КУЛЬТУРОЛОГИЯ

НОВЕЙШИЕ ИНТЕРНЕТ ТЕХНОЛОГИИ КОМПЛЕКСНО ОБРАБАТЫВАЮЩИЕ СОВРЕМЕННЫХ ЛЮДЕЙ

Дворянкин О.А.
кандидат юридических наук,
старший преподаватель кафедры информационной безопасности
Учебно-научного комплекса информационных технологий
Московского университета МВД России имени В.Я. Кикотя,
Москва

BRANDNEW INTERNET TECHNOLOGIES THAT WORK PEOPLE OF NOWADAYS

Dvoryankin O.A.
candidate of legal sciences,
lecturer at the chair of information security
of the Moscow Ministry of Internal Affairs
of the Russian Federation Kikot University,
Moscow

Аннотация

Информационные технологии – это один из ключевых векторов развития науки и образования в современном мире. Именно посредством данных технологий на сегодняшний день существуют самые инновационные разработки, повышающие эффективность работы различных предприятий и упрощающих процессы жизнедеятельности в быту обычных людей. Основной целью данной работы является изучение новейших Интернет технологий, комплексно обрабатывающих современных людей. В работе описана концепция информационных технологий, определены и выявлены основные тенденции, а также исследованы отдельные примеры технологий и их влияние на современного человека.

Abstarct

Information technologies are one of key vectors of development of science and education these days. Thanks to the technologies of this kind the brand-new development making the productivity of verious enterprises higher and our everyday lives easier. The main goal of this research is studying of brand-new information technologies that work people of nowadays. This article about information technologies describes the concept of information technologies, defines their basic tendencies. Author gives examples of information technologies themselves snd those ot their influence on people of nowadays.

Ключевые слова. Интернет, информационные технологии, информационная безопасность, образование, короновирус, COVID-19, вебкам моделинг, спуфинг, вишинг, фишинг

Keywords: Internet, information technologies, information security, education, coronavirus, COVID – 19, webcam modeling, spoofing, wishing, fishing.

Информационные технологии (ИТ) являются неотъемлемой частью жизни человека на сегодняшний день.

Они активно и быстро вошли в наше сознание и быт, что мы уже не представляем себя без их существования. При этом усовершенствования, включая в них «искусственный интеллект», «нейронные сети», мы даже не заметили, что ИТ не только стали нашим помощником в сети Интернет, но начали активно влиять на нас без нашего согласия.

Пока мы еще не чувствуем серьезную опасность в их влиянии, но первые и робкие попытки начали происходить и короновирус (COVID-19) это уже показал. Об этом я попробовал рассказать в статье «Covid-19. Первая информационная-инфекционная война или инфекционная-информационная война XXI века?»[1]

Далее ситуация будет только осложняться и обостряться. В этой связи мы должны заранее позаботиться о нашей личной информационной безопасности, предпринять все возможные предупреждающие мероприятия и действия.

Новые информационные технологии — это информационные технологии с «дружественным» интерфейсом работы пользователя, использующие персональные компьютеры и телекоммуникационные средства.

ИТ работают на базе использования множества средств и методов сбора, обработки данных «больших данных», а также передачи данных (больших данных) с целью получения информации

[1] Статья Дворянкина О.А. «Covid-19. Первая информационная-инфекционная война или инфекционная-информационная война XXI века?», опубликованная в журнале «Национальная Ассоциация Ученых» раздел «Юридические науки» 27/54 Том 1 2020. С. 43-47.

необходимого качества и состоянии какого-либо объекта, процесса или явления.

В этой связи основной целью информационных технологий является усовершенствование и автоматизация производственных процессов на предприятии и личных потребностей человека в быту.

На современных предприятиях происходит интенсивное распространение с совместным совершенствование цифровых и информационных технологий. Данное направление активно определяет основные траектории развития современной экономики и общества, а также приводит к колоссальным изменениям, касающихся жизни людей [1].

При этом ИТ ежедневно на современных предприятиях доказывают свое превосходство в сравнении с механическим трудом человека и рационализируют рабочую деятельность людей. Именно посредством информации организуется система последовательных операций с целью использования ресурсов и методов автоматизации различных процессов.

