www.volsu.ru

ИННОВАЦИИ В ИНФОРМАТИКЕ, ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКЕ И УПРАВЛЕНИИ

DOI: https://doi.org/10.15688/NBIT.jvolsu.2018.3.1

УДК 681.3
ББК 32.973

АНАЛИЗ СОВРЕМЕННЫХ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Дмитрий Анатольевич Тершуков

Начальник отдела специальной документальной связи и защиты информации,
аппарат Губернатора Волгоградской области
dmitryiddt@mail.ru, kancel@volganet.ru
просп. им. В.И. Ленина, 9, 400098 г. Волгоград, Российская Федерация

Аннотация. В статье анализируются внешние и внутренние угрозы информационной безопасности. Вследствие реализации данных угроз автором выделяются приоритеты для специалистов в сфере информационных технологий и безопасности.

Ключевые слова: информационная безопасность, информационная среда, ИТ-инфраструктура, угрозы, информационные системы.

В современном мире важнейшими продуктами стали знания и осведомленность, на лидирующие позиции вышла сфера услуг, стремительно развивается глобальное информационное пространство, при этом современные информационные технологии предоставляют не только новые возможности в решении различных проблем, но и создают принципиально новые вызовы и угрозы.

Появление новейших информационных технологий и систем, развитие и расширение функций социальных сетей, внедрение в социальные сети самых различных сервисов и их алгоритмизация создали инструменты превращения исторического процесса развития человечества из неуправляемого в управляемое и даже проектируемое, появились возможности создавать реальность, не соответствующую действительности, осуществлять воздействие на массовое сознание миллионов людей по всему миру.

Появилось понятие «информационная бедность», которое отражает возможности доступа к современным информационным технологиям и информационным ресурсам.

Государства с развитой информационной средой используют свое доминирующее положение в информационном пространстве для

достижения экономических и военно-политических целей. Традиционные средства войны достаточно дороги, тогда как информационные способы воздействия являются прекрасной альтернативой. Спектр воздействий достаточно широк: от дискредитации работы государственных органов до нанесения ударов по критически важной инфраструктуре. Проведение такого комплекса действий приводит к потере управляемости в стране, экономическому спаду, создаются условия для возникновения гражданских конфликтов.

В июле 2016 г. в Варшаве на очередной сессии Совета НАТО киберпространство отнесено к перечню сфер ведения военных действий. На сессии были приняты «Обязательства по обеспечению кибероборонны», предусматривающие финансирование профильных программ, развитие взаимодействия между национальными структурами, активизацию обмена данными о киберугрозах, повышение квалификации сотрудников национальных структур в сфере кибербезопасности, отработку вопросов кибероборонны в ходе мероприятий оперативной и боевой подготовки. При этом одним из основных источников угроз была признана Российская Федерация.

В сентябре 2016 г. в ходе работы 71-й Генеральной Ассамблеи ООН Российская Федерация предложила в рамках работы Группы правительственных экспертов ООН по международной информационной безопасности (ГПЭ) разработать Правила ответственного поведения государств в информационном пространстве. Конечным результатом работы ГПЭ могло бы стать внесение предложения о принятии Генеральной Ассамблеей ООН резолюции, закрепляющей эти Правила [1].

Российская Федерация предлагает закрепить следующие правила ответственного поведения государств в информационном пространстве [3]:

1. Информационно-коммуникационные технологии (ИКТ) должны использоваться исключительно в мирных целях.

2. С учетом уникальных особенностей ИКТ наряду с применимыми к сфере их использования нормами международного права и имеющими важное значение для поддержания международного мира, безопасности и создания открытого и мирного информационного пространства могут вырабатываться дополнительные правовые нормы для регулирования международных отношений в сфере использования ИКТ.

3. Государства должны обладать суверенитетом над информационно-телекоммуникационной инфраструктурой на своей территории.

4. Любые обвинения в адрес государств в причастности к компьютерным атакам должны быть обоснованными и доказанными.

5. Государства не должны допускать возможности использования своей территории для осуществления компьютерных атак и содействовать использованию в этих целях посредников.

6. Государства должны бороться с внедрением и использованием скрытых вредоносных функций и программных уязвимостей в IT-продукции, а также добиваться ее безопасности для пользователей.

