Confidential

RUSSIA

The circulation of this report has been strictly limited to the members of the *Trialogue* Club International and of the Centre russe d'études politiques.

This issue is for your personal use only.

Published monthly in Russian and in English by *Trialogue Company Ltd.*

Issue № 10, vol.1. October 2011.

15 октября 2011 г.

Олег Демидов, Владимир Орлов сообщают из Москвы:

КИБЕРПРЕСТУПНОСТЬ В РЯДУ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Боевые действия и массированные атаки в киберпространстве окончательно перешли из разряда медийных спекуляций и псевдонаучной фантастики в категорию острейших перспективных вызовов международной безопасности. Войны XXI в. из привычной реальности постепенно и неуклонно распространяются в информационное и космическое пространства. В интернете полноценные войны пока не развернулись, однако последние события (*Stuxnet*, *Shady RAT*, акции *LulzSecurity*) говорят о том, что эти события вероятны уже в самом ближайшем будущем.

Значительная часть угроз безопасности киберпространству в России сегодня связана с экономическими преступлениями. Неэффективно осуществляется защита персональных данных: данные россиян, пользующихся американскими или зарегистрированными в США социальными сетями, оказываются за пределами России, причем не только в США, но и в процессинговых центрах развивающихся стран.

Другим немаловажным аспектом проблемы, год от года приобретающим растущий размах, стал кибершпионаж. Одним из наиболее частых и наиболее востребованным объектом атак становятся госструктуры США. Наше недавнее общение с американскими конгрессменами показало, что для них эта угроза становится вровень с угрозой ядерного распространения. Для РФ этот вызов пока стоит не столь остро, однако число атак на сайты российских госструктур неуклонно растет – как и их уровень.

Вирусные атаки со стороны технологически *продвинутых* террористических организаций, а также атаки, санкционированные государствами, — один из самых опасных сюжетов скорого будущего. Атака, осуществленная в прошлом году с помощью компьютерного червя *Stuxnet* против промышленных систем целого ряда стран по своей эффективности сравнима с военной операцией. Подобная атака в отношении России может оказать крайне негативное

воздействие на национальную экономику, если не будут разработаны эффективные меры противодействия.

БОРЬБА С КИБЕРТЕРРОРИЗМОМ: ПРОБЛЕМА НОРМАТИВНОГО РЕГУЛИРОВАНИЯ

В таком контексте становится очевидно, что России необходим системный курс по противодействию высокотехнологичному терроризму, и прежде всего кибертерроризму. Именно кибертерроризм в ближайшие годы станет одной из наиболее острых проблем для ряда государств, включая Россию.

На данный момент проблематика противодействия кибертерроризму еще не нашла полного отражения в доктринальных документах РФ. Кибертерроризм не упоминается напрямую ни в Концепции внешней политики Российской Федерации от 28 июня 2000 г., ни в Военной доктрине РФ от 5 февраля 2010 г. В Стратегии национальной безопасности Российской Федерации до 2020 г. от 12 мая 2009 г. «совершенствование форм противоправной деятельности в кибернетической и биологической областях, в сфере высоких технологий» лишь отмечается в качестве перспективной угрозы, не сопровождаясь какой-либо конкретикой в части мер противодействия.

На национальном уровне противодействие кибертерроризму в РФ регулируется отдельными правовыми актами, не составляющими целостной политико-правовой концепции. 12 мая 2004 г. был подписан Указ Президента России № 611 «О мерах по обеспечению информационной безопасности Российской Федерации в сфере международного информационного обмена». Указ запрещает госорганам использовать интернет без средств защиты и регламентирует ответственность спецслужб за обеспечение безопасного использования Всемирной Сети. Указ направлен прежде всего на обеспечение защиты сетевых ресурсов российских госорганов от внешних угроз несанкционированного воздействия.

РФ также не является участником наиболее известного и комплексного международно-правового акта, регулирующего вопросы противодействия кибертерроризму на межгосударственном уровне – Конвенции Совета Европы «О киберпреступности», подписанной 23 ноября 2001 г. в Будапеште. Несмотря на то, что Конвенция носит открытый характер, РФ, в отличие от 43 государств-членов Совета Европы и 15 других стран, в конечном счете отказалась присоединиться к ней. Распоряжение Президента РФ от 15 ноября 2005 г. «О подписании Конвенции о киберпреступности» санкционировало присоединение РФ к Конвенции, однако на условиях пересмотра положений статьи Конвенции №32, пункта b. Пункт, вызывающий у российской стороны принципиальное несогласие, предполагает санкционированный доступ уполномоченных органов одного государства-участника к компьютерным данным, хранящимся на территории другого государства, без предварительного получения согласия последнего.

