УДК 004.02

МЕХАНИЗМЫ ПРОТИВОДЕЙСТВИЯ ЯВЛЕНИЙ КИБЕРЭКСТРЕМИСТСКОЙ НАПРАВЛЕННОСТИ В СИСТЕМЕ ЭЛЕКТРОННЫХ ПЛАТЕЖЕЙ

Ошурков В.А., Чернова Е.В., Сторожева Е.В., Давлеткиреева Л.З.

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

Проведен анализ состояния проблемы распространения идей экстремистской направленности в системе электронных платежных систем посредством использования современных коммуникативных технологий. Рассмотрено специфическое проявление девиантного поведения – киберэкстремизм, его виды и особенности. В статье предлагается форма предупреждения вовлечения пользователей сервисов электронных платежных систем в киберэкстремистскую деятельность. В силу специфики, низкого уровня раскрываемости и отсутствия опыта в защите сервисов электронных платежных систем в большинстве случаев невозможно определить киберэкстремистские послания, и пользователи электронных платежных систем попадаются на уловки киберэкстремистов. Для этого нами был проведен анализ и выявлены пути наиболее актуального и значимого решения поставленной задачи. Механизмы превенции (на техническом уровне) явлений киберэкстремизма являются основополагающим фактором защиты работы платежных электронных систем и, как следствие, благополучной работы пользователей этих сервисов.

Ключевые слова: киберэкстремизм, облачные технологии, информационная безопасность, электронные платежные системы

MECHANISMS FOR COMBATING PHENOMEN CYBER EXTREMISM ORIENTATION IN THE E-COMMERCE PAYMENT SYSTEM

Oshurkov V.A., Chernova E.V., Storozheva E.V., Davletkireeva L.Z.

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

The analysis of the proliferation of extremist ideas in the electronic payment systems through the use of modern communication technologies. Considered a specific manifestation of deviant behavior – cyber extremism, its types and features. The article suggests a form of prevention involving service users of electronic payment systems in cyber extremism activities. Because of the specificity of detection of low level and lack of experience in the defense services of electronic payment systems, in most cases it is impossible to determine cyber extremism messages, and users of electronic payment systems across the tricks cyber extremists. To do this, we have analyzed and identified ways the most relevant and meaningful for the task. Prevention mechanisms (at the technical level) phenomena cyber extremism are fundamental to the protection of the payment of electronic systems and, as a consequence of a happy user experience of those services.

Keywords: cyber extremism, information safety, cloud computing, e-commerce payment system

На сегодняшний день, особенно в условиях прогрессивно развивающихся информационных технологий, значительную долю в общем объеме уголовных преступлений начинает занимать преступность, связанная с использованием информационных технологий. Ее росту и развитию способствует сама природа данного вида преступлений, в частности, базирующаяся на открытом и общедоступном характере сети Интернет и, как говорят эксперты, на «безнаказанности правонарушителей, связанной с вопросами юрисдикции, а также еще недостаточной подготовкой правоохранительных органов по вопросам расследования таких преступлений» [3].

Согласно данным научно-исследовательского института обороны Норвегии в прошедшем десятилетии многочисленные террористические организации активно осваивали Интернет для вербовки новых сторонников и распространения пропагандистских материалов. Виртуальное пространство неоднократно использовалось такими группировками, как «Аль-Каида», для устрашения предполагаемого противника. Определить реальное количество подобного контента сложно, так как чаще всего сторонний наблюдатель не осознает, что отдельная информация в Интернете имеет экстремистский подтекст. Киберэкстремизм – «ориентация в политике на крайне радикальные идеи и цели, использующая в качестве основного инструмента кибертехнологии» [6]. Основной целью киберэкстремистов является получение желаемого эффекта посредством целенаправленного и продуманного внушения собственных идеологий. «Особенность такого явления заключается в сложном контроле огромной информационной Сети, посредством которой общества киберэкстремистской направленности с молниеносной скоростью находят своих сторонников и по-

лучают активную поддержку. Несмотря на многочисленные попытки, предпринимаемые на различных уровнях, от владельцев сайтов до правительств различных государств – поставить распространение данных явлений в Интернет под контроль, на сегодняшний день нельзя говорить о безоговорочном успехе» [11].

К оружию киберэкстремиста можно отнести как компьютерные вирусы, так и программные закладки, особенно фишинговые веб-ресурсы, сообщества в социальных сетях, статьи, носящие киберэкстремистский характер, разнообразные виды атак, которые делают возможным несанкционированный доступ к компьютерной системе. С развитием информационных технологий, у современных компьютерных преступников появляются новые инструменты, и «процесс распространения киберэкстремистских идеологий, преступлений продолжается» [11].

