МЕЖДУНАРОДНАЯ ЖИЗНЬ

Гармиш-Партенкирхен
2017

ГОСУДАРСТВО • БИЗНЕС • ГРАЖДАНСКОЕ ОБЩЕСТВО • ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Приложение к журналу «Международная жизнь»

ГОСУДАРСТВО • БИЗНЕС • ГРАЖДАНСКОЕ ОБЩЕСТВО • ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

XI Международный форум

«Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности»

Гармиш-Партенкирхен, Германия

24-27 апреля 2017 года

Семинар - «круглый стол» №2
Сессия 2
Потенциал использования ИКТ в военно-политических целях в контексте стратегической стабильности

сованные стороны, а также учет их национальных интересов. А во-вторых, в этой формуле должна быть обязательно учтена разнородность факторов стратегического воздействия и появление новых средств.

Армии «умных ботов» - инструмент достижения превосходства в информационном пространстве

Андрей Масалович, «ДиалогНаука» (Россия): Прошу извинить за некоторый непривычный стиль изложения, так как я больше привык к «хакерским» конференциям, чем к серьезным научным обществам, тем более что моя работа лучше всего определяется словосочетанием «менеджер по связям с реальностью».

Тема, которую хотелось бы осветить, надеюсь, будет интересна и здесь, поскольку она касается инструментария, который сейчас используется как на стороне светлых сил, так и во вред. Инструментария для манипулирования массовым сознанием, для воздействия на массовую аудиторию в социальных сетях и даже для задач, которые заставляют эту массовую аудиторию принимать те или иные решения вплоть до победы на выборах.

В ноябре 2016 года в Москве проходила конференция по кибербезопасности. Примерно в 11 часов 10 минут утра у меня пискнул телефон, и наша система экстренного оповещения «Аваланч» прислала мне сообщение, что через пять минут мировые СМИ объявят о том, что победил Трамп. Это уже серьезный повод, чтобы мировое сообщество проявило интерес к тому, что в России есть технологии, позволяющие анализировать ситуацию, и не просто анализировать, но и прогнозировать ее в глобальных сетях. После этого телефон у меня «взорвался», и вот уже который месяц мне задают два вопроса: первое - ответственны ли русские хакеры за победу Трампа, а второе - что я там такое рассказывал про российские методы и технологии для анализа массовой аудитории и для воздействия на эту аудиторию?

Что касается первого вопроса, то ответ простой - единственная в мире доказанная атака российских хакеров произошла в 1242 году, когда русские хакеры взломали лед Чудского озера. Все остальные атаки надо еще доказать.

Второе - что касается технологий, которые использовались для победы Трампа, то я не буду рассказывать о всех перипетиях борьбы и работы его избирательного штаба, но остановлюсь на одном аспекте, который, во-первых, касается работы с Интернетом, во-вторых, волею судеб очень сильно перекликается с тем, о чем мы говорили в этих стенах год назад.

Итак, победа Трампа в соцсетях была обусловлена последовательным выполнением трех шагов. Шаг первый - это использование так называемой психометрики. Это наука, разновидность прикладной психологии, о построении психологического портрета человека по поведению в соцсетях. Традиционно принято связывать данную технологию с Михаилом Казинским как одним из самых активных популяризаторов этой науки.

Самый известный его эксперимент - из доклада трехлетней давности, где он показывал, как по 68 лайкам в «Фейсбуке» удается определить цвет кожи испытуемого, то есть какой расы человек ставил лайки, только лайки, без репостов, без комментов, без фотографий. Далее - гомо- или гетеросексуальной ориентации, поддерживает Демократическую или Республиканскую партию. То есть по некоторому набору действий, которые мы выполняем в социальных сетях, даже самых простых действий, удается демаскировать те признаки, те маркеры, которые мы стараемся спрятать: пол, возраст, принадлежность, отношение к экстремистам, террористам, суицидникам или другим отклонениям. Эти технологии используются, в частности, для анализа психологических портретов подростков, а также для анализа окружения групп вокруг экстремистских сообществ и сообществ националистической направленности в соцсетях.

