индивидуального персонализированного подхода к обучению сотрудников органов внутренних дел, учитывающего специфику выполняемых специалистами стратегических задач и уровень их предварительной профессиональной подготовки. Обоснована целесообразность интеграции междисциплинарного подхода, сочетающего компетентные знания в области информационных технологий, психологии и права. Предлагается разработка эффективной системы обучения, позволяющей оперативно осваивать различные аспекты кибербезопасности. Выявлена потребность в постоянном обновлении учебных образовательных программ с учетом актуальных тенденций развития кибертерроризма.

Ключевые слова

педагогические подходы, обучение сотрудников, кибертеррористические угрозы, дополнительное профессиональное образование, национальная безопасность, система ведомственного образования, МВД России, профессионализм, преподавательская работа, ОВД.

Введение

XXI век – эпоха активного развития процессов интеграции и модернизации в международное пространство, в пределах которых проходит существенное расширение масштаба интернационализации важнейших аспектов государственной жизни. К таким аспектам, учитывая их глобальное внедрение, относят сплошную автоматизацию учреждений, компаний и организаций.

В последние годы мировое сообщество имело возможность наблюдать за ростом количества разного рода вмешательств в работу, приводящих информационные системы к последствиям в виде нарушения нормального функционирования важнейших систем жизнеобеспечения государства. К сожалению, ведущие государства мира, несмотря на развитость правовой и технической регламентации защиты от несанкционированного воздействия в деятельность инфраструктуры информационных технологий, не в состоянии обеспечить ее стопроцентную защиту. Можно констатировать факт того, что правоохранительные органы не в состоянии контролировать киберпреступность, которая, в результате, стала транснациональной проблемой. Однако осознание уязвимости информационных систем и, как следствие, наработка в сфере разработки адекватного законодательного регулирования и алгоритмов быстрого реагирования позволят минимизировать потери от подобного рода атак.

Говоря об истории вопроса об обучении сотрудников органов внутренних дел Российской Федерации основам противодействия кибертеррористическим угрозам, то можно сделать вывод о том, что эта тема достаточно молода, но при этом несомненно динамично развивается. Первоначально, акцент делался на общих мерах информационной безопасности, постепенно в повседневной служебной деятельности специалистов происходило осознание трансформации террористической деятельности в цифровое пространство, однако, с интенсивным ростом числа и сложности кибертеррористических атак, направленных на критическую инфраструктуру и информационные системы государственных органов, возникла необходимость в специализированной подготовке специалистов высокого уровня.

Несомненно, актуальная задача, которую необходимо решать на современном этапе состоит в разработке специальных унифицированных стандартов профессионального обучения и постоянном повышении квалификации сотрудников органов внутренних дел с получением необходимых компетенций, в соответствии с новейшими тенденциями в области киберугроз.

Мы предполагаем, что научная новизна исследования заключается в разработке и обосновании интегрированной модели обучения сотрудников органов внутренних дел основам противодействия кибертеррористическим угрозам в рамках системы ведомственного дополнительного профессионального образования. Необходима модель, основанная на применении современных педагогических подходов, в состав которой входит проблемно-ориентированное обучение, кейс-стади и использование интерактивных симуляций.

Важным аспектом выступает комплексная система оценки эффективности обучения, учитывающая не только теоретические знания, но и необходимые практические навыки, а также

психологическую готовность сотрудников к противодействию кибертерроризму. Целесообразно продолжить разработку методических рекомендаций по адаптации учебных материалов к специфике различных подразделений органов внутренних дел и уровню подготовки обучающихся в этой сфере. Необходимо использовать в этой работе инновационные подходы, которые позволят повысить эффективность профессионального обучения специалистов, сократит в свою очередь время адаптации сотрудников к новым угрозам и усилит при этом общую безопасность информационного пространства.

Цель исследования заключается в разработке и обосновании педагогических подходов, повышающих эффективность подготовки сотрудников полиции навыкам противодействия кибертеррористическим угрозам в рамках ведомственного профессионального обучения. Предмет исследования направлен на процесс обучения сотрудников органов внутренних дел основам противодействия кибертеррористическим угрозам в системе ведомственного дополнительного профессионального образования. Объект исследования заключается в различных педагогических подходах, методах, приемах и средствах, используемых в обучении сотрудников органов внутренних дел основам противодействия кибертеррористическим угрозам.

