

## АНАЛИТИЧЕСКАЯ ЗАПИСКА

**Тема:** Обратная сторона прогресса: как интернет стал площадкой для вербовки в радикальные религиозные течения.

**Исполнитель:** Алимгожинов Чингис Русланович

**Должность:** Руководитель информационно-аналитического отдела Управления по делам религий г.Алматы

### Введение

Появление интернета оказало значительное влияние на распространение радикальных религиозных течений. Интернет стал мощным инструментом, который радикальные группы начали активно использовать для различных целей, включая вербовку, пропаганду и распространение идей.

Интернет позволяет радикальным группам привлекать людей по всему миру, создавая сеть вербовщиков и поддерживающих сторонников. Это может приводить к радикализации, насилию и даже террористической активности, что угрожает безопасности как Казахстану, так и глобальной безопасности в целом.

Целью данной аналитической записки является проведение краткого исследования о том каким образом интернет способствует вербовке в радикальные религиозные течения, а также предложить эффективные меры для борьбы с этим явлением и минимизации рисков, связанных с интернет-радикализацией.

### Содержательная часть

Интернет предоставил радикальным группам возможность распространять свои идеи широкой аудитории без географических или политических ограничений. Это позволило радикальным течениям выйти за пределы локальных сообществ и достичь людей по всему миру. Например, такие организации, как «Исламское государство» (ИГИЛ) активно используют социальные сети и форумы для распространения своей идеологии и вербовки новых членов.

Теракт в **Крокус Сити Холле**, который произошёл в **2024** году является ярким примером использования интернета для вербовки в радикальные религиозные течения. В этом случае, как и во многих других, радикальные экстремистские группы использовали онлайн-платформы для распространения своей идеологии и вербовки людей.

По данным расследования, лица, совершившие террористический акт, были завербованы через интернет. Они вступил в контакт с радикальными группами через анонимные форумы и социальные сети, где были подвергнуты

воздействию экстремистской пропаганды, что в конечном итоге привело к решению совершить акт насилия. Необходимо отметить, что лица, совершившие данный террористический акт никогда не встречались с вербовщиками, координирующими их действия из-за рубежа что показывает огромные возможности интернет-пространства как одного из главных инструментов по координации действий террористических ячеек или отдельных лиц.

Как и в предыдущих случаях, интернет сыграл ключевую роль в процессе радикализации. В этом случае использовались закрытые чаты в мессенджерах, таких как **Telegram** и **Signal**, через которые вербовщики распространяли агрессивную пропаганду и деструктивные религиозные идеи. Эти платформы обеспечивали анонимность и безопасность, что позволяло радикалам скрытно координировать свои действия и убеждать людей в правоте своей идеи.

Через интернет вербовщики могли воздействовать на уязвимых людей, особенно тех, кто чувствовал социальную или личную изоляцию. Они предлагали им иллюзорное чувство принадлежности и важности, что было для них привлекательным в условиях жизненных трудностей. В результате вербовки человек становится частью глобальной сети радикалов, что может привести к совершению насильственных актов.

Одной из основных **причин**, почему интернет стал площадкой для радикализации, является **анонимность** общения. В отличие от традиционного общения в реальной жизни, где личность человека обычно легко идентифицируется, в интернете человек может оставаться анонимным, скрывая свою личность и истинные намерения. Это дает радикальным группам возможность распространять свои идеи без страха быть обнаруженными или привлечёнными к ответственности.

Кроме того, интернет не только обеспечивает анонимность, но и даёт возможность для **глобального распространения радикальных идей**. Интернет стирает географические и социальные барьеры, позволяя радикальным группам привлекать сторонников по всему миру. Благодаря платформам, таким как **YouTube**, **Twitter**, **Facebook**, радикальные группировки могут донести свои сообщения до широкой аудитории, независимо от того, где она находится. Это расширяет потенциал для вербовки и формирования глобальных сетей поддержки.

Для тех, кто чувствует социальную изоляцию, переживает кризис идентичности или ищет чувство принадлежности, интернет становится местом, где радикальные идеи могут выглядеть привлекательно. Вербовщики используют анонимность для того, чтобы установить доверительные отношения с потенциальными сторонниками и постепенно внедрить их в радикальную идеологию, не сталкиваясь с серьёзным сопротивлением или риском разоблачения.