Также ИТ активно «обрабатывают» «бытовую» повседневную деятельность человека, где в виде обычного общения, просмотра фильмов, прослушивания музыки, участия в играх, контроля за ребенком, бизнес мероприятия или «умный дом» и т.д. с одной стороны оказывает необходимую помощь, а с другой стороны становится контролером и даже надсмотрщиком.

С учетом изложенного представляется необходимо отметить, что на сегодняшний день существует множество подходов относительно проблемы классификации и понимания информационных технологий.

Так, несмотря на всю распространенность, определение «информация» остается одним из самых обсуждаемых понятий в науке, а сам термин имеет множество различных значений в разных отраслях деятельности человека.

Посредством информации и ИТ передаются конфиденциальные данные, производятся транзакции на различных предприятиях, финансовые сделки с цифровой валютой (криптовалюта) производится хранение и работа с засекреченной информацией, осуществляется информационная безопасность и так далее. Данный список можно перечислять бесконечно, так как в век информации практически все процессы, происходящие в жизнедеятельности человека, основывается на применении информационных технологий и информации, в частности [2].

Таким образом можно констатировать, что развитие компьютерных и ИТ полностью изменило реальность и действительность в которой живут современные люди.

В этой связи в современном языке появились новые понятия: киберпространство, киберкультура, киберторговля, киберполитика, киберреклама, киберпреступность, а киберпсихология – новый раздел психологии – изучает особенности киберобщения.

В предыдущих статьях (исследованиях) совместно с соавторами мною уже было обращено внимание на данную тему и нами предлагались конкурентные предложения.[2]

В настоящей работе продолжаю исследование и предлагаю новые определения и понятия ИТ.

Развитие интернет-технологий породило новые проблемы в философии, психологии, социологии и одна из них – проблема виртуального общения, где главное - информационная безопасность.

Появившись как результат технической революции и развития познания и науки, Интернет стал самодостаточным, а его создатели – простыми пользователями, также, как и другие "жители" Всемирной сети. При этом необходимо отметить, что у Интернета, возможно, есть границы, но эти границы расширяются вместе с возможностями и стремлениями человека.

Как и многие другие технические достижения, Интернет таит в себе не только огромный потенциал, но и опасности.

Отчаянные критики новой киберкультуры утверждают, что Интернет и ИТ разрушают традиционную культуру, образ мышления и жизни человека, а их победа будет иметь катастрофические последствия для человечества. Главный аргумент критиков заключается в том, что компьютерные технологии деформируют чувство реальности, позволяющее человеку отличать действительность от воображения, реальность от иллюзии. Подобные изменения сознания особенно заметны у любителей компьютерных игр, ученые заявляют о том, что каждый десятый киберигрок становится зависимым от игровой программы. Помимо изменений в психике погружение в виртуальную реальность влечет и очевидные проблемы со здоровьем, ведь человек большую часть времени проводит почти неподвижно за компьютером [3].

На сегодняшний день существует множество ИТ, влияющих на психологическую составляющую человека в Интернете в целом. Примерами

[2] Дворянкин О.А. Грибанская Е.Э., Никитина Е.С. «Повышение компьютерной, правовой и языковой грамотности бизнес-сообщества в интернет-сфере» Журнал «Национальная Ассоциация Ученых» раздел «Культурология» 28/55 Том 3 2020. С. 8-12.
Дворянкин О.А. Грибанская Е.Э., Никитина Е.С. «Информационное противоборство как манипулирование сознанием людей от прямых боевых столкновений до виртуальных боев в социальных сетях Интернета» Журнал «Национальная Ассоциация Ученых» раздел «Культурология» 28/55 Том 3 2020. С. 12-17.
Дворянкин О.А. «Как бизнес сообществу спастись от преступлений нового поколения?» Журнал «Безопасность бизнеса» №2 2020 С. 60-64

подобных технологий и процессов является работа в **вебкам моделинге, спуфинг, вишинг, фишинг** и другое. Рассмотрим наиболее подробно некоторые из них.

Работа **вебкам моделью** — вид заработка, который появился благодаря специфике виртуального общения. Если говорить просто: вам платят за общение с людьми через видеокамеру в Интернете. Чаще всего девушкам за общение с мужчинами. Это целое искусство — как сделать общение интересным для обоих, но максимально долгим и соответственно выгодным для модели. Объективно, даже в категориях без обнажения женщины или мужчины чаще всего стороны хотят общаться в романтическом ключе.

