МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

СБОРНИК МАТЕРИАЛОВ

«БЕЗОПАСНОСТЬ И ОБРАЗОВАНИЕ»

ИНФОРМАЦИОННО-ПРАКТИЧЕСКИЙ ФОРУМ

МИНОБРНАУКИ РОССИИ
ЮРАЦ
ЮЖНЫЙ РЕГИОНАЛЬНЫЙ
АТТЕСТАЦИОННЫЙ ЦЕНТР

МИНОБРНАУКИ РОССИИ
НЦПТИ

КРЫМСКИЙ ФЕДЕРАЛЬНЫЙ
УНИВЕРСИТЕТ

СИМФЕРОПОЛЬ

10:00 28-29 ОКТЯБРЯ 2015

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

СБОРНИК МАТЕРИАЛОВ

«БЕЗОПАСНОСТЬ И ОБРАЗОВАНИЕ»

ИНФОРМАЦИОННО-
ПРАКТИЧЕСКИЙ
ФОРУМ

СОДЕРЖАНИЕ

О ФОРУМЕ

В Г. СИМФЕРОПОЛЕ 28-29 ОКТЯБРЯ 2015 Г. СОСТОЯЛСЯ ВТОРОЙ ИНФОРМАЦИОННО-ПРАКТИЧЕСКИЙ ФОРУМ «БЕЗОПАСНОСТЬ И ОБРАЗОВАНИЕ»

В Симферополе 28 и 29 октября 2015 на базе Крымского федерального университета им. В.И. Вернадского состоялся второй информационно-практический форум «Безопасность и образование».

Тематика Форума затронула вопросы обеспечения физической и информационной защищенности образовательных организаций и работу с молодежью. Одна из основных задач Форума заключалась в организации деятельности по противодействию терроризма и профилактике распространения идеологии экстремизма в образовательных (научных) организациях России.

В Форуме приняли участие представители Министерства образования и науки Российской Федерации, Федеральной службы безопасности по Республике Крым и г.Севастополю, Министерства чрезвычайных ситуаций, Министерства внутренних дел, Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций Российской Федерации, Федеральной службы по техническому и экспортному контролю Российской Федерации и Министерства образования, науки и молодежи Республики Крым.

Целью выполнения работы является повышение уровня информационного обмена, систематизация и синхронизация действий, предпринимаемых в области обеспечения безопасности (физической и информационной) образовательных (научных) организаций.

ПРИВЕТСТВЕННОЕ СЛОВО ОТ ОТДЕЛА МОБИЛИЗАЦИОННОЙ ПОДГОТОВКИ МИНОБРНАУКИ РОССИИ

Морозов Олег Анатольевич,

Начальник Отдела мобилизационной подготовки Минобрнауки России

Уважаемые участники и гости форума!

Проблемы безопасности в образовательной среде в наши дни приобрели особую актуальность и жизненно важную необходимость.

В условиях развития общества и внедрения современных информационных технологий во все сферы его жизнедеятельности понятие «безопасность» объективно становится определяющим направлением обеспечения безопасности личности, общества и государства.

Сегодня перед Россией, как и перед всем мировым сообществом, стоит задача выработки новой технологии предупреждения и урегулирования конфликтов и кризисных ситуаций, по своему содержанию и характеру протекания существенно отличающихся от конфликтов недавнего прошлого. Эта технология должна вобрать в себя наиболее эффективные политико-правовые и силовые методы, апробированные предшествующим опытом, в сочетании с инструментарием, отвечающим реалиям глобализированного мира.

Хочу отметить, что все темы, заявленные для обсуждения, действительно актуальны и требуют внимания. Я искренне уверен, что в результате обсуждений появятся идеи новых проектов и интересных решений, и это позволит внести ощутимый вклад в развитие безопасности в образовательной сфере и в дальнейшем поможет вывести её на новый качественный уровень.

Выражаю глубокую благодарность организаторам форума за создание профессиональной информационной площадки и предложенного формата проведения мероприятия, предусматривающего возможность прямого диалога руководства и ведущих специалистов в области безопасности Министерства образования и науки России, Правительства Крымского федерального округа, Управления ФСТЭК России по Южному и Северо-Кавказскому федеральным округам, Главному управлению МЧС России по Республике Крым. Полагаю, что проведение форума «Безопасность и образование» поможет нам выработать эффективные меры и единый подход, которые позволят на высоком

уровне противостоять современным вызовам и угрозам.

Желаю всем участникам форума успешной и плодотворной работы.

№1

28 ОКТЯБРЯ 2015 Г.

МОДЕРАТОР: ЧУРИЛОВ СЕРГЕЙ АНАТОЛЬЕВИЧ – ДИРЕКТОР НАЦИОНАЛЬНОГО ЦЕНТРА ИНФОРМАЦИОННОГО ПРОТИВОДЕЙСТВИЯ ТЕРРОРИЗМУ И ЭКСТРЕМИЗМУ В ОБРАЗОВАТЕЛЬНОЙ СРЕДЕ И СЕТИ ИНТЕРНЕТ (НЦПТИ)

ПРОТИВОДЕЙСТВИЕ ЭКСТРЕМИЗМУ И ТЕРРОРИЗМУ В СЕТИ ИНТЕРНЕТ И ОБРАЗОВАТЕЛЬНОЙ СРЕДЕ: ВЫЗОВЫ 2015 ГОДА

Лашин Ренат Леонидович,

начальник отдела Департамента управления программами и конкурсных процедур Минобрнауки России

В 2015 году мировое интернет-сообщество столкнулось с массовой информационной угрозой со стороны экстремистских и террористических организаций. Специфика сети Интернет состоит в том, что большей частью ежедневной аудитории онлайн-ресурсов являются лица моложе 30 лет, а аудитория социальных сетей – это преимущественно подростки и молодые люди в возрасте от 14 до 20 лет, то есть учащиеся школ и вузов. Молодежь привлекают анонимность и масштабность сети Интернет, отсутствие как таковых социальных, нравственных и даже государственных границ. По этой причине Интернет стал, в том числе, и эффективным инструментом пропаганды террористической и экстремистской деятельности.

Экстремизм – это приверженность к крайним мерам и взглядам, радикально отрицающим существующие в обществе нормы и правила через совокупность насильственных проявлений, совершаемых отдельными лицами и специально организованными группами и сообществами. **Экстремизм** – это сложная и неоднородная форма выражения ненависти и вражды. Большинство и отечественных, и зарубежных исследователей полагают, что экстремизм в современном обществе – в основном, молодежный феномен.

Терроризм – определяется как идеология насилия и практика воздействия на общественное сознание, на принятие решений органами государственной власти, органами местного самоуправления или международными организациями, связанная с силовым воздействием, устрашением населения и/или иными формами противоправных насильственных действий.В 2014 году в Южном федеральном университете проводился социологический опрос среди студентов на тему «Терроризм в Интернете». Опрос показал, что молодые люди не интересуются терроризмом, только 3% из них заходили на сайты террористической направленности, а 1% – на сайты, посвященные антитеррору. Среди молодежи укрепилось мнение, что под влияние террористической пропаганды в Интернете попадают люди слабые (29%), с психическими

заболеваниями (16%), женщины и дети (9%), люди с несформированными жизненными ценностями (8%). 4% опрошенных студентов считают, что мусульмане также входят в группу риска. Молодые люди считают, что самым эффективным способом пропаганды террористической деятельности в сети являются видеоролики или фильмы (более 50% опрошенных), 19% считают, что вербовать террористов могут на форумах или в блогах.

Однако события 2015 года, когда иностранные (британские, французские и др) и российские студенты по одному и группами пытались присоединиться к Исламскому государству показали, что тактика, выбранная радикалами в сети Интернет, является успешной.

В 2015 году источниками массовой экстремистской и террористической пропаганды стали ресурсы, поддерживающие идеологию «Исламского государства Ирака и Леванта» или просто ИГИЛ.

Для вербовки и создания привлекательного образа террористических организаций используются практически все популярные социальные сети и ресурсы: «ВКонтакте», «Youtube», «Facebook», «Instagram», «Twitter». Более того, используются все возможности данных социальных сетей (массовые рассылки, «перепосты», размещение видео- и музыкальных материалов, фотографий, документов, на существующих страницах к публикациям в комментариях добавляются ссылки на материалы по соответствующей теме с других ресурсов).

Успешная военная кампания ИГИЛ сопровождается беспрецедентной по масштабам пропагандистской кампанией в онлайн-пространстве: ИГИЛ ведут трансляции боевых действий в «Twitter», выкладывают снимки своих жертв в «Instagram» и оперативно сообщают новости своим подписчикам в «Facebook». Со службой микроблогов «Twitter» террористы работают очень активно, ввиду больших возможностей быстрого распространения информации, удобства использования хештегов. Одним из способов работы ИГИЛ в «Twitter» является продвижение необходимых хештегов. Тысячи активистов одновременно размещают твиты с необходимыми хештегами. Этот метод позволил активистам ИГИЛ искажать результаты поисковой выдачи для рядовых пользователей социальной сети. Проводя свой хештег в чужие аккаунты, ИГИЛ обеспечивает себе дополнительную аудиторию (контент от ИГИЛ «попадается на глаза» тем пользователям, которые сами его не искали). Порядка 40 000 твитов в поддержку ИГИЛ появляются за неделю.

В «ВКонтакте» работают информационные подразделения террористов, есть паблики провинций халифата и аккаунты рядовых боевиков, а также большой пласт их сторонников. Пропаганда ведётся как на арабском, так и на русском языках. Вербовщики прибегают к индивидуальному подходу, используя ту информацию, которую могут найти в сети о сочувствующих своей организации.

При этом используется узнаваемый стиль, слоганы и символы. У молодежи формируется представление о некой общности – социальной группе, отличной от других цельностью представлений и знаний об окружающей действительности. Слоганы и символы подаются при помощи понятных и популярных среди молодежи форматов, легко приобретающих статус «вирусных явлений»: демотиваторов, мемов, подражаний и других.

Инструментами воздействия являются манипулятивные технологии: формирование идеологии «свой-чужой», превосходства одной национальности над другой, стереотипизация образа «врага».

Национальный Центр информационного противодействия терроризму и экстремизму в образовательной среде и сети Интернет (НЦПТИ) создан для решения задач, поставленных Министерством образования и науки Российской Федерации, по противодействию радикаль-

ным идеям терроризма и экстремизма.

В целях противодействия массовой информационной угрозе терроризма и экстремизма в 2015 году были проработаны методы:

– выявление и удаление уже размещенных материалов в социальных сетях и других ресурсах сети Интернет;

– взаимодействие с общественностью для эффективного совместного противодействия экстремистским и террористическим идеологиям.

Основным инструментом противодействия экстремистским материалам является ежедневный мониторинг интернет-среды. Он позволяет своевременно отслеживать материалы определенной тематики и оперативно удалять или блокировать к ним доступ.

Удаление экстремистских материалов без вмешательства правоохранительных органов возможно несколькими методами:

– использование прямого контакта с администрациями социальных сетей;

– использование краудсорсинга как метода, помогающего противодействию экстремистским идеологиям.

В первом случае пользователь (сотрудник НЦПТИ или любой другой) направляют информацию об обнаруженном противоправном контенте в администрацию социальной сети. К примеру, рассмотрение жалобы на аудиозапись через сервис социальной сети «ВКонтакте» осуществлялось в течение пяти рабочих дней. Аналогичным образом происходит взаимодействие с администрациями социальных сетей «Facebook», «Одноклассники», «Youtube» и другими.

Во втором случае – удаление экстремистского видео в «Youtube» - используется краудсорсинг. Сотрудниками НЦПТИ была создана группа единомышленников – пользователей сети, объединенных идеей защитить Интернет от экстремистских идеологий. В основном это молодежь до 35 лет с активной гражданской позицией. Усилиями группы уже были удалены несколько видео, пропагандирующих ИГИЛ.

НЦПТИ на региональном уровне активно сотрудничает с представителями правоохранительных и правоприменительных органов. Результаты мониторинга противоправного контента в сети Интернет доступны для партнеров Центра. Данный опыт взаимодействия в настоящее время масштабируется и на федеральном уровне.

Профилактика распространения радикальных идеологий в сети – одна из ключевых задач НЦПТИ. Она решается с помощью нескольких каналов.

Во-первых, в сети Интернет создан и поддерживается информационно-аналитический ресурс НЦПТИ.РФ, на котором размещен ряд просветительских материалов, форма изложения доступна широкой аудитории. Рядовой пользователь Интернета может сообщить о противоправном контенте.

Во-вторых, НЦПТИ выпускает периодическое издание «Обзор.НЦПТИ», которое предназначено для обмена опытом между различными ведомствами и отдельными специалистами в области профилактики и противодействия терроризму и экстремизму.

В-третьих, создана реальная площадка для обсуждения данных вопросов – это информационно-практический форум «Безопасность и образование». В этом году Форум объединяет представителей Минобрнауки России, ФСБ России, ФСТЭК России, Роскомнадзора, ведущих вузов страны и других экспертов для обсуждения лучших практик по организации комплексной безопасности в образовательных и научных учреждениях.

Профилактика идеологии терроризма и экстремизма является важной задачей в деле воспитании молодежи. Её решение требует

принятия следующих мер:

– ведение постоянного анализа Интернет-пространства с целью выявления и блокирования фактов пропаганды террористической идеологии;

– предоставление возможности подключения к процессу выявления противоправного контента бдительных Интернет-пользователей;

– разработка и актуализация методического обеспечения процесса информационного противодействия терроризму и экстремизму;

– ведение разъяснительной работы с целью описания сущности терроризма и экстремизма, а также формирование стойкого неприятия обществом идеологии насилия;

– привлечение молодежи к участию в противодействии терроризму, экстремизму, национализму и религиозному фундаментализму в образовательной среде.

ФУНКЦИОНАЛЬНАЯ ПОДСИСТЕМА МИНОБРНАУКИ РОССИИ ЕДИНОЙ СИСТЕМЫ РСЧС, КАК ЭЛЕМЕНТ КОМПЛЕКСНОЙ БЕЗОПАСНОСТИ СИСТЕМЫ ОБРАЗОВАНИЯ

Власов Виталий Леонидович,

Департамент государственной службы, кадров и управления делами Минобрнауки России

В последние годы в системе образования уделяется самое пристальное внимание вопросам безопасности подведомственных организаций Минобрнауки России, особое место среди которых занимают образовательные организации всех видов и уровней. Это обусловлено многочисленными фактами происшествий в организациях: пожарами, массовыми заболеваниями, травматизмом, правонарушениями, наркоманией, актами телефонного и политического терроризма. В связи с ростом числа чрезвычайных ситуаций (ЧС) одной из важнейших задач системы образования является формирование безопасной, здоровой образовательной среды и культуры безопасности.

Однако до настоящего времени не выработано единого понятия (определения) «Комплексная безопасность», что объясняется многоуровневостью и многокритериальностью включаемых в этот термин задач. Поэтому на сегодняшний момент правильней было бы говорить о достижении некоторого компро-

миссного решения по обеспечению безопасности образовательных организаций и обеспечивать защиту комплексно, только от наиболее опасных и реальных угроз.

Предлагаемый доклад посвящен единой государственной системе предупреждения и ликвидации чрезвычайных ситуаций (далее РСЧС) как части системы государственного управления, направленной на защиту населения и территорий Российской Федерации от чрезвычайных (кризисных) ситуаций в аспекте и терминологии МЧС России, а более конкретно, её функциональной подсистеме в сфере деятельности Минобрнауки России (далее функциональная подсистема РСЧС).

Задачи, возложенные на РСЧС, системы образования в большей степени касаются, так называемые, «превентивные» задачи, особое место в числе которых занимает обеспечение готовности к действиям органов управления, сил и средств.

Следует заметить, что одним из основных условий работоспособности системы РСЧС, как и любой другой системы в правовом государстве, является соответствующая эффективная нормативно-правовая база в предметной области. Наличие более 100 Федеральных законов, Указов Президента, Постановлений Правительства свидетельствует о достаточной проработке юридических аспектов в интересующей нас области.

Сложностью решаемых задач по обеспечению безопасности обусловлена структура системы РСЧС. Она включает функциональные и территориальные подсистемы и действует на федеральном, межрегиональном, региональном, муниципальном и объектовом уровнях. Функциональные - ведомственные, отраслевые (в силу специфики) подсистемы создают ФОИВ. Территориальные подсистемы создают органы исполнительной власти субъектов РФ.

В зависимости от способов решения конкретных задач по обеспечению безопасности населения и территорий, возникают варианты и формы взаимодействия того или иного субъекта системы внутри единой структуры. Так, в состав структуры РСЧС входит 45 функциональных подсистем и 85 территориальных подсистем.