Стратегически важным аспектом является адаптация имеющихся в арсенале образовательных организаций МВД России образовательных программ, по результатам освоения которых сотрудники будут способны ориентироваться в условиях быстро меняющихся реалий киберпространства. В свою очередь, это требует глубокой интеграции практико-ориентированных методов, моделирования реальных киберугроз и развития критического мышления у обучающихся. Применяемые педагогические подходы, безусловно, должны способствовать формированию у сотрудников органов внутренних дел компетенций, необходимых для эффективного выявления, предотвращения и пресечения кибертеррористических угроз.

Материалы и методы исследования

Проблемные вопросы в сфере информационной безопасности на своевременном этапе изучены В.С. Горбатовым, А.С., Эрдниевым, М.М. Гедгафовым, М.К. Кумышевой, А.Ю. Чуриковой, К.Р. Дорохиной, П.Н. Кобец, А.Н. Ксеник, В.А. Сошенко и др.

Так, авторами В.С. Горбатовым, А.С. Эрдниевым отмечается, что ведомственная система подготовки кадров МВД России накопила значительный опыт обучения специалистов по различным образовательным программам в области обеспечения информационной безопасности. За прошедшее десятилетие в данной области в силу различных факторов произошли значительные изменения, в частности, в аспекте ее государственного регулирования на основе директивных положений Доктрины информационной безопасности России, и они придали новый импульс по актуализации и адаптации этих изменений в существующих образовательных программах (Горбатов, 2024).

Изначально, первые рекомендации по подготовке сотрудников органов внутренних дел основам кибербезопасности появились в начале 2000-х годов, при этом акцент делался в основном на обеспечение надлежащей защиты собственных информационных ресурсов ведомства, с изучением технических вопросов защиты сетей и оборудования. Постепенно, программы обучения стали включать элементы анализа угроз, криминалистического исследования цифровых следов и международного сотрудничества.

В настоящее время обучение сотрудников носит комплексный характер, охватывая как технические, так и правовые аспекты противодействия кибертерроризму, с изучением различных психологических аспектов радикализации в сети, эффективных методов обнаружения и предотвращения кибератак, а также практические навыки работы с специализированным высокотехнологичным программным обеспечением. Так, к примеру, исследователь М.М. Гедгафов обращает внимание на важный аспект о том, что высокие технологии обусловили переход инфраструктуры на новый уровень функционирования, что привело к возникновению новых угроз национальной и международной системы безопасности и вызвало целый комплекс негативных геополитических последствий (Гедгафов, 2021). В свою очередь автор А.Ю. Чурикова в своей работе выделяет тот фактор, что организация противодействия кибертерроризму осложняется скоростью изменений в технологиях, низким уровнем

информационной грамотности как среди населения, так и представителей государственных органов, а также колоссальным объемом информации в киберпространстве (Чурикова, 2023).

Результаты и обсуждение

Кибертерроризм – это явление международного значения, уровень которого находится в прямой зависимости от уровня развития и внедрения современных компьютерных технологий и доступа к ним. Собственно природа киберпреступлений делает проблему всемирной, поскольку отчасти нет значения, где именно совершено подобное преступление. Террористические организации все чаще используют новые информационные технологии и Интернет с преступными намерениями пополнения средств, пропаганды или передачи секретной информации.

Как отмечает в своей работе М.К. Кумышева, понятие кибертерроризм должно отражать высокую степень опасности для общества, а также тот факт, что местом совершения преступления является киберпространство (Кумышева, 2023). Хотя террористы еще не применяли кибероружие по назначению, они используют новые информационные технологии и достижения компьютерного прогресса, а это уже сигнал об опасности (Ильин, 2000). Кибертерроризм, под которым понимается использование современных информационных технологий, прежде всего сети Интернет, когда такое оружие применяется с целью повреждения важных государственных инфраструктур. (таких, как энергетическая, транспортная, правительственная и т.п.), может в скором будущем стать реальной угрозой для информационной безопасности в первую очередь развитых стран мира.

Фундаментальной основой качественной борьбы с киберпреступностью является понимание сущности процессов, имеющих место при функционировании информационного пространства того или иного государства. А потому для качественного научного и практического осмысления данной проблематики требуется определить собственно сущность употребляемых терминов путем выделения понятийного аппарата в области киберпространства.