При этом есть и «жесткий» веб моделинг, когда сторона, которая заказывает веб модель требует от нее за деньги выполнение, как сексуальных, так и садистских или садомазохистских действий. При этом к просмотру подкачаются друзья и знакомые закачка и тогда мероприятие проходит в формат «видеоконференции», где они видят веб модель, а они их не видит.

Компании и люди, работающие в данной сфере, не всегда имеют строгий список правил общения, который защищает обе стороны. Некоторые веб модели работаю самостоятельно, чтобы ни от кого не завесить.

Если же правила обговорены заранее, то за несоответствующее поведение веб модели могут сделать предупреждение *(например, за оголение в категории, где это запрещено)*, а клиента блокируют если он нарушил правила. Также можно в любой момент прекратить разговор с клиентом, добавив его в черный список. Наряду с этим, очень важно — можно заблокировать клиентов из определенной страны *(например, заблокировав свою страну, таким образом Вы ограждает себя от риска «встретиться» со знакомыми или «нежелательными» людьми)*.

Еще одним видом защиты является выбор псевдонима и нужного образа. Кроме этого желательно находиться в безопасном месте, например, дома или в «студии» с партнерами или с охранниками, в том числе с специалистами информационной безопасности. *Наряду с этим, чтобы себя обезопасить, определяются условия, что к*лиенты не имеют права задавать личных вопросов о местонахождении или настоящем имени модели *(если и спросят, то можно выдумать все что угодно)*.

Для дополнительной защиты конфиденциальности, платежи моделям приходят от компании с анонимным названием, не связанным с веб-моделингом. Оплата проходит через электронные кошельки и посредством криптовалюты (О том, что такое криптовалюта и как она влияет на людей и на бизнес-отношения мною была подготовлена и выпущена книга[3].)

Так, например, некоторые веб-модели для получения денег используют «Payoneer» — платёжную систему, предоставляющую финансовые услуги и денежные онлайн-переводы. «Payoneer» является зарегистрированным провайдером MasterCard по всему миру. Штаб-квартира компании находится в Нью-Йорке.

Таким образом подводя итог вебкам моделингу можно отметить его преимущества и недостатки, т.е. особенности ИТ.

Преимущества вебкам моделинга:

– Вы не привязаны к времени или месту и сами формируете рабочий график. Работа может быть основной или служить дополнительным заработком. Общение обычно происходит вечером или ночью, что дает возможность сочетать работу вебкам моделью с обучением или основной работой;

– если раньше вы мечтали попробовать себя в качестве модели, однако внешние параметры не позволяли, то для веб-моделинга эти критерии не являются обязательными, главное подать себя как интересную личность и хорошего собеседника;

– работа вебкам моделью приносит «определенный» доход, зарплата выплачивается в различных валютах;

– не требуется предварительного опыта, который так часто сразу требуют работодатели.

Недостатки:

– в традиционном обществе, с религиозными устоями и традициями, данный вид заработка считается чем-то неприемлемым.

– можно столкнуться с неадекватными клиентами, с которыми вы не обязаны общаться. Их легко заблокировать, и сосредоточится на общении только с интересными вам людьми;

– данная деятельность в каком-то смысле предпринимательство, и для многих на первом этапе будет сложно в нее сразу войти и понять все сложности и трудности. Но «определенный» заработок в разных видах валют мотивирует достаточно или даже очень сильно.

– общение иногда может оказаться непривычным. Например, клиентами может оказаться пара, которая захотела разнообразия в своих отношениях или компания, которая празднует мальчишник (девичник) и тому подобное;

– могут произойти и другие действия, к которым Вы можете оказаться не готовы, и они покажутся Вам приятными, интересными, увлекательными или наоборот недостойными, противными, враждебными, омерзительными и т.д.

Следующей технологией, которая будет изучена в настоящей статье, психологического воздействия в Интернете является IP-спуфинг.

[3] Дворянкин О.А «По ту сторону Введенских ворот. Криптовалюта – виртуальная реальность…?!» LAP LAMBERT Academic Publishing RU, 2020 г. С. 110.

