Секция 4. Электронная информационно-образовательная среда вуза

УДК 37.014.53

И.В. Гаврилова

МОЛОДЕЖНЫЙ КИБЕРЭКСТРЕМИЗМ И КИБЕРТЕРРОРИЗМ КАК УГРОЗА БЕЗОПАСНОСТИ ЭЛЕКТРОННОЙ ИНФОРМАЦИОННО-ОБРАЗОВАТЕЛЬНОЙ СРЕДЫ УНИВЕРСИТЕТА

Гаврилова Ирина Викторовна
Old_raven@mail.ru
ФГБОУ ВПО «Магнитогорский государственный технический университет им. Г.И. Носова», Россия, г. Магнитогорск

A YOUTH CYBEREXTREMISM AND CYBERTERRORISM AS THREAT TO SECURITY OF THE ELECTRONIC INFORMATION AND EDUCATION ENVIRONMENT OF UNIVERITY

Gavrilova Irina Victorovna
Nosov Magnitogorsk State Technical University, Russia, Magnitogorsk

Аннотация. *В статье рассматриваются угрозы безопасности электронной информационно-образовательной среды со стороны молодежного киберэкстремизма и кибертерроризма.*

Abstract. *In article threats to security of the electronic information and education environment from youth cyberextremism and cyberterrorism are considered.)*

Ключевые слова*: киберэкстремизм, кибертерроризм, электронная информационно-образовательная среда, угроза*

Keywords*: cyberactivism, cyberterrorism, electronic information-educational environment, the threat.*

Электронная информационно-образовательная среда вуза (ЭИОС) – своеобразный полигон, на котором будущие специалисты, в том числе в области информационных технологий, оттачивают свои профессиональные умения. Кроме образовательной нагрузки ЭИОС несет также воспитательную составляющую, связанную с формированием культуры поведения в информационной среде. К сожалению, как и любая система, ЭИОС повергается внутренним и внешним угрозам безопасности, наиболее острый характер из которых носит угроза со стороны молодежного киберэкстремизма и кибертерроризма (КЭиКТ).

Киберэкстремизм - это новая форма экстремизма, использующая для достижения своих целей компьютеры и электронные сети, новейшие коммуникационные технологии Крайним проявлением киберэкстремизма является кибертерроризм. Исследователи М. Дж. Девост, Б. Х. Хьютон, Н. А. Поллард отмечают, что в информационном терроризме (кибертерроризме) соединяются преступное использование информационных систем с помощью мошенничества

или злоупотреблений со свойственным терроризму физическим насилием, и сознательное злоупотребление цифровыми информационными системами, сетями или их компонентами в целях, которые способствуют осуществлению террористических операций или актов. [3].

Появление проблемы КЭиКТ обусловлено становлением и развитием российского экстремизма и терроризма на благоприятном криминогенном фоне, ростом ИКТ-грамотности среди населения, а также особенностями молодежи как возрастной группы. Именно молодежь, т.е. лица 14-30 лет, наиболее подвержена нетерпимости, мыслит характерными для экстремистских взглядов граничными категориями, а также среди всех возрастных групп наиболее быстро осваивает появляющиеся ИКТ и по данным ВЦИОМ составляет около 70% пользователей Интернета.[4]. Студенческая молодежь (17-25 лет) - самая организованная из возможных целевых групп, она сосредоточена в университетах, объединена средствами ЭИОС и наиболее доступна с точки зрения как формирования и распространения идеологии КЭиКТ, так и для профилактической работы в области противодействия КЭиКТ.

Как отмечают ученые, киберэкстремисты используют компьютерные сети для пропаганды своих взглядов, вербовки сообщников, размещения руководств по организации терактов, психологического терроризма, сбора информации о потенциальных объектах шантажа, подготовки террористов, пропаганды расовой, религиозной и других форм нетерпимости[2]. Все эти действия могут быть реализованы средствами ЭИОС. Ярчайший пример такого использования среды – рассылка по локальной сети националистических сообщений из разряда «Россия для русских». Другой пример: замена на всех рабочих станциях локальной сети типового фонового рисунка рабочего стола на изображение, пропагандирующее нетерпимое отношение к иммигрантам. Кибертеррористы могут использовать ресурсы ЭИОС для осуществления терактов в глобальной сети, например, осуществить взлом сайта общественной или коммерческой организации с целью размещения на нем экстремистских материалов.