Вторая часть успеха Трампа базировалась на технологиях так называемого точного таргетирования, или точного выбора целевой аудитории. Лидером в данной области принято счи-

тать компанию «Кембридж Аналитикс», которая просто дальше других продвинулась и более старательно рассказывает и показывает, как эти технологии работают.

Третья часть успеха Трампа базировалась на конкретной группе внутри его избирательного штаба, даже сейчас часто показывают трейлеры, в которых она перемещалась по стране. Эта группа выявляла точки наиболее эффективного воздействия, то есть точки вокруг лидеров мнений, где собирается целевая аудитория, тот контент, который она готова воспринимать, и целевым образом направляла его в эти точки. Это был так называемый ударный контент. То есть та информация, которую хотели впрыснуть в мозги аудитории.

Не знаю, кто взломал мозг 40 млн. американцев, которые в итоге определили победу Трампа, но подозреваю, что вот эта технология очень-очень сильно в этом помогла. Чуть позже расскажу, почему она настолько эффективна. Дело в том, что при таком подходе - очень глубокий точечный анализ, а потом точечное воздействие - резко уменьшаются бюджеты, бюджеты продвижения. Нам не надо облучать большие аудитории, мы можем впрыскивать информацию именно в те мозги, которые готовы ее воспринимать, именно в тех местах, где они находятся.

Итак, после того, как ученые-аналитики подтвердили, что в феномене Трампа достаточно большую если не ключевую роль сыграли новые технологии массового воздействия в соцсетях, тема стала топовой.

Хотелось бы рассказать о некоем базовом механизме, то есть «заглянуть» под капот этой технологии, посмотреть, как она работает внутри.

Возможно, вы спросите: «Если вы такие умные, это все уже знаете и используете пять лет, то почему не пишете научных статей?» Нам не надо писать научных статей, о наших результатах пишет «Форбс», уже дважды российские результаты попадали в «Форбс», например в №2 за 2015 год, статья называлась «Разведка сетью…», а в мартовском номере прошлого года статья называлась «Виртуальный халифат. Как Россия воюет с ИГ в интернете».

Каждый из нас искренне верит, что он видит Интернет, я тоже в это верил и много лет в нем работал, считая, что та среда, в которой я работаю, и есть Интернет. Пока один раз мы к своей программе не приделали трехмерный визуализатор, который стал показывать, как выглядит активность в Интернете прямо сейчас, то есть генерировать картинку в реальном времени.

Каждый из нас видел много-много разных графиков, но эти графики просчитаны, то есть сначала что-то происходит, потом данные собираются, обрабатываются и вам показывают через какое-то время. Оказалось, что когда смотришь на активность в Интернете в реальном времени, то появляется картина, которую раньше не видел и не предполагал даже, как она выглядит.

Итак, давайте наденем очки 3D визуализации и посмотрим, как выглядит одна минута в «Твиттере». Его аудитория представляет собой некую ночную планету, в которой четко выделяются люди, у которых сравнительно мало друзей, плотный, так называемый органический, круг общения. Иногда они группируются обсудить какую-то новость.

Над ними политики, популярные артисты, всевозможные медийные персоны. У них совершенно необычная, раздутая популярность, и их практически не видно. Близко к реальному миру живут так называемые лидеры общественного мнения, или по-русски это называется сокращением «ЛОМ», которые что-то говорят, и их слушает их целевая аудитория, например секта «Свидетели Навального». В этой картине мира есть какие-то странные кластеры, которые живут совершенно по своим законам и их действия не похожи на действия обычных людей, реакция на новости не похожа на реакцию обычных людей.

Это ботнеты. Для того чтобы они стали эффективными, для того чтобы они нормально работали, таких ботов должно быть сотни, тысячи если не миллионы, иначе их действия не будут видны, их результаты, их активность не будет иметь результата.