Важно отметить и то обстоятельство, что сегодня в ходе выработки и реализации эффективных мер противодействия кибертерроризму необходимо обратиться к опыту зарубежных партнеров, которые имеют качественные наработки в этой сфере. Так, интересное исследование проведено А.Н. Ксеник и В.А. Сошенко, которые обратили внимание на то, что, к примеру одной из ключевых сфер деятельности Шанхайской организации сотрудничества является борьба с экстремизмом и терроризмом во всех его проявлениях. Многие страны и организации участвуют в крупномасштабных учения по сетевой обороне «Locked Shields», ежегодных учениях «Cyber Coalition», компьютеризированных командно-штабных учениях «Steadfast Jupiter», конференции «CyCon». На основе общности интересов в сфере противодействия терроризму в рамках ШОС организации осуществляют продуктивную работу по соответствующим направлениям: обнаружение и предупреждение терроризма. РАТС ШОС разрабатывает методы и механизмы, обеспечивающие качественное сотрудничество ее членов в данной области (Ксеник, 2023).

П.Н. Кобец в своем исследовании предлагает обратить внимание на необходимость совершенствования превентивной кибербезопасности, и разработки эффективных способов противодействия международным проявлениям кибертерроризма (Кобец, 2024).

Впервые термин «кибертерроризм» был введен в обращение в 1980-х годах. Научным сотрудником Калифорнийского Института безопасности и разведки Барри Коллином, сформулировавшим его в контексте тенденции к переходу терроризма от физического к виртуальному. Позже, в 1997 году, агент ФБР Марк Поллит истолковал относительно новую дефиницию, как: «кибертерроризм – это намеренная политически мотивированная атака против информаций, компьютерных систем, компьютерных программ и баз данных в виде насильственного вмешательства со стороны международных групп или секретных агентов» (Машекуашева, 2018).

Кибертерроризм - «преступление, которого в будущем будет прибегать криминалитет, используя компьютеры». При этом отмечается, что «кибертеррористы имеют политическую мотивацию для их преступлений» (Васильева, 2018).

М. Каветли предлагает следующее определение кибертерроризма: «Под кибертерроризмом понимается незаконное нападение со стороны негосударственных субъектов в отношении компьютеров, сетей и информации, содержащейся в них, которое осуществляются с целью запугивания правительства (или населения) или с целью достижения определенного поведения субъекта, который запугивается. Кибератака может пониматься как кибертерроризм только в том случае, если это приводит к физическому насилию против лиц или собственности или возникновению значительного страха в связи с возможностью осуществления таких последствий» (Соколов, 2020). Мы считаем, что в дополнение к этому разъяснению в части определения круга субъектов совершения преступления возможно считать и государственные структуры в том числе.

В то же время О.Б. Скородумова отмечает, что кибертерроризм является родословным терроризма, однако наряду с такими его формами, как ядерный, биологический, химический, экологический, компьютерный (кибернетический), учитывая массовую информатизацию общества, несет одну из самых больших и серьезных угроз человечеству (Скородумова, 2004). Несмотря на основательные доктринальные разработки в сфере определения изучаемого понятия, единого четкого определения понятие «кибертерроризма» как на уровне национального, так и международного законодательства нет. В мировом киберпространстве уже давно осуществляются спецоперации и фактически идет необъявленная информационная война.

В начале XXI века мир вошел в период разрушительных войн в киберпространстве неподготовленным, поскольку в интернет нет системы международной безопасности, международных договоров или структур, способных остановить его милитаризацию или хотя бы не допустить масштабного использования военной силы. В то же время интернет все чаще используется для психологического и экономического давления на оппонента. Расширение возможностей интернета и вступление общества в эру информационных технологий вызывает появление новых видов преступлений и делает общество уязвимым перед угрозой кибертерроризма и преступности. Правоохранители всего мира считают своей первоочередной задачей создание эффективной системы регулирования роста преступности в Интернете. Безусловно, глобальная информационная сеть Интернет является важным фактором ускорения мирового прогресса, технологической основой международного информационного обмена.