По результатам исследования корпорации «Symantec», специализирующейся на обеспечении безопасности и хранения данных, можно сказать, что число жертв кибератак среди взрослого населения в мире снизилось, среди молодежи – повысилось, средний ущерб из расчета на одного потерпевшего увеличился на 50%. Потери на каждого потерпевшего составили в среднем $287, в том числе [2]: 85% россиян сталкивались с киберпреступлениями; 59% пользователей интернета были подвержены «разводам» на деньги киберэкстремистами; 56% пользователей интернет в России не знают о существовании решений для их безопасности.

Каждая киберэкстремистская атака наносит колоссальный финансовый ущерб организации в среднем на сумму в $695 тысяч. Компании среднего и малого бизнеса теряют около $14 тысяч за один киберинцидент. Такие выводы сделаны в совместном исследовании компании «B2B International» и «Лаборатории Касперского» [1].

Примечательно, что в 2013 году увеличилась доля атак с использованием фальшивых страниц социальных сетей и составила 35,39% от общей доли фишинговых атак в 2013 году, где [1]: на финансовые сервисы – 31,45%; на электронную почту – 31,45%; на онлайн игры – 2,33%; другое – 7,53%. Увеличилась доля финансовых атак на электронные платежные системы [1] на 2,74%, в том числе на следующие финансовые институты: на банки – 22,2%; на интернет-магазины – 6,51%.

Увеличение доли атак на электронные платежные системы и современные условия подтолкнули финансовые институты к поиску новых решений в области защиты электронных платежных систем. Одним из набирающих популярность инструментов стали специализированные облачные технологии. Электронные платежи на основе облачных технологий позволяют обеспечить наилучшую безопасность при верификации и проведении транзакций, не полагаясь на аппаратную систему безопасности.

В результате проведенного анализа нами была построена модель взаимосвязи между облачными технологиями, электронными платежными системами и обществом киберэкстремистской направленности (рисунок). Выделим объекты, которые подвергаются нападению киберэкстремистского сообщества:

1. Пользователь электронной платежной системы.

2. Электронная платежная система.

Опираясь на данные специалистов по вопросам киберэкстремизма, а также на результаты, полученные в ходе обобщения и анализа существующего опыта, мы выделили два основных направления киберэкстремистской деятельности в сети Интернет:

1. Пропаганда.

2. Пополнение финансовых активов.

Рассмотрим подробно выделенные направления киберэкстремистской деятельности в сети Интернет:

I. Пропаганда – «организованное и целенаправленное распространение идей, мнений, утверждений, символов и слухов через СМИ и по другим каналам общественной коммуникации». Различают позитивные и негативные виды пропаганды [4].

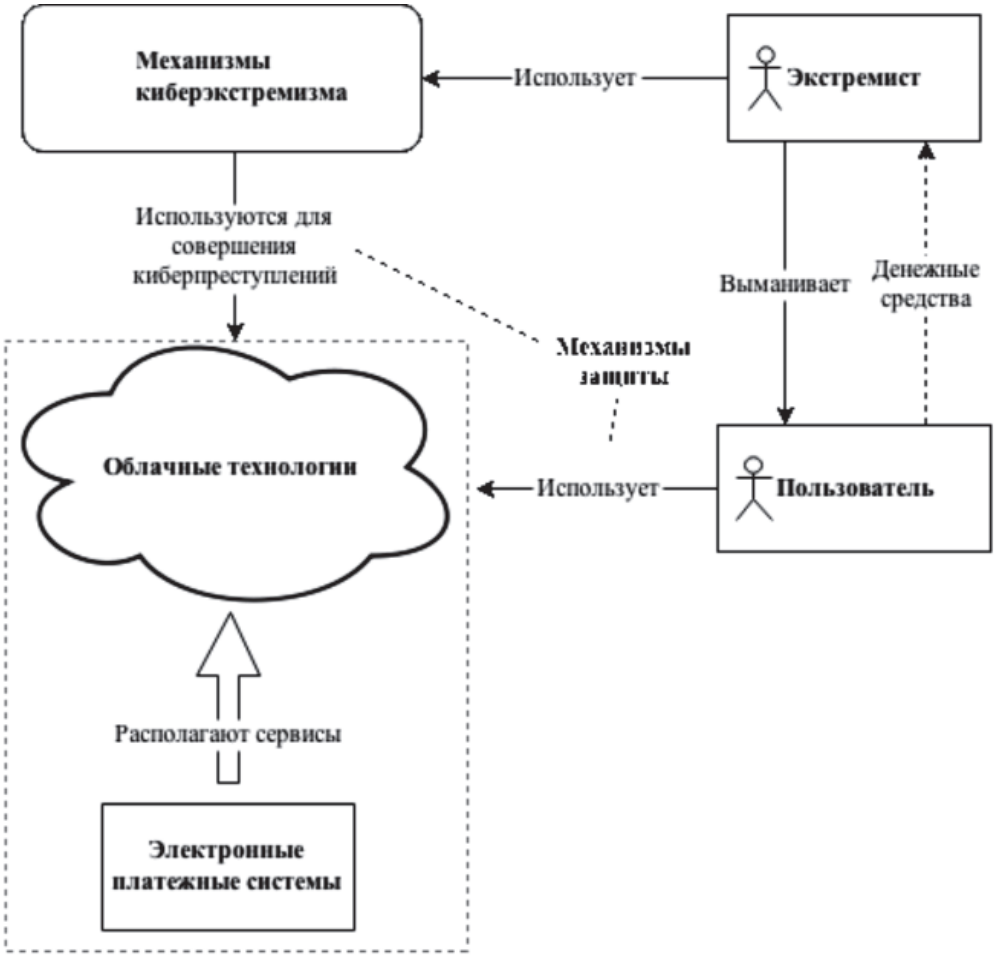
Основными орудиями любой пропаганды в современном мире являются СМИ, фишинговые веб-ресурсы, сообщества в социальных сетях и статьи, носящие киберэкстремистский характер.

