ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ: МИФ ИЛИ РЕАЛЬНОСТЬ

Александра СЁМА

Рязанский институт (филиал) Московского политехнического университета,
Рязань, Россия

Corresponding author: Сёма Александра syomaalexa-aandra@yandex.ru

INFORMATION SECURITY: MYTH OR REALITY

Abstract: *The article is devoted to information security. Today, when computers and cell phones contain numerous data about its owner, when transactions are made through electronic document management, the lack of security of this information threatens material losses, loss of trust, damage to the reputation of both an individual and a company, or an entire country. Therefore, the state and society face new challenges: to protect themselves from cyber fraud, theft of personal data, computer viruses and cyber-attacks.*

Keywords*: Internet, information, information technologies, information protection, security, computer viruses, threats.*

Аннотация. *Статья посвящена информационной безопасности. Сегодня, когда компьютеры и сотовые телефоны содержат многочисленные данные о его владельце, когда сделки совершаются через электронный документооборот, отсутствие защищенности этой информации грозит материальными потерями, утратой доверия, ущерба для репутации как для отдельной личности, так и для компании, или целой страны. Поэтому перед государством и обществом встают новые задачи: защититься от кибермошенничества, похищения персональных данных, компьютерных вирусов и кибератак.*

Ключевые слова: *интернет, информация, информационные технологии, защита информации, безопасность, компьютерные вирусы, угрозы.*

Умение собирать, защищать и передавать информацию на протяжении веков определяло судьбы людей и наций. Когда-то наличие системы сигнальных факелов, гонцов или обученных почтовых голубей позволяло предупредить союзников о приближении врагов, тем самым решив исход сражений и целых войн. Телефон и телеграф помогали сколотить колоссальные состояния, предоставляя доступ к последним котировкам фондовых бирж. Именно для обмена информации люди веками создавали все необходимое: от наскальных рисунков до телевидения, от письменности до интернета.

Теперь любые письма моментально передаются через сеть. Гигантские массивы данных хранятся в облачных сервисах, а число мобильных телефонов превысило общую численность населения земли. С каждым днем новые технологии делают способы обмена информацией доступней и чем легче становится передать сообщение, тем проще и украсть его содержимое.

В далеком 1821 году Натан Ротшильд произнес свою знаменитую фразу: «Кто владеет информацией, владеет миром» не подозревая, как значима она будет 200 лет спустя, в век информационных технологий (Рис. 1).

Рис. 1 - Натан Ротшильд

Если мы посмотрим на 20-25 лет назад то видим, что мы живем уже в четвертой исторической эпохе: мы вошли в internet - web один, социальные сети - web два, вошли в web три – семантический интернет и когнитивный интернет – web четере.

Информационные технологии применяются в промышленности, торговле, в управление, в банковской системе, образовании, здравоохранении, медицине и науке, транспорте и связи, в сельском хозяйстве, системе социального обеспечения, помогают людям различных профессий и домохозяйкам. И с Эйнштейном теперь можно поспорить… Пока результаты спора неоднозначны, но можно с уверенностью сказать, что ускорение передачи информации до скорости света только дело времени и верных расчетов.

Любые технологии имеют две стороны: позитивную, если использовать их в целях развития и в рамках, не противоречащих международному праву, но с другой стороны любые технологии, которые порождают, провоцируют тех, кто овладел ими первыми, для того чтобы использовать их в геополитической борьбе.

С самого начала интернет бросил вызов традиционной журналистике по очень разным направлениям: первое это оперативность. Если раньше говорили о том, что бумажные средства информации газеты, журналы уступали электронным – телевидению и радио, то интернет уже бросил вызов электронным средствам массовой информации. То есть быстрота подачи любого текста, любой новости, репортажа.

Информационные технологии 21 века подобно мощному потоку способному мгновенно донести и сохранить огромные объемы различных сведений. На фоне удобств мы видим возрастание угроз: представим, что вы находитесь в банке, а с вашей карты с возможностями без контактной передачи данных, мимо прошёл человек, отсканировал вашу карту, списал с вашего счета все деньги (Рис. 2).