По мнению Д.А. Киприч, в этих условиях информационные ресурсы являются огромной материальной ценностью, а несанкционированный доступ к этим ресурсам, если они недостаточно защищены, может привести к глобальным катастрофам (Кирпич, 2003). Тенденции преступного использования достижений в сфере телекоммуникаций и информатизации (ущерб от киберпреступности, кибермошенничества и кибертерроризма оценивается в миллиарды долларов) вызывают необходимость выработки единой международной политики в сфере международной информационной безопасности и создания международного механизма контроля для предупреждения и пресечения правонарушений в международном информационном пространстве (Юркин, 2007).

Педагогические подходы к обучению сотрудников органов внутренних дел основам противодействия кибертеррористическим угрозам в системе ведомственного дополнительного профессионального образования представляют собой сложную и важную проблему современного общества. С увеличением числа кибератак и развитием технологий киберпреступности важность обучения сотрудников МВД России в области кибербезопасности становится все более актуальной. В данной статье рассмотрим основные аспекты педагогических подходов к обучению сотрудников органов внутренних дел в области кибербезопасности:

1. Теоретические основы обучения сотрудников МВД России в области кибербезопасности. Обучение сотрудников полиции в области кибербезопасности представляет собой многоуровневый и многогранный процесс, начинающийся с осознания и уяснения ключевых понятий, лежащих в основе данной темы. Важно, чтобы сотрудники органов внутренних дел понимали суть кибертерроризма, который охватывает использование компьютерных технологий для совершения террористических актов или угроз. Это включает в себя различные формы атак, направленных на нарушение работы информационных систем, нанесение ущерба критической инфраструктуре, а также угрозы безопасности

национального уровня. Далее обучение расширяется на понимание киберугроз, которые могут принимать различные формы: от взломов и вирусов до фишинга и социальной инженерии. Важно, чтобы сотрудники были готовы к различным видам атак и знали, каким образом защитить информацию и обеспечить безопасность данных.

2. Комплекс стратегических мер, в основу которых вложены современные технологии, обеспечивающие защиту инфраструктуры и информационных ресурсов. Специалистами в этой связи разрабатываются стратегии политики безопасности с использованием средств криптографической защиты, сетевого мониторинга и ряда других подходов, целью которой является обеспечение безопасности организации. Этим технологиям, безусловно, необходимо обучать профессионально сотрудников органов внутренних дел. Несомненно, национальная безопасность состоит из ряда многоотраслевых, многокомпонентных аспектов, в основу которых вложена специальная терминология, которой должны оперировать сотрудники полиции. Эти компетенции позволяют сотрудникам органов внутренних дел быстро реагировать на вызовы и угрозы, осуществлять анализ и принимать исчерпывающие меры по защите информации правоохранительной структуры. Ну и, конечно, важно отметить, что не только практика, но и теоретическая подготовка должна постоянно проводиться с привлечением специалистов самого высокого уровня. Здесь можно рассматривать и использовать в качестве помощи базовые педагогические подходы к обучению специалистов. Как мы отмечали выше приглашение специалистов из I-сферы, ведущих экспертов, однозначно скажется на эффективности обучения сотрудников органов внутренних дел. Актуальным остается вопрос изучения способностей, возможностей и специальных функций виртуальных тренажеров, киберсимуляторов обучающих игр и т. д.

3. Привлекательность и мотивация. Игровой формат обучения привлекателен для сотрудников органов внутренних дел и мотивирует их активно участвовать в процессе обучения. Участие в игре создает интерес к теме кибербезопасности и стимулирует обучаемых к активной деятельности. Интерактивное взаимодействие. Обучающие игры позволяют сотрудникам взаимодействовать с различными сценариями кибератак и принимать решения в реальном времени. Это помогает им лучше понять суть проблемы и осознать последствия своих действий. Формирование навыков. Игры способствуют развитию навыков быстрой реакции, аналитического мышления и принятия решений в условиях стресса. Сотрудники могут практиковаться в различных сценариях кибератак и обучаться эффективным методам предотвращения и противодействия угрозам.

4. Проверка знаний. Через игровые сценарии можно оценивать уровень знаний и навыков сотрудников органов внутренних дел в области кибербезопасности. Игровые результаты могут служить основой для анализа и дальнейшего улучшения образовательного процесса.