IP-спуфинг — это:

1) вид хакерской атаки, заключающийся в использовании чужого IP-адреса источника с целью обмана системы безопасности. 2) Метод, используемый в некоторых сетевых атаках и состоит в изменении поля «адрес отправителя» IP-пакета. Применяется с целью сокрытия истинного адреса атакующего, с целью вызвать ответный пакет на нужный адрес, а также с иными целями.

Для злоумышленника базовый принцип атаки заключается в фальсификации собственных заголовков IP-пакетов, в которых изменяется, среди прочего, IP-адрес источника. Атака IP-спуфинг часто называется «слепой подменой» (Blind Spoofing). Однако всё-таки существуют два метода получения ответов:

Маршрутизация от источника (en:Source routing): В компьютерных сетях маршрутизация источника, также называемая адресацией пути, позволяет отправителю пакета частично или полностью указать маршрут, по которому пакет проходит через сеть. Напротив, в обычной маршрутизации маршрутизаторы в сети определяют путь постепенно, основываясь на пункте назначения пакета.

Перемаршрутизация (Re-routing): процесс определения маршрута данных в сетях связи. Маршруты могут задаваться административно, либо вычисляться с помощью алгоритмов маршрутизации, базируясь на информации о топологии и состоянии сети, полученной с помощью протоколов маршрутизации.

Тактикой выдачи себя за кого-то в целях получения доступа к конфиденциальным данным или банковским счетам успешно пользуются не только преступники в реальном мире, но и их коллеги по цеху в виртуальном пространстве.

Данная практика носит название **спуфинг** — собирательная категория, включающая в себя понятия спуфинга IP адресов (отправка сообщений на компьютеры с использованием IP-адреса доверенного источника), email спуфинг (подделка заголовка писем для маскировки истинного отправителя) и DNS спуфинг (изменение настроек сервера DNS для переадресации доменного имени на IP адрес злоумышленников) [4].

Спуфинг - это технический прием выдачи себя за другое лицо, чтобы обмануть сеть или конкретного пользователя с целью вызвать доверие в надежность источника информации. К примеру, хакеры посредством email спуфинга могут ввести пользователя в заблуждение относительно подлинности отправителя и получить доступ к конфиденциальным данным. Или они могут попытаться применить технику спуфинга IP и DNS-запросов, чтобы обмануть сеть пользователя и переадресовать его на мошеннические сайты, маскирующиеся под настоящие, в результате чего компьютер пользователя будет заражен [5].

Наиболее просто распознать email-спуфинг вследствие того, что непосредственной мишенью является сам пользователь. Любое сообщение по электронной почте, в котором от пользователя требуется личная информация, может быть попыткой спуфинга, в особенности, если запрашиваются учетные данные. ***(Ни одна надежная частная или государственная организация не запрашивает персональные данные таким путем.)***

Обратите внимание на адрес отправителя, чтобы убедиться в его легитимности.

Тем не менее, пользователь практически никогда не узнает, что он стал жертвой IP или DNS-спуфинга, хотя привычка обращать пристальное внимание на детали и изменения привычного поведения сайта могут оказаться чрезвычайно полезны. Если сайт или его поведение вызывают малейшее сомнение, лучше отказаться от совершения запланированной операции, чтобы сохранить данные и финансовые средства в безопасности.

Спуфинг заключается в маскировке истинного источника, поэтому его не так просто "устранить". Обезопасить себя можно лишь следуя здравому смыслу и соблюдая базовые правила безопасной работы в сети (информационная безопасность), например, не при каких условиях, не сообщая свои персональные данные по электронной почте, даже если репутация отправителя не вызывает сомнения [6].

С одной стороны, защита от спуфинга может заключаться в следовании базовым принципам безопасной работы в Интернете. Однако Вы можете сделать значительно больше в целях собственной безопасности. Прежде всего можете доверить защиту своего персонального компьютера и хранимых на нем данных компаниям, занимающихся информационной безопасностью, которые надежно защищают от мошеннических сайтов и блокируют вирусы, пытающиеся проникнуть в вашу сеть.

Еще одной информационной технологией, воздействующей в Интернете, является фишинг.