Наиболее задействованными ведомствами в области безопасности являются Минприроды и Минтранс, что вполне объяснимо и исходит из решаемых ими задач. За Минобрнауки закреплена единственная функциональная подсистема.

ФП РСЧС Минобрнауки России состоит из координационных органов федерального и объектового уровней; постоянно действующих органов управления, соответственно, федерального и объектового уровней; органов повседневного управления федерального и объектового уровней; сил и средств федерального и объектового уровней; а также из резервов финансовых и материальных ресурсов федерального и объектового уровней; систем связи и информационного обеспечения федерального и объектового уровней.

Особое внимание следует обратить на то, что отсутствие любого компонента ФП РСЧС на любом уровне ведет к срыву выполнения возложенных на систему задач, и, как следствие, к невыполнению требований федерального законодательства.

Основным нормативно-правовым Актом (НПА), регулирующим действие ФП РСЧС Минобрнауки России, является приказ Минобрнауки России от 29 июня 2009 года №2080.

В соответствии с принципами, заложенными в НПА при определении эффективности функционирования ФП РСЧС, основными условиями эффективного функционирования ФП РСЧС являются:

1. Наличие и легитимность объектов структуры ФП РСЧС;

2. Наличие финансирования мероприятий ФП РСЧС на соответствующих уровнях;

3. Наличие работоспособной системы подготовки должностных лиц.

Система подготовки работников органов РСЧС определена постановлением Правительства РФ от 4 сентября 2003 года №547 и уточнена ведомственными приказами. Так, приказом Минобрнауки России от 29 июня 2011 года №2080 определен порядок обучения должностных лиц ФП РСЧС, который гласит о подготовке в УМЦ ОЗ и ПК, созданных в соответствии с приказом Минобрнауки России от 29 мая 2007 года №154 и от 26 октября 2011 года №2542, и в Академии гражданской защиты МЧС России. Однако, в соответствии с постановлением Правительства РФ от 4 сентября 2003 года №547, обучение за счет средств федерального бюджета в АГЗ МЧС России предусмотрено только для соответствующих работников ФОИВ и представителей УМЦ ОЗ И ПК.

В соответствии с методическими рекомендациями, разработанными МЧС России о подготовке сведений в Государственный доклад по РСЧС, необходимо подавать достоверные сведения о состоянии органов управления ФП РСЧС на объектах (наличие, штат, укомплектованность, компетентность и т.д.) и подготовке соответствующих должностных лиц.

Наличие более 100 Федеральных законов, Указов Президента, Постановлений Правительства свидетельствует о достаточной проработке юридических аспектов в интересующей нас области.

ОРГАНИЗАЦИЯ ПОДГОТОВКИ СПЕЦИАЛИСТОВ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РОССИЙСКОЙ ФЕДЕРАЦИИ ОСНОВНЫЕ ПРОБЛЕМНЫЕ ВОПРОСЫ РЕАЛИЗАЦИИ ПОЛНОМОЧИЙ ФСТЭК РОССИИ

Шилин Вадим Викторович,

Начальник второго отдела Управления ФСТЭК России по Южному и Северо-Кавказскому федеральным округам

1. Организация подготовки специалистов в области информационной безопасности в Российской Федерации.

Подготовка специалистов со средним профессиональным и высшим образованием, а также дополнительное профессиональное образование специалистов в области информационной безопасности осуществляется в соответствии с требованиями следующих законодательных, нормативных правовых актов и методических документов:

№273-ФЗ от 29 декабря 2012 г; №197-ФЗ от 30 декабря 2001 г.; №79-ФЗ от 27 июля 2004 г.; ПП РФ от 27 марта 2015 г. №285; Приказ Минобрнауки России от 19 декабря 2013 №1367; Приказ Минобрнауки России от 14 июня 2013 №464; Указ Президента РФ от 28 декабря 2006 г. №1474; ПП РФ от 6 мая 2008 г. №362; Приказ ФСТЭК России от 24 августа 2012 г. №100; Приказ Минобрнауки России от 1 июля 2013 г. №499; Приказ Минобрнауки России от 5 декабря 2013 г. №1310; Методические документы ФСТЭК России (методические рекомендации, типовые и примерные программы профессиональной переподготовки и повышения квалификации специалистов по защите информации).

Приказами Минобрнауки России от 12 сентября 2013 г. №1060, 1061, от 29 октября 2013 г. № 1199 утверждены перечни специальностей среднего профессионального и высшего образования.

Подготовку специалистов в области информационной безопасности со средним профессиональным образованием осуществляют более 30 образовательных организаций, а специалистов с высшим образованием – около 150 организаций.

Дополнительное профессиональное образование осуществляется на базе высшего или среднего профессионального образования и направлено на непрерывное профессиональное развитие специалистов.

Дополнительное профессиональное образование включает в себя профессиональную переподготовку и повышение квалификации.

Программа повышения квалификации направлена на совершенствование и (или) получение новой компетенции, необходимой для профессиональной деятельности, и (или) повышение профессионального уровня в рамках имеющейся компетенции.

В свою очередь **программа профессиональной переподготовки направлена** на получение

компетенции, необходимой для выполнения нового вида профессиональной деятельности, приобретение новой квалификации.

Повышение квалификации гражданских служащих проводится по мере необходимости в течение всей трудовой деятельности работников, но не реже одного раза в три года.

Периодичность прохождения повышения квалификации специалистами, не входящими в число государственных гражданских служащих, устанавливается работодателями.

Объем времени, отводимый на повышение квалификации, в зависимости от вида обучения не может быть менее 40 часов.

При этом образовательные организации дополнительного профессионального образования, после успешного освоения обучаемыми образовательных программ повышения квалификации выдают им удостоверение о повышении квалификации.

Профессиональная переподготовка гражданских служащих проводится по мере необходимости, определяемой представителем нанимателя.

Объем времени на освоение образовательной программы профессиональной переподготовки составляет более 360 часов.

Необходимо отметить, что ФСТЭК России, реализуя свое полномочие по методическому руководству подготовкой, профессиональной переподготовкой и повышением квалификации специалистов по защите информации, осуществляет рассмотрение и согласование представляемых образовательными учреждениями программ подготовки, профессиональной переподготовки и повышения квалификации указанных специалистов.

Программы повышения квалификации рассматриваются в ФСТЭК России с учетом имеющихся на сегодняшний день 18 типовых программ указанного уровня подготовки и объемом учебного времени в 72 часа, которые представлены в утвержденных ФСТЭК России методических рекомендациях по разработке образовательных программ дополнительного профессионального образования.

Образовательные учреждения, которые приняли решение осуществлять свою образовательную деятельность по программам, согласованным с ФСТЭК России, представляют их в Службу, где они проходят экспертизу на предмет соответствия вышеуказанным типовым программам.

В настоящее время в ФСТЭК России зарегистрировано более 290 согласованных Службой программ профессиональной переподготовки и повышения квалификации специалистов по защите информации. С перечнем этих программ, а также образовательных учреждений, разработавших их, можно ознакомиться на официальном сайте ФСТЭК России.

К настоящему времени в Российской Федерации ведут обучение по программам ДПО в области информационной безопасности около 150 высших учебных заведений, 29 региональных учебно-научных центров, а также более 40 образовательных учреждений дополнительного профессионального образования.

Если говорить об образовательных учреждениях, ведущих повышение квалификации и профессиональную переподготовку специалистов, работающих в области ПД ИТР, то к ним можно отнести образовательные организации, которые согласовали с ФСТЭК России свои образовательные программы.

Кроме того, по заказу ФСТЭК России разработаны и утверждены две примерные программы профессиональной переподготовки:

«Техническая защита информации, содержащей сведения, составляющие государственную тайну»;

«Техническая защита информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну».

В ближайшее время планируется утвердить также примерную программу профессиональной переподготовки «Противодействие техническим разведкам».

Кроме того, к настоящему времени разработаны первые редакции проектов восьми новых примерных программ повышения квалификации специалистов по защите информации, которые после утверждения в конце 2015 – начале 2016 года заменят упомянутые выше типовые программы.

Основными предстоящими направлениями работ, определенными руководством ФСТЭК России по вопросу выполнения решений, принятых на оперативном совещании Совета безопасности Российской Федерации по вопросу «О кадровом обеспечении безопасности в информационной сфере» (23 июля 2015 г.), являются:

формирование прогноза баланса трудовых ресурсов и прогноза подготовки кадров в области информационной безопасности;

исполнение ФСТЭК России полномочий центра ответственности по определению ежегодных контрольных цифр приема по специальностям и направлениям подготовки в области информационной безопасности для обучения по образовательным программам среднего и высшего образования за счет бюджетных ассигнований федерального бюджета;

подготовка предложений по созданию системы учебно-научных (производственных) центров по проблемам информационной безопасности на базе образовательных организаций в федеральных округах;

подготовка предложений по принятию дополнительных мер по методическому обеспечению подготовки, переподготовки и повышения квалификации кадров в области информационной безопасности по направлениям противодействия иностранным техническим разведкам и технической защиты информации.

Большая часть указанных работ являются новыми, так как ранее Службой не выполнялись. Работы объемные, трудоемкие и для их выполнения потребуется приложение максимальных усилий работников, на которых будут возложены соответствующие должностные обязанности по выполнению данных работ.

2. Требования нормативных правовых актов Российской Федерации по технической защите информации, содержащей сведения, составляющие государственную тайну.

В ходе учебного процесса по подготовке, переподготовке и повышению квалификации специалистов, при выполнении научно-исследовательских, опытно-конструкторских работ в вузах, зачастую возникает необходимость в использовании сведений, составляющих государственную тайну.

В соответствии с Законом Российской Федерации «О Государственной тайне» №5485-1 от 21 июля 1993 г. такой вид деятельности подлежит обязательному лицензированию. Государственным органом лицензирования в данном случае является Федеральная служба безопасности Российской Федерации.

Пройдя этап получения лицензии ФСБ России и оформления допусков сотрудников на работу с государственной тайной, следует приступить к этапу формирования системы защиты информации.

Одним из этапов построения системы защиты информации является подготовка к проведению аттестации, разработка и утверждение технического задания на выполнение работ по ТЗИ и непосредственно сама аттестация объектов информатизации.

Завершающим этапом является подготовка заключения по результатам аттестации и получение аттестата соответствия на объект информатизации.

3. Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных.

Никто не станет оспаривать тот факт, что в каждом вузе обрабатывается конфиденциальная информация и большую часть этой информации составляют персональные данные (далее – ПДн) сотрудников, профессорско-преподавательского состава, студентов.

В свою очередь, законодательство Российской Федерации накладывает определенные рамки на порядок использования персональных данных, в частности, обязывает распорядителя персональных данных выполнять мероприятия по защите персональных данных, переданных ему физическими лицами.

3.1 Основные нормативные правовые и методические документы в сфере защиты ПДн.

Постановление Правительства РФ от 1 ноября 2012 г. №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» является основным нормативным актом, определяющим требования по защите персональных данных. На основе требований данного постановления разрабатываются руководящие и методические документы ФСТЭК России и ФСБ России, касающиеся вопросов защиты персональных данных.

Приказ ФСТЭК России №21 от 18 февраля 2013 г. «Состав и содержание организационных и технических мер по защите персональных данных при их обработке в информационных системах персональных данных».

Документ определяет организационно-технические меры по обеспечению безопасности ПДн. Каждая из мер предусматривает реализацию ряда требований по защите ПДн. В приложении к Приказу приведены конкретные требования по защите ПДн в зависимости от уровня защищенности ПДн.

Одной из главных мер по защите ПДн является моделирование угроз безопасности ПДн. Для разработки модели угроз существует 2 методических документа ФСТЭК России:

Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. (Утверждена заместителем директора ФСТЭК России 15 февраля 2008 г.)

«Базовая модель …» содержит полный перечень угроз, возможных при автоматизированной обработке ПДн, вводит их классификацию, характеризует источники угроз и каналы их реализации, описывает уязвимости информационных систем, в которых обрабатываются ПДн. Руководствуясь «Базовой моделью …», можно определить перечень угроз, потенциально возможных в конкретной информационной системе.

Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных (Утверждена заместителем директора ФСТЭК России 14 февраля 2008 г.).

«Методика определения актуальных угроз…» позволяет определить, какие из возможных угроз безопасности ПДн являются актуальными и требуют проведения мероприятий по защите от них.

Постановление Правительства РФ от 1 ноября 2012 г. №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»

3.2 Порядок создания системы защиты ПДн.

Для обеспечения безопасности ПДн создаются системы защиты персональных данных (СЗПДн), которые включают в себя:

– организационные и технические меры;

– средства защиты информации (в том числе шифровальные криптографические), средства предотвращения несанкционированного доступа, утечки информации по техническим каналам, программно-технических воздействий на технические средства обработки персональных данных;

– используемые в информационной системе информационные технологии.

В действующих руководящих документах нет прямых указаний или рекомендаций по порядку (последовательности) разработки и внедрения СЗПДн. Однако, как показывает сложившаяся практика, при создании СЗПДн целесообразно придерживаться традиционного порядка разработки систем защиты информации ограниченного доступа. Процесс создания СЗПДн должен включать в себя три основных этапа, которые при необходимости могут быть разбиты на ряд подэтапов.

а) Предпроектное обследование ИСПДн.

Основными целями этого этапа является оценка текущего уровня защиты ИСПДн, соответствие требованиям нормативных документов, сбор сведений, необходимых для построения системы защиты ПДн, определение объема и стоимости работ по ее внедрению, принятие технических решений по защите ПДн.

В ходе предпроектного обследования ИСПДн разрабатываются внутренние документы (локальные акты) по вопросам обработки и защиты персональных данных, содержание которых можно определить на данном этапе.

б) Проектирование и создание ИСПДн.

На этом этапе осуществляется проектирование СЗПДн, поставка сертифицированных средств защиты информации, их установка, размещение и пуско-наладочные работы в соответствии с техническим заданием.

в) Испытания СЗПДн и ввод в эксплуатацию.

Основной целью данного этапа является контроль соответствия созданной СЗПДн предъявленным требованиям и разработка документов, необходимых для ввода системы в эксплуатацию. Испытания могут проводиться как своими силами, так и с привлечением сторонних организаций. Форма и порядок испытаний определяется оператором ПДн.

Таким образом, порядок создания системы защиты ПДн в целом аналогичен порядку создания любой другой системы защиты информации с ограниченным доступом, однако имеет ряд особенностей, вытекающих из требований законодательства в области обработки и защиты персональных данных.

Приказ ФСТЭК России №21 от 18 февраля 2013 г. «Состав и содержание организационных и технических мер по защите персональных данных при их обработке в информационных системах персональных данных».

3.3 Документы, необходимые для аттестации информационной системы персональных данных.

№ п/п	НЕОБХОДИМЫЕ ДОКУМЕНТЫ	ОСНОВАНИЕ*
1.	Перечень угроз безопасности персональных данных при их обработке в информационных системах персональных данных.	п. 2 ст. 19 152-ФЗ
2.	Матрица доступа к персональным данным, обрабатываемым в информационной системе персональных данных.	п. 2 ст. 19 152-ФЗ
3.	Акт классификации уровней защищенности персональных данных при их обработке в информационных системах персональных данных в зависимости от угроз безопасности этих данных.	п. 3 ст. 19 152-ФЗ
4.	Протоколы оценки эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных.	п. 2 ст. 19 152-ФЗ
5.	Журнал учета машинных носителей информации, на которых хранятся и (или) обрабатываются персональные данные.	п. 8 Приказ №21
6.	Инструкция по антивирусной защите	п. 8 Приказ №21
7.	Инструкция администратора системы	п. 8 Приказ №21
8.	Приказ о назначении ответственного за обеспечение безопасности персональных данных в информационной системе	п. 8 Приказ №21 п.13 «Требований ...»
9.	Инструкция пользователя системы	п. 8 Приказ №21
10.	Сертификат на применяемое средство защиты	п. 12 Приказ №21 п.1 «Положения ...» п.13 «Требования...»
11.	Перечень лиц, которым разрешен доступ к помещению, где обрабатываются ПДн и самим персональным данным	п.13 «Требований ...»
12.	Решение о создании структурного подразделения, ответственного за обеспечение безопасности персональных данных в информационной системе, либо возложение на одно из структурных подразделений функций по обеспечению такой безопасности	п.16 «Требования...»
13.	Протокол о выполнении требований Постановления Правительства Российской Федерации от 01.11.2012 №1119	п.17 «Требования...»
14.	Аттестат соответствия (оценка соответствия) объекта информатизации требованиям по безопасности информации	п.4 Приказ №21

*152 ФЗ – Федеральный закон от 27 июля 2006 г. №152-ФЗ «О персональных данных»;

Приказ №21 – Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

«Требования …» - «Требования к защите персональных данных при их обработке в информационных системах персональных данных», утвержденные Постановлением Правительства РФ от 1 ноября 2012 г. №1119;

«Положение …» - «Положение о сертификации средств защиты информации», утвержденное Постановлением Правительства РФ от 26 июня 1995 г. №608.

