

УДК: 343.2.7

Улан уулу Авакан
ОИӨК “Кыргыз Республикасынын Эл аралык университети”
Докторант
Улан уулу Авакан
УНПК «Международный университет Кыргызстана»
Докторант
Ulan uulu Avakan
ERPC “International University of Kyrgyzstan”
PhD

КИБЕРЭКСТРЕМИЗМ МАМЛЕКЕТТИН КООПСУЗДУГУНА КОРКУНУЧУ

КИБЕРЭКСТРЕМИЗМ КАК СЕРЬЕЗНАЯ УГРОЗА БЕЗОПАСНОСТИ ГОСУДАРСТВА

CYBERTERRORISM AS A THREAT TO THE NATIONAL SECURITY OF THE STATE

Аннотациясы: Автор интернет желедеги экстремисттик идеологиялардын таратылышы жөнүндө маселерди көтөрүп чыкты. Экстремизмге каршы күрөшүдө иш-чараларынын кемчиликти жана алардын чечилиши жөнүндө.

Негизги сөздөр: Экстремизм, дин, интернет, каршы иш-чаралар, укук коргоо органдары.

Аннотация: Автор рассматривает эскалацию масштабов экстремизма в интернет-ресурсах. Рассмотрены механизмы, способствующие профилактике распространения данного вида преступления.

Ключевые слова: Экстремизм, религия, интернет, противодействие, правоохранительные органы, интернет, противодействие.

Abstract: Operatively - search activity Department of internal Affairs countering extremist Ideology in Internet.

Key words: Extremism, religion, ideological policy, law enforcement, internet, counteraction.

В настоящее время многие государства столкнулись с серьезной проблемой – распространением экстремистской идеологии через интернет. В информационном пространстве слово «экстремизм» часто связывают с религией. Экстремизм во всех его проявлениях подрывает общественную безопасность, создает реальную угрозу основам конституционного строя, ведет к негативным социальным явлениям. Идеи экстремистских организаций оказались заразны для людей с неустойчивой психикой и жизненными принципами. Последователи экстремизма, прикрываясь священным писанием, уничтожают мировую культуру, повседневный образ жизни людей, их веру в

будущее, навязывают свои догмы и идеи.

Информационная сфера, получившая наибольшее развитие в последнее время, является системообразующим фактором жизни современного общества и активно влияет на такие составляющие национальной безопасности Кыргызской Республики, как политическая, экономическая, информационная. Киберэкстремизм представляет угрозу, набирающую силу быстрыми темпами. Под киберэкстремизмом мы понимаем новую форму экстремизма, которая использует для достижения своих целей компьютеры и компьютерные сети, а также информационно-коммуникационные технологии.

Компьютерные сети вкупе с информационно-коммуникационными технологиями, предоставляют неограниченные возможности для обучения и образования, для общения и развлечений. Наряду с этим в сети Интернет есть и скрытые угрозы, связанные зачастую с незнанием правил общения и простейших правил безопасной работы в компьютерных сетях. При этом значительную группу пользователей сети Интернет составляют школьники [1].

Одним из способов профилактики и предотвращения киберэкстремизма является обучение пользователей компьютерных сетей этическим и правовым нормам информационной деятельности.

15 января 2016 года на пресс-конференции в Бишкеке глава 10-го Главного управления Сталбек Рахманов подвел итоги работы в 2015 году. «За прошлый год выявлены 508 кыргызстанцев, принимающих участие в боевых действиях (или ранее сражавшихся на стороне боевиков) в Сирии, – сказал он. Среди них 387 мужчин, 121 женщина, 83 несовершеннолетних» [2]. В своем интервью «ITON TV» специалист по региональной безопасности в Центральной Азии Александр Зеличенко рассказал, что «реально существует сеть, которая вербует, готовит в Центральной Азии людей для подготовки терактов, недавно произошедшие взрывы в Кыргызстане, это глобализация, это все звенья одной цепи» [3].

Оперативно-розыскная деятельность представляет собой одну из разновидностей правоохранительной деятельности, осуществляемой гласно и негласно уполномоченными на то оперативными подразделениями государственных органов. Одним из эффективных и действенных способов противостояния экстремизму является проведение оперативно-розыскных мероприятий, направленных на своевременное выявление, предотвращение преступных экстремистских замыслов и раскрытие данной категории преступлений по «горячим следам» [4]. Этому и способствует ведение оперативно-розыскных мероприятий направленных на выявление экстремистских замыслов в сети Интернет. Предупреждение преступлений оперативно-розыскными мерами – весьма действенное и перспективное

направление деятельности оперативных подразделений органов внутренних дел. Службой противодействия экстремизму и незаконной миграции МВД Кыргызской Республики проводятся профилактические работы. Многие выехавшие в Сирию были завербованы через социальные сети. Очень много групп и видеороликов экстремистского характера, которые сотрудники отдела отслеживают и удаляют. Есть проект «Онлайн патруль», также есть отдел по киберугрозе, именно по профилактике экстремизма и терроризма. Сотрудники данного отдела за 2017 год удалили более 50 вебсайтов в Кыргызстане, которые имели экстремистско-террористический контент. Также решениями судов были заблокированы около 50 сайтов [5].

