УДК 316

ИНФОРМАЦИОННАЯ АГРЕССИЯ – НОВЫЕ ВЫЗОВЫ И ПЕРСПЕКТИВЫ В ОБЛАСТИ ТЕХНИКИ И ИДЕОЛОГИИ

Information aggression – new challenges and prospects in the field of technology and ideology

Д. Н. Багрецов
кандидат филологических наук, доцент кафедры иностранных языков
Уральский государственный юридический институт МВД РФ
(Екатеринбург, ул. Корепина, 66)
аспирант
Уральский институт управления – филиала РАНХиГС
(Екатеринбург, ул. 8 Марта, 66)

Рецензент: Б. А. Воронин, доктор юридических наук, профессор

Аннотация

Синтезируя выводы известных зарубежных ученых, автор делает заключение о трансформации мирового пространства в новое пространство – информационное.

Это обстоятельство вызывает проявление информационной агрессии, например, внедрение компьютерных вирусов, атаки на интернет-ресурсы иные противоправные действия, о чем информирует автор научной статьи.

Разнообразие информационного оружия, форм и способов особенности появления и применение порождают сложнейшие задачи по защите от него.

Ключевые слова: интернет, информация, информацтонное оружие.

Summary

Synthesizing the conclusions of well-known foreign scientists, the author makes a conclusion about the transformation of the world space into a new space - information.

This circumstance causes the manifestation of information aggression, for example, the introduction of computer viruses, attacks on Internet resources, and other illegal actions, as reported by the author of the scientific article.

A variety of information weapons, forms and methods, the features of their appearance and use give rise to the most difficult tasks of protecting against them.

Keywords: Internet, information, information weapon.

На современном этапе развития общества все большее значение приобретает информация. Вместе с этим многие традиционные ресурсы человеческого прогресса постепенно утрачивают свое первоначальное значение. Идеологии в активно изменяющемся обществе физически не могут сохраняться в прежнем виде и различным образом эволюционируют. Изменения связаны прежде всего с тем, что информация становится главным ресурсом научно-технического и социально-экономического развития. Уже принято говорить о новой общественной формации - об «информационном обществе» (основу этой концепции заложили З. Бжезинский, Д. Белл, О. Тоффлер) [1, 2, 3]. При этом речь зачастую идет о принципиально новой общественной формации. С развитием технологий изменились отношения между эксплуататором и эксплуатируемым, - эксплуатация физическая уступает место эксплуатации интеллектуаль-

ной. Сместилось ощущение пространства и времени, иное содержание вносит эпоха в традиционные понятия «близко - далеко», «давно - недавно». Яркий пример технологически обусловленного глобального сдвига в общественном сознании дает развитие сети Internet. В определенном смысле, происходит трансформация мирового пространства: наряду с географическим пространством формируется новое пространство – информационное [4].

Итак, информация - новый ресурс, уникальный продукт не убывающий, а растущий со временем, и обладание им дает новые возможности [6]. Чем больше и быстрее внедряется качественной информации в народное хозяйство и специальные приложения, тем выше жизненный уровень народа, экономический, оборонный и политический потенциал страны. Оттуда же не могут не исходить новые угрозы и вызовы – возможности одних как правило превращаются в угрозы для других.

Глобальная сеть Internet инициирует процесс создания новой, виртуальной среды обитания человеческой цивилизации. Совокупное воздействие информационной технологии, Internet и электронной торговли позволяет сегодня фиксировать такой же преобразовательный эффект, какой вызвала в свое время промышленная революция в Европе. По нашему предположению, именно эти два фактора будут и далее изменять мировой экономический ландшафт и трансформировать организационные структуры государств.

Очевидно, что целостность современного мира как сообщества обеспечивается в основном за счет интенсивного информационного обмена. Приостановка глобальных информационных потоков даже на короткое время способно привести к не меньшему кризису, чем разрыв межгосударственных экономических отношений.

