УДК 004.02

МЕХАНИЗМЫ ЗАЩИТЫ ОБУЧАЮЩИХСЯ ОТ КИБЕРЭКСТРЕМИЗМА В УСЛОВИЯХ РАЗВИТИЯ ОБЛАЧНЫХ ОБРАЗОВАТЕЛЬНЫХ СЕРВИСОВ

Ошурков В.А., Макашова В.Н., Цуприк Л.С.

ФГБОУ ВПО «Магнитогорский государственный технический университет имени Г.И. Носова», Магнитогорск, e-mail: oshurkov92@mail.ru

Актуальность темы обусловлена широким применением современных информационных технологий в образовательных учреждениях и повышением требований к содержанию Интернет-контента. В статье описаны механизмы противодействия различным угрозам, в том числе идеологии киберэкстремизма. Рассмотрены основные механизмы обеспечения информационной безопасности образовательного учреждения (фильтрация и мониторинг) как с точки зрения входящего потока данных, так и исходящего. Даны рекомендации по применению программных продуктов, обеспечивающих информационную безопасность, для различных конфигураций аппаратных средств образовательных учреждений. Затронуты вопросы просвещения учащихся и выявлена проблема недостатка нынешних систем, осуществляющих управление политикой информационной безопасности образовательных учреждений.

Ключевые слова: киберэкстремизм, облачные технологии, информационная безопасность, фильтрация контента

MECHANISMS FOR THE PROTECTION OF STUDENTS FROM CYBER EXTREMISM IN A CLOUD COMPUTING OF EDUCATIONAL SERVICES

Oshurkov V.A., Makashova V.N., Tsuprik L.S.

Nosov Magnitogorsk State Technical University, Magnitogorsk, e-mail: oshurkov92@mail.ru

The widespread use of Internet technologies at educational institutions has created a need for the strict control of the Internet content. The information age has brought to the world, not only the widespread development of technology and computerization of all life, but also led to the emergence of a form of social deviance as cyber crime, which is now gaining wider development. Hacks electronic banking network, propaganda war, extremism on the Internet, attacks on government websites – this is not a complete list of what often turns to states and individuals information age. In its mechanism, methods to commit and conceal such crimes are characterized by high latency, low levels of detection and cause incomparably greater harm than the crime «in the real world» as its purpose have damage and incapacitation of critical infrastructure, information and blackmail perpetrated remotely. The experience that already exists in the international community in this area supposedly shows undeniable vulnerability of any state, especially as cyber terrorism has no borders and age limits. Cyber extremism can be equally threatening information systems located virtually anywhere in the world. How can you resist cyber extremism how to prepare the younger generation to live in a sea of global information and do not drown in it? Consider the basic countermeasures to cyber extremism: the control of the state and society, and countermeasures that are used directly in the educational institutions.

Keywords: cyber extremism, information safety, cloud computing, content filtering

Современные интернет-технологии стали доступными и занимают важное место практически во всех областях человеческой деятельности, включая и образование. Опираясь на опыт развитых зарубежных стран, отличным решением для оптимизации учебного процесса являются облачные технологие, доступ к которым осуществляется через сеть Интернет [5]. Популярный сейчас термин «облачные технологии» стал употребляться в мире с 2008 года. В образовательных учреждениях России облачные сервисы изначально появились в основном как бесплатные хостинги почтовых служб. Другие многочисленные инструменты облачных вычислений для образования практически не использовались в силу недостаточности информации о них и отсутствия практических навыков их использования для учебных целей. Лучший способ подготовки школьников к работе с новейшими технологиями – внедрение этих технологий в образовательный процесс. В результате анализа нам удалось выделить 2 вида облачных образовательных сервисов [4]:

1. Сервисы собственной разработки образовательных учреждений:

1.1. Персональный виртуальный компьютер (далее ПВК). Единая точка доступа к сервисам, формируемая на базе технологии облачных вычислений. Для каждого учащегося создается отдельный персональный виртуальный компьютер с индивидуальным профилем.

1.2. Конструктор нелинейного расписания. С помощью данного модуля педагоги совместно в режиме реального времени могут планировать формы проведения тех или иных занятий с детьми.

2. Существующие сервисы на облачных технологиях:

2.1. Электронный журнал. Является аналогом бумажного журнала с возможностью блокировки полей на исправление по истечении двухнедельного срока.

2.2. Виртуальные уроки, интерактивные совещания, видео- и голосовое общение.

2.3. Сайты классов и групп. Создание сайтов классов и групп для совместного доступа к документам и информации с помощью специализированной программы «SharePoint Online 2010».