Фишинг – это совокупность методов, позволяющих обмануть пользователя и заставить его раскрыть свой пароль, номер кредитной карты и другую конфиденциальную информацию. Чаще всего злоумышленники выдают себя за представителей известных организаций в электронных письмах или телефонных звонках [7].

Фишинг (от англ. fishing – рыбная ловля) представляет собой противоправное действие, совершаемое с целью заставить то или иное лицо поделиться своей конфиденциальной информацией, например, паролем или номером кредитной карты. Как и обычные рыбаки, использующие множество способов ловли рыбы, «коварные» мастера фишинга также применяют ряд методов, позволяющих «поймать на крючок» свою жертву.

Одной из распространенных тактик ИТ фишинга является следующая: жертва получает электронное письмо или текстовое сообщение, отправитель которого выдает себя за определенное лицо или организацию, которым жертва доверяет, например, за коллегу по работе, сотрудника банка

или за представителя государственного учреждения. Когда ничего не подозревающий получатель открывает это электронное письмо или сообщение, то он обнаруживает пугающий текст, специально составленный таким образом, чтобы подавить здравый смысл и внушить страх. Текст требует от жертвы перейти на веб-сайт и немедленно выполнить определенные действия, чтобы избежать опасности или каких-либо серьезных последствий.

Если пользователь «клюет на наживку» и переходит по ссылке, то он попадает на веб-сайт, имитирующий тот или иной законный Интернет-ресурс. На этом веб-сайте пользователя просят «войти в систему», используя имя своей учетной записи и пароль. Если пользователь оказывается достаточно доверчивым и соглашается, то введенные данные попадают напрямую к злоумышленникам, которые затем используют их для кражи конфиденциальной информации или денежных средств с банковских счетов; кроме того, они могут продавать полученные личные данные на черном рынке [8].

В отличие от других угроз, встречающихся на просторах Интернета, фишинг не требует наличия глубоких технических знаний.

Адам Куява, директор компании «Malwarebytes Labs», заметил, что фишинг представляет собой простейший способ кибератаки, который, тем не менее, является одним из самых опасных и эффективных. Происходит это потому, что объектом атаки становится самый мощный, но одновременно и самый уязвимый компьютер в мире – человеческий разум.

Фишинговые мошенники не пытаются воспользоваться техническими уязвимостями в операционной системе устройства, они прибегают к методам так называемой социальной инженерии. От «Windows» и «iPhone» до «Mac» и «Android» – ни одна операционная система не обладает полной защитой от фишинга, какими бы мощными ни были ее антивирусные средства.

В действительности злоумышленники часто прибегают к фишингу, *потому что* не могут найти какие-либо технические уязвимости. Зачем тратить время на взлом многоуровневой защиты, когда можно обманным путем заставить пользователя добровольно раскрыть свои данные?

В большинстве случаев самым слабым звеном в защите системы является не ошибка, затерянная глубоко в программном коде, а сам пользователь, который не обращает внимание на отправителя очередного электронного письма.

Еще до того, как термин «фишинг» прочно вошел в обиход, методы фишинга были подробно описаны в докладе и презентации, которые подготовила в 1987 году компания «Interex» (International HP Users Group).

Использование этого термина начинается в середине 1990-х годов, а его первое упоминание приписывается печально известному спамеру и хакеру Хану Си Смиту (Khan C Smith).

Кроме того, в Интернете сохранился первый случай публичного упоминания термина «фишинг». Это произошло 2 января 1996 года в электронном портале «Usenet» – в новостной группе «AOHell». На тот момент компания «America Online» (AOL) являлась крупнейшим Интернет-провайдером, ежедневно обслуживающим миллионы подключений.

Разумеется, популярность компании «AOL» непременно сделала ее целью мошенников. Хакеры и распространители пиратских программ использовали ее ресурсы для обмена сообщениями, а также для совершения фишинговых атак на компьютеры законопослушных пользователей. Когда «AOL» приняла меры и закрыла группу «AOHell», злоумышленники взяли на вооружение другие методы. Они отправляли пользователям сетей «AOL» сообщения, в которых представлялись сотрудниками «AOL» и просили пользователей проверить данные своих учетных записей или передать им свои платежные реквизиты. В итоге проблема стала настолько острой, что компания «AOL» начала добавлять предупреждения к каждому электронному письму, особым образом указывая, что ни один сотрудник «AOL» не станет просить сообщить ему пароль или платежные реквизиты пользователей [9].