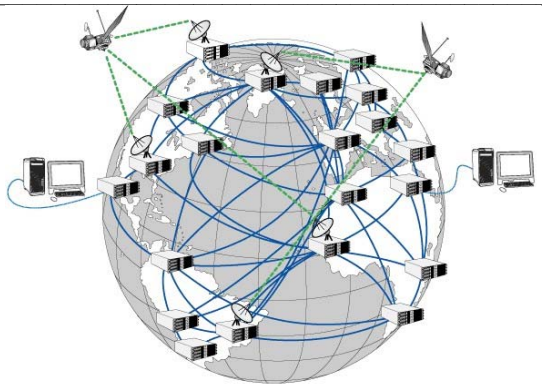

Рис. 2 – Глобальная сеть интернет

Тема защиты информации, в том числе персональных данных клиентов сейчас крайне актуальна. Сотрудники компании, включая руководителей высшего и среднего звена стремятся повысить свою квалификацию в области информационных технологий и способов защиты информации. Например, Генеральный секретарь ООН заявил, что мы вышли на уровень двух триллионов долларов ущерба для глобальной экономики, по оценкам российских экспертов, например, сбербанка мы выходим уже на уровень восьми триллионов, которые потенциально киберпреступность отнимает у мировой экономики. Этот стремительный поток, это огромное хранилище сведений, эта могучая сила способна поразить, уничтожить, исказить и исчезнуть… Эта сила действует, путем контентного воздействия, то есть воздействия на уровне мемов, хайпов, вбросов фэйков, а тем более deepfake, то есть глубоких фэйков с использованием искусственного интеллекта может влиять на подсознательном уровне на население. На территории России работала группа под названием F57, которая доводила подростков определенными заданиями, так называемые квестами, до суицида. Благодаря современным сетевым технологиям активность этой группировки блокировалась.

Выходит, парадокс, все мировое сообщество в век развитых экономических систем и технологий, которые призваны развивать, ускорять и защищать, вдруг оказалась тотально уязвимым и нуждающимся в безопасности. Наряду с военно-политическим измерением угроз использования информационно-коммуникационной технологий в виде боевых химер, вирусов, в виде иных зловредных программ используется методы, связанные с цифровым джихадом. Террористы активно используют новейшие технологии для вербовки и проведения терактов в мире. Методы, которые используют террористы, известны они находятся в тех же социальных сетях используя технологии вербовки. Кибер-инструменты позволяют анализировать, это элементы того же искусственного интеллекта которые большую часть работы обеспечивают по анализу, формированию и поиску таких преступных группировок.

Важно привлекать к разработке и внедрению методов только профессионалов, необходимо четко организовать взаимодействие внутри системы защиты с единым координационным центром. Соблюдение всех этих принципов намного снизит риск угроз и активно будет противостоять нежелательному контенту несанкционированному доступу и утечки информации, мошенничеству и все возрастающей террористической угрозе, кибер шпионажу и информационной войне.

Несколько лет назад была разработана открытая автоматизированная система под названием «Демон Лапласа» (Рис. 3), которая круглосуточно мониторит и собирает данные из сети Интернет, она позволяет получать и анализировать широкий спектр информации из социальных сетей «Facebook» и «VKontakte», микроблогов «Twitter», онлайн-СМИ.

Рис. 3 - Автоматизированная система «Демон Лапласа»

Нашими учеными специалистами используется практика применения целых блоков различного рода электронных словарей, например, социально психологический словарь, оксфордский словарь, целый пул инструментов базовых, на основе которых формируются программные комплексы и анализируется активность айпи-адресов, с которых распространяется экстремистская информация, вплоть до использования оружия, формирования, создания бомб, взрывчатых веществ и т.д. Выборка делается после того, как короткий список таких адресов сформирован и анализируется, далее определяется местоположение тех или иных компьютеров, с которых, запускаются эти ресурсы.

Важно учитывать комплексность задачи и обеспечить безопасность всех ресурсов и материальных, и финансовых, и информационных. Другой вызов – это достоверность, потому что по канонам традиционной, качественной журналистики, прежде чем дать информацию в массы у вас должно быть два или три источника, подтверждающие одну и ту же информацию. Социальные сети – как феномен, который последовал за развитием интернета и сейчас расцвел и живет бурным цветом. Некоторые пользователи, которые становятся быстро популярными в социальных сетях не придерживаются закона необходимости проверять информацию на достоверность. На самом деле это проблема многими СМИ была решена в определенной мере, когда они сами вышли в интернет, и стали работать в интернете. Тот же Китай, например, активно борется с фейковой ложной информацией, запустив определенные аналитические платформы, используя возможности искусственного интеллекта, например, платформа Quark Dot Com, которая запускалась как венчурный проект, но сейчас фактически с помощью этой платформы отслеживаются все фейковые новости, и вся ложная информация. Сейчас современный век такой быстротечный, что весь поток информации, если взять его за 100 процентов, всего лишь 10 процентов имплантированной в этот поток ложной информации, может перевернуть картину совершенно на противоположную, радикальную. Именно эта китайская платформа позволила спокойно измельчить и найти вот эту имплантированную

фальшь в потоке конкретной правдивой информации и ее опровергать, в том числе против Китая и других стран.