Уже сегодня, по заявлениям некоторых иностранных экспертов, отключение компьютерных систем приведет к разорению 20% средних компаний в течение нескольких часов, 48% потерпят крах в течение нескольких суток. Около 33% банков будут разорены спустя несколько часов после такой катастрофы, а 50% из них разорятся спустя несколько суток. Сегодня Internet - это динамическая, в значительной степени самоорганизующаяся система, позволяющая говорить о новом социальном явлении - открытом Internet-сообществе.

По данным статистики агентства "ИнфоАрт", в России более 350 тысяч компьютеров подключены к Internet, что обеспечивает доступ к сети примерно 900 тысячам человек. При этом основные информационные источники системы находится в США, и отношения между нашими странами оставляют серьезный шанс для негативных последствий вплоть до полного отключения сети и почтовой связи [7].

Первичное проявление информационной агрессии – несанкционированное проникновение в информационную систему (ИС). По итогам 1999 года в США зафиксировано около 250000 случаев вторжения в ИС государственного назначения (кроме ИС военного назначения). Почти 160000 (65%) таких вторжений оказались успешными. Зафиксировано свыше 160000 вторжений в ИС Министерства обороны США. Количество вторжений в ИС государственного и военного назначения каждый год увеличивается, в среднем, в два раза.

Возросло количество случаев намеренного внедрения компьютерных вирусов в ИС государственного и военного назначения: с 583 в 1995 году и 896 - в 1996 г, 1200 - в 1999 году. По данным Kaspersky Security Network, во втором квартале 2021 года:

«Решения «Лаборатории Касперского» отразили 1 686 025 551 атаку с интернет-ресурсов, размещенных по всему миру.

Зафиксировано 675 832 360 уникальных URL, на которых происходило срабатывание веб-антивируса.

Запуск вредоносного ПО для кражи денежных средств через онлайн-доступ к банковским счетам предотвращен на компьютерах 119 252 уникальных пользователей.

Атаки шифровальщиков отражены на компьютерах 97 451 уникального пользователя» [8].

Как видим, налицо взрывной рост информационной агрессии.

Наиболее часто используемый канал, по которому осуществляется несанкционированный доступ - это сеть Internet (65% случаев). По результатам тестирования установлено, что 2/3 коммерческих и государственных узлов Internet не защищены от вторжения хакеров.

Внешние атаки могут преследовать и более серьезные цели, чем пассивный сбор данных, - такие, как, например, выведение из строя главных компьютерных узлов. По мнению экспертов, чтобы парализовать жизненно важные точки созданной инфраструктуры, достаточно нанести удар всего по нескольким десяткам объектов.

Результаты тестирования в 1995-1996 г.г. Министерством обороны США 8932 ИС военного назначения с применением средств проникновения, используемых хакерами, показали, что в 7860 (88%) случаях попытки проникновения обнаружены не были [5].

В последние годы в США и в отдельных государствах Европы (Франции, Великобритании, Швейцарии) активно осуществляется реализация концепций комплексной защиты информационных инфраструктур государств, основой которых являются информационные системы.

Сейчас как никогда актуальна проблема информационного вторжения в компьютерные сети с применением информационного оружия. Выход этой угрозы на первый план связан с тем, что современные системы управления являются системами критических приложений с высоким уровнем компьютеризации. Они могут оказаться весьма уязвимыми с точки зрения воздействия информационного оружия, как в военное, так и в мирное время. Такое воздействие может привести к тому, что к угрожаемому периоду (т.е. периоду времени, предшествующему вооруженному конфликту) оружие сдерживания страны, подвергшейся агрессии, за счет скрытого внедрения в программное обеспечение систем управления программных закладок окажется полностью или частично заблокированным. О реальности этого утверждения свидетельствует опыт войны в Персидском заливе. Ирак практически не смог применить закупленные во Франции системы ПВО потому, что их программное обеспечение содержало логические бомбы, которые были активизированы с началом боевых действий.