С наступлением 2000-х годов фишинговые мошенники начали обращать свое внимание на уязвимости систем электронных платежей. Клиенты банков и платежных систем стали все чаще становиться жертвами фишинга, а в некоторых случаях – как показало последующее расследование – злоумышленникам даже удавалось не только точно идентифицировать своих жертв, но и узнавать, каким банком они пользовались. Социальные сети также стали одной из главных целей фишинга в силу своей привлекательности для мошенников: личная информация, публикуемая в социальных сетях, является отличным подспорьем для кражи идентификационных данных.

Киберпреступники регистрировали десятки доменов, которые настолько изящно имитировали такие ресурсы, как «eBay» и «PayPal», что многие не слишком внимательные пользователи просто не замечали подмены. Клиенты системы «PayPal» получали фишинговые электронные письма (содержащие ссылки на подставной веб-сайт) с просьбой обновить номер кредитной карты и другие персональные данные. В сентябре 2003 года о первой фишинговой атаке против банка сообщил журнал «The Banker» (принадлежащий компании The Financial Times Ltd.).

В середине 2000-х годов на черном рынке можно было заказать «под ключ» вредоносное ПО для фишинга. В то же время хакеры начали координировать свои действия, чтобы организовывать все более изощренные фишинговые атаки. Трудно оценить даже приблизительные потери от успешных фишинговых атак: как сообщал в 2007 году отчет компании «Gartner», за период с августа 2006 года

по август 2007 года около 3,6 миллиона взрослых пользователей потеряли 3,2 миллиарда долларов.

Следующей технологией, которая будет изучена в данной статье, психологического воздействия в Интернете является вишинг.

Вишинг (англ. vishing, от Voice phishing) — один из методов мошенничества с использованием социальной инженерии, который заключается в том, что злоумышленники, используя телефонную коммуникацию и играя определённую роль (сотрудника банка, покупателя и т. д.), под разными предлогами выманивают у держателя платежной карты конфиденциальную информацию или стимулируют к совершению определённых действий со своим карточным счетом / платежной картой. Это распространенный сценарий. Кто-то заходит в социальную сеть, нажимает на соблазнительную ссылку и видит перед собой синий экран с предупреждающим сообщением и бесплатным номером телефона, по которому следует позвонить для устранения серьезной проблемы с компьютером [10].

На звонок отвечает вежливый технический специалист, который готов оказать вам любую помощь. После того, как пользователь предоставит информацию о своей кредитной карте для оплаты программного обеспечения, необходимого для решения проблемы с компьютером, мошенническая акция, которая дорого обходится жертве, завершается.

Программное обеспечение не работает, вежливый технический специалист исчезает. А пользователь становится еще одной жертвой мошенничества, называемой «вишинг» [11].

Вишинг – это устная разновидность мошенничества, при которой злоумышленники, используя телефонную коммуникацию, под разными предлогами стимулируют людей к совершению действий якобы в их собственных интересах.

По данным экспертов в 2015 году мошенничество с кредитными картами стало глобальным бизнесом, принесшим его участникам доход в 16 миллиардов долларов США, и доля вишинга в нем составила более 1 миллиард долларов США.

По сути, вишинг начинает действовать в любое время, как только преступники получают доступ к личной информации жертв.

Сегодня существуют технологии, которые позволяют злоумышленникам заблокировать телефонную линию жертвы после окончания разговора, и перенаправлять все следующие звонки пользователя на мошенническое вызывное устройство.

Людям, которые считают, что проблема может действительно существовать, следует использовать другой телефон для звонка на официальный номер.

В этой связи технический специалист, который устраняет последствия инцидента безопасности на вашем компьютере, всегда настоятельно рекомендует Вам пароли к аккаунтам, уведомлять об инцидентах свои банки и кредитные организации и внимательно отслеживать финансовые транзакции и его предупреждения являются своевременными и актуальными.