Если мы возьмем классическое определение бота, так, как оно дано в «Википедии», то бот - это программа, которая ха-

рактеризуется простым, повторяемым поведением. Больше половины мирового интернет-трафика сейчас порождается ботами, а не людьми, то есть, это программы, которые выполняют какие-то свои программные действия, это не органический, не живой трафик.

Боты известны более 20 лет. Когда Интернет начинался, у меня, например, номер пользователя Интернета в России, так называемый «Рунет-АйДи» 2200, то есть, представьте, на всю Россию тогда было всего две с небольшим тысячи человек, которые вообще в Интернет заходили. Но даже из этих 2200 700 номеров было ассигновано под так называемые технические аккаунты, то есть фактически под ботов. Таким образом, боты были уже 25 и 30 лет назад. Но действия бота легко распознаются. Он простой, понятный, он ходит с одного IP. Он не может делать ничего сложного, его очень легко проверить, задав ему какой-нибудь вопрос. Он не понимает, как обойти так называемую «капчу», и долгое время считалось, что любая система может таких ботов фильтровать, тем более система типа социальных сетей или массовых ресурсов. Это одна из самых важных задач - пропускать трафик живых людей и не пропускать всяких рекламных спам-ботов.

Попробуем включить мозг хакера. Хакер знает не больше, у него просто более гибкий мозг. Давайте попробуем обойти капчу. Если перед нами один бот, он хочет попасть в социальную сеть и поговорить с участниками, то у социальной сети возникают сомнения, а живой ли это человек. Она ставит ему капчу.

Технически до сих пор нельзя с высоким качеством распознать капчу, особенно если у нее есть языковые особенности или если у нее есть какое-нибудь визуальное обобщение, например показать на картинке все бензоколонки. Вот, вроде бы бот это пройти не может, если он один. А теперь представьте себе, что у нас есть два бота и один хакер. Один бот должен пройти в соцсеть, но его не пускает капча, тогда хакер берет другого бота, взламывает какой-нибудь форум, где защита послабее, чаще всего, кстати, хакеры любят форумы, где занима-

ются всякой такой тематикой, как «веселые картинки, не вполне традиционное порно». Вот, хакер взламывает этот форум, и тогда один бот, получая капчу, отдает ее другому, другой находит живого участника, который прямо сейчас сидит, разглядывает «веселые картинки», подставляет ему капчу и говорит: «Твои действия оказались подозрительными, пожалуйста, подтверди, что ты человек, а не робот, ответь на эту капчу». Человек в полной уверенности, что он полез туда, куда не надо, что это он, его действия вызывают подозрения, заполняет капчу, которую получает бот, отдает другому, и тот проходит дальше.

Таким образом, два бота смогли совершенно спокойно обмануть, обойти механизм защиты соцсети. А поскольку в таких порночатах всегда есть аудитория, у нас получается бесплатная дежурная смена, которая будет эти задачи решать круглосуточно, причем на том языке, на котором должна быть отработана капча. Не спасет, даже если капча будет китайской или какой-то еще.

Появляются боты со сложным поведением, которые могут копировать или изображать действия человека, что привело к нескольким видам атак. Расскажу о трех простых видах новых атак, о которых еще не знают журналисты.

Первый вид атаки, назовем его «горизонтальный брутфорс», или «брутфорс по мультилогинам». Представим себе, что нам надо сломать почтовый сервер и получить логины и пароли миллионов пользователей. Ну, например, какой-нибудь хорошо защищенной почты, «мэйл.ру» или «gmail». Технически это сделать кажется невозможно. Почему? Базовый вид атаки, так называемый «брутфорс», грубой силой, или атака подбором, будет сразу заблокирована. То есть если я возьму один логин и начну подбирать пароли, то сервер увидит, что идет подбор паролей к одному логину и на третьей попытке заблокирует.