Пропаганда – действенное оружие в руках киберэкстремиста, при правильном применении можно легко внушить человеку ложное видение, которое впоследствии сложно искоренить. Мы считаем, что «надежным фактором защиты электронных платежей пользователей является экономическая грамотность» [9].

II. Под пополнением финансовых активов будем понимать выманивание денежных средств пользователей путем применения экстремистами киберэкстремистских механизмов.

Основным инструментом пополнения финансовых активов киберэкстремиста является «Фишинг». «Фишинг» (поддельный сайт) – это сетевое мошенничество. Фишеры – это технически подкованные жулики и воры, иначе говоря киберэкстремисты.

С помощью спама (чаще всего фишеры используют эмоциональные выражения, пытаясь напугать или взволновать пользователя и заставить сразу же ответить на письмо), вредоносных веб-ресурсов, почтовых и мгновенных сообщений они выманивают у пользователей конфиденциальную информацию [10].



Модель взаимосвязи между облачными технологиями, электронными платежными системами и обществом киберэкстремистской направленности

Приведем наиболее распространенные характеристики, свойственные фальшивым электронным сообщениям [10]:

– Использование наименований существующих компаний. Имитация корпоративного сайта существующей компании в целях получения доверия получателей.

– Использование имени реального сотрудника компании в качестве отправителя фальшивого сообщения.

– Ложные веб-адреса. Фальшивые электронные веб-сайты, имитирующие внешний вид официального ресурса компании, которая используется в качестве приманки.

– Фактор страха. Возможность обмана пользователей для мошенников краткосрочна, поскольку как только компания получает информацию о том, что ее клиенты стали жертвами подобных технологий, сервер, на котором расположен фальшивый вебсайт, отключают в течение нескольких дней. Таким образом, для мошенников особенно важно получить от пользователя немедленный отклик.

В результате изучения выделенных нами направлений киберэкстремистской деятельности в сети Интернет был получен материал, после анализа которого мы можем предложить механизмы предупреждения действий киберэкстремистских групп на техническом уровне. Технические меры защиты основаны на использовании

различных электронных устройств и специальных программ, выполняющих функции защиты.

1. Закрытый доступ к данным.

Закрытый доступ к данным – это улучшение качества и обеспечение целостности данных посредством безопасного доступа к общим ресурсам данных в коллективной рабочей области. При этом необходимо обеспечить надежное управление ключами шифрования, так как в нем хранится секретная информация, используемая криптографическим алгоритмом при шифровании/расшифровке сообщений, постановке и проверке цифровой подписи, вычислении кодов аутентичности. При использовании одного и того же алгоритма результат шифрования зависит от ключа. Надежность криптографической системы должна определяться сокрытием секретных ключей, но не сокрытием используемых алгоритмов или их особенностей. Конфиденциальность и защита информации при ее передаче по каналам связи должна обеспечиваться также за счет применения в системе шифросредств абонентского шифрования: формирование и проверка электронной цифровой подписи, обеспечивающие целостность и юридически доказательное подтверждение подлинности сообщений, а также аутентификацию пользователей, абонентских пунктов и подтверждение времени отправления сообщений.