Анализ информационной обстановки в сети показывает, что контент основных Интернет-ресурсов по продвижению идеологии экстремизма носит наступательный, агрессивный характер, отличается хорошей теоретической базой, продуманным спектром методов управляемого информационно-психологического воздействия на пользователей и защищенностью ресурсов. Этому способствует специфика глобальной сети, которая обеспечивает такие преимущества, как простота доступа, независимость от географического расположения, неограниченная потенциальная аудитория, высокая скорость передачи информации, трудности в осуществлении контроля со стороны правоохранительных органов и другие [6]. В виртуальном пространстве осуществляется управление деятельностью автономных групп, проводится идеологическая работа, сбор средств, а также непосредственная подготовка к совершению экстремистских акций. Одной из главных задач, решаемых экстремистскими и террористическими объединениями с помощью Интернета, является как можно более широкое освещение своих акций с привязкой их к идеологическим установкам и устрашением общества. Прекращение деятельности таких Интернет-ресурсов зачастую невозможно в силу правовых и юридических сложностей, а иногда малоэффективно, т.к. их место быстро занимают новые.

Так, действующие нормы предполагают

обеспечение однозначной идентификации лица, разместившего в сети Интернет экстремистские материалы, владельца домена, в рамках которого опубликованы указанные материалы, а также оператора связи, на технических средствах которого они размещены. Сайты, размещающие экстремистские материалы, зарегистрированы, как правило, вне пределов Кыргызской Республики, установить и процессуально идентифицировать лиц, размещающих такие материалы, и владельцев сайтов зачастую технически не возможно.

С учетом современного развития средств коммуникации и повышению оперативно-розыскной деятельности в сфере выявления экстремистской идеологии и помыслов предлагаем, совместно с Службой противодействия экстремизму и нелегальной миграции МВД Кыргызской Республики разработать инструкции по проведению оперативно-розыскных мероприятий, таких как:

1. снятие информации с технических каналов связи;
2. оперативный поиск в сетях и на каналах связи.

Исходя из того, что законодателем не определено содержание снятия информации, такая операция (действие) может включать сканирование технического канала, радиоперехват, копирование и другие действия с последующей фиксацией информации на магнитных, текстовых (бумажных), электронных носителях. Пункт 19 статьи 7 Закона Кыргызской Республики «Об оперативно-розыскной деятельности» [7]. предлагаем изложить в следующей редакции – «Оперативный поиск в сетях и на каналах связи по выявлению лиц и фактов, представляющих оперативный интерес в открытой печати,

виртуальных досках объявлений, блогах, сайтах и спам-рассылках».

Для проведения этой работы наличие специализированного штата сотрудников представляется недостаточным, поэтому весьма актуальным представляется вопрос привлечения к сотрудничеству анонимных пользователей интернет-сервисами, создание сайтов-приманок, предназначенных для документирования злонамеренных действий, а также привлечение к сотрудничеству штатных служб информационной безопасности предприятий.

Список использованных источников:

1. Мовчан И.В. Профилактика киберэкстремизма в школьной среде в рамках школьного курса информатики // <https://www.top-technologies.ru/ru/article/view?id=35167>.
2. См. материалы сайта <http://www.islamsng.com/kgz/news/10330> (дата обращения 22.11.2016 года).
3. Интервью «Террор на экспорт» <http://www.iton.tv/art/6775/Terror-na-eksport/>.
4. Методическое пособие по религиозному экстремизму в Кыргызской Республике, подготовлен отделом по противодействию религиозному экстремизму Десятого Управления ГУВД, г. Бишкек, 2015 С.13-14.
5. Начальник отдела «десятки» Э.Бакиев: Ни одна запрещенная радикальная организация не создана в Кыргызстане (интервью) // <https://svodka.akipress.org/news:1432938>
6. Статья «Противодействие идеологии терроризма в сети Интернет» МВД по Республике Коми. https://11.mvd.pf/Protivodejstvie_ideologii_terrorizma_v.
7. Закон Кыргызской Республики «Об оперативно-розыскной деятельности» от 16 октября 1998 года № 131