Представьте себе, что у меня уже в руках не один бот, не два, а миллион, и у меня в руках есть список из миллиона логинов, взятый из какой-то спам-рассылки. Тогда миллион ботов одновременно могут обратиться к серверу, задать разные логины и один и тот же пароль, например «123456», и серверу по-

кажется, что к нему одновременно обратился 1 млн. человек, каждый из которых сделал одну ошибку, что вполне допустимо. И он каждому ответит, что ошибся. Но из этого миллиона найдется, по моей практике, примерно 300-350 аккаунтов, у которых действительно будет пароль «123456».

В следующую минуту ботам ничего не стоит организовать атаку, проверить пароль «qwerty», или проверить пароль «ohmygod», или проверить какой-нибудь пароль со словом «Obama». *И таким образом, через десять или через тридцать* минут в руках у хакера будут тысячи если не миллионы взломанных аккаунтов, при этом сервер ничего не увидит. Просто к такому типу атаки, когда атакуют тысячи, миллионы ботов, серверы не готовы.

Второй вид атаки - атака на «Фейсбук». Один молодой исследователь пару месяцев назад заметил такую штуку. Если нажать кнопочку «напомнить пароль» на «Фейсбуке», то прилетит некоторый код. На почту придет письмо, в этом письме будет код и приписка «нажмите вот этот код подтверждения».

Дважды повторив эту операцию, он в этом адресе, который прилетает, нашел токен, собственно, то место, которое образует уникальный код для операции. Увидел, что оно очень сильно привязано ко времени, то есть его невозможно подделать, его невозможно расшифровать, его невозможно потом повторить, но оно привязано к текущей секунде, это первое. И второе - он обнаружил, что в силу длины таких кодов можно сгенерировать не более миллиона одновременно.

Соответственно, он взял 2 млн. ботов, в одну и ту же секунду отправил их в Интернет, нажав кнопку «напомнить пароль», один аккаунт у него был настоящий, он получил один настоящий токен, соответствующий текущей секунде, и раздал его 2 миллионам. Заставил 2 млн. ботов откликнуться, что «я забыл пароль, вот мой код, вы мне прислали код подтверждения, вот он».

И поскольку кодов было всего миллион, а пользователей было два, для нескольких аккаунтов код совпал. Их было, кста-

ти, не два, их было около 20. То есть за одну секунду он получил доступ к 20 аккаунтам в «Фэйсбуке». Это тоже возможный вид атаки, он тоже сейчас никак не бьется, не покрывается.

Третий вид атаки, который, может быть, будет вам интересен. У вас в руках или в кошельке есть кредитная карточка. Почти все ее данные очень легко восстановить, почти всеми вы делитесь, то есть легко найти номер вашей кредитки, легко понять «экспирейшн дэйт». Естественно, элементарно узнать вашу фамилию и имя, секретным остается единственные три цифры CVV, так называемый код идентификации с обратной стороны карточки. Он не передается, он не открывается, он не фигурирует в открытых базах, но там всего три цифры, то есть таких кодов всего 1 тысяча.

Если я попытаюсь подобрать CVV, работая с каким-нибудь интернет-магазином, банк «Эсквайр» меня заблокирует на третьей попытке. Он зафиксирует попытку подбора кода, но в мире есть 400 интернет-магазинов, из них у 360 нет даже элементарных средств защиты от такого вида атаки. То есть достаточно мне три раза обратиться в каждый интернет-магазин, у меня получится более 1 тыс. обращений на то, чтобы сделать какую-нибудь минимальную покупку на один доллар. То есть трех обращений в один магазин мне достаточно, чтобы перебрать всю тысячу, и через несколько секунд у меня в руках будет ваш код CVV.

Это тоже реальная атака, которая появилась за последний месяц, и связана она как раз с использованием таких вот армий «умных» ботов, когда много ботов с нескольких аккаунтов, с нескольких IP-адресов стартуют одновременно и при этом имитируют активность живых людей.