22 марта 2008 г. вступило в силу распоряжение президента РФ, в соответствии с которым распоряжение 2005 г. признано утратившим силу. С тех пор Россия не проявляла интереса к конвенции Совета Европы, сосредоточившись на продвижении собственных инициатив в области противодействия кибертерроризму. Как заявил в ноябре 2010 г. чиновник Росфинмониторинга Павел Ливадный, «РФ продвигает подход, предусматривающий разработку глобальной конвенции по борьбе с преступлениями в информационной сфере».

Значительное внимание в последние три-четыре года РФ уделяет продвижению проблематики кибертерроризма (и киберпреступности в целом) через каналы ООН. Инициатива и предложение РФ лежали в основе решения Комиссии ООН по противодействию преступности и уголовному правосудию об учреждении открытой межправительственной группы экспертов для всеобъемлющего изучения проблем киберпреступности, принятому в мае 2010 г. Одной из приоритетных целей деятельности группы является выработка и формирование предложений по совершенствованию международно-правового измерения борьбы с киберпреступностью и кибертерроризмом. На 65-й сессии Генеральной ассамблеи в июле 2010 г. был представлен доклад Генеральному секретарю ООН по вопросам информационной безопасности, подготовленный группой правительственных экспертов из 15 стран, которую возглавлял замдиректора ДНВ МИД России Андрей Крутских. Единогласно принятый Генассамблеей ООН доклад, который заостряет внимание на необходимости выработки общих подходов в отражении киберугроз и борьбе с киберпреступностью (а также кибертерроризмом), стал прорывом после малорезультативной работы группы с момента ее основания в 2005 г.

Однако амбициозность и всеобъемлющий характер российских предложений, регулирующих в том числе вопросы агрессивного поведения государств в киберпространстве, пока не позволяют продвинуть их на глобальном уровне. Ни ООН, ни ключевые державы на данный момент не склонны воспринимать российские проекты регулирования киберпространства как руководство к действию – что может печально сказаться на судьбе последнего российского проекта Конвенции ООН об обеспечении международной информационной безопасности, о котором стало известно в конце сентября 2011 г.. В Москве осознают эти риски. Не случайно в последние годы со стороны РФ резко вырос интерес к региональным форматам сотрудничества (таким как БРИКС, ШОС и ОДКБ) как альтернативным площадкам для продвижения инициатив по регулированию киберпространства.

На неформальном саммите ОДКБ в Астане генеральный секретарь Организации Николай Бордюжа заявил о том, что к декабрю 2011 г. ОДКБ планирует разработать системный подход по противодействию угрозе кибертерроризма, назвав работу по информационному противодействию одним из приоритетов Организации. Тема противодействия кибертерроризму с подачи РФ также возведена в ранг ключевых приоритетов ШОС. 2 июня 2011 г. вступило в силу межправительственное соглашение государств-членов ШОС о сотрудничестве в области обеспечения международной информационной безопасности, подписанное 16 июня 2009 г. в Екатеринбурге. 12 сентября 2011 г. 4 страны-члена ШОС (РФ, Узбекистан, Кыргызстан, Китай) направили Генеральному Секретарю ООН обращение с проектом кодекса, регулирующего поведение государств в информационном пространстве, включая предотвращение кибервойн и кибертерроризма.

Проблематика кибертерроризма не входит в первоочередную повестку такого формата как БРИКС, но Россия активно пытается использовать и эту площадку. По данным источников ПИР-Центра, в 2009-2011 гг. РФ лоббировала по линии БРИКС (прежде всего ЮАР и КНР) инициативу создания альтернативного международно-правового документа, регулирующего противодействие киберпреступности и кибертерроризму. На 2011 г. данная инициатива так и не получила развития, в основном из-за отсутствия поддержки в рядах самой БРИКС. Тем не менее, в настоящее время тема кибертерроризма все активнее педалируется в рамках БРИКС, пусть и на декларативном уровне. В итоговой декларации саммита БРИКС от 14 апреля 2011 г. в пункте о противодействии

терроризму говорится о приверженности сторон «сотрудничеству в укреплении международной информационной безопасности» и необходимости «уделить особое внимание борьбе с киберпреступностью».

ИДЕНТИФИКАЦИЯ ПОЛЬЗОВАТЕЛЕЙ - ПРОБЛЕМА №1?