Разнообразие информационного оружия, форм и способов его воздействия, особенности появления и применения породили сложнейшие задачи защиты от него. К сожалению, иностранные специалисты первыми поняли и оценили значение информационного оружия, что послужило поводом к разработке стратегической концепции строительства вооруженных сил стран НАТО на ближайшую перспективу, - "Единая перспектива 2010" (Joint Vision 2010) - в основу которой положено информационное превосходство над противником на всех стадиях развития конфликта.

Военные эксперты США военные неоднократно выражали уверенность, что информационное оружие является, наряду с ядерным, стратегический, при существенно меньших рисках его применения. Вывод: господство в области разработки и применения информационного оружия укрепит мировое лидерство США в новом веке. Господство это носит двоякий характер – технический и идеологический, при этом первый достаточно молод, в то время как второй, идеологический, разрабатывался еще в эпоху тайных обществ [10].

Новейшая история показывает правильносмть э

Того вывода, особенно показателен пример Украины. Крупнейшее европейское государство в резуоьтате массированного и безконтрольного применения иенформационного оружия

оказалось, по выражение президентиа России В.В.Путина, «под внешним управлением», стало объектом грабежа со стороны соседей и ареной боевых действий между регионами собственной страны.

Необходимо противостоять угрозе», на всех уровнях, то есть укреплять техническую оснащенность и защищенность отечественного сегмента сети Интернет, и при этом готовить новое поколение россиян к противостоянию угрозам идеологическим и психологическим.

Этим объясняется большой интерес и активность американцев в исследовании проблем информационной войны. Все сказанное подтверждается докладами и дискуссиями на ряде международных конференции по информационной войне, большую часть участников которых составляют сотрудники государственных учреждений, армии и разведывательного сообщества США - АНБ, ЦРУ, ФБР.

В феврале – мае 2020 года чётко прослеживается постоянный помесячный рост (с последующим снижением в июне) процента компьютеров АСУ, на которых решениями «Лаборатории Касперского» фиксировались попытки подбора паролей к RDP.

По всей видимости рост по этому параметру процента атакованных компьютеров АСУ спровоцирован увеличением частоты использования RDP в феврале – июне этого года.