Такого рода активность используется не только молодыми нарушителями, которые пытаются взломать e-mail или получить доступ к вашей кредитке. Такие технологии используются и при массированных атаках. Например, атака на серверы «Клинтон фаундейшн» и серверы Демократической партии, которые приписывают российским хакерам, на самом деле исходно была инициирована румынским хакером под псевдонимом «Гуччифер 2.0».

Открою секрет. Лингвистический анализ показывает, что по происхождению он молдаванин, так что его можно с натяжкой назвать русским хакером. Скорее всего, его родители жили на территории бывшего Союза. Почему появились основания называть его русским хакером? Он использовал так называемое «дистортинг прокси».

Обычное назначение прокси-серверов - это скрывать, анонимизировать IP-адрес. Но при этом через прокси проходит так называемое ваше переменное окружение, то есть виден ваш язык раскладки клавиатуры, видны ваши дата, время и версия установки браузера, видна ваша версия «Майкрософт Офиса» и самого «Майкрософта», то есть вектор параметров, по которым вас потом криминалисты легко определят.

Поэтому после появления анонимизирующих прокси появились прокси, которые скрывают переменные окружения, но это тоже подозрительно. Сейчас появилось поколение так называемых элитных прокси - «элайт прокси», или их еще называют «дистортинг прокси», то есть искажающие прокси, которые не прячут переменное окружение, а подменяют их, воруя аккаунты, воруя личности у других пользователей. Соответственно, Гуччифер, выполняя атаки, выступал то как китаец, то как русский, то как испанец, то как англичанин. Это те четыре вида, которые я знаю. Поэтому, исследователи схватились, что среди его «скинов», или «масок», была русская и объявили его русским хакером.

Таким образом, подобного рода массированное применение «умных» ботов может быть использовано и теми, кто занимается более серьезными политическими атаками, а не только мелкими правонарушениями.

Мощь этих инструментов можно использовать и на светлой стороне. Можно на их основе делать средства для массированного анализа социальных сетей и решения всяких полезных задач. Например, 18 декабря 2014 года, когда Россию взорвали СМСки о том, что дела у Сбербанка идут плохо, вот-вот прекратятся платежи по кредитным картам, и эти СМСки шли волнами, началось волнение по всей России. Почему? На самом деле средний размер вклада тогда составлял не более 30 тыс. рублей на одно частное лицо. Вроде бы для крупного банка это немного, но у Сбербанка, как оказалось, не было экшн-плана, то есть не было системы отработки, моделирования такого вида атак. И, в частности, они не проверили, как работает колл-центр под нагрузкой.

Что происходило? Люди у нас серьезные, люди у нас спокойные, никто не бежал снимать деньги, все звонили в Сбербанк спросить, что там реально с карточками, и ласковый женский голос отвечал: «Ваш звонок очень важен для нас, к сожалению, все операторы сейчас заняты, ориентировочное время ожидания в очереди две недели». Вот после чего человек понимал, что мир рушится, и уже бежал снимать свои 30 тыс. рублей. И когда таких набралось 10 миллионов и со счетов слетели первые 300 миллиардов, Сбербанк понял, что не такой уж он и крупный.

Мне позвонили 18 декабря в полдень, это была суббота, и к вечеру у нас уже были готовы «тепловые карты»: оказалось, что атака была не равно размазанной, а были такие кластеры по России. И насколько я могу представить, на следующий день по этим адресам уже летели транспортные самолеты с наличными деньгами, загружались банкоматы, с тем чтобы погасить первую волну паники. Такого рода массированный анализ можно использовать и для решения массовых проблем.

Если выбрать некоторый уровень между человеком и соцсетью, а именно выбрать два круга вокруг человека - друзья и

друзья друзей, это примерно 50 тыс. аккаунтов вокруг нас, то они позволяют полностью создавать картинку, чем человек дышит, чем он увлекается, с кем дружит, кто еще вокруг него увлекается тем же.