23 июня 2017 г. в Нью-Йорке завершила свою работу Группа правительственных экспертов ООН по международной информационной безопасности под председательством ФРГ. Предполагалось, что в ходе последнего заседания будет принят итоговой доклад, однако этого не произошло.

В ходе дискуссии на ГПЭ российская сторона продвигала идею о необходимости предотвращения конфликтов в цифровой сфере, закрепления принципов неприменения силы, уважения государственного суверенитета, невмешательства во внутренние дела других государств, соблюдения основных прав и свобод человека. Однако инициатива России, нашедшая поддержку многих членов Группы, была заблокирована западными странами, итоговый доклад принят не был.

В интервью информационному агентству ТАСС спецпредставитель Президента Российской Федерации по вопросам международного сотрудничества в области информационной безопасности А.В. Крутских сообщил о том, что «миротворческая концепция России вступила в противоречие с позицией отдельных стран, стремящихся навязать миру собственные, выгодные только для них “правила игры” в информационном пространстве.

Опираясь на свои технологические преимущества, они добиваются закрепления в

информационном пространстве "права сильного" и стремятся создать международно-правовое обоснование для своей "свободы рук". В этих целях ими предпринята попытка закрепить в ооновском формате решения варшавского саммита НАТО о признании цифровой сферы новым театром военных действий».

Необходимо отметить, что информационные войны уже ведутся не только государствами, но и корпорациями, и политиками, и религиозными организациями [2]. Основным оружием при этом выступают средства массовой информации.

По мере нарастания объема информации людям становится труднее ориентироваться в ее содержании, ограждать себя от ее избытка и нежелательного контента. Распространение «экранной» культуры, неизбежность столкновения с виртуальной реальностью, в которой трудно различимы иллюзия и действительность, создают проблемы психологического характера.

Расширяются масштабы применения вредоносного программного обеспечения. 2017 г. можно назвать годом применения вирусов-шифровальщиков. В течение всего года осуществлялись масштабные кибератаки на нефтяные, телекоммуникационные, финансовые и логистические компании.

12 мая 2017 г. в Испании нападению с использованием вируса-шифровальщика WannaCry подверглись компьютерные сети крупнейших компаний в сфере телекоммуникаций, газоснабжения и поставок электричества с требованием выкупа.

Пользователям предлагалось перевести сумму в биткойнах, эквивалентную 300 долларам США, в течение трех дней по указанному адресу, после чего пользователю на электронную почту будет выслан ключ для разблокировки компьютера. Если выкуп не поступал своевременно, то его сумма автоматически удваивалась. На седьмой день, если WannaCry не был удален с инфицированной системы, зашифрованные файлы уничтожались. Параллельно с шифрованием данных вредоносная программа проводила сканирование адресов локальной сети для последующего заражения новых компьютеров.

Всего за три майских дня 2017 г. вирус-шифровальщик атаковал 200 000 компьютеров в 150 странах мира. Вирус прошелся по сетям университетов в Китае, заводов Renault во Франции и Nissan в Японии, железнодорожного оператора Deutsche Bahn в Германии. В России атаки были совершены на сети МВД, Мегафона, Сбербанка.

В июне 2017 г. атаки повторились уже с использованием новой модификации вируса-шифровальщика Petya. В отличие от WannaCry истинная цель нового вируса заключалась не в получении денежной выгоды, а в нанесении максимального ущерба. Новая версия вируса, получившая название NotPetya, не предполагала возможность расшифровки информации на жестком диске.

27 июня 2017 г. была совершена масштабная атака на нефтяные, телекоммуникационные и финансовые компании России и Украины.

Компьютеры в НПЗ «Башнефти», «Башнефть-Добычи» и управлении «Башнефти» единовременно перезагрузились, после чего скачали неустановленное программное обеспечение и вывели на экран заставку вредоносной программы – вымогателя денежных средств. Только переход на резервную систему управления позволил избежать серьезных последствий.

В ходе атак была атакована крупнейшая логистическая компания A.P. Moller – Maersk. Атака оказалась пагубной для APM Terminals, управляющего работой десятков грузовых портов и контейнерных терминалов. В сутки через них проходит более 100 000 грузовых контейнеров.