2.4. Документы в Интернете. Просмотр, редактирование и совместное использование файлов Microsoft Word в сети с помощью SharePoint и Office Web Apps.

2.5. Планировщик проектов в режиме реального времени позволяет ставить задачи, контролировать ход выполнения и отслеживать динамику во времени.

В результате анализа образовательных сервисов на облачных технологиях можно сказать, что внедрение такого современного инновационного подхода в процесс обучения в высшей и средней школе обеспечит [4]:

1. Снижение затрат и обеспечение гибкости. Все службы работают на удаленных серверах и обслуживаются представителями облачных технологий, что говорит о высокой производительности и снижении затрат.

2. Частичную защищенность данных. На сегодняшний день «облака» обеспечивают два базовых принципа информационной безопасности: целостность данных — защита от сбоев, ведущих к потере информации; конфиденциальность и доступность информации для всех авторизованных пользователей.

3. Эффективное использование учебных площадей. Отпадает необходимость выделять отдельные и специально оборудованные помещения под компьютерные классы.

4. Качественно иной уровень получения современных знаний. Учащиеся получают возможность находиться в процессе обучения в любое время и в любом месте при наличии сети Интернет.

5. Более эффективный интерактивный обучающий процесс.

6. Возможность быстро создавать, адаптировать и тиражировать образовательные сервисы в ходе учебного процесса.

7. Централизованное администрирование программных и информационных ресурсов, используемых в учебном процессе.

8. Максимально эффективное использование имеющихся вычислительных систем, т.к. к облачным сервисам предъявлены минимальные требования к аппаратному обеспечению.

Выделенные достоинства позволяют сделать следующий вывод – образовательные сервисы на облачных технологиях являются огромной перспективой развития образовательного процесса, но есть вероятность уязвимости облачных технологий перед атаками киберэкстремистов. Ведь именно молодежь в наибольшей степени подвержена деструктивному влиянию. Молодежная среда в силу своих социальных характеристик и остроты восприятия окружающей обстановки является той частью общества, в которой наиболее быстро происходит накопление и реализация негативного протестного потенциала. В прошлом году 132 тысячи подростков совершили преступления, свыше 284 тысяч несовершеннолетних милиция поставила на профилактические учеты. По данным 2014 года в России действует 141 молодежная группировка экстремистского характера. А количество преступлений с каждым годом растет [2].

Тенденции развития Интернета позволяют эффективно прогнозировать развитие возможностей киберэкстремистских организаций, разрабатывающих новые формы и методы информационно-психологического воздействия и проводящих их апробацию, что позволяет достаточно быстро и эффективно распространять киберэкстремистские послания. В силу специфики, низкого уровня раскрываемости и отсутствия опыта в защите, в большинстве случаев невозможно вовремя определить киберэкстремистские послания, и учащиеся попадаются на уловки киберэкстремистов.

Для успешного решения проблемы явлений киберэкстремизма в молодежной среде, необходимо четко представлять себе конечные цели. В первую очередь необходимо выделить особенности киберэкстремизма в целях последующего предупреждения:

– киберэкстремизм постоянно подпитывается неопределенностью положения молодого человека и его неустановившимися взглядами на происходящее;

– киберэкстремизм приживается в обществах и группах, где проявляется низкий уровень самоуважения или же условия способствуют игнорированию прав личности;

– данный феномен характерен для общностей не столько с так называемым «низким уровнем культуры», сколько с культурой разорванной, деформированной, не являющей собой целостности.

В целях обеспечения информационной безопасности и, как следствие, ограничения учащихся от киберэкстремистского явления мы предлагаем использовать технические средства защиты (программные, аппаратные и программно-аппаратные комплексы).

Необходимость технических средств защиты диктуется тем, что Интернет – это источник информации, за который никто не несет ответственности, и вероятность получения из него недостоверной, оскорбительной, пиратской или запрещенной по другим причинам информации весьма велика [1].

Рассмотрим основные механизмы технических средств защиты:

1. Защита внешних соединений

Для защиты внешних соединений используется криптографический протокол SSL (Secure Socket Layer) [6]. Этот протокол использует асимметричную криптосистему с открытым ключом. Для осуществления SSL соединения необходимо, чтобы сервер имел инсталлированный цифровой сертификат. Цифровой сертификат – это файл, который уникальным образом идентифицирует пользователей и серверы.

Протокол SSL обеспечивает защищенный обмен данными за счет сочетания двух следующих элементов [6]:

– Аутентификация. Цифровой сертификат привязан к конкретному домену сети Интернет, а центр сертификации проводит проверки, подтверждающие подлинность организации, и уже затем создает и подписывает цифровой сертификат для этой организации.