Очень легко, таким образом, во-первых, ставить первичный диагноз и какой-нибудь школе, и какому-нибудь региону, и даже ребенку, и классу, можно следить за текущем состоянием и нарастанием всевозможных настроений. Буду использовать русские термины из практики нашего МВД: это «суицидники», «зацеперы», «живодерки», «синий кит».

Видно, что одна за другой идут какие-то проблемные виды групп детей, которых на самом деле можно легко контролировать, если эту технологию действительно использовать на благо правоохранителей. Делать это можно, кстати, не только в России.

Весной прошлого года в Казахстане прокатились массовые волнения после объявления о том, что будут, возможно, приватизировать землю и что всю землю скупят китайцы. В Интернете мы эти волнения увидели за два дня до того, как они выплеснулись на улицы. Но, судя по реакции казахских правоохранителей, они это видели только на улицах. Предварительного анализа обстановки в Интернете, как выяснилось, у них не было.

Почему это использовалось в кампании Трампа, почему это важно, в чем здесь экономия бюджета? Дело в том, что такого рода анализ поведения массовой аудитории связан с одной любопытной особенностью Интернета, которой раньше не было, это кнопка «репост».

Если у меня в руках нет кнопки «репост», я могу просто послушать новость и обсудить ее с соседями. Картина распространения новости точно расписывается формулами трехмерной ударной волны. То есть первый всплеск, потом затишье, потом вторая волна, обсуждение уже маленькое, и волна уходит в фон. Вот, смотрите, например новость - день рождения Путина. Поговорили про день рождения Путина, потом еще поговорили, тема ушла в фон. Вот в этот же день полетели калибры, о них говорили меньше. Произошло событие, о нем поговорили, оно ушло в фон. Что это дает?

Это приводит к двум следствиям, которые знает каждый специалист по пиару. Первое - если я трехмерной «бомбой» пытаюсь поразить аудиторию, двухмерное покрытие людей, большая часть осколков, большая часть энергии улетит в никуда и пользы не принесет. Точно так же пиарщик знает, что большая часть бюджета любого события улетает в никуда, но ему придется ее потратить, чтобы нужное количество осколков этой информации поразило его целевую аудиторию. То есть в традиционном пиаре все готовы к тому, что деньги выжигаются, деньги тратятся неэффективно. Второе - если у меня аудитория линейно увеличится, например, в два раза, то размер заряда, размер «бомбы», мне надо увеличить в квадрате или даже в кубе. Точно так же бюджет пиар-мероприятия. Одно дело - мне нужно собрать 30 тыс. человек, другое дело - 60 тыс. человек. Для 60 тысяч бюджет будет не в два раза больше, а в четыре, а то и, может быть, в восемь. И все были к этому готовы.

В реальном мире других путей нет, но в Интернете, где есть кнопка «репост», поведение аудитории лучше всего описывается формулами двухмерного взрыва. Каждый из нас видел, как падает капля дождя на воду. Кажется, что каждая капля становится центром волны. Некоторым каплям не повезло и их энергия будет погашена. Но некоторые капли попадут в резонанс, от них действительно пойдет волна, и эта волна уже не тратит нашей энергии, нашего бюджета, мы просто капнули каплю, а дальше она сама начала распространяться.

Если, условно говоря, один пригласит военного, он возьмет большую бомбу «взрывать» свою большую аудиторию, это будет дорого. А у меня будет фея, такая маленькая фея, которая будет летать с пипеткой и капать отравленными каплями на мозги моей целевой аудитории, я потрачу гораздо меньше сил и меньший бюджет. И вот именно так была устроена кампания Трампа, именно так устроен механизм воздействия на аудиторию в соцсетях, то есть нужно понять, где образуются сгустки нашей целевой аудитории, надо понять, в каких еще группах активны эти же люди, надо выделить среди них лидеров мнений и именно туда впрыскивать информацию.