2. Политики доступа.

Политики доступа подразумевают собой совокупность норм, правил и практических рекомендаций, регламентирующих работу средств защиты облачных технологий от множества угроз, в том числе и киберэкстремизма. Только авторизированные пользователи должны иметь доступ к конфиденциальной информации. Запросы о предоставлении конфиденциальной информации посредством электронной почты или мгновенных сообщений.

Для реализации перечисленных механизмов предупреждения киберэкстремизма необходимо соблюдать следующие правила:

– определить роли и обязанности должностных лиц, отвечающих за проведение политики безопасности информации;

– определить тех, кто имеет права доступа к информации ограниченного распространения, кто и при каких условиях может читать и модифицировать информацию;

– предусматривать регламент информационных отношений, исключающих возможность произвольных, монопольных или несанкционированных действий в отношении информационных ресурсов;

– определять коалиционные и иерархические принципы и методы разделения секретов и разграничения доступа к информации ограниченного распространения;

– регистрация всех действий пользователя в защищенном журнале, наличие нескольких уровней регистрации;

– выбирать программно-технические (аппаратные) средства криптозащиты, противодействия НСД, аутентификации, авторизации, идентификации и других защитных механизмов, обеспечивающих гарантии реализации прав и ответственности субъектов информационных отношений.

3. Электронная интеллектуальная система распознавания и расшифровки текстов.

Электронная интеллектуальная система распознавания и расшифровки текстов на предмет наличия киберэкстремистских посланий, интеллектуальные системы защиты от спама, интеллектуальные системы сбора и систематизации информации о поведении пользователей позволят накопить базу знаний для последующего использования и распространения, что позволит избежать киберэкстремистских атак, появления фишинговых веб-ресурсов и оградить пользователей электронных платежных систем от киберпреступников.

Таким образом, в условиях глобальной информатизации общества возрастают угрозы проявления киберэкстремизма. В силу специфики, низкого уровня раскрываемости и отсутствия опыта в защите сервисов электронных платежных систем, в большинстве случаев невозможно определить киберэкстремистские послания, и пользователи Интернета попадаются на уловки киберэкстремистов. Во избежание этого нами были разработаны механизмы предупреждения явлений киберэкстремистской направленности, являющиеся основополагающим фактором защиты работы платежных электронных систем и, как следствие, благополучной работы пользователей этих сервисов.

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. CNews: За год 95% российских компаний подверглись кибератакам [интернет портал]. URL: http://www.cnews.ru/news/top/index.shtml?2013/09/25/544215.

2. Исследования корпорации «Symantec» [интернет портал]. URL: http://go.symantec.com/norton-report-2013.

3. Киберпреступность – угрозы и прогнозы [интернет портал]. URL: http://hack-articles.org/item/74.

4. Киселев М.В. Психология пропаганды [интернет портал]. URL: http://psyfactor.org/propaganda5.htm.

5. 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.

6. Мырза М.В. Молодежный киберэкстремизм как девиация поведения в сфере ИКТ [интернет портал]. URL: http://www.sworld.com.ua/konfer33/859.pdf.

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

8. Сороченко В.А. Энциклопедия методов пропаганды [интернет портал]. URL: http://psyfactor.org/propaganda.htm.

9. 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.

10. Фишинг [интернет портал]. URL: http://ru.norton.com/security_response/phishing.jsp.

11. 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. CNews: During the year 95% of Russian companies have been cyberattacks [Internet portal]. URL: http://www.cnews.ru/news/top/index.shtml?2013/09/25/544215.

3. Cybercrime – threats and projections [Internet portal]. URL: http://hack-articles.org/item/74.

4. Kiselev M.V. Psychology propaganda [Internet portal]. URL: http://psyfactor.org/propaganda5.htm.

5. Makashova VN 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.

6. Mirza M.V. Youth cyber extremism as a deviation behavior in ICT [Internet portal]. URL: http://www.sworld.com.ua/konfer33/859.pdf.

7. 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.

8. Phishing [Internet portal]. URL: http://ru.norton.com/security_response/phishing.jsp

9. Research corporation «Symantec» [Internet portal]. URL: http://go.symantec.com/norton-report-2013.

10. Sorochenko V.A. Encyclopedia of methods to promote [Internet portal]. URL: http://psyfactor.org/propaganda.htm.

11. 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.

Рецензенты:

Назарова О.Л., д.п.н., профессор, проректор по учебной работе, 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.