Работа ИТ-инфраструктуры была приостановлена, десятки судов вынужденно простаивали на рейде. Компании пришлось передать управление перевозками непосредственно в филиалы, расположенные более чем в 130 странах мира, создать с чистого листа временную службу заказов, а также обновить ИТ-инфраструктуру. Ущерб компании составил около 300 млн долларов.

Сейчас мир столкнулся с новой проблемой – искусственный интеллект. Бесконтрольное распространение технологии искусственного интеллекта (AI) может привести к росту киберпреступности и появлению ее новых форм.

В феврале этого года 26 экспертами в сфере кибербезопасности из Оксфордского,

Кембриджского и Стэнфордского университетов и некоммерческих организаций Electronic Frontier Foundation и OpenAI был опубликован 100-страничный доклад «Преступное использование AI: прогноз, профилактика и предотвращение».

Авторы выделяют три главных направления угроз [4].

Первое – искусственный интеллект будет использован для выявления потенциальных жертв, обнаружения уязвимостей программного обеспечения и проведения хакерских атак.

Хакерские атаки станут намного масштабнее и эффективнее, при этом искусственный интеллект позволит использовать уязвимости человека.

В настоящее время с использованием искусственного интеллекта проводятся работы по созданию реалистичных оригинальных изображений и звуков. Использование таких технологий позволит автомобилям-беспилотникам получать изображения пешеходов и автомобилей в самых разных ситуациях и тренировать себя, не выезжая на улицу.

Между тем использование злоумышленниками синтеза речи человека увеличивает вероятность того, что пользователь нажмет на ссылку, запускающую вирус, или скачает нужное злоумышленникам приложение.

Второе направление – это применение искусственного интеллекта в политической сфере.

Политические силы могут использовать искусственный интеллект для манипулирования общественным мнением. Искусственный интеллект может генерировать фейковые новости в таких количествах, что пользователю практически невозможно будет вычленить среди них настоящие. Повысится эффективность и адресность пропаганды.

С помощью искусственного интеллекта может быть сделан шаг вперед в изучении основ психологии поведения человека, что также будет использовано для манипулирования поведением человека.

Третье направление – это организация атак на физические объекты. Такие атаки могут быть совершены с использованием массового применения беспилотников или автоматизированных боевых комплексов.

Появятся возможности по злонамеренному внедрению в системы беспилотных автомобилей с дальнейшими авариями или нападениями с их участием.

Рост потенциала угроз кибербезопасности ставит задачи найти оптимальные механизмы предотвращения и противодействия современным информационно-технологическим угрозам, что напрямую связано с проблемами науки и образования.

31 августа 2017 г. Секретарем Совета Безопасности Российской Федерации Н.П. Патрушевым были утверждены «Основные направления научных исследований в области обеспечения информационной безопасности Российской Федерации».

Документ отражает следующие основные группы научных проблем обеспечения информационной безопасности Российской Федерации:

1. *Общенаучные проблемы обеспечения информационной безопасности Российской Федерации*:

– общеметодологические проблемы обеспечения информационной безопасности (проблемы формирования понятийного (терминологического) аппарата в области информационной безопасности, развития системы обеспечения информационной безопасности Российской Федерации, выявления и др.);

– проблемы развития нормативного правового и нормативного технического обеспечения информационной безопасности;

– проблемы обеспечения безопасности индивидуального, группового и массового сознания (проблемы обеспечения защищенности личности, общества и государства от деструктивных информационных воздействий, проблемы противодействия информационному воздействию на российских граждан, в том числе направленному на подрыв исторических основ и патриотических традиций, связанных с защитой Отечества и др.);

– проблемы противодействия использованию информационных технологий в преступных целях;

– проблемы сдерживания и предотвращения военных конфликтов, которые могут возникнуть в результате агрессивного и иного враждебного использования информационных технологий.