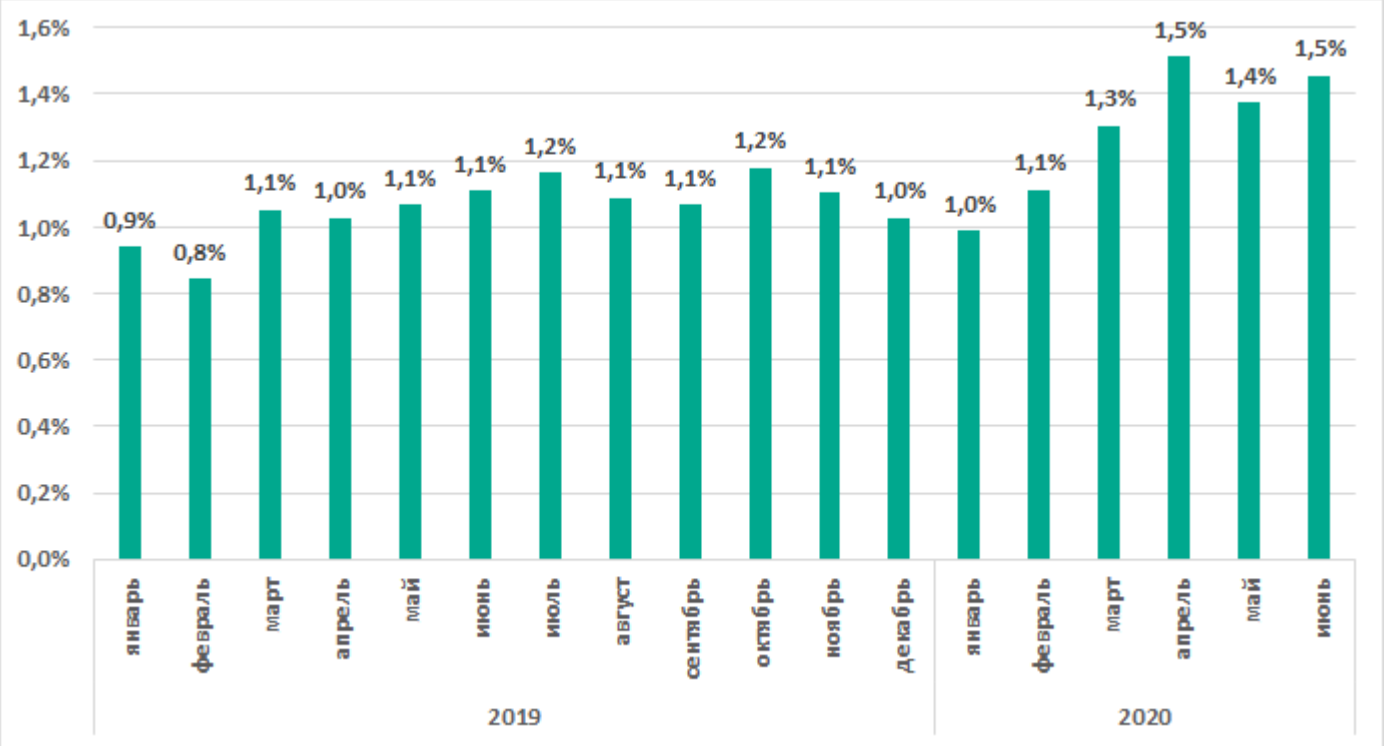

Рис. 1. Процент компьютеров АСУ, доступных по RDP, январь 2019 – июнь 2020

Примечательно, что рост процента компьютеров АСУ, на которых поднят RDP, в первом квартале 2020 года произошел на фоне довольно длительного периода борьбы с использованием RAT на промышленных предприятиях. На графике ниже хорошо видно уменьшение процента компьютеров АСУ, на которых используются программы удаленного администрирования, в течение 2019 года. Отметим, что в первом полугодии 2020 этот показатель стабилизировался (и даже немного вырос в феврале – апреле в сравнении с январём), чего не наблюдалось зимой и весной 2021 года, и что также может быть связано с последствиями пандемии.

Нет сомнений, что безопасность в информационном обществе – это информационная безопасность. При этом главным объектом защиты выступает компьютерная техника как основной носитель информации. В случае внешнего конфликта или внутренней мобилизации первый удар будет нанесен именно в этой области.

Для парирования потенциальных угроз в области информационной составляющей обществу необходимы специальные структуры информационно-психологической безопасности как важнейшие составные части структур морально-психологического обеспечения. Здесь можно выделить две стороны – техническую и психолого-идеологическую. Разумеется, они диалектически связаны друг с другом и образуют в целом совершенно новый феномен, специфический для информационного общества.

С технической стороны легко прогнозируются постоянные обновления и увеличение количества угроз; со стороны идеологии и психологии видна непрерывно развивающаяся система приемов манипулятивного воздействия, ставшая в виде психологии манипуляций компонентом общественной и индивидуальной психологии в США и в Западной Европе. Там разработаны технологии воздействия [11, 12], которые активно экспортируется в третьи страны, становящиеся целью информационной агрессии (последние примеры – Украина, Белоруссия и Казахстан). Она получила в настоящее время массовое распространение на данный момент – в социальных сетях и продолжает активно проникать в систему информационно-коммуникативных процессов, оказывая разрушающее влияние на психику людей.

Чтобы эффективно противостоять манипулятивным воздействиям, необходимо обладать следующими качествами:

- иметь развитое логическое мышление (оно позволяет видеть логические нестыковки в информационно-психологических построениях);
- уметь производить элементарные математические операции по проверке сообщаемых «точных» данных (о жертвах террора, катастроф и подобное);
- иметь развитую память (часто политические деятели и комментаторы через небольшое время меняют позицию на противоположную, но зрители, электорат живут одним днем);
- быть способным к самостоятельной оценке сообщений (разумная критичность к сообщениям СМИ - непременное условие борьбы с манипулятивными воздействиями).