Однако, возможно, ключевой для России проблемой, связанной с обеспечением безопасности киберпространства, на сегодняшний день является идентификация интернет-пользователей, которая в свою очередь, входит в более широкую проблематику идентификации пользователей в Сети как таковой. Ситуация, когда пользователь может с легкостью обойти существующие средства идентификации, открывает возможности для кибермошенничества, размещения общественно опасного и неприемлемого контента, проявлений экстремизма и социальной агрессии в Сети, что недопустимо для РФ.

Уже сейчас эта тема включается в рабочую повестку российских структур, в ведении которых находятся вопросы национальной безопасности. Согласно нашему источнику в СБ РФ, «в последнее время в повестке Совета стало уделяться внимание проблеме терроризма в социальных сетях». Корни проблемы во многом уходят в максимально свободный (до июня 2011 г.) режим регистрации пользователей *ВКонтакте*. До сих пор эта социальная сеть выдает сотни и тысячи результатов в поиске страниц, групп, заметок и видео с призывами к «джихаду против неверных», построению «имарата кавказ», бунту мусульманского населения РФ против «федералов» и т.д. В свою очередь, обилие неприемлемого контента объясняется тем, что установить личность юзера, выложившего материал в сеть, практически невозможно. Результатом становится огромное количество профилей «моджахедов», «воинов ислама», немыслимых для *Facebook* или *Google+*. Даже наполняя подобный профиль некоторым количеством личной информации, пользователи знают, что останутся безнаказанными, если только лично ими не заинтересуется ФСБ – что крайне маловероятно по понятной причине: за всеми не уследишь. Еще одна сторона проблемы состоит в том, что не так давно – 26 января 2011 г. –*ВКонтакте* удалось выиграть в суде во многом прецедентное дело, связанное с размещением в сети контента, нарушающего права правообладателя. Однако согласие суда с доводами представителей социальной сети, что ответственность за размещаемые материалы лежит на пользователях, лишь дает зеленый свет дальнейшим нарушениям подобного рода со стороны *де-факто анонимных* пользователей.

Между тем, сами социальные сети в России пытаются решать проблему идентификации пользователей исходя из собственной логики, далеко не всегда успешной. С 11 июля 2011 г. *ВКонтакте.ру* ввела процедуру регистрации пользователей по номерам мобильных телефонов, избрав компромиссный вариант между закрытой системой регистрации и открытой, имевшей место ранее. Привязка аккаунта пользователя к номеру мобильного довольно эффективна в том случае, когда пользователь является гражданином РФ, где мобильный номер (промежуточная ступень идентичности) приобретается по паспорту. Но стать полностью успешным такому способу идентификации мешает трансграничность *ВКонтакте*, характерная для любой крупной социальной сети. Около 40 млн. аккаунтов в сети Павла Дурова зарегистрированы за пределами РФ, а значит, их хозяева приобретают мобильные номера в соответствии с зарубежным законодательством.

По данным на начало апреля 2011 г. *ВКонтакте* насчитывалось 16,5 млн. аккаунтов пользователей из Украины, где мобильные номера не привязаны к

документам, удостоверяющим личность владельца. В странах Европы, таких как Испания, мобильные номера вообще не закреплены за тем или иным провайдером сотовой связи. В результате, идентификация 30% пользователей соцсети оказывается полностью фиктивной. Таким образом, избранный *ВКонтакте* подход (который могут взять на вооружение и другие сети), недостаточно эффективен и должен дополняться решениями, которые покрывали бы перечисленные *серые зоны*.

Одним из таких решений может стать привязка аккаунта в социальных сетях к банковскому счету пользователя, вариантом которой можно считать распространение на социальные сети правил электронных платежных систем, таких как *PayPal*, *Webmoney*, *Яндекс.Деньги* и другие. Преимуществом такого решения стала бы высокая надежность идентификации и ценность аккаунта в глазах пользователя (особенно если в Пользовательское соглашение с соцсетью будет включен пункт о заморозке определенной суммы на счете в случае нарушения его положений). Однако в настоящее время реализацию этой идеи тормозят ее две серьезные уязвимости.

Во-первых, охват пользовательской аудитории в данном случае будет опять же неполным. По информации на март 2011 г., банковские счета имеют лишь 47% россиян, хотя среди молодежи, которая составляет костяк аудитории социальных сетей, этот процент существенно выше. Кроме того, неясно, каким образом удастся выстроить сотрудничество социальных сетей с зарубежными банками, не ведущими деятельность в РФ. *Во-вторых*, увязка аккаунта с банковским счетом может встретить сопротивление самих социальных сетей и всех стейкхолдеров отрасли, а также банков, которые попросту столкнутся с необходимостью обработки потока не нужных им данных.