2. *Научно-технические проблемы обеспечения информационной безопасности Российской Федерации*:

– проблемы развития современных информационных технологий, отечественной индустрии средств информатизации, телекоммуникации и связи (проблемы развития и совершенствования информационной инфраструктуры Российской Федерации; обеспечения технологической независимости России в области создания и использования отечественной электронной компонентной базы и микропрограммного обеспечения, доверенных информационных технологий, вычислительной техники, телекоммуникации и связи; предотвращения возможности включения в информационные технологии скрытых вредоносных функций, снижения опасности их применения);

– проблемы защиты информационных ресурсов, информационных систем и сетей связи;

– проблемы использования информационных технологий в оперативно-разыскной деятельности (выявления и пресечения преступлений, совершенных с использованием информационных технологий; разработки методов и средств проведения оперативно-разыскных мероприятий в информационных системах и сетях связи).

3. *Проблемы кадрового обеспечения информационной безопасности Российской Федерации*:

– общеметодологические проблемы кадрового обеспечения информационной безопасности и развития содержания профессионального образования в области информационной безопасности;

– проблемы организационного и нормативного правового обеспечения системы подготовки кадров в области информационной безопасности;

– проблемы ресурсного и технологического обеспечения подготовки кадров в области информационной безопасности (разработки концепции материально-технического обеспечения образовательных программ различного уровня в области информационной безопасности и использования комплексов учебно-тренировочных средств и полигонов (компьютерных полигонов) для обеспечения учебного процесса по образовательным программам в области информационной безопасности).

4. *Проблемы формирования системы международной информационной безопасности*:

– проблемы установления международного правового режима нераспространения «информационного оружия», уменьшения опасности его использования;

– проблемы противодействия использованию информационных и коммуникационных технологий в террористических целях;

– проблемы обеспечения информационной безопасности трансграничных критических информационных инфраструктур, в области противодействия преступности в сфере использования информационных и коммуникационных технологий и др.

В настоящее время от специалистов в области информационной безопасности требуются знания и навыки, которые находятся на пересечении самых разных областей знаний: информационные технологии, психология, политология, юриспруденция, криминалистика и др. Между тем выпускники технических вузов не всегда обладают достаточными знаниями и навыками, позволяющими правильно оценить действия нарушителя информационной безопасности, понять политическую составляющую проблем обеспечения информационной безопасности. Выпускники гуманитарных вузов недостаточно разбираются в специфике угроз информационной безопасности, физической природе возникновения каналов утечки информации. Выходом из сложившейся ситуации может стать использование системы переподготовки и повышения квалификации специалистов по защите информации.

20 декабря 2013 г. было издано распоряжение Губернатора Волгоградской области № 1940-р «О повышении квалификации специалистов по технической защите информации в органах исполнительной власти Волгоградской области». Согласно указанному распоряжению руководители органов исполнительной власти Волгоградской области обязаны организовать прохождение курсов повышения квалификации специалистами по технической защите информации в организациях, осуществляющих образовательную деятельность, реализующих дополнительные профессиональные программы в

области информационной безопасности, согласованные с Федеральной службой по техническому и экспортному контролю. В данный момент повышение квалификации прошли 43 работника органов исполнительной власти Волгоградской области и органов местного самоуправления Волгоградской области, 7 работников прошли профессиональную переподготовку.

СПИСОК ЛИТЕРАТУРЫ

1. Выступление заместителя Секретаря Совета Безопасности Российской Федерации О.В. Храмова на Саммите по вопросам кибербезопасности, Тель-Авив, 28 июня 2017 года. – Электрон. дан. – Режим доступа: http://www.mid.ru/foreign_policy/news/-/asset_publisher/cKNonkJE02Bw/content/id/2804268 (дата обращения: 10.04.2018). – Загл. с экрана.

2. Выписка из Основных направлений научных исследований в области обеспечения информационной безопасности Российской Федерации. – Электрон. дан. – Режим доступа: http://www.scrf.gov.ru/security/information/document155/ (дата обращения: 10.04.2018). – Загл. с экрана.

3. Ответ спецпредставителя Президента Российской Федерации по вопросам международного сотрудничества в области информационной безопасности А.В. Крутских на вопрос информагентства ТАСС о состоянии международного диалога в этой сфере. – Электрон. дан. – 29.06.2017. – Режим доступа: http://www.mid.ru/foreign_policy/news/-/asset_publisher/cKNonkJE02Bw/content/id/2804288 (дата обращения: 10.04.2018). – Загл. с экрана.