3.4 Административная ответственность за нарушение требований по защите информации при ее обработке в информационных системах.

Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 №195-ФЗ

Статья 13.12. Нарушение правил защиты информации

Статья 13.12. (ч.3) Нарушение лицензионных условий на проведение работ, связанных с использованием и защитой информации, составляющей государственную тайну.

Штраф: на должностных лиц от 2 000 до 3 000 руб.;

на юридических лиц от 20 000 до 25 000 руб.

Статья 13.12. (ч.4) Использование несертифицированных средств, предназначенных для защиты информации, составляющей государственную тайну.

Штраф: на должностных лиц от 3 000 до 4 000 руб.;

на юридических лиц от 20 000 до 30 000 руб. с конфискацией несертифицированных средств.

Статья 13.12. (ч.7) Нарушение требований о защите информации, составляющей государственную тайну, установленных федеральными законами и иными нормативными правовыми актами Российской Федерации (если такие действия\бездействия не содержат уголовно наказуемого деяния).

Штраф: на граждан от 1 000 до 2 000 руб.;

на должностных лиц от 3 000 до 4 000 руб.;

на юридических лиц от 15 000 до 20 000 руб.

Статья 13.13. Незаконная деятельность в области защиты информации

Статья 13.13. (ч.2) Незаконная деятельность в области защиты информации, составляющей государственную тайну.

Штраф: на должностных лиц от 4 000 до 5 000 руб.;

на юридических лиц от 30 000 до 40 000 руб. с конфискацией созданных средств защиты государственной тайны.

Статья 13.14. Разглашение информации, доступ к которой ограничен федеральным законом (за исключением случаев, если разглашение такой информации влечет уголовную ответственность)**, лицом, получившим доступ к такой информации в связи с исполнением служебных или профессиональных обязанностей.**

Штраф: на граждан от 500 до 1 000 руб.;

на должностных лиц от 4 000 до 5 000 руб.

ОПЫТ СОЗДАНИЯ, ИСПОЛЬЗОВАНИЯ В ОБРАЗОВАТЕЛЬНОМ ПРОЦЕССЕ И ПЕРСПЕКТИВЫ РАЗВИТИЯ НАУЧНО-УЧЕБНОГО ЦУКС МГТУ ИМ. Н. Э. БАУМАНА В РАМКАХ КОНЦЕПЦИИ РАЗВИТИЯ НАЦИОНАЛЬНОГО ЦУКС МЧС РОССИИ

Копытов Дмитрий Олегович,

Старший преподаватель кафедры «Экология и промышленная безопасность» МГТУ им. Н.Э. Баумана

Девисилов Владимир Аркадьевич,

Первый заместитель заведующего кафедрой «Экология и промышленная безопасность» МГТУ им. Н.Э. Баумана

Учитывая особую ответственность и техническую сложность задач по защите населения, территорий и предупреждению ЧС, один из старейших и уважаемых технических вузов страны – МГТУ им. Н.Э. Баумана уделяет большое внимание профессиональному обучению высококвалифицированных специалистов по направлению «Техносферная безопасность» – бакалавров профиля подготовки «Защита в ЧС» и магистров – «Управление рисками», способных решать технически сложные задачи в условиях динамично меняющейся обстановки и развития современных информационных технологий.

Подготовка этих специалистов ведется на кафедре «Экология и промышленная безопасность» (Э9): бакалавров – с 1 сентября 2014 года, магистров – с 1 сентября 2015 года.

Профессиональное обучение делится на теоретическое (осуществляется на кафедре) и практическое (в виде практики в органах управления МЧС России и Минобрнауки России).

Общими функциями управления образовательным процессом являются планирование, организация, мотивация, контроль, координация, связанные между собой процессами принятия решений и коммуникацией.

При планировании обучения бакалавров и магистров на кафедре Э9 был выполнен следующий комплекс мероприятий.

1. Проанализированы подходы, применяемые при реализации профиля в ведущих вузах страны, приняты во внимание подходы, используемые в образовательном процессе МГТУ им. Н.Э. Баумана.

2. Определены пути реализации профиля подготовки на кафедре: для подготовки бакалавров разработаны рабочие программы шести дисциплин, для подготовки магистров – 12 дисциплин, изучение которых обеспечит выполнение требований основной образовательной программы высшего профессионального образования к выпускнику; обеспечена разработка ТЗ, сопровождение разработки и приемка специального программного обеспечения (СПО) и аппаратного обеспечения (АО) научно-учебного центра управления в кризисных ситуациях (НУ ЦУКС).

3. Создана секция «Управление рисками и защита в ЧС» в структуре кафедры Э9. В её составе работают действующие офицеры и офицеры запаса ВС РФ и МЧС, каждому из которых определены разрабатываемые дисциплины. Организовано взаимодействие с руководителями секции и кафедры с целью обеспечения подготовки высококвалифицированных специалистов по профилю «Защита в ЧС».

Организационный аспект включал разработку рабочих программ шести дисциплин.

Подготовка бакалавров «Защита в ЧС» обеспечивается дисциплинами: 1) Управленческие и правовые аспекты гражданской защиты; 2) Системы защиты населения; 3) Геоинформационные системы и моделирование; 4) Прогнозирование чрезвычайных ситуаций; 5) Организация и обеспечение гражданской защиты и обороны; 6) Инженерная защита в чрезвычайных ситуациях.

В ходе подготовки магистров преподаются следующие учебные дисциплины: 1) Теория анализа и управления рисками; 2) Динамический анализ рисков; 3) Применение ГИС-технологий для анализа рисков на опасных территориях и объектах; 4) Анализ рисков на опасных территориях и объектах с применением ГИС – курсовая работа; 5) Прикладные методы анализа рисков природных и техногенных ЧС; 6) Прикладные методы анализа рисков природных и техногенных ЧС – курсовая работа; 7) Анализ рисков при землетрясениях и воздействии космических тел; 8) Управление пожарными рисками производственных объектов, зданий и сооружений; 9) Анализ рисков при наводнениях и авариях на гидротехнических сооружениях; 10) Анализ рисков при аварийных разливах нефтепродуктов на суше и в акваториях; 11) Государственная политика в области управления рисками; 12) Экономические методы управления рисками ЧС.

Для современных студентов, живущих в постиндустриальную, информационную эпоху, оптимальной формой обучения является использование современных и перспективных образовательных технологий, основанных на компьютерном моделировании, использовании ГИС, элементов виртуальной реальности, позволяющих эффективно и в короткие сроки формировать необходимые индивидуальные и групповые умения и навыки по практическому использованию программ поведения человека в условиях ЧС.

Для поддержки подготовки по профилю «Защита в ЧС» был разработан программно-аппаратный комплекс НУ ЦУКС. Его торжественное открытие состоялось 24 сентября 2014 года. В ходе мероприятия было подписано соглашение о сотрудничестве между МЧС России и МГТУ имени Баумана.

Специальное программное обеспечение НУ ЦУКС было разработано в результате совместной работы ученых и специалистов кафедры Э9, Центра исследований экстремальных ситуаций (ЦИЭКС) и Научно-исследовательского центра «Стратегические технологии анализа рисков» (НИЦ СТАРК) – отечественных лидеров по оценке последствий и рисков техногенных аварий и природных процессов.

НУ ЦУКС позволяет:

1) проводить профессиональную подготовку и повышение квалификации специалистов, отвечающих за БЖД, ГО, прогнозирование ЧС, обучать бакалавров и магистров, проводить научные исследования;

2) проводить все виды учебных занятий с трансляцией видео и аудио, видеоконференции и информационные обмены с Национальным ЦУКС МЧС России;

3) отрабатывать функциональные обязанности председателя, членов комиссии по предупреждению, ликвидации ЧС и обеспечению пожарной безопасности, должностных лиц оперативного штаба по ликвидации ЧС и оперативной дежурной смены ЦУКС в ходе КШУ и КШВИ различных уровней.

Аппаратная часть НУ ЦУКС включает подсистемы отображения информации; озвучивания; аудио- и видеоконференцсвязи; коммутации; управления; автоматизированные рабочие места (АРМ).

В состав специального программного обеспечения НУ ЦУКС входят: 1) управляющая система; 2) программное обеспечение АРМ должностных лиц НУ ЦУКС; 3) программный комплекс оценки комплексного риска в городе на основе ГИС; 4) 3D-модель виртуального города для визуализации последствий ЧС; 5) программный комплекс для подготовки специалистов по применению сил и средств при ликвидации последствий ЧС.

1) Управляющая система предназначена для поддержки учебного процесса, ведения отчетной документации и данных об обучаемых, включает подсистемы авторизации, управления пользователями, учебными материалами, обучением, 2D и 3D визуализацией результатов расчетов.

2) Программное обеспечение АРМ (ПО АРМ) объединяет программно-аппаратные средства подсистемы оперативного управления и поддержки принятия решений и позволяет фиксировать и регистрировать информацию о ЧС с привязкой всей информации; получать сформированные в автоматическом режиме регламенты действий указанных должностных лиц по функционированию в режиме ЧС, вести контроль их исполнения; осуществлять планирование сил и средств для ликвидации ЧС и др.

3) ПК оценки комплексного риска в городе на основе ГИС предназначен для сбора, хранения, анализа, визуализации пространственных данных и связанной информации об объектах ГИС, выполнения специальных задач моделирования, результатами которых являются пространственные данные, сохраняемые в БД и отображаемые на электронной карте.

С помощью комплекса на векторной и растровой картографической основе с использованием нормативной базы в области оценки рисков ЧС решаются различные прикладные задачи: прогнозирование масштабов и последствий ЧС; определение различных видов риска и др.

4) МВГ для визуализации последствий ЧС предназначена для 3D-моделирования различных ЧС на объектах городской и транспортной инфраструктуры, их имитации с аудиовизуальным отображением последствий.

5) ПК для подготовки специалистов по применению сил и средств при ликвидации последствий ЧС предназначен для повышения эффективности с помощью инновационных образовательных технологий, позволяющих моделировать деятельность подразделений РСЧС при ликвидации последствий ЧС в условиях изменяющейся обстановки.

Обучаемый в реальном режиме времени имеет возможность получать справочную информацию об объекте, влиять на текущую ситуацию управлением силами и средствами ликвидации ЧС на территории объекта.

Обстановка на месте ЧС максимально детализирована, развитие сценариев сопровождается эффектами, предусмотрена возможность вывода параметров, характеризующих действия обучаемых.

СПО НУ ЦУКС находит широкое применение в ходе проведения занятий по дисциплинам «Прогнозирование чрезвычайных ситуаций», «Инженерная защита в чрезвычайных ситуациях», «Системы защиты населения». Его использование позволяет интенсифицировать процесс обучения, делает его более эффективным и наглядным.

Студенты, получив практику работы с программным обеспечением НУ ЦУКС в ходе обучения в Университете, смогут быстрее адаптироваться в будущей профессиональной деятельности в области обеспечения защиты населения и территорий в условиях возникновения ЧС.

НУ ЦУКС позволит эффективно готовить специалистов, проводить научные исследования, командно-штабные учения и тренировки в об-

ласти защиты от ЧС, может стать важным элементом в предполагаемой к развертыванию Минобрнауки России пилотной сети ЦУКС для отработки вопросов обеспечения комплексной безопасности на объектах образования и науки.

Результатом работы секции «Управление рисками и защита в ЧС» по повышению **мотивации** студентов стала разработка рабочих программ и планирующей документации с учетом интересов обучающихся. Содержание рабочего учебного плана разработано с точки зрения подбора разнообразных видов самостоятельной работы (индивидуально и в группе), совершенствования дидактического материала, разнообразных средств обучения, повышающих эффективность обучения.

Контроль качества отрабатываемых материалов, своевременности их представления и соответствия принятым в университете стандартам проводился руководством секции непрерывно в ходе разработки учебной документации и материалов учебно-методических комплексов дисциплин. Наряду с общепринятыми формами контроля – очными заслушиваниями, совещаниями, заседаниями секции, методическими советами кафедры, широко использовалась электронная почта, сервисы Google, видеоконференции Skype, электронный университет МГТУ им. Н.Э. Баумана, контактная форма сайта секции, система управления проектами MS Project 2013.

Для контроля учебной деятельности студентов, планирования и управления учебным процессом, ведения отчетной документации и данных об обучаемых используется управляющая система, входящая в состав СПО НУ ЦУКС.

Координация работы членов секции при разработке ими планирующих и учебно-методических материалов, взаимодействия их со студентами обеспечивается с помощью очных и дистанционных форм общения: совещаний, собраний, мобильной и стационарной телефонной связи, видеоконференций, электронной почты, сервисов Google и MS SharePoint.

Использование традиционных и современных информационно-коммуникационных методов управления обеспечит, на взгляд авторов, максимально полное взаимодействие между участниками образовательного процесса – преподавателями и студентами, сделает возможным маневр ресурсами, создаст единство и согласованность всех стадий процесса управления профессиональным обучением по направлению «Техносферная безопасность», профилям подготовки «Защита в ЧС» и «Управление рисками» на кафедре «Экология и промышленная безопасность» МГТУ им. Н.Э. Баумана.

Перспективы развития НУ ЦУКС полностью соответствуют Концепции развития Национального ЦУКС МЧС России, разработанной специалистами МГТУ им. Н.Э. Баумана с привлечением потенциала ведущих отечественных научных организаций. Согласно концепции, целью развития Национального центра управления в кризисных ситуациях является повышение эффективности его деятельности как органа управления РСЧС, направленной на снижение показателей риска для населения и территорий Российской Федерации, сокращение времени реагирования, повышение эффективности оказания помощи населению, пострадавшему в ЧС.

В соответствии с Концепцией, основными принципами развития Национального ЦУКС являются: переход от оперативного реагирования к управлению рисками; комплексный, системный подход к управлению рисками; научность; децентрализация; обратная связь; эффективность; мотивация; импортозамещение; поэтапное развитие.

СОСТОЯНИЕ И РАЗВИТИЕ СИСТЕМЫ УПРАВЛЕНИЯ ПО ВОПРОСАМ КОМПЛЕКСНОЙ БЕЗОПАСНОСТИ В СФЕРЕ ДЕЯТЕЛЬНОСТИ ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ

Мызин Станислав Константинович,

Начальник отдела ГО ЧС Санкт-Петербургский политехнический университет Петра Великого

Современный этап мирового развития характеризуется нарастанием опасностей, угроз и рисков человечеству.

Одним из фундаментальных факторов обеспечения национальной безопасности и устойчивого развития России в реальных условиях современного мира является защита населения, материальных и культурных ценностей при ведении войн и военных конфликтов и т.д.

Для обеспечения их практической реализации созданы система гражданской обороны и единая государственная система предупреждения и ликвидации чрезвычайных ситуаций (РСЧС).

Правовую и методологическую основу вопросов комплексной безопасности составляют Федеральный закон от 12 февраля 1998 г. №28-ФЗ «О гражданской обороне» (в ред. Федеральных законов от 09.10.2002 №123-ФЗ, от 19.06.2004 №51-ФЗ, от 22.08.2004 №122-ФЗ, от 19.06.2007 №103-ФЗ, от 25.11.2009 №267-ФЗ, от 27.07.2010 №223-ФЗ, от 23.12.2010 №377-ФЗ, от 02.07.2013 №158-ФЗ), Федеральный закон от 01 декабря 1994 г. №68-ФЗ «О защите населения и территорий от чрезвычайных ситуаций природного и техногенного характера» (в ред. Федеральных законов от 28.10.2002 №129-ФЗ, от 22.08.2004 №122-ФЗ, от 04.12.2006 №206-ФЗ, от 18.12.2006 №232-ФЗ, от 30.10.2007 №241-ФЗ, от 30.12.2008 №309-ФЗ, от 07.05.2009 №84-ФЗ, от 25.11.2009 №267-ФЗ, от 19.05.2010 №91-ФЗ, от 27.07.2010 №223-ФЗ, от 28.12.2010 №412-ФЗ, от 29.12.2010 №442-ФЗ, от 01.04.2012 №23-ФЗ, от 11.02.2013 №9-ФЗ, от 02.07.2013 №158-ФЗ, от 02.07.2013 №185-ФЗ), Постановление Правительства Российской Федерации от 10 июля 1999 г. №782 «О создании (назначении) в организациях структурных подразделений (работников), уполномоченных на решение задач в области гражданской обороны» (в ред. Постановлений Правительства РФ от 02.12.2004 №724, от 01.02.2005 №49, от 30.05.2013 №457), Приказ Министерства Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий от 31 июля 2006 г. №440 «Об утверждении положения об уполномоченных на решение задач в области гражданской обороны структурных подразделениях (работниках) организаций», Приказ Министерства Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий от 11 сентября 2013 г. № 600 «О внесении изменений в приказ МЧС России от 31 июля 2006 г. № 440».