Таким образом, обучающие игры представляют собой эффективный и интересный способ обучения сотрудников органов внутренних дел основам кибербезопасности, способствуя повышению уровня их компетенций и готовности к действиям в условиях угроз. Использование как традиционных, так и инновационных методов обучения позволяет создать комплексную программу обучения сотрудников органов внутренних дел в области кибербезопасности, обеспечивая им необходимые знания и навыки для эффективного противодействия киберугрозам. Как мы уже отмечали, последние годы и особенно в настоящее время вопросам качественной и профессиональной подготовки сотрудников правоохранительных органов Российской Федерации придается повышенное значение (Садеков, 2023).

Организация системы ведомственного дополнительного профессионального образования. Создание специализированных образовательных программ для сотрудников органов внутренних дел в области кибербезопасности является критическим компонентом организации системы ведомственного дополнительного профессионального образования. Эти программы должны быть разработаны с учетом специфики работы правоохранительных органов и актуальных угроз, с которыми они сталкиваются в сфере кибербезопасности. Одним из важных шагов в этом процессе является установление партнерских отношений с ведущими учебными заведениями и специализированными центрами кибербезопасности. Эти партнерства позволяют органам внутренних дел иметь доступ к актуальной информации, передовым

методикам обучения и современным технологиям в области кибербезопасности. Кроме того, сотрудничество с учебными заведениями способствует развитию совместных образовательных программ, которые соответствуют специфике деятельности правоохранительных органов и требованиям современного мира.

Особое значение, безусловно, следует придать важности комплексной разработки педагогического инструментария, методов и приемов, используемых в образовательном процессе в системе МВД России. Эффективность их будет зависеть от полного соответствия разрабатываемых образовательных программ требованиям и задачам ОВД в сфере противодействия киберугрозам. В ходе подготовки образовательных ресурсов важно обратить внимание на запросы практических подразделений в этой области правоохранительной деятельности. А непосредственно подходы к обучению должны быть гибкими и адаптированными к конкретным группам сотрудников. В целом же, эффективная организация системы ведомственного образования в области кибербезопасности позволяет создать прочную базу знаний и навыков у сотрудников органов внутренних дел, что способствует эффективному противодействию киберугрозам и обеспечивает национальную безопасность.

Заключение

Можно сделать выводы, что таким образом, педагогические подходы к обучению сотрудников органов внутренних дел в области кибербезопасности играют ключевую роль в обеспечении национальной безопасности и эффективном противодействии кибертеррористическим угрозам. Продуманное и системное обучение с использованием современных методов и технологий способствует повышению квалификации персонала и укреплению кибербезопасности государства. Перспективы дальнейшего исследования темы «Педагогические подходы к обучению сотрудников органов внутренних дел основам противодействия кибертеррористическим угрозам в системе ведомственного дополнительного профессионального образования» нами видятся в углублении понимания эффективности различных педагогических технологий и моделей, адаптированных к специфике контингента обучающихся в системе дополнительного профессионального образования МВД России.

Важным направлением является продолжение работы по разработке и апробации интерактивных методов обучения, основанных на моделировании реальных киберугроз и проведении практических занятий в условиях, максимально приближенных к оперативной обстановке. Немаловажным звеном в профессиональном обучении остается изучение влияния индивидуальных психофизиологических особенностей сотрудников на усвоение знаний и формирование навыков в области кибербезопасности. В свою очередь это позволит профессорско-преподавательскому звену персонализировать образовательный процесс и повысить его эффективность и результативность.

На наш взгляд, перспективным представляется дальнейшее исследование возможностей использования искусственного интеллекта для создания адаптивных обучающих образовательных программ. Также целесообразно уделять внимание разработке современных критериев оценки эффективности обучения, а также системы мониторинга уровня подготовки слушателей, позволяющей своевременно выявлять и устранять пробелы в получаемых знаниях.

И безусловно, актуальным остается вопрос о создании единой методической базы, объединяющей лучшие эффективные практики и инновационные подходы к обучению противодействию кибертерроризму, которые подготавливаются и внедряются в служебную деятельность представителями научного сообщества МВД России.

Список литературы

1. Васильева С.А., Ягнакова Э.З. Актуальные вопросы кадрового обеспечения в сфере профилактики экстремизма и терроризма // Вестник ЮУрГУ Серия: Право. 2018. Т. 18. № 1. С. 104-109.