– Шифрование. Шифрование – это процесс преобразования информации в нечитаемый для всех вид, кроме конкретного получателя. Оно основывается на необходимых для электронной коммерции гарантиях конфиденциальности передачи информации и невозможности ее фальсификации.

Необходимо идентифицировать внешние соединения в целях обеспечения защиты данных от фальсификации и предотвращения следующих явлений:

– «Спуфинг» (имитация соединения). Поддельные сайты, предназначены для получения номера кредитной карты.

– Фальсификация данных. Содержание транзакции может быть перехвачено и злонамеренно либо случайно в процессе передачи изменено.

2. Авторизация через специализированный каталог «Active Directory»

Службы «Active Directory» (службы активного каталога) представляют собой распределенную базу данных, которая содержит все объекты домена [6]. Доменная среда «Active Directory» является единой точкой аутентификации и авторизации пользователей и приложений в масштабах объекта.

Приведем преимущества «Active Directory», которые позволят защитить образовательное учреждение от киберэкстремистских атак [6]:

– Единая точка аутентификации. При использовании «Active Directory» все учетные записи пользователей хранятся в одной базе данных, и все компьютеры обращаются к ней за авторизацией.

– Единая точка управления политиками. При использовании единого каталога «Active Directory» все пользователи и компьютеры иерархически распределяются по организационным подразделениям, к каждому из которых применяются единые групповые политики.

– Повышенный уровень информационной безопасности. Использование служб «Active Directory» значительно повышает уровень безопасности сети за счет единого и защищенного хранилища учетных записей и использования безопасного протокола аутентификации «Kerberos».

– Интеграция с классами и кафедрами, приложениями и оборудованием. «Active Directory» соответствует стандарту LDAP, который поддерживается другими системами.

3. Мониторинг и анализ сетевого трафика при помощи специализированного программного обеспечения

Мониторинг и анализ сетевого трафика необходимы для того, чтобы более эффективно диагностировать, предугадать и решать проблемы киберэкстремизма [3]. На сегодняшний день доступно много различных инструментов, которые позволяют помочь администраторам и обычным пользователям с мониторингом и анализом сетевого трафика.

Для анализа и мониторинга сети используются специальные протоколы и утилиты. Однако не все они информативны с точки зрения имеющихся в их арсенале возможностей по анализу. Опытные специалисты выделяют программу «WireShark», которая имеет достаточно аналитических возможностей, а также может работать в разных операционных системах [3].

4. Контроль действий пользователя в сети и фильтрация контента на предмет киберэкстремистских посланий

Системы мониторинга и анализа действий пользователей позволяют отследить передачу конфиденциальной информации за пределы организации по различным каналам и с использованием различных приложений [8]. Вместе с тем основной функцией таких систем является детальное протоколирование действий пользователей.

Существует ряд программных продуктов мониторинга и анализа действий пользователей, основными функциями которых являются: отслеживание общения пользователя в сети образовательного учреждения и того, какими приложениями, сетевыми сервисами, социальными сетями они пользовались; протоколирование и анализ содержимого общений или переписок; поддерживание отслеживания действий пользователей различными способами общения, в том числе общения голосом; формирование картины рабочего дня пользователя; предоставление отчетов об активности пользователей различной степени детализации.

Результат применения решения позволит достичь следующих преимуществ: снижение рисков утечки конфиденциальной информации; мониторинг и запись действий пользователей, их коммуникаций и, как следствие, обнаружение и пресечение киберэкстремистских посланий; поддержка и анализ различных форматов представления данных.

Вторая проблема – это некомпетентность учащихся, преподавателей в вопросах киберэкстремизма и информационной безопасности.

«Администраторы в школах имеют различный опыт работы с компьютерами, и даже непрофессионал должен иметь возможность создавать и поддерживать политику фильтрации. Образовательный процесс включает множество различных областей науки, и фильтрация должна быть всеобъемлющей, настраиваемой, а также обеспечивать защиту от новейших угроз» [1].

Мы предлагаем проведение следующих организационных мер для повышения компетенции учащихся и преподавателей в вопросах киберэкстремизма и информационной безопасности:

– проведение презентаций, организация бесед по повышению знаний учащихся и преподавателей в области киберэкстремизма;

– пресечение фактов распространения кибератериалов, содержащих призывы к социальной, расовой, национальной и религиозной розни, а также экстремистской литературы;

– осуществление последовательных действий по выявлению и применению установленных законом мер к лицам, причастным к киберэкстремистской деятельности.