1. Организация и управление гражданской обороной и при чрезвычайных ситуациях ФГАОУ ВО «СПбПУ»

Руководство гражданской обороной и при ЧС в организациях осуществляют их руководители. Руководители организаций несут персональную ответственность за организацию и проведение мероприятий по ГО и защите населения (статья 11 ФЗ от 12.02.1998 г. №28-ФЗ)

Органами, осуществляющими управление ГО и ведающими вопросами комплексной безопасности в организации, являются структурные подразделения, уполномоченные на решение задач в области ГО. В СПбПУ создан Департамент гражданской защиты.

Руководители структурных подразделений (работники) по ГО подчиняются непосредственно руководителю организации.

2. Общие сведения об университете

В состав ФГАОУ ВО «СПбПУ» входит комплекс зданий и сооружений различного функционального назначения, расположенных на территории Калининского и Выборгского районов Санкт-Петербурга, из них

учебные корпуса и здания учебно-лабораторного назначения – 43;

– жилые здания и помещения – 82;

– объекты вспомогательного назначения – 79.

Общая площадь объектов – 435,4 тыс. м2 .

Численность студентов дневного

обучения – 14800.

Профессорско-преподавательский состав

и администрация – 7530.

Институтов – 12.

Кафедр – 113.

3. Выполнение требований комплексной безопасности в соответствии с федеральными законами, постановлениями Правительства РФ и нормативными актами

Система оповещения.

Учитывая события, происшедшие в Крымске и Новомихайловке в 2012 году и то особое внимание, которое уделяется Президентом и Правительством России вопросам безопасности, в СпбПУ создана и реализуется система комплексной безопасности университета. Большое внимание уделяется развитию системы оповещения.

В настоящее время все общежития и учебные корпуса оснащены средствами доступной информации о ЧС, включающей дублированную световую, звуковую и визуальную сигнализацию. Сигнал выводится на мониторы вахт и дежурно-диспетчерскую службу.

Надежно работает общероссийская комплексная система информирования и оповещения населения («ОКСИОН»). Проводится работа по внедрению автоматической пожарной сигнализации с выводом радиосигналов на пункты пожарных частей.

Эвакуация и спасение

Здания общежитий оснащены различными средствами эвакуации людей:

– «Каскад-5» («Куб жизни»);

– устройство спусковое – рукав СУ21.7.00РЭ;

– канатно-спасательное снаряжение («слип-эвакуатор»);

– устройство канатно-спусковое пожарное автоматическое Е-16;

– надувной трап («Тобогган») и др.

Эвакуация проводится в соответствии с планами эвакуации каждого здания. Оборудована «безопасная зона» в общежитиях повышенной этажности.

УПДК «Политехник»

В ноябре 2011 года создана учебная добровольная пожарная команда (УПДК), которая принимает участие в ликвидации различных возгораний на территории учреждения, учениях (проводимых раз в квартал), а также в профилактических мероприятиях. УПДК оснащена автомобилем первой помощи на базе модели

«ГАЗЕЛЬ» с современной экипировкой и другой аварийно-спасательной техникой.

Управление в случае ЧС

Управление в случае ЧС и ее ликвидации осуществляется с запасного пункта управления с защитой 0,15 кг/м2.

Пункт управления оборудован:

– мультимедийным оборудованием,

– АТС («Сименс»), - радиостанцией («Гранит»),

– факсимильной связью,

– резервным питанием,

– запасом питьевой воды,

– фильтровентиляционными устройствами и др.

Оперативная емкость ЗПУ – 20 человек.

Создан центр управления в кризисных ситуациях в удаленном структурном подразделении Университета (учебно-оздоровительная база «Политехник» по адресу пос. Новомихайловский, Туапсинский р-н, Краснодарский край). Создан полигон для мониторинга ситуаций образовательных учреждений Северо-Западного региона и обучения руководящего состава и специалистов образовательных учреждений Северо-Запада.

Проблемы:

Вместе с тем анализ показывает, что несмотря на принимаемые меры по обеспечению комплексной безопасности университета, еще остаются проблемы, требующие незамедлительного решения. В их числе:

– оснащение объекта современными средствами оповещения, защиты и эвакуации;

– приобретение индивидуальных спасательных средств, особенно для зданий повышенной этажности;

– приобретение для обучающихся и проживающих в общежитиях индивидуальных средств защиты органов дыхания;

– финансирование мероприятий по вопросам комплексной безопасности.

Вместе с тем анализ показывает, что несмотря на принимаемые меры по обеспечению комплексной безопасности университета, еще остаются проблемы, требующие незамедлительного решения.

ОРГАНИЗАЦИЯ СИСТЕМЫ ПОЖАРНОЙ БЕЗОПАСНОСТИ В ОБРАЗОВАТЕЛЬНОМ УЧРЕЖДЕНИИ

Савошинский Олег Петрович,

Директор Департамента пожарной безопасности Санкт-Петербургский политехнический университет Петра Великого

В университете Департамент пожарной безопасности (ДПБ) и Учебно-пожарная добровольная команда «Политехник» (УПДК «Политехник») были созданы 14 ноября 2011 года приказом ректора от 16.11.2011 № 842 «Об изменении структуры ФГБОУ ВПО «СПбГПУ».

Департаментом пожарной безопасности выполняется следующие работы:

– постоянный мониторинг территории и объектов Университета в области обеспечения пожарной безопасности по системе предупреждения, выявления и пресечения нарушений, установленных законодательством Российской Федерации о пожарной безопасности;

– поддержание и сохранение стабильности стратегического паритета в обеспечении пожарной безопасности университета. Всегда готовы к оперативному немедленному решению поставленных задач;

– формирование плана оснащения зданий Университета системами пожарной защиты;

– постоянный контроль соблюдения требований пожарной безопасности при проведении ремонтно-восстановительных работ, временных огневых и других пожароопасных работ.

– проведение профилактических работ, работ разъяснительного характера, а также практические занятия с представителями структурных подразделений, оказание помощи в оформлении документов в области пожарной безопасности.

– проводится активное и постоянное формирование, обучение и специальная подготовка добровольцев УПДК «Политехник»;

– освещаются вопросы обеспечения пожарной безопасности и пропаганды добровольческих пожарных формирований в печатных и электронных изданиях;

– проводится обучение сотрудников университета по программам пожарно-технического минимума;

– проводится работа по обеспечению объектов университета первичными средствами пожаротушения;

– осуществляются работы по лицензионным видам деятельности в области пожарной безопасности: монтаж, техническое обслуживание и ремонт систем пожарной и охранно-пожарной сигнализации и их элементов, включая диспетчеризацию и проведение пусконаладочных работ.

Функции УПДК «Политехник»:

– защита личности, имущества и зданий от пожаров (первоочередные боевые действия по тушению пожаров до прибытия подразделений

пожарной охраны МЧС России);

– мониторинг установленного противопожарного режима на территории Университета.

За весь период существования УПДК «Политехник» на базе пожарного депо прошли учебу 112 студентов Института военно-технического образования и безопасности (бывшего Факультета комплексной безопасности).

За 3,5 года было проведено более 20 учений и тренировок, как по пожарной, так и по комплексной безопасности с привлечением сил и средств Главного управления МЧС России по г. Санкт-Петербургу, ФГКУ «1 отряд ФПС по Санкт-Петербургу», ФГКУ «4 отряд ФПС по Санкт-Петербургу», Отделов надзорной деятельности Калининского и Выборгского районов УНД ГУ МЧС России по Санкт-Петербургу, Территориального отдела по Калининскому району Управления гражданской защиты ГУ МЧС России по г Санкт-Петербургу, Санкт-Петербургского государственного казенного учреждения «Пожарно-спасательный отряд противопожарной службы Санкт-Петербурга по Выборгскому району Санкт-Петербурга», Федерального государственного казенного учреждения «Северо-Западный региональный поисково-спасательный отряд МЧС России», СОБР ГУ МВД России по Санкт-Петербургу и Ленинградской области, Управления МВД России по Выборгскому району г. Санкт-Петербурга, Управления ГИБДД ГУ МВД России по г. Санкт-Петербургу и Ленинградской области.

В ходе проведения учений и тренировок отрабатывались навыки использования первичных средств пожаротушения, современных способов борьбы с возгораниями, эвакуации людей, проведения аварийно-спасательных работ.

В соответствие планом учебных мероприятий ДПБ проводит активную работу по комплектации караулов студентами I-II курсов и подготовку добровольцев УПДК «Политехник» в области пожаротушения на объектах образования и применения современных средств эвакуации и спасения людей при пожаре. К студентам-кандидатам в добровольцы, предъявляются строгие требования. На сегодняшний день в УПДК «Политехник» добровольцами числятся 30 студентов, зарегистрированных в реестре ГУ МЧС России по г. Санкт-Петербургу.

За период функционирования УПДК «Политехник» добровольцами без привлечения сотрудников государственной пожарной службы было потушено 28 загораний, спасено 4 человека.

База Департамента пожарной безопасности и УПДК «Политехник» среди ВУЗов города занимает лидирующие позиции.

Основным направлением деятельности Департамента была и остается работа, направленная на обеспечение противопожарной устойчивости объектов ВУЗа и безопасность учащихся, работников и имущества университета.

Как показывает практика, существование Департамента пожарной безопасности и учебно-пожарной добровольной команды – это важная необходимость, как в профилактике, так и в тушении загораний. Поэтому это направление необходимо и далее развивать на более профессиональном уровне.

№2

29 ОКТЯБРЯ 2015 Г.

МОДЕРАТОР: ШАТИЛОВА АЛИНА АЛЕКСАНДРОВНА – ДИРЕКТОР ЮЖНОГО РЕГИОНАЛЬНОГО АТТЕСТАЦИОННОГО ЦЕНТРА МИНОБРНАУКИ РОССИИ

ПОРЯДОК ОГРАНИЧЕНИЯ ДОСТУПА К ИНФОРМАЦИИ В ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ ИНТЕРНЕТ, ЗАПРЕЩЕННОЙ К РАСПРОСТРАНЕНИЮ В РОССИЙСКОЙ ФЕДЕРАЦИИ

Худолей Сергей Николаевич,

руководитель Управления Роскомнадзора по Республике Крым и г.Севастополь

Управление Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по Республике Крым и городу Севастополь осуществляет государственный контроль и надзор за соблюдением законодательства Российской Федерации в сфере средств массовой информации на основании Положения об Управлении Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по Республике Крым и городу Севастополь, утвержденного приказом Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 02.04.2014 № 50.

Справочно:

В соответствии со ст. 8 Закона РФ от 27.12.1991 №2124-1 «О средствах массовой информации», сайт в информационно-телекоммуникационной сети Интернет, не зарегистрированный в качестве средств массовой информации, средством массовой информации не является.

Регистрация СМИ, распространяемых преимущественно на территории одного субъекта Федерации, производится территориальными управлениями Роскомнадзора.

Регистрация сетевых изданий осуществляется исключительно центральным аппаратом Роскомнадзора, в связи с тем, что не представляется возможным ограничить распространение информации в сети Интернет территорией одного субъекта Федерации.

Интернет-сайт, не зарегистрированный в качестве средства массовой информации, не попадает под действие Закона РФ от 27.12.1991 № 2124-1 «О средствах массовой информации».

Регистрация доменных имен для идентификации сайта в информационно-телекоммуникационной сети Интернет, а также ведение реестров доменных имен, не входит в компетенцию Роскомнадзора. Регистрация доменных имен производится аккредитованными регистраторами доменных имен.

В соответствии с требованиями статьи 15.1 Федерального закона от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации» с 1 ноября 2012 года создана и ведется единая автоматизированная информационная система «Единый реестр доменных имен, указателей страниц сайтов в сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено» (далее – Единый Реестр).

Постановлением Правительства Российской Федерации от 26 октября 2012 г. №1101 установлены Правила создания, формирования и ведения Единого Реестра (далее - Правила), согласно которым основаниями для включения в Единый реестр являются:

а) решения следующих уполномоченных федеральных органов исполнительной власти:

Федеральная служба Российской Федерации по контролю за оборотом наркотиков - в отношении распространяемой посредством сети «Интернет» информации о способах, методах разработки, изготовления и использования наркотических средств, психотропных веществ и их прекурсоров, местах приобретения таких средств, веществ и их прекурсоров, а также о способах и местах культивирования наркосодержащих растений;

Федеральная служба по надзору в сфере защиты прав потребителей и благополучия человека - в отношении распространяемой посредством сети «Интернет» информации о способах совершения самоубийства, а также призывов к совершению самоубийства;

Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций - в отношении:

- материалов с порнографическими изображениями несовершеннолетних и (или) объявлений о привлечении несовершеннолетних в качестве исполнителей для участия в зрелищных мероприятиях порнографического характера, распространяемых посредством сети «Интернет»;

- информации о способах, методах разработки, изготовления и использования наркотических средств, психотропных веществ и их прекурсоров, местах приобретения таких средств, веществ и их прекурсоров, о способах и местах культивирования наркосодержащих растений и о способах совершения самоубийства и призывов к совершению самоубийства, размещенной в продукции средств массовой информации, распространяемой посредством сети «Интернет»;

- информации, распространяемой посредством сети «Интернет», решение о запрете к распространению которой на территории Российской Федерации принято уполномоченными органами или судом;

б) вступившее в законную силу решение суда о признании информации, распространяемой посредством сети «Интернет», запрещенной информацией.

В соответствии с требованиями статьи 15.3 Федерального закона № 149-ФЗ доступ к сайтам ограничивается на основании требования Генерального прокурора или его заместителей.

Обращаем внимание, что в случае обнаружения в информационно-телекоммуникационных сетях, в том числе в сети Интернет, информации, содержащей призывы к массовым беспорядкам, осуществлению экстремистской деятельности, участию в массовых (публичных) мероприятиях, проводимых с нарушением установленного порядка, включая случай поступления уведомления о распространении такой информации от федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, органов местного самоуправления, организаций или граждан, Генеральный прокурор Российской Федерации или его заместители направляют требование

в федеральный орган исполнительной власти (Роскомнадзор), осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, о принятии мер по ограничению доступа к информационным ресурсам, распространяющим такую информацию.

Других оснований для включения в Единый Реестр законодательством Российской Федерации не предусмотрено.

Сообщить о конкретных ссылках на сайты в сети «Интернет», содержащие, по вашему мнению, информацию, подпадающую под основания для включения в Единый Реестр, можно, заполнив форму на сайте центрального аппарата Роскомнадзора http://eais.rkn.gov.ru/feedback/, а также на сайте Прокуратуры Республики Крым http://rkproc.ru/ в разделе «уведомления об экстремизме».

Государственная функция по проведению расследований, экспертиз, анализа, оценки и проверочных мероприятий в отношении экстремистских материалов, распространяемых на сайтах в сети Интернет, не зарегистрированных в качестве СМИ, на Роскомнадзор не возложена.

В рамках реализации статьи 15.1 Федерального закона № 149-ФЗ Роскомнадзор осуществляет ведение Единого реестра.

Полномочия по созданию, формированию и ведению Единого Реестра отнесены к компетенции центрального аппарата Роскомнадзора.

К основаниям ограничения доступа к интернет-ресурсам, определенным статьей 15.1 Федерального закона № 149-ФЗ, относится, в том числе, распространение информации, признанной судом запрещенной к распространению на территории Российской Федерации (или экстремистской, распространение которой запрещено российским законодательством).

В целях ограничения доступа к сайтам в сети «Интернет», содержащим экстремистские материалы, Роскомнадзором совместно с Министерством юстиции Российской Федерации в постоянном режиме ведется работа по направлению в Службу судебных решений, содержащихся в Федеральном списке экстремистских материалов.

В настоящее время в Роскомнадзоре сформирован и постоянно обновляется перечень судебных решений о признании информации, распространяемой посредством сети «Интернет», экстремистской.