2. Гедгафов, М. М. Меры противодействия кибертеррористическим угрозам в условиях глобализации информационного пространства // Пробелы в российском законодательстве. 2021. Т. 14. № 4. С. 112-115.

3. Горбатов В.С., Эрдниев А.С. Совершенствование подготовки кадров по обеспечению безопасности информационной инфраструктуры органов внутренних дел // Безопасность информационных технологий. 2024. Т. 31. № 1. С. 100-119.
4. Ильин Г.П. От педагогической парадигмы к образованию // Высшее образование в России. 2000. № 1. С. 64.
5. Киприч, Д. А. Формирование рынка услуг по защите информации: дисс. … канд. эк. наук. М., 2003. 165 с.
6. Кобец П.Н. Необходимость совершенствования превентивной кибербезопасности, и разработки эффективных способов противодействия международным проявлениям кибертерроризма // Современные вопросы устойчивого развития общества в эпоху трансформационных процессов: мат. XV Межд. науч.-прак. конф. (23 февраля 2024 г., Москва). М.: АНО ДПО «ЦРОН», 2024. С. 28-35.
7. Ксеник А.Н., Сошенко А.Н. Международное сотрудничество в борьбе с кибертерроризмом: опыт ШОС и НАТО // Ключевые слова: мат. III Студ. конф. Института социально-гуманитарных наук Тюменского государственного университета (27 апреля 2023 г., Тюмень). Тюмень: ТюмГУ-Press, 2023. С. 62-65.
8. Кумышева М.К. Современные аспекты противодействия кибертеррористическим угрозам // Право и управление. 2023. № 8. С. 228-231.
9. Машекуашева М.Х. Организация деятельности органов внутренних дел по профилактике экстремизма // Социально-политические науки. 2018. № 3. С. 40-41.
10. Садеков Р.Р., Крохина Ю.В. Организационно-правовые аспекты организации профессиональной подготовки сотрудников МВД России в системе дополнительного профессионального образования // Вопросы безопасности. 2023. № 1. С. 58-65.
11. Скородумова О.Б. Хакеры как феномен информационного пространства // Социологические исследования. 2004. № 2. С. 9.
12. Соколов, А. С., Поволотцкий А.Ю. Кибертерроризм в России и странах Центральной Азии // Российско-азиатский правовой журнал. 2020. № 2. С. 75-79.
13. Чурикова А.Ю. Применение технологий big-data для противодействия кибертеррористической угрозе // Основные направления совершенствования системы национальной безопасности. 2023. № 3. С. 395-399.
14. Юркин И.З. Кибертерроризм: вызов XXI века. Газета Исполнительного комитета СНГ «Республика». 2007. № 5. С. 11-12.

Pedagogical approaches to training law enforcement officers on the basics of countering cyberterrorist threats in the system of departmental additional professional education

Rustem R. Sadekov
Candidate of Pedagogical Sciences, Associate Professor, Associate Professor of the Department of Psychology, Pedagogy and Human Resources Management
Academy of the Ministry of Internal Affairs of Russia
Moscow, Russia
dotsentkaf.aumvd@yandex.ru
ORCID 0000-0002-2739-5490

Julia V. Krokhina
Senior Lecturer at the Department of Fire and Physical Training
International Interdepartmental Center for Training and Retraining of Specialists in Combating Terrorism and Extremism of All-Russian Institute for Advanced Training of Employees of the Ministry of Internal Affairs of Russia
Domodedovo, Russia
i1lya@mail.ru
ORCID 0000-0002-0122-5418

Received 09.03.2025
Accepted 30.04.2025
Published 30.05.2025

UDC 351.82:37.037.3
DOI 10.25726/g2468-7534-7315-v
EDN XNUPUU
VAK 5.8.7. Methodology and technology of vocational education (pedagogical sciences)
OECD 05.03.HE. EDUCATION, SPECIAL