Развитие в себе этих качеств является в современных условиях насущной потребностью человека, желающего стать сознательным гражданином [9, 11], защититься от недобросовестных манипуляций и с успехом противостоять настоящим и будущим угрозам в области идеологии.

Библиографический список

1. *Тоффлер О.* Смещение власти: знание, богатство и принуждение на пороге XXI века. М.: Изд-во АН СССР, 1991.
2. Новая технократическая волна на Западе / под ред. П. С. Гуревича. М.: Прогресс, 1986.
3. *Ракитов А. И.* Философия компьютерной революции. М.: Политиздат, 1991.
4. Воздействие на общественное мнение входе вооруженных конфликтов // IV Международная студенческая научная конференция Студенческий научный форум – 2012 [Электронный ресурс]. Режим доступа: https://scienceforum.ru/2012/article/2012002063. (дата обращения: 17.02.2022).

5. *Лисичкин В. А., Шелепин Л. А.* Глобальная империя зла. Новая геополитическая расстановка сил. М., 2001. С. 104.

6. *Соколов А., Степанюк О.* Защита от компьютерного терроризма. БХВ-Петербург, 2002. 496 с.

7. *Храмцов П.* РНЦ «Курчатовский Институт», dobr@kiae.su Российские компьютерные сети [Электронный ресурс]. Режим доступа: https://www.osp.ru/os/1996/01/178799 (дата обращения: 17.02.2022).

8. Статистика по вредоносным программам для ПК, второй квартал 2021 г. / Securelist. [Электронный ресурс]. Режим доступа: https://securelist.ru/it-threat-evolution-in-q2-2021-pc-statistics/103374/ (дата обращения:17.02.2021).

9. *Luneva E. V., Khomutnikova E. A., Khripunova O. G., Berg L. N., Bagretsov D. N., Golishev E.V.* PATRIOTIC EDUCATION OF YOUNG PEOPLE BY MEANS OF INTERNET PROJECTS: DOMESTIC AND FOREIGN EXPERIENCE // ADVANCES IN SOCIAL SCIENCE, EDUCATION AND HUMANITIES RESEARCH. Proceedings of the 1st International Scientific Practical Conference "The Individual and Society in the Modern Geopolitical Environment" (ISMGE 2019). 2019. С. 338-341.

10. *Аржанухин С. В.* ФИЛОСОФСКИЕ И ОБЩЕСТВЕННО-ПОЛИТИЧЕСКИЕ ВЗГЛЯДЫ РУССКИХ МАСОНОВ ВТОРОЙ ПОЛОВИНЫ XVIII-ПЕРВОЙ ЧЕТВЕРТИ XIX ВВ**:** автореф. докт. философ. наук. Екатеринбург, 1996.

11. *Аржанухин С. В., Васильева Е. И., Зерчанинова Т. Е., Качанова Е. А., Костина Н. Б., Кох И. А., Маковичч Г. В., Мудрецова Н. П., Никитина А. С., Саранчук С. Ю., Симонов С. Г., Танчук О. Г., Тишина Е. В., Фельдман М. А., Чевтаева Н. Г., Шаталова Н. И.* СОВРЕМЕННОЕ РОССИЙСКОЕ ОБЩЕСТВО И УПРАВЛЕНИЕ: СОСТОЯНИЕ, ПРОБЛЕМЫ И ТЕНДЕНЦИИ РАЗВИТИЯ**: м**онография. Екатеринбург, 2018.

12. *Яушева А. З.* ИНФОРМАЦИОННЫЕ ВОЙНЫ И МЕТОДЫ ЗАЩИТЫ ОТ ИНФОРМАЦИОННОЙ ВОЙНЫ // ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ ОБЕСПЕЧЕНИЯ КОМПЛЕКСНОЙ БЕЗОПАСНОСТИ В ЦИФРОВОМ ОБЩЕСТВЕ: сборник материалов IV Всероссийской молодежной научно-практической конференции с международным участием. Уфа, 2021. С. 285-287.