Таким образом, в случае поступления в территориальный орган Роскомнадзора (далее – ТО) информации о выявлении правоохранительными органами, органами государственной безопасности или органами прокуратуры фактов размещения на сайтах в сети «Интернет», не зарегистрированных в качестве СМИ, экстремистских материалов, признанных таковыми решениями судов, указанные сведения с приложением соответствующего акта осмотра интернет-страницы, содержащего сведения о том, что на данном интернет-сайте размещены материалы из Федерального списка экстремистских материалов, произведенного вышеуказанными органами государственной власти, после проведения сотрудниками ТО проверки доступности противоправных материалов, следует направлять в центральный аппарат Роскомнадзора.

При этом Управление Роскомнадзора по Республике Крым и г. Севастополь осуществляет контроль и надзор за своевременным получением выгрузки из Единого Реестра операторами связи, предоставляющими доступ к сети Интернет на территории Республики Крым и г. Севастополь.

Согласно п. 5 ст. 46 Федерального закона от 07.07.2003 №126-ФЗ «О связи» оператор связи, оказывающий услуги по предоставлению доступа к информационно-телекоммуникационной сети «Интернет», обязан осуществлять ограничение и возобновление доступа к информации, распространяемой посредством информаци-

онно-телекоммуникационной сети «Интернет», в порядке, установленном Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

Согласно п. 13 Правил перечень доменных имен, указателей страниц сайтов в сети «Интернет», а также сетевых адресов, позволяющих идентифицировать сайты сети «Интернет», доступ к которым обязан ограничить оператор связи, оказывающий услуги по предоставлению доступа к сети «Интернет», обновляется ежедневно в 9 часов 00 минут и 21 час 00 минут по московскому времени.

В течении суток с момента такого обновления оператор связи обязан ограничить доступ к таким сайтам в сети «Интернет».

Доступ к выгрузке из Единого реестра предоставляется операторам связи в ручном и автоматическом режимах круглосуточно. Роскомнадзор обращает внимание, что доступ к выгрузке осуществляется исключительно с использованием квалифицированной электронной подписи, выданной любым удостоверяющим центром из числа аккредитованных Минкомсвязи России.

Для проведения мониторинга на доступность информационных ресурсов, включенных в Единый реестр, Управлению Роскомнадзора операторами связи в добровольном порядке предоставляется удаленный доступ к сети Интернет.

В случае выявления нерегулярного получения выгрузки из Единого реестра, частью 3 ст. 14.1 КоАП предусмотрена ответственность за нарушение лицензионных условий, согласно которой юридические лица могут быть оштрафованы на сумму от 30 до 40 тысяч рублей.

Справочно:

Основными поставщиками трафика в сеть Интернет на территории Республики Крыма и г. Севастополь являются ООО «Миранда Медиа», ООО «Крымком Юг», ООО «Крэлком».

Все действующие операторы получают файл-выгрузку из Единого реестра и осуществляют ограничение доступа к запрещенной информации.

По Республике Крым и г. Севастополь на 01.10.2015

– Всего выдано лицензий на оказание телематических услуг – 210;

– Осуществляют деятельность –

136 операторов;

– Предоставляют удаленный доступ к сети оператора для мониторинга – 41;

– Всего решений об ограничении доступа в реестре – 13568;

– Из них:

– Экстремизм – 6, 37%;

– Наркотические средства – 29,6%;

– Детская порнография – 26,76%;

– Прочее – 37,24%;

– Доля незаблокированных ресурсов в среднем составляет 1,6%.

ОСОБЕННОСТИ ПОРЯДКА РЕАЛИЗАЦИИ ФГОС ВО ПО НЕКОТОРЫМ СПЕЦИАЛЬНОСТЯМ И НАПРАВЛЕНИЯМ ПОДГОТОВКИ

Крушная Светлана Павловна,

заместитель начальника отдела защиты государственной тайны Минобрнауки России

Об особенностях порядка реализации федеральных государственных образовательных стандартов высшего образования (ФГОС ВО), требующих особого порядка реализации основных образовательных программ в соответствии с ФГОС ВО по отдельным специальностям (направлениям подготовки).

Разъяснения по критериям и порядку отнесения отдельных специальностей (направлений подготовки) к открытому или закрытому аналогу при реализации основных образовательных программ в соответствии с ФГОС ВО в образовательном учреждении.

Взаимодействие с Минобрнауки России, органами безопасности и подразделениями ФСТЭК России по вопросам подготовки специалистов по открытым и закрытым аналогам отдельных специальностей (направлений подготовки).

ПОДГОТОВКА КАДРОВ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ЮЖНОМ ФЕДЕРАЛЬНОМ УНИВЕРСИТЕТЕ

Горбунов Александр Валерьевич,

заместитель директора Института компьютерных технологий и информационной безопасности Южного федерального университета

Подготовка кадров в сфере информационной безопасности в Южном федеральном университете (ЮФУ) осуществляется в Институте компьютерных технологий и информационной безопасности (ИКТИБ), образованном в декабре 2013 года путём реорганизации факультета информационной безопасности, факультета автоматики и вычислительной техники и естественно-научного и гуманитарного факультета.

В состав ИКТИБ ЮФУ входит 12 кафедр, четыре из которых занимаются подготовкой в сфере информационной безопасности: кафедра безопасности информационных технологий (БИТ), кафедра информационной безопасности телекоммуникационных систем (ИБТКС), кафедра информационно-аналитических систем безопасности (ИАСБ) и кафедра психологии и безопасности жизнедеятельности (ПиБЖ). Также в состав ИКТИБ ЮФУ входят научные и научно-образовательные подразделения, одним из которых является Южно-Российский региональный учебно-научный центр по проблемам информационной безопасности в системе высшей школы (ЮР РУНЦ ИБ), ведущий активную подготовку по программам дополнительного профессионального образования в области защиты информации, а также выполняющий значительное количество научно-исследовательских работ.

В настоящее время в ИКТИБ ЮФУ ведётся подготовка по четырем специальностям, восьми направлениям подготовки бакалавров, шести направлениям магистратуры и трем направлениям аспирантуры (по 13 научным специальностям), среди которых к сфере информационной безопасности относятся:

– 10.03.01 (090900.62) «Информационная безопасность» – 83 обучающихся;

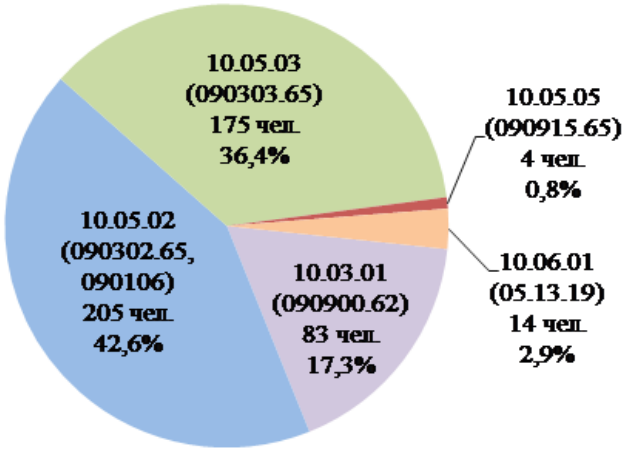
– 10.05.02 (090302.65, 090106) «Информационная безопасность телекоммуни-кационных систем» – 205 обучающихся;

– 10.05.03 (090303.65) «Информационная безопасность автоматизированных систем» – 175 обучающихся;

– 10.05.05 (090915.65) «Безопасность информационных технологий в правоохрани¬тельной сфере» – 4 обучающихся;

– 10.06.01 «Информационная безопасность» (научная специальность 05.13.19 «Методы и системы защиты информации, информационная безопасность») – 14 обучающихся.Общее количество обучающихся по укрупнённой группе направлений и специальностей (УГНС) «Информационная безопасность» в ИКТИБ ЮФУ составляет 481 человек (структура контингента в графическом виде показана на рис. 1).

Рис. 1. Структура контингента ИКТИБ ЮФУ, обучающегося по УГНС «Информационная безопасность» (на 01.10.2015)



За последние пять лет осуществлён выпуск 336 обучающихся по укрупнённой группе направлений и специальностей (УГНС) «Информационная безопасность» (рис. 2): 2011 год – 78, 2012 – 72, 2013 – 66, 2014 – 64, 2015 – 56, в 2016 году планируется выпуск 81 человека.

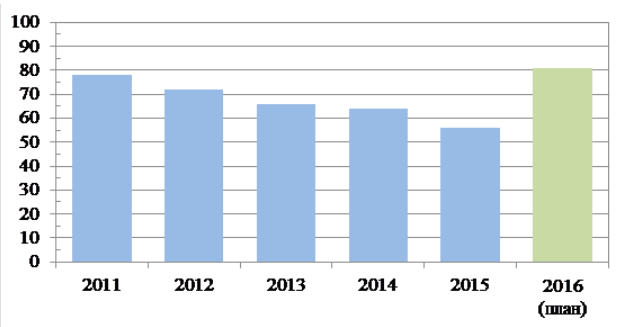


Рис. 2. Динамика выпуска обучающихся по УГНС «Информационная безопасность» в ИКТИБ ЮФУ.

По результатам приёмной кампании 2015 года по УГНС «Информационная безопасность» в ИКТИБ ЮФУ был принят 121 абитуриент, в том числе на направление подготовки бакалавров 10.03.01 – 26 человек, на специальности 10.05.02, 10.05.03 и 10.05.05 – 43, 46 и 1 человек соответственно, на направление аспирантуры 10.06.01 – 5 человек.

Необходимо отметить, что к особенностям приёмной кампании в ЮФУ следует отнести установление достаточно высоких минимальных баллов ЕГЭ по отдельным предметам – на уровне 50 или 60 баллов. Среди поступивших в ИКТИБ ЮФУ на направление подготовки бакалавров и специальности УГНС «Информационная безопасность» по результатам единого государственного экзамена (ЕГЭ) средний балл за 1 экзамен ЕГЭ составил 69,6.

География поступивших (по прописке) представлена 10 регионами Российской федерации (в том числе на Ростовскую область приходится 76 человек или 62,8% от общего числа поступивших в ИКТИБ ЮФУ по УГНС «Информационная безопасность», Краснодарский край – 17 человек или 14,0%, Ставропольский край – 11 человек или 9,1%, также представлены Республика Адыгея – четыре человека, Республика Калмыкия – три человека, Республика Северная Осетия – Алания – два человека, Астраханская область, Кабардино-Балкарская Республика, Карачаево-Черкесская Республика и Республика Крым – по одному человеку) и четырьмя зарубежными странами (Армения, Таджикистан, Колумбия и Палестина – по одному человеку).

С целью привлечения поступающих и повышения качества их подготовки ИКТИБ ЮФУ, помимо традиционных дней открытых дверей и участия в различных фестивалях абитуриентов, ежегодно организует работу курсов подготовки к ЕГЭ по информатике и математике, меж-региональные олимпиады для школьников по информатике и информационно-коммуникационным технологиям, информационной безопасности, математике и криптографии, программированию.

28-29 ноября 2015 года на базе ИКТИБ ЮФУ для школьников старших классов и обучающихся колледжей будет проводиться первая конференция «IT будущее» по следующим на-

правлениям: «Информационная безопасность», «Современные информационные технологии», «Разработка программного обеспечения» и «Робототехника». Участники конференции, отмеченные дипломами за лучшие доклады, получат возможность набрать до 10 баллов индивидуальных достижений, учитываемых при поступлении в ЮФУ.

Также следует отметить организацию в 2015 году профильного класса на базе лицея №4 г. Таганрога, в котором часть дисциплин школьной программы и несколько факультативов проводятся сотрудниками ИКТИБ ЮФУ на базе своих аудиторий и лабораторного фонда.

Выпускающие кафедры ИКТИБ ЮФУ, работающие в сфере информационной безопасности, имеют в своём составе более 20 специализированных лабораторий, в том числе 3 сетевые академии Cisco, лаборатории программно-аппаратных средств защиты информации, технических средств охраны и технических средств защиты информации, защищённых оптических систем связи, безопасности интеллектуальных информационно-телекоммуникационных систем, радиоэлектронных технологий информационной безопасности, безопасности банковских информационных систем, информационно-аналитических систем финансового мониторинга, моделирования перспективных средств защиты информации, научно-исследовательскую лабораторию квантовой криптографии, центр психологической безопасности личности.

Лаборатории оснащены современным оборудованием, в составе которого можно выделить различное сетевое оборудование Cisco, системы мониторинга, анализа и ответной реакции, межсетевые экраны, системы обнаружения и предотвращения атак, аппаратные брандмауэры и сканеры защищённости, генераторы радиошума, зонды для обнаружения микропередач и обследования линий связи, нелинейные локаторы, комплекты для оценки каналов утечки информации, системы виброакустического зашумления, технологические средства подавления звукозаписывающей аппаратуры и др.

Одним из направлений исследований кафедры информационной безопасности телекоммуникационных систем является построение защищённых оптических систем связи. В составе оборудования лабораторий кафедры имеются устройства ввода/вывода части излучения из волоконно-оптических линий связи без нарушения их целостности, промышленные образцы оптических систем передачи различного назначения, волоконно-оптические пассивные элементы, оптическое контрольно-измерительное и технологическое оборудование.

Помимо основных образовательных программ высшего образования в ИКТИБ ЮФУ ведётся подготовка кадров в сфере информационной безопасности по программам дополнительного профессионального образования. На настоящий момент открыты и реализуются 1 программа профессиональной переподготовки и 6 программ повышения квалификации:

– Организация и технология защиты информации (530 часов);

– Информационная безопасность телекоммуникационных систем (102 часа);

– Организация и технология защиты информации в образовательных учреждениях (72 часа);

– Комплексная защита объектов информатизации в образовательных учреждениях (72 часа);

– Методы и аппаратура радиомониторинга современных систем телекоммуникации и защищенной радиосвязи (72 часа);

– Информационно-телекоммуникационное противодействие угрозам безопасности банковских информационных систем (72 часа);

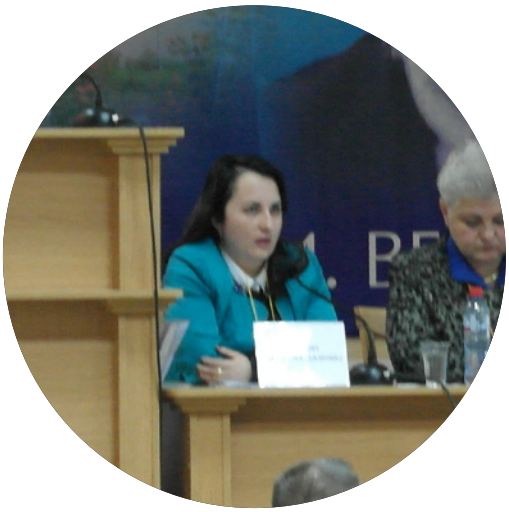
– Нормативно-правовое и научно-методическое обеспечение учебного процесса в контексте практического опыта реализации ФГОС нового поколения и образовательных программ в обла-

сти информационной безопасности (48 часов). Количество выпускников программ дополнительного профессионального образования за последние 5 лет составило 487 человек, из них 89 – по программе профессиональной переподготовки.

ОСОБЕННОСТИ ОРГАНИЗАЦИИ РАБОТЫ ПО ПРОФИЛАКТИКЕ РАСПРОСТРАНЕНИЯ ИДЕОЛОГИИ ТЕРРОРИЗМА В ОБРАЗОВАТЕЛЬНОМ ПРОСТРАНСТВЕ. НЕОБХОДИМЫЕ КОМПЕТЕНЦИИ

Иванова Олеся Александровна,

Департамент государственной службы, кадров и управления делами Минобрнауки России



Напряженная геополитическая ситуация, а также сохранение экстремистских и террористических угроз являются серьезным вызовом национальной безопасности, источником рисков дестабилизации социально-политической обстановки в Российской Федерации в целом и в каждом отдельном регионе. Проявления межэтнических, межнациональных и межконфессиональных противоречий, распространение идеологии экстремизма и терроризма требуют повышенного внимания со стороны органов исполнительной власти всех уровней и гражданского общества, консолидации усилий по реализации государственной политики в этом направлении. Для противодействия деструктивным тенденциям, связанным с распространением идеологии экстремизма и терроризма, снижения уровня радикализации, прежде всего молодежи, и недопущения вовлечения ее в экстремистскую деятельность разработан и реализуется Комплексный план противодействия идеологии терроризма в Российской Федерации на 2013-2018 годы, утвержденный Президентом РФ 26 апреля 2013 года № Пр-1069 (далее – Комплексный план). Успех проведения мероприятий Комплексного плана зависит от того, как организована деятельность всех уровней исполнительной власти в сфере профилактики и противодействия идеологии экстремизма и терроризма. Такая деятельность требует от государственных и муниципальных служащих профессиональных компетенций, комплексных знаний, умений и навыков для работы в этой сфере.