В завершение еще два красивых примера, как эти технологии использовать на стороне добра.

Пример первый: как мы боролись с пиратами. В последний четверг прошлого года вышел очень популярный в России фильм «Елки-5». Его тут же украли пираты, тут же выложили на торренты, но кроме этого какой-то парень начал звонить в студию Т.Бекмамбетова и шантажировать, что он сейчас сделает так называемую «посевную», то есть начнет разбрасывать по Интернету ссылки с этим пиратским контентом.

Они пробовали обратиться к юристам и правоохранителям, что-то с ходу не получилось, они обратились к нам. Что мы сделали? Первое - мы запустили ботов, которые стали распространять по Интернету точно такой же текст, как у этого парня, такие же заголовки, такие же хештеги, но ссылка была неправильная, ссылка вела или на порнушку, или на старые фильмы, или на платный контент. У меня ребята еще хотели поставить ссылку на приемную ФСБ, но я им не разрешил. И атака самого этого парня стала незаметной, то есть его ссылки уже были не видны. Второе - мы сделали встречную атаку: стали распространять информацию о том, что не надо нажимать на эти ссылки, хештеги, потому что это вирус «троян», который заразит компьютер. И третье, мы сделали бота-юриста, который «ходил» по социальным сетям, находил этот противоправный контент, нажимал на кнопку «пожаловаться» и заполнял форму «пожаловаться».

В итоге активности этого парня хватило на полдня, потом он понял, что бесполезно, с ботами сражаться человек не может.

И последний пример. 25 января в Оптиной пустыне сгорел женский монастырь. Большой проблемы бы не было, потому что их духовник, отец Илий, является духовником Патриарха - деньги на ремонт нашлись бы мгновенно. Но в Интернете образовалось порядка 50 сайтов-мошенников, где начали собирать деньги вроде как на ремонт, на восстановление обители, а надо сказать, что наша церковь крайне неумело работает с интернет-аудиторией.

К нам обратились за помощью. Что мы сделали? Первое - мы сделали бота, который находил все места размещения про-

тивоправного контента и верхним комментарием писал: «А ведь это мошенники. Вас хотят обмануть. Сами мошенники, и счет мошеннический. Если хотите помочь, переводите деньги вот на этот счет», и показывал правильный счет. Естественно, мошенники это видели, тут же комментарий стирали. У бота стоял регламент 15 минут, он через 15 минут заходил, говорил: «А ведь это мошенники и счет у них неправильный, мошеннический». Человек не может каждые 15 минут бороться с железным ботом. После этого мы сделали еще встречную атаку, стали распространять ссылки с правильными реквизитами, ну и сделали бота-юриста, который «бродил» по Интернету, находил вот этот противоправный контент, нажимал кнопку «пожаловаться».

Итак, резюмирую. Технологии, о которых я хотел рассказать, сейчас стали реальностью. Нам очень помогло, что именно они использовались при выборах Президента Трампа и «наши» победили. Поэтому сейчас эта тема привлекает внимание и, надеюсь, будет востребована и представителями правоохранительных, силовых и государственных структур разных стран во имя добра.

Обеспечение информационной безопасности - одна из составляющих стратегической стабильности

Наталья Ромашкина, Институт мировой экономики и международных отношений им. Е.М.Примакова РАН: Хотелось бы поблагодарить организаторов форума за то, что проблема обеспечения стратегической стабильности стала темой столь авторитетного мероприятия. Уже много лет я занимаюсь проблематикой стратегической стабильности и в качестве математика, и в качестве международника, поэтому для меня это просто подарок. Предлагаю вашему вниманию результаты наших исследований по теме информационная безопасность как часть проблемы стратегической стабильности.

В первую очередь надо отметить, что, к сожалению, проблема обеспечения стратегической стабильности уже очень много лет не обсуждалась с Россией на международном уровне. Россия