Ожидать подвижек по второму пункту можно лишь при условии успешной и массовой коммерциализации услуг социальных сетей, ориентированной именно на их оплату с банковских счетов. Первые шаги в этом направлении в начале июля 2011 г. сделали две крупнейшие социальные сети РФ (*ВКонтакте* и *Одноклассники*), которые ввели возможность привязки оплаты платных услуг с карт банков-партнеров (вместо платных СМС). Ключевых вопроса здесь два: возможно ли будет со временем превратить *опцию* в *обязательство* и достаточны ли меры безопасности, применяемые для защиты вводимых пользователем банковских реквизитов. В плане безопасности предпочтителен путь *Одноклассников*, когда при регистрации пользователь работает в защищенной базе самого банка, уже после этого переходя в обычный интерфейс социальной сети.

Так или иначе, перечисленные меры не решают проблемы идентификации пользователей полностью. Необходим комплексный подход, распространяющийся на все интернет-пространство. В РФ он пока отсутствует, так как не существует, во-первых, консенсуса относительно должной степени вмешательства государства в данную область; во-вторых, отсутствует единое видение этого подхода на техническом и юридическом уровнях. В данных условиях целесообразно тщательное и многоуровневое изучение зарубежного опыта, как положительного, так и негативного. По мнению одного из крупнейших российских киберюристов, «сегодня российским органам власти необходим мониторинг наработок и решений других стран и международных организаций в данной области».

За рубежом наиболее интересные решения предлагают США, где в последние годы обсуждается идея *интернет-паспортов*, действие которых охватит не

только социальные сервисы, но и всех пользователей Сети. В конце 2010 г. была опубликована черновая версия Национальной стратегии достоверной идентификации в киберпространстве, (National Strategy for Trusted Identities in Cyberspace). В основе документа лежит идея единой, комплексной многоуровневой безопасной интернет-среды, действующей в условиях достоверной идентификации пользователей и надежной защиты их персональных данных. Стратегия ориентирована на физических лиц, а также иных субъектов (не физических лиц, НФЛ) – организации, услуги, продукцию software. Она учитывает глобальный характер Сети, подразумевая необходимость действия предлагаемых средств идентификации на трансграничном уровне. Ключевой принцип обеспечения безопасности интернет-среды – позволить всем субъектам коммуникации сообщать свои данные лишь в минимально необходимом объеме в каждом необходимом случае, при многоуровневом и предельно гибком ранжировании требований по тем ли иным транзакциям и разным типам субъектов – сохраняя в остальных случаях анонимность, не сообщая лишнюю информацию.

НЕОБХОДИМАЯ СТРАТЕГИЯ В СЕТИ

Во-первых, одной из приоритетных задач для России в рамках повестки вызовов безопасности в связи с развитием ИКТ должно стать развитие новых проектов в сфере идентификации пользователей, а также анализ зарубежного опыта в этой области. В этой связи всестороннее изучение *Экосистемы идентификации* должно стать неотложной задачей российских органов власти с последующим применением ее удачных решений и принципов для создания аналогичной отечественной концепции целостной системы идентификации пользователей. При этом органичной составляющей подобной системы по умолчанию должна стать идентификация пользователей в социальных сетях.

Во-вторых, выход на устойчивое взаимодействие со структурами интернет-сообщества, которые могут быть полезны в развитии данных направлений, должен стать приоритетной задачей МЧС, МВД, ФСБ, Минобороны РФ и других органов, ответственных за обеспечение безопасности. На данный момент взаимодействие государства с интернет-сообществом развивается недостаточными темпами.

В-третьих, проблематика киберпреступности и кибертерроризма должна найти системное отражение в российских доктринальных документах. Доктрина информационной безопасности и другие нормативные акты более не достаточны для адекватного описания современной реальности кибервызовов. Модернизация национального законодательства должна упрочить фундамент, на который могли бы опираться продвигаемые РФ стратегии международного и многостороннего сотрудничества в сфере противодействия киберпреступности.

Авторы – научные сотрудники ПИР-Центра.

Выпускающий редактор – Ирина Миронова.

Международный клуб *Триалог:* trialogue@pircenter.org

Centre russe d'etudes politiques: crep@pircenter.org

Москва – Женева, Октябрь 2011