Департаментом государственной службы, кадров и управления делами в период с 09 июня по 26 июня 2015 года был организован сбор информации в рамках «Мониторинга организации и состояния деятельности по реализации Комплексного плана органами исполнительной власти субъектов Российской Федерации, осуществляющими управление в сфере образования».

По полученным материалам была проведена предварительная оценка уровня нормативно-правовой обеспеченности реализации программ и планов, организации непосредственной работы по противодействию идеологии терроризма и экстремизма органами исполнительной власти в сфере образования в субъектах Российской Федерации.

Анализ имеющихся материалов, отражающих практику деятельности по противодействию идеологии терроризма, позволяет выявить некоторые недостатки, а именно:

– в планировании мероприятий органами исполнительной власти субъектов Российской Федерации, осуществляющими управление в сфере образования на основании Комплексного плана;

– в работе с информацией, предоставляемой подведомственными организациями и учреждениями субъектов Российской Федерации, осуществляющими управление в сфере образования: сбор, обобщение, анализ;

– в организации взаимодействия с другими территориальными органами федеральных министерств и ведомств, входящих в систему органов исполнительной власти субъекта Российской Федерации, в рамках исполнения мероприятий Комплексного плана;

– ведении учета и анализа мероприятий с участием представителей общественных и религиозных организаций по противодействию идеологии экстремизма и терроризма;

– в системном сопровождении (организация методических центров, учебно-методических объединений) реализации планов, программ по противодействию идеологии терроризма, профилактике проявлений экстремизма на региональном и муниципальном уровнях.

Для устранения указанных выше недостатков государственные и муниципальные служащие должны владеть необходимыми компетенциями для организации работы по противодействию идеологии экстремизма и терроризма.

В результате проведенного в 2015 году мониторинга выявлены существенные пробелы в соответствующей подготовке кадров. Совершенствование профессиональной и организационно-управленческой подготовки кадров позволит вести более эффективную работу по противодействию идеологии экстремизма и терроризма.

Задача государственных и муниципальных служащих – обеспечить такую организацию и регулирование образовательной среды, в которой максимально эффективно реализуются не только пункты Комплексного плана, но и требования Федерального государственного образовательного стандарта среднего (полного) общего образования и высшего образования в части:

– формирования российской гражданской идентичности обучающихся;

– сохранения и развития культурного разнообразия и языкового наследия многонационального народа Российской Федерации, реализации права на изучение родного языка, овладения духовными ценностями и культурой многонационального народа России;

– духовно-нравственного развития, воспитания и социализации обучающихся.

С целью повышении эффективности действий федеральных органов исполнительной власти, органов государственной власти субъектов Российской Федерации, органов местного самоуправления по профилактике террористических угроз и распространению идеологии экстремиз-

ма разработана программа повышения квалификации государственных и муниципальных служащих.

В результате освоения программы у слушателя должны быть сформированы и усовершенствованы профессиональные компетенции (ПК), включающие способность:

ПК-1: находить организационно-управленческие решения по вопросам противодействия экстремизму и терроризму, оценивать результаты и последствия принятого управленческого решения и готовность нести за них ответственность с позиций социальной значимости принимаемых решений;

ПК-2: проектировать организационные структуры с целью реализации мероприятий по противодействию идеологии экстремизма и терроризма в рамках своих функциональных обязанностей, участвовать в разработке стратегий управления человеческими ресурсами организаций, планировать и осуществлять мероприятия в соответствии с Комплексным планом, распределять и делегировать полномочия с учетом личной ответственности за осуществляемые мероприятия;

ПК-3: составлять бюджетное прогнозирование и финансовую отчетность, распределять ресурсы;

ПК-4:определять приоритеты профессиональной деятельности по противодействию идеологии экстремизма и терроризма, разрабатывать и эффективно исполнять управленческие решения, в том числе в условиях неопределенности и рисков, применять адекватные инструменты и технологии регулирующего воздействия при реализации управленческого решения;

ПК-5: проводить оценку программ и проектов по противодействию идеологии экстремизма и терроризма при различных условиях финансирования;

ПК-6: планировать, организовывать и разрабатывать организационную структуру, адекватную стратегии, целям и задачам, внутренним и внешним условиям деятельности органа исполнительной власти, осуществлять распределение функций, полномочий и ответственности между исполнителями;

ПК-7: разрабатывать диагностический инструментарий, диагностировать, проводить анализ количественных и качественных показателей (индикаторов) реализации мероприятий по противодействию идеологии экстремизма и терроризма;

ПК-8: оценивать состояние экономической, социальной, этнополитической, конфессиональной, поликультурной среды, деятельность органов государственной власти Российской Федерации, органов государственной власти субъектов Российской Федерации; органов местного самоуправления, государственных и муниципальных предприятий и учреждений, политических партий, общественно-политических, коммерческих и некоммерческих организаций для выработки оптимальных путей решения задач противодействия идеологии экстремизма и терроризма;

ПК-9: применять информационно-коммуникационные технологии в профессиональной деятельности, в том числе в сфере информационного противодействия идеологии терроризма и экстремизма, с видением их взаимосвязей и перспектив использования;

ПК-10: разрабатывать проекты и программы, направленные на противодействие распространению идеологии экстремизма и терроризма, с учетом экономических, социальных, этнических, конфессиональных, политических условий и прогноза последствий их реализации;

ПК-11: использовать современные методы управления проектами, направленными на своевременное получение качественных результатов, определение рисков, эффективное управление ресурсами, готовность к их реализации с использованием современных инновационных технологий в сфере противодействия идеологии

экстремизма и терроризма;

ПК-12: организовывать сотрудничество с общественными организациями, национальными и религиозными объединениями, иными институтами гражданского общества в рамках межведомственных проектов по противодействию идеологии экстремизма и терроризма;

ПК-13: применять методы рационального использования ресурсов и эффективно взаимодействовать с другими исполнителями.

Слушатель, освоивший курс, должен:

1. Владеть навыками:

– выявления происходящих изменений и корректировки действий в целях повышения результативности;

– работы с разными источниками информации (включая расширенный поиск в сети Интернет), а также с разнородными данными (статистическими, аналитическими);

– анализа множества взаимодействующих факторов, основываясь на неполной и/или противоречивой информации;

– системного мышления: воссоздание полной картины событий на основании отдельных фактов.

– целеполагания, умением пользоваться методикой «дерева целей»;

– формирования прогностических моделей;

– составления текущих и перспективных планов достижения цели структурного подразделения с учетом необходимых ресурсов, возможных изменений обстоятельств и влияния внешних факторов;

– управления проектами: навыки планирования и координации проектов от стадии инициирования до стадии завершения, а также навыками осуществления контроля над ходом исполнения документов, проектов и решений поставленных задач структурного подразделения с учетом установленных сроков;

– контроля эффективного использования всех ресурсов, условий, целей, процессов коммуникации, времени, рисков, затрат и издержек, качества итогового продукта, услуги.

2. Уметь:

– определять и формулировать цели, приоритеты;

– планировать деятельность по реализации мероприятий в рамках противодействия идеологии экстремизма и терроризма;

– проводить мониторинг выполнения работ, оценку и коррекцию планов;

– прогнозировать, выявлять, предупреждать и решать проблемы;

– принимать решения, прогнозировать и анализировать последствия принятых решений;

– эффективно и результативно использовать материальные, временные, финансовые и человеческие ресурсы (планирование и контроль эффективности), необходимые для достижения целей;

– использовать научные результаты в практике решения поставленных задач;

– работать с информацией: поиск, сбор, систематизация информации в соответствии с выделенным параметром (критерием, принципом), анализ и формулировка выводов (в том числе и на основе неполных данных);

– выстраивать межличностные коммуникации с учетом этнокультурных, этноконфессиональных и этнопсихологических особенностей поведения и общения, владеть навыками межкультурной коммуникации, воспринимать разные точки зрения, позиции и находить компромисс;

– устанавливать эффективное взаимодействие с коллегами внутри государственного (муниципального) органа, а также межведомственное взаимодействие с органами внебюджетных фондов в целях выполнения мероприятий анти-

экстремистской и антитеррористической направленности.

3. Знать:

– назначение и функции общегосударственной системы противодействия экстремизму и терроризму;

– факторы, виды, тенденции развития современного экстремизма и терроризма в РФ и в мире;

– методы распространения идей экстремизма в различных слоях общества, в том числе с использованием информационно-коммуникационных технологий;

– нормативно-правовые основы противодействия экстремизму и терроризму;

– принципы, основные задачи, направления противодействия терроризму и экстремизму;

– социокультурные, религиозные и этнические аспекты политики противодействия экстремизму и терроризму, специфику проявления фактора конфессиональной и этнической принадлежности представителей различных социальных групп в проявлении и росте экстремизма и терроризма;

– организационную основу деятельности государственных и муниципальных служащих;

– методику проведения оценки эффективности мер по противодействию экстремизму и терроризму на территории административного субъекта;

– основы управления проектами;

– информационно-коммуникационные технологии с видением их взаимосвязей и перспектив использования в противодействии распространению и влиянию идеологии экстремизма и терроризма.

МЕТОДЫ ВЫЯВЛЕНИЯ ПРИЗНАКОВ ПРОПАГАНДЫ ЭКСТРЕМИЗМА В ОБРАЗОВАТЕЛЬНОЙ СРЕДЕ ПОСРЕДСТВОМ СЕТИ ИНТЕРНЕТ

Чурилов Сергей Анатольевич,

директор Национального центра информационного противодействия терроризму и экстремизму в образовательной среде и сети Интернет

Большинство отечественных и зарубежных исследователей полагают, что экстремизм в современном обществе – в основном, молодежный феномен. Эксперты считают, что причина заключается в несопротивляющемся сознании молодежи и неработающей системе социализации молодежи.

Для осуществления своей деятельности экстремистские и террористические организации используют различные ресурсы интернета: сайты, форумы, блоги, социальные сети.

Интернет-коммуникация характеризуется массовым охватом, отложенной доставкой сообщений и постоянно расширяющейся географией.

В последнее время наиболее популярным способом распространения информации, а также привлечения последователей являются социальные сети «ВКонтакте», «Одноклассники» и «Facebook». Не менее привлекательными являются служба микроблогов «Twitter», приложение для обмена фотографиями и видеозаписями «Instagram», видеохостинг «Youtube».

Практически у каждого молодого человека есть своя страничка, хотя бы на одной из этих площадок. Но мало кто ограничивается одной регистрацией, чаще молодежь предпочитает находиться на нескольких ресурсах одновременно.

Далее представлены и прокомментированы те признаки экстремизма, которые могут быть отслежены в сети Интернет, согласно Федеральному Закону №114-ФЗ "О противодействии экстремистской деятельности":

1. Насильственное изменение основ конституционного строя и нарушение целостности Российской Федерации

В данном случае следует обращать внимание не на цели, а на методы, с помощью которых предлагается их осуществить. Изменение конституционного строя и целостности Российской Федерации может происходить только

законным путем, то есть через выборы и референдум. Поэтому экстремистскими высказываниями являются призывы к революции, восстанию, неповиновению законно избранной власти, а также собственно эта деятельность, названная в уголовном законодательстве вооруженным мятежом. Революция ставит перед собой цель захвата или присвоения властных полномочий. Таковым является любой приход к власти лиц вопреки законной процедуре выборов и передачи властных полномочий.

Насильственное изменение основ конституционного строя может быть связано с посягательством на безопасность государства.

2. Публичное оправдание терроризма и иная террористическая деятельность

Согласно Федеральному Закону "О противодействии терроризму", терроризм – идеология насилия и практика воздействия на принятие решения органами государственной власти, органами местного самоуправления или международными организациями, связанные с устрашением населения и (или) иными формами противоправных насильственных действий. Поэтому в качестве призывов к террористической деятельности можно рассматривать призывы к насильственным акциям с целью оказания давления на органы власти и общественное мнение для проведения решения в свою пользу.

3. Возбуждение социальной, расовой, национальной или религиозной розни

Существенным здесь является насильственный характер действий или призывов к таким действиям. К таковым относятся призывы к убийству, избиению или выселению лиц определенной национальности или вероисповедания; организация, совершение или подстрекательство к таковым действиям.

4. Пропаганда исключительности, превосходства либо неполноценности человека по признаку его социальной, расовой, национальной, религиозной или языковой принадлежности или отношения к религии

Понятие пропаганды подразумевает систематические действия, направленные на внедрение в общественное сознание идей и формирование установок. Поэтому к данному признаку нельзя отнести единичные высказывания и суждения, выдвинутые в качестве тезиса в мировоззренческой или политической дискуссии.

5. Нарушение прав, свобод и законных интересов человека и гражданина в зависимости от его социальной, расовой, национальной, религиозной или языковой принадлежности или отношения к религии

Имеется в виду весь спектр прав и свобод человека и гражданина: экономические, политические, социальные, культурные.

6. Пропаганда и публичное демонстрирование нацистской атрибутики или символики либо атрибутики или символики, сходных с нацистской атрибутикой или символикой до степени смешения

Народ России, являясь историческим правопреемником народов Советского Союза, внесших наибольший вклад в разгром германского нацизма и его союзников в XX веке и понесших при этом наибольшие потери, не может терпимо относиться к пропаганде нацистских идей и публичному демонстрированию нацистской символики. По существующему законодательству нацизмом является идеология и практика Германского Рейха и его союзников в XX веке. Поэтому в оценках иных идеологий и движений как нацистских необходимо доказывать их идеологическую связь с европейским нацизмом времен Второй мировой войны.

7. Публичные призывы к осуществлению указанных деяний либо массовое распространение заведомо экстремистских материалов, а равно их изготовление или хранение в целях массового распространения

В этом пункте главной проблемой является квалификация материалов как экстремистских.

8. Публичное, заведомо ложное обвинение лица, замещающего государственную должность Российской Федерации или государственную должность субъекта Российской Федерации, в совершении им в период исполнения своих должностных обязанностей деяний, указанных в настоящей статье и являющихся преступлением

Клеветой является распространение сведений о лице, заведомо не соответствующих действительности и задевающих его честь и достоинство. Поэтому следует отличать политическую полемику, допускающую порой жесткие высказывания, от собственно публичной клеветы, факт которой должен быть установлен в судебном порядке.

9. Организация и подготовка указанных деяний, а также подстрекательство к их осуществлению

10. Финансирование указанных деяний либо иное содействие в их организации, подготовке и осуществлении, в том числе путем предоставления учебной, полиграфической и материально-технической базы, телефонной и иных видов связи или оказания информационных услуг

Пункты 9 и 10 касаются организационного аспекта экстремистской деятельности. Согласно федеральному Закону «О противодействии экстремистской деятельности» экстремистская организация – общественное или религиозное объединение либо иная организация, в отношении которых по основаниям, предусмотренным настоящим Федеральным законом, судом принято вступившее в законную силу решение о ликвидации или запрете деятельности в связи с осуществлением экстремистской деятельности.

Вышеописанные признаки экстремизма могут оказать существенную помощь в оценке материала на предмет экстремистской направленности.

Существует несколько способов выявления экстремистских ресурсов в сети Интернет. Ключевые слова – вспомогательные слова, вводимые в строку запроса, способные фильтровать поисковый запрос и выдавать необходимую информацию. Поиск по ключевым словам может проводиться не только при помощи поисковых сервисов, но и в социальных сетях, блогах. Ниже описаны особенности поиска информации в социальной сети «ВКонтакте», «Facebook», в службе микроблогов «Twitter» и системе поиска «Яндекс.Блоги».

Анализ страниц – это контекстный анализ вербальных и невербальных средств информационного воздействия и содержательного аспекта пользовательских страниц.

Сбор информации в социальной сети может осуществляться различными способами в зависимости от цели и информации, которую необходимо найти.

Поиск данных осуществляется через функцию встроенного поиска и делится на общий поиск информации; поиск по хештегам; поиск видео; поиск сообщества.

На примере сети «Вконтакте», общий поиск информации – это функция, которая служит для поиска абсолютно любой информации. В поисковую строку можно ввести как отдельное слово, так и фразу. Но полученный результат не всегда будет релевантным, и это является большим недостатком при сборе информации. Чтобы приблизить результаты поиска к искомым, следует использовать дополнительные настройки поиска, такие как тип сообщения, исключение слов и другие.