Благодаря применению механизмов технических средств защиты и организационных мер можно не только обеспечить безопасное подключение для передачи данных, контролировать работу и деятельность учащихся, отслеживая посещаемость Интернет-ресурсов, но и выявить и предотвратить факты распространения в облачных образовательных сервисах материалов киберэкстремистского характера. Все это позволит оградить обучающихся от нежелательного контента, тем самым препятствовать негативному развитию учащихся.

Публикация выполнена в рамках работы над проектом РГНФ № 13-06-00156 «Подготовка педагогических кадров к профилактике и противодействию идеологии киберэкстремизма среди молодежи».

Список литературы

1. Макашова В.Н. Механизмы противодействия киберэкстремизму и кибертерроризму в системе образования [интернет портал]. URL: http://www.rae.ru/fs/?section=content&op=show_article&article_id=10001809.

2. Молодежный экстремизм: состояние, тенденции и проблемы реагирования [интернет портал]. URL: www.nbrkomi.ru/dabook/47731/Информационный%20список.pdf.xml.

3. Мониторинг и анализ сетевого трафика при помощи специализированного программного обеспечения [интернет портал]. URL: http://it-bloknot.ru/.

4. Облачные технологии как инструмент организации учебного процесса в российских вузах [интернет портал]. URL: http://cyberleninka.ru/article/n/oblachnye-tehnologii-kak-instrument-organizatsii-uchebnogo-protsessa-v-rossiyskih-vuzah.

5. Ошурков В.А., Макашова В.Н. Механизмы оптимизации управления программой ИТ-проектов [интернет портал]. URL: http://www.sworld.com.ua/konfer34/280.pdf.

6. Протокол SSL [интернет портал]. URL: http://www.inssl.com/about-ssl-protocol.html%20.

7. Сторожева Е.В., Валеев А.С., Кружилина Т.В., Сергеев А.Н. Моделирование процесса формирования экономической грамотности студентов в структуре дополнительного образования вуза [интернет портал]. URL: http://elibrary.ru/item.asp?id=18319444.

8. Фильтрация контента [интернет портал]. URL: http://www.microtest.ru/it-infrastruktura/informacyonnaya-bezopasnost/1055/.

9. Чернова Е.В. Компетенции педагогических кадров в области превенции идеологии киберэкстремизма среди молодежи [интернет портал]. URL: http://www.rae.ru/fs/?section=content&op=show_article&article_id=10001813.

References

1. Chernova E.V. Competence of teachers in the field of ideology cyber extremism prevention among young people [Internet portal]. URL: http://www.rae.ru/fs/?section=content&op=show_article&article_id=10001813.

2. Cloud technology as a tool for organizing the learning process in the Russian universities [Internet portal]. URL: http://cyberleninka.ru/article/n/oblachnye-tehnologii-kak-instrument-organizatsii-uchebnogo-protsessa-v-rossiyskih-vuzah.

3. Content filtering [Internet portal]. URL: http://www.microtest.ru/it-infrastruktura/informacyonnaya-bezopasnost/1055/.

4. Makashova V.N. Mechanisms to counter cyber extremism and cyber terrorism in the education system [Internet portal]. URL: http://www.rae.ru/fs/?section=content&op=show_article&article_id=10001809.

5. Monitoring and analysis of network traffic using specialized software [Internet portal]. URL: http://it-bloknot.ru/.

6. Oshurkov V.A., Makashova V.N. Mechanisms to optimize program management of IT-projects [Internet portal]. URL: http://www.sworld.com.ua/konfer34/280.pdf.

7. Protocol SSL [Internet portal]. URL: http://www.inssl.com/about-ssl-protocol.html%20.

8. Storozheva E.V., Valeev A.S., Kruzhilina T.V., Sergeev A.N. Modeling of the process of formation of economic literacy of students in the structure of additional education university [Internet portal]. URL: http://elibrary.ru/item.asp?id=18319444.

9. Youth extremism: Status, Trends and Challenges response [Internet portal]. URL: www.nbrkomi.ru/dabook/47731/Информационный%20список.pdf.xml.

Рецензенты:

Мусийчук М.В., д.ф.н., профессор кафедры психологии, ФГБОУ ВПО «Магнитогорский государственный технический университет им. Г.И. Носова», г. Магнитогорск;

Савва Л.И., д.п.н., профессор кафедры педагогики профессионального образования, ФГБОУ ВПО «Магнитогорский государственный технический университет им. Г.И. Носова», г. Магнитогорск.

Работа поступила в редакцию 19.12.2014.