Abstract

The article presented by the authors examines pedagogical approaches to training employees of the internal affairs bodies of the Russian Federation on the basics of countering cyberterrorist threats in the system of departmental additional professional education. Research has been conducted on the theoretical foundations of cybersecurity education, including defining key concepts and understanding their impact on national security. Various pedagogical approaches to learning are discussed, including traditional methods and innovative technologies such as virtual trainers and educational games. The organization of a system of departmental additional professional education and partnership with educational institutions and cybersecurity centers are also being considered. Effective training of law enforcement officers in the field of cybersecurity is considered a key factor in ensuring national security and countering cyber threats. The research methodology is complex in nature and includes: theoretical analysis, empirical methods, pedagogical experiment, statistical data processing, modeling methods. The main conclusions of the study are devoted to optimizing pedagogical approaches to training employees of the internal affairs bodies of the Ministry of Internal Affairs of Russia on the basics of countering cyberterrorist threats at educational institutions departmental additional professional education. The study revealed the need to introduce modern interactive methods, simulations of real cyberattacks into the educational process, as well as focus on practical skills in analyzing and promptly responding to emerging potential threats. The authors emphasize the importance of an individual personalized approach to the training of law enforcement officers, taking into account the specifics of the strategic tasks performed by specialists and the level of their preliminary professional training. The expediency of integrating an interdisciplinary approach combining competent knowledge in the field of information technology, psychology and law is substantiated. It is proposed to develop an effective training system that makes it possible to quickly master various aspects of cybersecurity. The need for constant updating of educational curricula has been identified, taking into account the current trends in the development of cyberterrorism.

Keywords

pedagogical approaches, employee training, cyberterrorist threats, additional professional education, national security, departmental education system, Ministry of Internal Affairs of Russia, professionalism, teaching, ATS.

References

1. Vasilyeva S.A., Yagnakova E.Z. Current issues of staffing in the field of extremism and terrorism prevention // SUSU Bulletin. Series: Law. 2018. Vol. 18. № 1. pp. 104-109.
2. Gedgafov, M. M. Measures to counter cyberterrorist threats in the context of the globalization of the information space // Gaps in Russian legislation. 2021. Vol. 14. № 4. pp. 112-115.
3. Gorbatov V.S., Erdniev A.S. Improving the training of personnel to ensure the security of the information infrastructure of internal affairs bodies // Information technology security. 2024. Vol. 31. № 1. pp. 100-119.
4. Ilyin G.P. From the pedagogical paradigm to education // Higher education in Russia. 2000. № 1. p. 64.
5. Kiprich, D. A. Formation of the market of information security services: diss. ... cand. of econ. scien. M., 2003. 165 p.
6. Kobets P.N. The need to improve preventive cybersecurity and develop effective ways to counter international manifestations of cyberterrorism // Modern issues of sustainable development of society in the era of transformational processes: mat. XV International Scientific and Practical conference (February 23, 2024, Moscow). M.: Autonomous non-profit organization of additional professional education «The Center for the development of education and science», 2024. pp. 28-35.
7. Ksenik A.N., Soshenko A.N. International cooperation in the fight against cyberterrorism: the experience of the SCO and NATO // Keywords: mat. III Student Conference Institute of Social Sciences and Humanities of Tyumen State University (April 27, 2023, Tyumen). Tyumen: TumSU-Press, 2023. pp. 62-65.
8. Kumysheva M.K. Modern aspects of countering cyberterrorist threats // Law and Management. 2023. № 8. pp. 228-231.
9. Mashekuasheva M.X. Organization of the activities of internal affairs bodies for the prevention of extremism // Socio-political Sciences. 2018. № 3. pp. 40-41.
10. Sadekov R.R., Krokhina Yu.V. Organizational and legal aspects of the organization of professional training of employees of the Ministry of Internal Affairs of Russia in the system of additional professional education // Security issues. 2023. № 1. pp. 58-65.
11. Skorodumova O.B. Hackers as a phenomenon of the information space // Sociological research. 2004. № 2. pp.
12. 9-12. Sokolov, A. S., Povolotsky, A.Y. Cyberterrorism in Russia and Central Asian countries // Russian-Asian law journal. 2020. № 2. pp. 75-79.
13. Churikova A.Y. The use of big-data technologies to counter the cyberterrorist threat // The main directions of improving the national security system. 2023. № 3. pp. 395-399.
14. Yurkin I.3. Cyberterrorism: a challenge of the 21st century // Newspaper of the CIS Executive Committee «Republic». 2007. № 5. pp. 11-12.