Поиск видео осуществляется через встроенную функцию поиска по видеозаписям. В поисковую строку вводится запрос, связанный с тематикой искомого видео.

Поиск сообщества осуществляется через встроенную функцию поиска по сообществам (группам), в строку поиска вводится название искомого сообщества.

При осуществлении поиска сообщества по

интересующей тематике, запрос необходимо составлять наиболее точно. Результаты поиска будут содержать поисковое слово без изменений, не учитывая другие вариации написания запроса. Поэтому целесообразно здесь использовать только одно ключевое слово. Если результат не оправдывает ожиданий, необходимо изменить написание ключевого слова или подобрать слово синоним.

На примере социальной сети «Facebook» показан поиск через поисковые сервисы Яндекс и Гугл. Здесь необходимо использование дополнительных операторов.

Поиск по хэштэгам поддерживает большая часть социальных сетей, хотя считается, что хэштэги - это основная особенность поиска в «Twitter» и «Instagram».

Отбор страниц через список друзей

Каждая страница в социальных сетях имеет раздел, где отражен список друзей или подписчиков. Просмотр этого списка позволяет выявить других пользователей, также занимающих активную позицию в распространении экстремистских или террористических идей.

Необходимо обратить внимание на фотографию пользователя и оформление страницы. В качестве фотографии часто используются различные иллюстрации, отражающие тематику публикаций: логотипы движения ИГИЛ, фотографии с оружием, иллюстрации священных исламских книг. При последующем изучении данных пользователей гипотеза о принадлежности их к радикальному исламу в большинстве случаев подтверждается. В различной степени на этих страницах будет публиковаться информация о военных действиях в Сирии и Ираке, формирующая необходимые искаженные представления о реальной ситуации.

Зачастую именно для этих целей создается большое количество зарегистрированных пользователей, у которых периодически появляются новости радикального ислама.

Просмотр списка друзей возможен не только в службе микроблогов «Twitter». В остальных социальных сетях отбор страниц для последующего мониторинга осуществляется аналогичным способом.

В настоящее время при продвижении сообщества в социальных сетях возникают некоторые трудности, связанные с защитой от спама. Одним из безопасных способов рекламы сообщества является функция взаимного обмена ссылками. Администраторы этих страниц договариваются о том, что размещают у себя ссылку на другое сообщество. Подписчики группы при желании могут увидеть дополнительные ресурсы, которые наполняются информационно по схожей тематике, если им интересно получать обновления, они подписываются на эту страницу тоже.

В этом же разделе указываются ссылки на дополнительные ресурсы данного сообщества. Например, видеоканал на "Youtube" или страница на «Facebook», «Twitter». Так как сообщество может быть закрыто в любой момент, часто есть запасная страница, адрес которой указывается здесь же.

В социальной сети «Facebook» есть похожий раздел, здесь он называется «Отметки» «нравится».

Через страницы в социальных сетях можно выявить других пользователей, которые также ведут пропаганду, размещают видео- и аудиоматериалы, информационные сообщения подстрекательского характера. Поиск осуществляется через список друзей и публикации в ленте новостей.

Служба микроблогов «Twitter» в последнее время является одной из самых распространенных площадок, где ведется работа по привлечению новых последователей. Здесь публикуются краткие заметки, может быть ссылка на полную новость. Для рекламы и продвижения других страниц автор публикует информацию со ссылкой на источник.

В социальных сетях «Facebook» и «Вконтакте» подобным образом выявляются взаимосвязи между единомышленниками. В ленте новостей необходимо смотреть публикации со ссылкой на другую страницу. Имя автора сообщения является активной ссылкой, по ней можно перейти на страницу пользователя и продолжить работу по тому же принципу.

Данный способ выявления ранее неизвестных страниц, ведущих активную деятельность по агитации и пропаганде экстремистских настроений, позволяет обнаружить не только самостоятельных пользователей, но и тематические сообщества. Технически отражается одинаково. Понять, что репост был осуществлен из группы можно, перейдя по активной ссылке.

Несмотря на простоту вышеописанного способа поиска новых страниц, он является одним из самых эффективных. Для начала необходимо иметь несколько ранее выявленных действующих (не заблокированных) страниц по тематике экстремистской пропаганды. Путем просмотра их новостной ленты осуществляется поиск и пополнение базы активных пользователей.

Постепенно формируется реестр запрещенных сайтов или страниц социальных сетей, с которых ведется активная пропаганда экстремистских настроений. Проводя мониторинг данных страниц, можно обнаружить различные связи. Это помогает выявлять новые, недавно зарегистрированные ресурсы, которые не всегда удается найти по ключевым словам.

В первую очередь необходимо обратить внимание на ссылки, которые указаны в разделе «Контакты», «О нас», «Ссылки» или «Мы в социальных сетях». Также ссылки на другие ресурсы указываются на главной странице и обозначаются либо названием ресурса, на котором зарегистрирована страница, либо его логотипом. На сайте «VDAGESTAN.COM» можно обнаружить ссылки на его страницы в социальных сетях «Facebook» и «Twitter», а в разделе «Ссылки» указаны другие сайты движения «Имарат Кавказ».

Таким образом, сайт целенаправленно оставляет свои дополнительные контакты в сети Интернет.

Помимо этого есть возможность выявить и другие страницы, на которых движение «Имарат Кавказ» распространяет экстремистские материалы. Например, на сайте размещены видеозаписи. Через видеозапись можно выйти на видеохостинг, где она хранится.

Списки запрещенных организаций могут быть представлены в различных документах, отчетах, научно-исследовательских работах. В сети Интернет наиболее популярные форматы документов: PDF (Portable Document Format) и DOC (текстовый файл, редактируемый в программе Microsoft Word).

При поиске документов в системе Google необходимо написать запрос (например, «список международные террористические организации») и добавить PDF или DOC.

Народ России, являясь историческим правопреемником народов Советского Союза, внесших наибольший вклад в разгром германского нацизма и его союзников в XX веке и понесших при этом наибольшие потери, не может терпимо относиться к пропаганде нацистских идей и публичному демонстрированию нацистской символики.

ОРГАНИЗАЦИЯ ДЕЯТЕЛЬНОСТИ ПО ПРОТИВОДЕЙСТВИЮ ТЕРРОРИЗМУ И ПРОФИЛАКТИКЕ РАСПРОСТРАНЕНИЯ ИДЕОЛОГИИ ЭКСТРЕМИЗМА В ВУЗАХ

Солонько Игорь Викторович,

Проректор по административно-кадровой и воспитательной работе СПбГАУ, доцент, к.ф.н. ФГБОУ ВО Санкт-Петербургский государственный аграрный университет

Мы живем и работаем в многонациональной и многоконфессиональной стране с идеологическим многообразием, которое закреплено в Конституции России. Это обстоятельство определяет принципиальные особенности в проведении воспитательной работы и профилактике экстремистских проявлений в молодежной среде. В своей деятельности мы должны подняться над различиями (национальными, религиозными, идеологическими), которые активно используются в манипулятивных технологиях, и ставить вопрос о формировании у молодежи **мировоззренческой безопасности** в условиях глобализации.

Сегодня на личностное становление молодого человека постоянно оказывает влияние целый комплекс факторов. Молодежь живет и формируется в современном информационном пространстве, далеком от совершенства и влияющем на неё значительно сильнее, чем традиционные институты – семья, школа, вуз. Следовательно, и воспитательная работа должна носить комплексный систематический характер, адекватный современным вызовам, не навязывая, а предлагая здоровую альтернативу высоких нравственных стандартов, чтобы у студентов было реальное представление о всех возможных вариантах выбора между добром и злом. Если мы хотим жить в здоровом обществе, то обязаны позаботиться о том, чтобы каждый молодой человек имел нравственный компас, способствующий становлению духовной личности. При этом очень важно учитывать особенности современных условий: процесс глобализации, динамичная внешняя среда, активное влияние средств массовой коммуникации и многое другое. Следовательно, каждый коллектив специалистов по воспитательной работе любого вуза должен сделать выбор приоритетных направлений и способов воспитательной работы с учетом специфики студенческого контингента (количество студентов, доля и состав иностранных студентов, доля иногородних студентов, общий культурный уровень, социальный и национальный состав, гендерное соотношение и т. д.).

Отталкиваясь от многолетнего успешного практического опыта воспитательной работы, мы сформировали следующие приоритеты:

1) Положительный личный пример субъектов воспитательного процесса. Расхождение слов с делом – это наиболее опасный путь дискредитации воспитательной работы. Молодежь чутко реагирует на фальшь воспитателя и делает противоположные выводы из сказанного. Кроме того, специалисты знают, что подсознательно молодой человек посредством социального

импринтинга копирует поведенческие модели референтной группы. Следовательно, руководство университета, факультетов, институтов, воспитательная структура, а в идеале и каждый сотрудник университета должны личным повседневным примером демонстрировать на практике что такое хорошо и что такое плохо. А самое главное – стараться доходчиво и в интересной для студенчества форме объяснять, почему именно так правильно.

2) Формирование мировоззренческой безопасности у субъектов воспитательного процесса. Помощь студенчеству в формировании адекватного современным реалиям представления о жизни вообще, об обществе как сложной социокультурной системе, о внешних факторах, активно влияющих на каждого студента и студенчество в целом (мировоззренческий, исторический, фактологический, экономический, генетический и силовой приоритеты социального управления) [1], о феномене концептуальной власти [2], о типах строя психики и смене логики социального поведения в массовой статистике общества [3], о способах манипуляции индивидом и массовым сознанием, о главных ценностных ориентирах в жизни (нравственный компас) [4; 5]. Без того, что мы называем мировоззренческой безопасностью, невозможен современный качественный и эффективный воспитательный процесс. Для этого в университете должны проводиться соответствующие элективные и факультативные образовательные курсы, а так же специальные занятия со студенческим активом во внеаудиторное время [6].

3) Активное вовлечение студенчества в различные конкретные проекты и дела, а также помощь в организации молодежных общественных объединений и организаций и их межвузовское взаимодействие. Необходимая часть студенческой жизни, помимо учебы, – это активный отдых и творчество, направленные на формирование командного духа и командного подхода при решении сложных задач. Все эти навыки им пригодятся и в дальнейшей жизни.

4) Активное использование средств массовой коммуникации в воспитательном процессе: Интернет-сайты молодежных общественных организаций (http://golos-molodeji.org/ и др.), студенческие газеты, кабельное телевидение, новостные и мировоззренческие видеоролики (http://tv.vsem-eu.ru/), еженедельный просмотр кинофильмов с их последующим обсуждением, фото- и видео-отчеты о прошедших мероприятиях на молодежном сайте и в студенческой газете и т.д. Все эти средства повышают скорость и эффективность циркуляции полезной информации о жизни студенчества, направленной на воспитание не только высококвалифицированного специалиста, но и человека с высокой и активной гражданской позицией, носителя великой русской культуры.

5) Развитие всех возможных форм студенческого самоуправления. Делая ставку на развитие студенческого самоуправления, как на одно из важнейших направлений воспитательной работы, мы убедились в том, что интересное и доходчивое объяснение своих же сверстников - студентов и аспирантов более эффективно, чем запреты администрации. Молодой человек скорее послушает своего товарища старшекурсника, который, ближе ему по возрасту и интересам, является для него примером для подражания. Поэтому подбор и подготовка студенческого актива и помощь в его становлении - это важнейшая задача воспитательной структуры университета на первом этапе. Затем необходимо обеспечить преемственность в работе студенческого самоуправления при смене поколений. При таком подходе студенческое самоуправление входит в режим реального самоуправления и самовоспитания, что позволяет ему быть настоящим помощником и опорой ректората и деканатов университета.

Патриотическое воспитание в системе высшего образования, профилактика асоциальных явлений и экстремизма в молодежной среде, должны осуществляться, основываясь на самых передовых достижениях гуманитарных

наук специально подготовленными специалистами с учетом современных вызовов и условий глобализации.

В самом понятии «образование», заложен вопрос – образование кого? То есть, какая цель у этого процесса? Мы считаем, что цель процесса образования – это образование высококвалифицированного специалиста с высоконравственным патриотическим самосознанием, которое позволяет ему не быть объектом манипулирования чуждой ему власти, а быть полноправным субъектом самоуправления в рамках своей легитимной власти. Только в такой социальной системе возможны развитые институты гражданского общества и подлинной демократии. Воспитательный процесс должен быть приоритетной составляющей процесса образования, так как любые знания – это всего лишь приложение к типу строя психики человека. Знания, оторванные от нравственности, зачастую оборачиваются для общества оружием самоуничтожения. Если студент понимает, что происходит с ним и вокруг него (мировоззренческая безопасность), если студент чувствует искренность старших (положительный личный пример), если он активно вовлечен в жизнь своего факультета, института, университета, города и страны, то ему интересно жить и учиться, работать и отдыхать. При активном взаимодействии со своими товарищами и администрацией университета он самостоятельно решит большинство проблем студенчества и своего университета в настоящем, и своей страны в будущем, так как молодежь – это действительно наше общее будущее.

Основные сферы автоматизации в госсекторе представляют собой создание базовых инфраструктурных систем, таких как система межведомственного взаимодействия, единая система идентификации и аутентификации, единая система нормативно-справочной и документированной информации и др.

СТРАТЕГИИ ЭКСТРЕМИСТСКИХ ДВИЖЕНИЙ В СЕТИ ИНТЕРНЕТ И ОБРАЗОВАТЕЛЬНОЙ СРЕДЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

Чурилов Сергей Анатольевич,

директор Национального центра информационного противодействия терроризму и экстремизму в образовательной среде и сети Интернет

Влияние сети Интернет на формирование базовых ценностей гражданского общества и социальных связей за последние 10 лет возросло многократно. Из-за ряда свойств в XXI веке «всемирная паутина» становится такой средой, в которой приверженцы радикальных движений, националистических взглядов продвигают искаженные представления как об отдельных явлениях, так и о миропорядке в целом.

Понятие экстремистская деятельность (экстремизм) содержит в себе следующие характеристики:

– насильственное изменение основ конституционного строя и нарушение целостности Российской Федерации;

– публичное оправдание терроризма и иная террористическая деятельность;

– возбуждение социальной, расовой, национальной или религиозной розни;

– пропаганда исключительности, превосходства либо неполноценности человека по признаку его социальной, расовой, национальной, религиозной или языковой принадлежности или отношения к религии;

– нарушение прав, свобод и законных интересов человека и гражданина в зависимости от его социальной, расовой, национальной, религиозной или языковой принадлежности или отношения к религии.

Исследователи дают следующее определение экстремизма. Экстремизм – это приверженность к крайним мерам и взглядам, радикально отрицающим существующие в обществе нормы и правила через совокупность насильственных проявлений, совершаемых отдельными лицами и специально организованными группами и сообществами. Экстремизм – это сложная и неоднородная форма выражения ненависти и вражды. Большинство отечественных и зарубежных исследователей полагают, что экстремизм в современном обществе – в основном, молодежный феномен. Эксперты считают, что причина заключается в несопротивляющемся сознании молодежи и неработающей системе социализации молодежи.

В современных исследованиях выделены такие виды экстремизма, как социальный, политический, национальный и религиозный. Одним из самых ярких примеров национального экстремизма является движение скинхедов. Национальный экстремизм часто отличается лозунгами защиты «своего народа», его экономических интересов, культурных ценностей, как правило, в ущерб представителям других национально-

стей, проживающим на этой же территории.

Под религиозным экстремизмом понимают нетерпимость по отношению к инакомыслящим представителям той же или другой религий.

Политический экстремизм – это движения или течения, деятельность которых направлена против существующего конституционного строя. Иногда политический экстремизм разделяют на «левый», «революционный» и «правый», но подобное деление не исчерпывает все формы политических экстремистских проявлений. К основным характеристикам политического экстремизма эксперты относят политическую направленность, желание прийти к власти любым путем и отказ от компромиссов, стремление угрожать политическим оппонентам. Как его вариация, социальный экстремизм – это общественное явление, посягающее на социальные устои, общественную справедливость и равноправие граждан.