Угрозы безопасности ЭИОС со стороны КЭиКТ включают в себя:

- потерю функциональности ЭИОС в случаях пропаганды экстремистских взглядов, фальсификации или уничтожения ресурсов ЭИОС (учебных материалов);
- кражу персональных данных пользователей ЭИОС и другой конфиденциальной информации;
- потерю работоспособности ЭОИС в случае, если в качестве интересов кибертеррористов выступает сам университет;
- потерю производительности ЭОИС в случае, если её ресурсы используются для осуществления киберэкстремистских или кибертеррористических актов.

Предотвращение их реализации только техническими мерами не может обеспечить полной безопасности ЭИОС, поскольку при сильной мотивации и высоком профессиональном уровне может быть сломана любая программная защита. Необходимо активно работать с молодежью, ведь, как правило, подобные действия осуществляются студентами, владеющими необходимым набором профессиональных ИТ-компетенций, но не всегда до конца представляющих, какие последствия могут иметь их поступки. Анализ опыта реализации различных программ профилактики и противодействия КЭиКТ показал, что при составлении программ профилактики КЭиКТ редко обращается внимание на необходимость просвещения студентов относительно существующей политики государства в области КЭиКТ [1]. Студенты

должны понимать величину ответственности за свои действия и неизбежность наказания. Иногда безобидная, на первый взгляд, «проба пера» может отрицательно сказаться на профессиональном будущем выпускника.

Таким образом, в целях обеспечения безопасности ЭИОС целесообразно проводить мероприятия по профилактике противодействия КЭиКТ на ранних этапах обучения в университете.

Список литературы

1. *Гаврилова, И.В.* Профилактика киберэкстремизма и кибертерроризма среди будущих специалистов по информационным технологиям // Информационная безопасность и вопросы профилактики киберэкстремизма среди молодежи: сборник статей / под ред. Г.Н. Чусавитиной, Е.В. Черновой. – Магнитогорск: Дом Печати, 2014. – 203 с.

2. *Тамаев, РС.* Уголовно-правовое и криминологическое обеспечение противодействия экстремизму: монография. / Р.С. Тамаев. – М.: ЮНИТИ-ДАНА: Закон и право, 2012

3. *Томас Тимоти Л.* Сдерживание асимметричных террористических угроз, стоящих перед обществом в информационную эпоху // Мировое сообщество против глобализации преступности и терроризма. М., 2002. – С. 165.

4. *Фридинский С.Н*. Молодежный экстремизм как особо опасная форма проявления экстремистской деятельности // Юридический мир. - 2008. - №6 – С. 24.

УДК 004.41

Л.Ф. Ганиева

ПРИМЕНЕНИЕ ПРОЕКТНОГО МЕНЕДЖМЕНТА ПРИ ПРОВЕДЕНИИ МЕРОПРИЯТИЙ ПО ПРОФИЛАКТИКЕ И ПРОТИВОДЕЙСТВИЮ ИДЕОЛОГИИ КИБЕРЭКСТРЕМИЗМА СРЕДИ МОЛОДЕЖИ В ВУЗЕ

Лилия Фанисовна Ганиева

lilit1708_@mail.ru

ФГБОУ ВПО «Магнитогорский государственный технический университет им. Г.И. Носова », Россия, г. Магнитогорск

THE USE OF PROJECT MANAGEMENT ACTIVITIES FOR THE PREVENTION AND TO COUNTER THE IDEOLOGY OF CYBER EXTREMISM AMONG YOUNG PEOPLE IN HIGH SCHOOL

Liliya Fanisovna Ganieva

«Nosov Magnitogorsk State Technical University», Russia, Magnitogorsk

Аннотация*. В статье описывается применение проектного менеджмента при проведении мероприятий по профилактике и противодействию идеологии киберэкстремизма среди молодежи в вузе. Рассматриваются преимущества проектного менеджмента в образовании. Описываются мероприятия в рамках проекта «Неделя киберэкстремизма».*

Abstract. *This article describes the application of project management during implementation of measures for the prevention and countering the ideology of cyberactivism among youth in high*