Хотя вишинг и его онлайн-брат фишинг в ближайшее время никуда не денутся, бдительность и здоровая доза скептицизма помогут уменьшить риск потерь от этих типов мошенничества.

Таким образом, можно констатировать, что на сегодняшний день, в XXI веке, информационные технологии в Интернете не всегда используются с положительными и рациональными намерениями, а очень часто и с целью незаконного обогащения, травли людей, иных негативных действий и в будущем, вероятно, они будут совершенствоваться и улучшаться. В этой связи необходимо уже сейчас задуматься о мерах защиты, оптимизации мер информационной безопасности и верным, грамотным действиям в будущем.

Государства и правительства в последнее время все активнее обсуждают вопросы информационного развития и информационной безопасности общества и стараются принимать необходимые нормативные правовые документы, но при этом очень часто запаздывают и ИТ молниеносно прорываются дальше в просторах сети Интернет.

При этом некоторые эксперты и политики считают возможным, необходимым и предлагают ввести цензуру в Интернете, что по их мнению прекратит и ограничит «информационный хаос» и «противозаконные действия», но выглядят такие пожелания и действия «весьма» сомнительно.

Информационные технологии стали основным инструментом в работе человека с информацией, которые охватывают всю компьютерную технику, бытовую электронику, телевидение, радио и, конечно, Интернет, но при этом и инструментом в работе информации с человеком.

Таким образом, невозможно, в новом тысячелетии цифровизации будет игнорировать или просто отмахнуться от влияния ИТ в сети Интернет на бизнес, политику и повседневную жизнь, но делать что-то надо, и в этом случае представляется целесообразным обратиться к старым ИТ, и, модернизировав их с учетом краеугольных положений современности, т.е. свободы слова, свободы волеизъявления, независимости, самодостаточности, безопасности и т.д., применить на практике.

В этой связи, кто первый из мировых государств и лидеров, с участием государственных и частных компаний сможет грамотно и верно осуществить такие действия, тот на долгие годы обеспечит свое лидерство на мировой арене и при этом минимизирует криминальную составляющую.

Список литературы

1. Минькович Т.В. Информационные технологии: понятийно-терминологический аспект // ОТО. 2012. №2.

2. Развитие определений "информатика" и "информационные технологии" / И.А. Мизин, И.Н. Синицын, Б.Г. Доступов, В.Н. Захаров, А.Н.

Красавин / Под ред. И.А. Мизина. - М.: ИПИ АН СССР, 1991.

3. Информатика: Учебник. – 3-е перераб. изд. / Макарова Н. В., Матвеева Л. А., Бройдо В. Л. И др. / Под ред. Н.В. Макаровой. - М.: Финансы и статистика, 2004.

4. Колин К.К. Социальная информатика: Учебное пособие для вузов. – М.: Академический Проект; М.: Фонд «Мир», 2003.

5. Кузнецов Н.А., Любецкий В.А., Чернавский А.В. О понятии информационного взаимодействия, 1: допсихический уровень // Информационные процессы. Том 3. – 2003.

6. Лаврентьева Г.М., Новосёлов С.А., Козлов А.В., Кудашев О.Ю., Щемелинин В.Л., Матвеев Ю.Н., Де Марсико М. Методы детектирования спуфинг-атак повторного воспроизведения на голосовые биометрические системы // Научно-технический вестник информационных технологий, механики и оптики. 2018.

7. Lee K.A., Larcher A., Wang G. et al. The RedDots data collection for speaker recognition // Proc. of Interspeech. Dresden, Germany, 2015.

8. Todisco M., Delgado H., Evans N. A new feature for automatic speaker verification antispoofing: Constant Q cepstral coefficients // Proc. Odyssey. Bilbao, Spain, 2016.

9. Lavrentyeva G., Novoselov S., Malykh E., Kozlov A., Kudashev O., Shchemelinin V. Audio replay attack detection with deep learning frameworks // Proc. of Interspeech. Stockholm, Sweden, 2017.

10. Sebastien M., Nixon M.S., Li S.Z. Handbook of Biometric AntiSpoofing: Trusted Biometrics under Spoofing Attacks. Springer, 2014.

11. Faundez-Zanuy M., Hagmuller M., Kubin G. Speaker verification security improvement by means of speech watermarking // Speech Communication. 2006.