Все перечисленные виды экстремизма встречаются в сети Интернет. Используя его возможности, экстремисты привлекают сторонников, спонсоров, нагнетают страх на тех, против кого они выступают. Анонимность глобальной сети позволяет религиозным экстремистам, например, вдохновляемым террористической организацией «Аль-Каида», использовать Интернет для создания коммуникативных и организационных площадок:

– собственные сайты как основные источники текстовых и аудиовизуальных материалов;

– сообщества в социальных сетях или страницы виртуальных личностей, которые публикуют в своих новостных лентах экстремистские тексты, размещают экстремистские видеозаписи (согласно отчету ОБСЕ, существуют некоторые свидетельства, показывающие, что приверженцы идеологии «Аль-Каиды», применяющие насилие, используют социальные сети в рамках своей официальной стратегии);

– текстовые материалы, возбуждающие религиозную рознь, путем добавления в доступные документы социальной сети «ВКонтакте», анонимных хостингов для публикации, библиотек и торрентов;

– распространение инструкций по изготовлению оружия и взрывчатых веществ;

– сбор средств на экстремистскую деятельность: публикуются номера виртуальных кошельков и банковских счетов, куда следует перечислять средства (согласно отчету ОБСЕ, террористы занимаются онлайн-мошенничеством с кредитными картами, хищением персональных данных и другими видами незаконной деятельности для финансирования своих операций). Известно, что посредством социальной сети «Facebook» и «ВКонтакт» представители экстремистских и террористических сообществ собирают деньги для организации акций, содержания боевиков и их жен. Иногда террористические сообщества продают атрибутику – футболки и другую одежду, флаги, иногда – специальную еду;

– обмен контактами среди активистов для координации деятельности.

Согласно данным экспертов Интернет дает больше возможностей религиозным экстремистам для повышения активности среди женщин и подростков, так как они (из-за определенной изолированности и меньшей способности к критическому восприятию действительности) легче поддаются идеологической пропаганде. Например, на интернет-ресурсах религиозных организаций даже раздел новостей имеет основную задачу идеологической корректировки информации. Экстремисты не только ставят под сомнение точность информации, поступающей из российских источников, но и пытаются популяризировать принятые в их среде географические названия, которые имеют выраженную идеологическую окраску. Так, в сводках новостей от представителей экстремистских и террористических движений районы называются «вилайятами» (провинциями), например, вилай-

ят Нохчийчоь (Чечня), объединенный вилайят Кабарды, Балкарии и Карачая.

В пропагандистских материалах используются символы, которым приписывается неконвенциональное значение: исламские термины, такие как «джихад» (усердие на пути Всевышнего), «моджахеды» (борцы), «муртады» (отступники), «кафиры» (неверные). При этом толкования перечисленных выше понятий значительно отличаются от традиционных: джихадом называют войну против России и западного мира, моджахедами именуются боевики, муртады – мусульмане из полиции северокавказских республик. Действия сепаратистов изображаются как мученические, а действия полиции на Северном Кавказе преподносятся как террор против мирных жителей. Данный прием в теории манипулятивного воздействия называется «подмена понятий».

Таким образом, для впечатлительных и подверженных влиянию пользователей Интернета создается обновленная реальность с искаженными новостями, использованием языка вражды. Большая часть экстремистских материалов размещается на серверах за пределами Российской Федерации.

Как считают эксперты, одной из особенностей политических и национальных экстремистских движений в сети Интернет является вирусное распространение учебных пособий, продвигающих искаженные мировоззренческие ценности в молодежной среде. Учебные материалы содержат как прямые призывы к действию, так и более сдержанные формулировки, например, подмену понятий через создание ассоциативных рядов (по отношению к представителю конкретной партии или национальности выстраивается логическая цепочка: «не разделяет наши взгляды» – «чужой» – «враг»), косвенные указания на «неправильные» ценности и др.

В Интернете и социальных сетях экстремисты нацеливаются на молодежь, используя узнаваемый стиль, слоганы и символы. При этом у пользователей формируется представление о некой общности – социальной группе, отличной от других цельностью представлений и знаний об окружающей действительности. Слоганы и символы при этом подаются при помощи понятных и популярных среди молодежи форматов, легко приобретающих статус «вирусных явлений»: демотиваторов, мемов, подражаний и другие.

Онлайн-пространство является основным источником финансирования для «правых» движений. Многие интернет-сайты продают атрибуты, символизирующие нацизм, активно развиваются интернет-магазины «правого» толка.

Несмотря на то, что сообщества, нарушающие законодательство, закрываются по требованиям надзорных органов, либо же самих пользователей социальных сетей, множество пользователей размещают тексты, видеозаписи, фотографии и аудиофайлы, пропагандирующие насилие по отношению к представителям другой национальности.

Обзор современных сообществ, посвященных тематике национализма, показал, что контент групп характеризуется агрессией, но при этом отличается достаточно прогрессивным спектром методов психологического воздействия – манипуляции массовым сознанием пользователей. Многие сообщества могут вовлекать молодых людей в экстремистскую деятельность, популяризируя образ современного националиста, который освобождает от захватчиков (нерусских) исконно русские земли.

Практически все экстремистские сообщества, предназначенные для студентов и школьников, используют специфические черты восприятия информации аудиторией: отсутствие критического подхода к информации, поступающей от знакомых людей, селекционных механизмов восприятия бытовой и иной информации, максималистские взгляды на действительность, склонность к восприятию визуальной, невербальной информации. В связи с этим выделим ряд особенностей националистических сообществ,

рассчитанных на молодежь:

– слогановый характер сообщений, посты обязательно сопровождаются картинкой;

– эмоциональные картинки, дополненные призывом к конкретному действию (часто текст отсутствует и используются хэштег #бей «наименование национальности», как призыв к насилию);

– использование стереотипных представлений о людях разных национальностей, присвоение ярлыков (употребляются слова с ярко выраженной негативной окраской), бранные, оценочные и нецензурные выражения.

В сообществах в социальных сетях, направленных на молодых людей – школьников или студентов вузов – предлагается искаженная реальность, которая выдается за реальное положение дел в мире. Содержание сообществ четко делится по теории М.Г. Стадникова на «их мир» (врагов), в котором врагов следует игнорировать («не покупайте овощи у азербайджанцев, и тогда они разорятся и уедут обратно»), бить (фотографии с насилием над нерусскими, «травить их надо дихлофосом»), убивать («поубивал бы всех ***»). Образ человека другой национальности рисуется с помощью сообщений, имеющих острую эмоциональную окраску.

Таким образом, специалисты НЦПТИ приходят к следующим выводам. Формирование идеологии превосходства идет в двух направлениях: принижение представителей других национальностей, восхваление, «избранность» своей национальности. Ненависть к жителям страны, не подпадающим под общепринятые критерии «своего», формируется посредством следующих стратегий:

– демонстрация ненависти «чужих» по отношению к «своему» народу (вариация, горожанам «своего» города) и «своим» представлениям о мире;

– акцентирование внимания на преступлениях, совершенных представителями других национальностей, особенно тяжких, жертвами которых стали представители «своей» национальности.

На следующем этапе воздействия членам сообществ внушают, что необходимо убивать тех, кто не соответствует представлениям о «своей» нации. При этом молодежи транслируются следующие идеи:

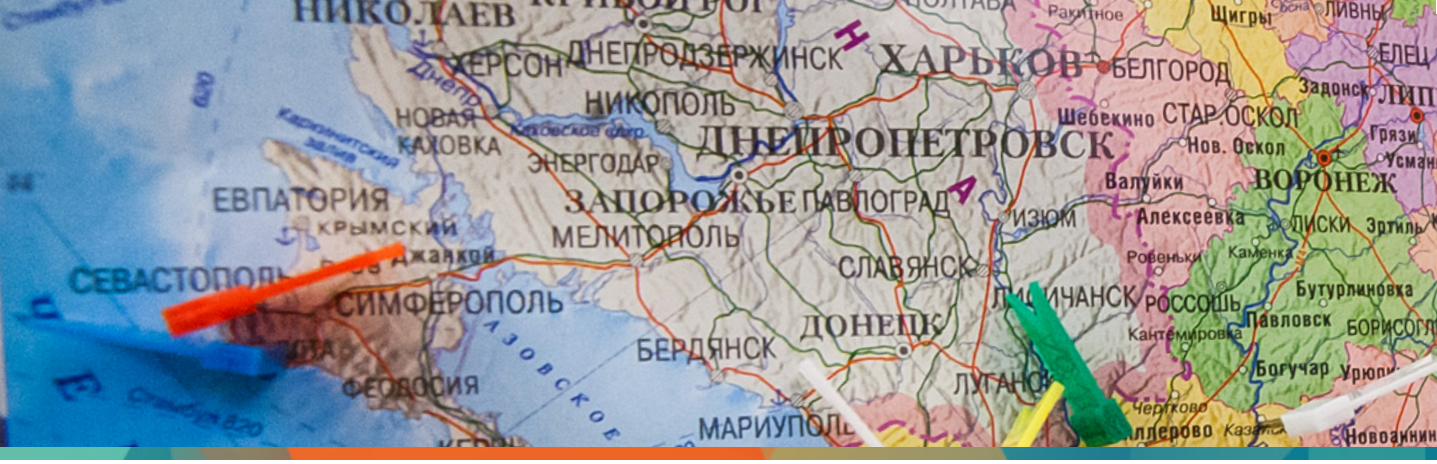
– нацистская идея о чистоте крови;

– представление об исключительности националистов, только они являются силой, способной противостоять несправедливости в обществе и «спасти русский народ»;

– необходимость объединиться и запасаться оружием для защиты территории;

– идея о необходимости мести за убийство нерусскими русских.

Стратегии экстремистских движений по отношению к молодежной среде и другие инструменты влияния экстремистских сообществ в сети Интернет, перечисленные выше, являются доминирующими и соответствуют теории ведения психологических войн, цель которых – достижение устойчивого результата в формировании общественного мнения, внедрение установок и паттернов поведения в подсознание масс. В реализации стратегий используются такие каналы коммуникации, как сайты, сообщества в социальных сетях, страницы анонимных пользователей сети Интернет.



РЕЗОЛЮЦИЯ ВТОРОГО ИНФОРМАЦИОННО-ПРАКТИЧЕСКОГО ФОРУМА «БЕЗОПАСНОСТЬ И ОБРАЗОВАНИЕ»

28-29 октября 2015 г., г. Симферополь

28 и 29 октября 2015 года при поддержке Министерства образования и науки Российской Федерации, Министерства внутренних дел, Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций Российской Федерации, Федеральной службы по техническому и экспортному контролю Российской Федерации, Министерства чрезвычайных ситуаций состоялся второй информационно-практический форум "Безопасность и образование", посвященный обсуждению вопросов физической безопасности образовательных организаций, их антитеррористической защищенности, организации работ по ГО и ЧС, информационной безопасности, в том числе предупреждению информационно-технологических угроз национальным интересам России, противодействию терроризму, экстремизму, насилию.

В Форуме приняли участие 178 представителей 95 образовательных организаций из 36 субъектов и 3 городов федерального значения Российской Федерации.

В ходе работы Форума участники отметили:

– важность развития системы управления по вопросам комплексной безопасности в сфере деятельности образовательных организаций;

– необходимость совершенствования мер профилактики терроризма и экстремизма, мониторинга процесса межнациональных и межконфессиональных отношений в молодежной среде;

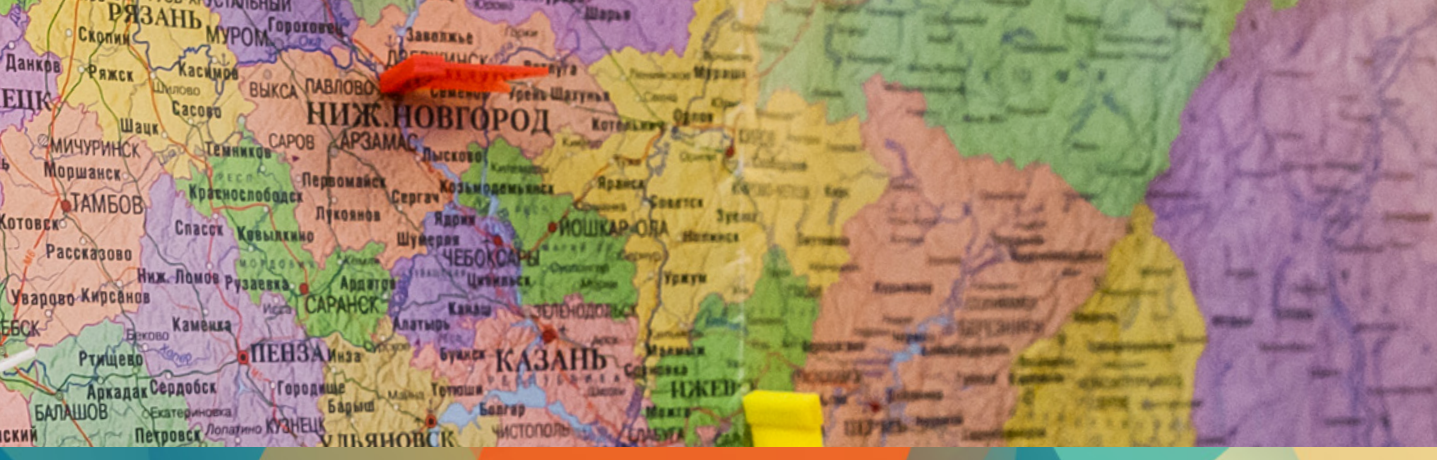
– направленность на выработку общих подходов и стандартов в области обеспечения безопасности (как физической, так и информационной);

– необходимость работы по подготовке высококвалифицированных кадров в области информационной безопасности;

– необходимость ведения работы по выявлению очагов пропаганды терроризма и экстремизма, как в сети Интернет, так и в образовательной среде.

Признавая важность происходящих процессов в области обеспечения комплексной безопасности образовательных организаций, с целью повышения защищенности в т.ч. информационных ресурсов, **участники форума по итогам своей работы считают необходимым:**

– проводить подобные мероприятия на регулярной основе, в том числе с освещением вопросов безопасности образовательных организаций в части (вопросах) взаимодействия с МЧС



Участники форума решили обратиться к Министерству образования и науки Российской Федерации, Национальному антитеррористическому комитету, Федеральной службе по техническому и экспортному контролю Российской Федерации, Министерству связи и массовых коммуникаций Российской Федерации, Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций, Министерству внутренних дел, Министерству Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий с предложением о скорейшей реализации указанных предложений в части касающейся.

и МВД России;

– переработать, уточнить и дополнить отраслевые нормативно-правовые акты в части ГО и ЧС (Приказ Минобрнауки России № 833 от 28.12.2009г. и приказ Минобрнауки России от 29 июня 2011 г. № 2080 «О функциональной подсистеме РСЧС Минобрнауки»);

– сформировать единые внутриведомственные методические подходы к процессам разработки, согласования и утверждения документов в области обеспечения безопасности образовательных организаций;

– инициировать процесс совершенствования системы профессиональной подготовки и переподготовки специалистов в области информационной безопасности;

– проводить на постоянной основе мониторинг интернет-среды и, в первую очередь, социальных сетей с целью заблаговременного выявления среди молодежи признаков межнациональной и межконфессиональной розни, пропаганды терроризма и экстремизма;

– инициировать организацию на постоянной основе мониторинг образовательной среды и сети Интернет с целью выявления фактов пропаганды терроризма и экстремизма;

– создать Совет уполномоченных по ГО и ЧС (начальников штабов) подведомственных организаций, собирающийся на регулярной основе для обсуждения важных вопросов, обмена передовым опытом и т.д. (по аналогии с УМО - учебно-методическими объединениями);

– инициировать подготовку совместно методических рекомендаций по профилактике терроризма и экстремизма в молодежной среде и распространению результатов работы в социальных сетях и других типах интернет-ресурсов для наи-

большего охвата аудитории.

Участники форума решили обратиться к Министерству образования и науки Российской Федерации, Национальному антитеррористическому комитету, Федеральной службе по техническому и экспортному контролю Российской Федерации, Министерству связи и массовых коммуникаций Российской Федерации, Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций, Министерству внутренних дел Российской Федерации, Министерству Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий с предложением о скорейшей реализации указанных предложений в части касающейся.

344011, Г. РОСТОВ-НА-ДОНУ,
УЛ. ГОРОДА ВОЛОС, Д. 6

+7 (863) 201-28-22 (Г. РОСТОВ-НА-ДОНУ)

НЦПТИ.РФ

МИНОБРНАУКИ РОССИИ
НЦПТИ

344002, Г. РОСТОВ-НА-ДОНУ, ПЕР. ГАЗЕТНЫЙ, 51

+7 (863) 201-28-15 (Г. РОСТОВ-НА-ДОНУ)
+7 (495) 705-93-21 (Г. МОСКВА)

INFO@NIISVA.ORG/WWW.NIISVA.RU

МИНОБРНАУКИ РОССИИ
ЮРАЦ
ЮЖНЫЙ РЕГИОНАЛЬНЫЙ
АТТЕСТАЦИОННЫЙ ЦЕНТР