Актуальность этой темы обусловлена с одной стороны тем, что все больше количество государств начинает понимать необходимость координации усилий международного сообщества в противодействие угрозам, с другой стороны, снижением доверия граждан, бизнес-организаций, органов государственной власти к использованию информационных и коммуникационных технологий. Поток фейковой информации в социальных сетях, медийных сетях достиг такого уровня, что доверие в результате к этому информационному потоку падает и журналисты часто попадают в ловушки, используя возможности современных медийных агрегаторов, не проверив данные. Ответственность за достоверность информации, за ее правдивость и так далее фактически никто не несет. Этой теме посвящены многие международные форумы, встречи и совещания, на которых вырабатывается совместная тактика и стратегия, принимается решение о практических мерах, формируется общее понимание наиболее опасных угроз (Рис. 4). ООН (организация объединённых наций), ОБСЕ, БРИКС, СНГ и многие другие региональные структуры Asian занимаются данной проблемой, ибо информационные войны ведутся, и они становятся все более и более доступными для многих стран мира [1].

Рис. 4 – Распознавание фейковой ложной информации

Сформировалось общее понимание того, что наиболее опасными угрозами международной информационной безопасности на данном этапе являются продолжающийся рост масштабов компьютерной преступности, подготовка и осуществление актов компьютерного терроризма, а также использование информационных и коммуникационных технологий для силового разрешения межгосударственных противоречий. Конечно, самое неприятное использование и угрозы использования этих технологий заключается в нарушении цифрового суверенитета. Коллективный Запад, Соединенные Штаты активно используют гибридные воздействия для сдерживания России. В гибридном воздействие понимается политика дипломатическая, экономическая в виде санкций, военная и самое главное это информационная. Для гибридной войны не требуется объявление, она не подпадает под действие тех или иных правил, ведения войны, согласно международному праву.

Россия выступала с очень важными инициативами, некоторые из них были поддержаны большинством членов ООН, о необходимости создать международные правила поведения в информационно-коммуникационной среде, но, к сожалению, это наталкивается на противодействие Соединенных Штатах других крупных стран, которые хотят доминировать. Почему? Потому что считают, что ключи и командные высоты в информационных технологиях и в самом интернете принадлежат им, и они не хотят сдавать позиции. У России здесь есть союзники, в том числе и среди развитых стран в западной Европе, которые поддерживают необходимость каких-то общих правил, иначе заинтересованные лица будут обвинять кого угодно в вмешательстве в процессы выборов, потому что хакер может работать с территории любой страны будь то Гренландия, Россия или США. Это не значит, что его действия преступны, или санкционированные государством и приписывать какой-то стране ответственность за действия какого-то отдельного преступника нельзя. Провокации политического уровня могут иметь вплоть до непредсказуемых последствий.

Все большее количество государств объединяется для координации усилий, чтобы сообща противодействовать угрозам, которые все чаще возникают при использовании современных информационных и коммуникационных технологий. Это проблематика очень серьезна и поэтому Россия выступает за равноправное участие в формировании международного информационного правового поля с равными правами и обязанностями всех стран в этой сфере. Эти страны должны договориться между собой о правилах, которые могли бы в какой-то мере гарантировать международную безопасность в глобальной информационно-коммуникационной сети, могли бы совместно бороться с проявлением зла, особенно, конечно, это преступление против детей, которые с каждым годом растут.

Профессионалы и лидеры многих стран мира готовы к открытому диалогу и общим действиям, которые будут противостоять угрозам и защищать информацию в целом и информационные технологии в частности. Всех нас объединяет понимание того, что для развития глобального информационного общества необходимо обеспечить эффективное противодействие угрозам устойчивому функционированию и безопасному использованию глобальной информационной инфраструктуры, основу которой составляет интернет.

Сегодня, когда компьютеры и сотовые телефоны содержат многочисленные данные о его владельце, когда сделки совершаются через электронный документооборот, отсутствие защищенности этой информации грозит материальными потерями, утратой доверия, ущерба для репутации как для отдельной личности, так и для компании, или целой страны. Поэтому перед государством и обществом встают новые задачи: защититься от кибермошенничества, похищения персональных данных, компьютерных вирусов и кибератак. Поиск путей сохранения позитивного потенциала влияния глобальной информационной инфраструктуры на развитие человечества задача чрезвычайно важная и заслуживает самого пристального внимания.

Литература:

1. Прокопьева В.А. *Политика противодействия кибертерроризму в современной России: Выпускная квалификационная работа ФГБОУ ВО «УГПУ»* - Екатеринбург, 2017..
2. https://digital.report/aktualnyie-problemyi-mezhdunarodnoy-informatsionnoy-bezopasnosti/
3. http://protestonline.ru