Распространение радикальных религиозных течений через интернет может иметь серьёзные **последствия** как для Казахстана, так и для мира в целом. Для Казахстана это чревато угрозой безопасности и социальной

стабильности. В стране, где сосуществуют представители разных этносов и религий, радикализация может привести к усилению внутренней напряжённости между различными группами. В результате это может способствовать росту конфликтов, а также повышенному риску возникновения террористических актов, организованных сторонниками радикальных идей, вербовка которых активно осуществляется через интернет.

Например, вербовка через мессенджеры и соцсети даёт возможность радикальным группам набрать сторонников среди молодежи, что может привести к террористической активности на территории страны.

Кроме того, если радикальные идеологии проникнут в широкие массы, это может дестабилизировать социальную структуру Казахстана. Часть населения, поддавшаяся влиянию экстремистских идей, может начать действовать агрессивно, что приведет к увеличению числа насильственных инцидентов и распространению радикальных настроений в обществе. В условиях таких угроз правительство будет вынуждено тратить ресурсы на усиление безопасности, что отвлечет внимание от других важных задач, таких как развитие экономики и социальной сферы.

Для мира в целом проблема радикализации через интернет несет ещё более масштабные угрозы. Одной из основных опасностей является рост террористических группировок, которые могут действовать на международном уровне. Интернет позволяет радикальным организациям легко координировать свои действия и распространять идеологии, что значительно увеличивает вероятность транснациональных террористических актов. Этот процесс ведет к глобализации радикализации, так как люди из разных стран могут быть вовлечены в экстремистские сети, что создаёт международную угрозу безопасности.

Кроме того, радикализация через интернет может подрвать межкультурные и межрелигиозные отношения на глобальном уровне, что приведет к усилению вражды и недовольства между различными этническими и религиозными группами. Это может спровоцировать масштабные конфликты, усугубляя нестабильность в разных регионах мира. На фоне таких угроз международная безопасность окажется под риском, а экономическое развитие и политическая стабильность в странах могут пострадать, так как значительные ресурсы будут направлены на борьбу с терроризмом и экстремизмом.

Таким образом, распространение радикальных религиозных течений в интернете представляет собой серьёзную угрозу как для Казахстана, так и для всего мира. Это может привести к дестабилизации внутренней и международной безопасности, росту террористической активности и усилению межрелигиозных конфликтов, что требует разработки комплексных мер для предотвращения и борьбы с радикализацией в цифровом пространстве

## **Пути решения:**

Для решения проблемы вербовки радикальных религиозных течений через интернет необходимо разработать комплексные меры, включающие как технологические, так и социальные подходы. Вот несколько ключевых путей решения этой проблемы:

### **1. Усиление мониторинга и регулирования интернета с использованием ИС КИБЕРНАДЗОР**

Один из самых очевидных шагов — это **усиление мониторинга** социальных платформ и онлайн-ресурсов для выявления экстремистского контента. Включает в себя:

**Сотрудничество с интернет-компаниями:** Платформы, такие как Facebook, Twitter, YouTube, Telegram, должны работать с государствами и правоохранительными органами для выявления и блокировки экстремистских материалов. Это может быть осуществлено с помощью **алгоритмов искусственного интеллекта**, которые автоматически отслеживают и удаляют пропагандистский контент, видеоролики с насилием или рекрутингом. Для блокировки на территории Республики Казахстан радикального контента необходимо активное сотрудничество с зарубежными компаниями.

К примеру, в 2023 году Генеральная прокуратура РК опубликовала статью, где приводятся отчеты по пресечению предпосылок терроризма и экстремизма в онлайн сфере и об ограничении 900 тысяч экстремистских веб-ссылок в Казахстане. Для проверки сайтов на экстремизм, использовалась так называемая информационная система «Кибернадзор».

**Разработка законодательных инициатив:** Внедрение национальных и международных стандартов и законов, которые обязывают онлайн-платформы более строго контролировать контент. Например, обязательства по удалению экстремистских материалов в рамках определенного времени после их публикации.

**Глобальное сотрудничество:** Для борьбы с международной вербовкой необходимы усилия на глобальном уровне. Требуется улучшение сотрудничества между государствами, международными организациями и технологическими гигантами для мониторинга и блокировки экстремистского контента.