4. Тершуков, Д. А. Об обеспечении международной информационной безопасности / Д. А. Тершуков // Материалы VI Всероссийской научно-практической конференции «Актуальные вопросы информационной безопасности регионов в условиях глобализации информационного пространства», г. Волгоград, 27–28 апреля 2017 г. – Волгоград : Изд-во ВолГУ, 2017. – С. 3–6.

REFERENCES

1. *Vystuplenie zamestitelya Sekretarya Soveta Bezopasnosti Rossiyskoy Federatsii O.V. KHramova na Sammite po voprosam kiberbezopasnosti, Tel-Aviv, 28 iyunya 2017 goda* [Speech by the Deputy Secretary of the Security Council of the Russian Federation O. V. Khramov at the Cyber Security Summit, Tel-Aviv, 28 June 2017]. URL: http://www.scrf.gov.ru/news/allnews/2242/ (accessed 10 April 2018).

2. *Vypiska iz Osnovnykh napravleniy nauchnykh issledovaniy v oblasti obespecheniya informatsionnoy bezopasnosti Rossiyskoy Federatsii* [Extract from the Main Directions of Scientific Research in the Field of Ensuring the Information Security of the Russian Federation]. URL: http://www.scrf.gov.ru/security/information/document155/ (accessed 10 April 2018).

3. *Otvet spetspredstavitelya Prezidenta Rossiyskoy Federatsii po voprosam mezhdunarodnogo sotrudnichestva v oblasti informatsionnoy bezopasnosti A.V. Krutskikh na vopros informagentstva TASC o sostoyanii mezhdunarodnogo dialoga v etoy sfere* [Response of the Special Representative of the President of the Russian Federation for International Cooperation in the Field of Information Security A.V. Krutskikh to the Question of ITAR TASS News Agency about the Status of International Dialogue in this Sphere]. URL: http://www.mid.ru/foreign_policy/news/-/asset_publisher/cKNonkJE02Bw/content/id/2804288 (accessed 10 April 2018).

4. Tershukov D.A. Ob obespechenii mezhdunarodnoy informatsionnoy bezopasnosti [On ensuring international information security]. *Materialy VI Vserossiyskoy nauchno-prakticheskoy konferentsii «Aktualnye voprosy informatsionnoy bezopasnosti regionov v usloviyakh globalizatsii informatsionnogo prostranstva», g. Volgograd, 27–28 aprelya 2017 g.* [Proceedings of the 6th All-Russian Research and Practice Conference on Current Issues of Information Security of Regions in the Conditions of Information Space Globalization, Volgograd, 27-28 April 2017]. Volgograd, Izd-vo VolGU, 2017, pp. 3-6.

ANALYSIS OF MODERN INFORMATION SECURITY THREATS

Dmitry A. Tershukov

Head of Department of Special Documentary Communication and Information Protection,
Volgograd Region Governor's Office
dmitryiddt@mail.ru, kancel@volganet.ru
Prosp. Lenina, 9, 400098 Volgograd, Russian Federation

Abstract. In the modern world, knowledge and awareness have become the most important products, services have taken the lead, the global information space is rapidly

developing, while modern information technologies represent not only new opportunities in solving various problems, but also create fundamentally new challenges and threats.

The emergence of new information technologies and systems, the development and expansion of the functions of social networks, the introduction of a variety of services in social networks and their algorithmization have created tools for turning the historical process of human development from uncontrollable to manageable and even projected, there are opportunities to create a reality that does not correspond to reality, to influence the mass consciousness of millions of people around the world.

Currently, specialists in the field of information security require knowledge and skills that are at the intersection of various fields of knowledge: information technology, psychology, political science, law, criminology.

Meanwhile, graduates of technical universities do not always have sufficient knowledge and skills to properly assess the actions of the violator of information security, to understand the political component of the problems of information security. Graduates of humanities universities are not sufficiently versed in the specifics of threats to information security, the physical nature of the channels of information leakage. The way out of this situation can be the use of a system of retraining and advanced training of specialists in information protection.

Key words: information security, information environment, IT-infrastructure, threats, information systems.