### **2. Образовательные инициативы и программы противодействия радикализации**

Важно не только ограничить доступ к экстремистским материалам, но и противостоять радикализации на уровне социальных и образовательных программ:

**Образовательные программы:** Внедрение программ для молодежи, направленных на развитие критического мышления и умения распознавать фальшивые или манипулятивные идеологии. Это поможет людям осознавать риски вербовки и избегать попадания под влияние радикальных идей.

**Программы профилактики радикализации:** Создание социально-психологических программ, направленных на предотвращение радикализации в уязвимых группах (например, среди молодежи, находящейся в социальной изоляции). Включение тренингов для педагогов и социальных работников, чтобы они могли выявлять признаки радикализации на ранних этапах.

**Психологическая поддержка:** Обеспечение доступа к психологическим службам для тех, кто может стать жертвой манипуляций радикалов. Специальные программы по реабилитации для людей, которые ранее были вовлечены в экстремистскую деятельность.

### **3. Широкое использование интернета для контрпропаганды с упором на целевую аудиторию**

Важно не только блокировать радикальные идеи, но и активно противостоять им через контрпропаганду. Это можно делать через:

**Контрпропагандистские кампании:** Создание позитивных онлайн-кампаний, которые будут нацелены на разоблачение радикальных идеологий и предложения альтернативных, мирных и конструктивных путей для людей, ищущих ответы на свои вопросы. Эти кампании могут использовать популярные социальные сети и онлайн-платформы.

**Использование реальных историй:** Привлечение людей, которые прошли через радикализацию, для создания материалов и видео, которые показывают последствия вовлечения в экстремизм и возможные пути выхода из этой ситуации.

**Партнёрства с религиозными и общественными лидерами:** Религиозные и общественные деятели могут стать важными союзниками в распространении умеренных интерпретаций религий, противопоставляя их радикальным и искаженным трактовкам.

### **4. Технические решения**

Разработка технологий, которые будут помогать в борьбе с распространением радикальных материалов:

**Искусственный интеллект и машинное обучение:** Разработка более совершенных алгоритмов для автоматического выявления и удаления экстремистского контента. ИИ может быть использован для распознавания не только текста, но и изображений и видеоматериалов, которые содержат пропаганду насилия или радикальных идеологий.

**Верификация информации:** Создание инструментов для верификации информации в интернете, чтобы люди могли легко проверять источники и достоверность материалов, которые они находят. Это помогает снизить влияние фейковых новостей и манипуляций со стороны экстремистов.

**Инструменты для анонимного доклада:** Создание платформ, на которых пользователи смогут анонимно сообщать о экстремистском контенте или подозрительных действиях без страха преследования.

## **Заключение**

В заключение, проблема распространения радикальных религиозных течений в интернете представляет собой серьёзную угрозу как для отдельных стран, так и для мирового сообщества. Анонимность и доступность цифровых платформ создают благоприятные условия для вербовки и распространения экстремистских идей, что может привести к росту террористической активности и усилению социальных конфликтов. Казахстан и другие страны, столкнувшиеся с этим явлением, рискуют потерять внутреннюю стабильность и безопасность.

Для решения этой проблемы необходимо усилить контроль за интернет-платформами и разработать меры для выявления и пресечения распространения экстремистской пропаганды. Важным шагом является сотрудничество с международными организациями для создания единой сети борьбы с интернет-радикализацией, а также проведение образовательных программ, направленных на повышение цифровой грамотности и снижение уязвимости граждан к радикальным идеям.

Перспективы выбранных решений могут включать значительное снижение уровня радикализации и терроризма, если будет обеспечен надёжный контроль за интернет-пространством, а также будет развиваться сотрудничество между государствами и частными компаниями для предотвращения распространения экстремистской идеологии. Прогрессивные и комплексные меры по борьбе с интернет-радикализацией могут стать основой для формирования безопасного и стабильного цифрового будущего.

**Все материалы, использованные в аналитической записке, были взяты из открытых источников.**

### **Использованные открытые источники:**

<https://drfl.kz/ru/cybernadzor/>

<https://tengrinews.kz/russia/smi-soobschili-zaderjanii-podozrevaemyih-napadenii-krokus-530027/>