Возникновение и история развития проблемы защиты информации

Григорьев Сергей Михайлович, Магистрант МГУТУ, Россия, г. Москва,E-mail: grismi@bk.ru

Научный руководитель: **Попов Олег Вячеславович,** доцент, кандидат юридических наук. Кафедра государственно-правовых дисциплин МГУТУ, Россия,, г. Москва

Информация, подобно экономическим ресурсам человеческого общества, подвергается накоплению, хранению для дальнейшего использования и распространению. Т. Стоуньер подчеркивает, что уже в капиталистическом обществе XVШ и XIX веков существовало мнение о том, что овеществленный труд человека представлен в технических образцах. Он вкладывает в данное понятие новую мысль о том, что технические изобретения, представляя собой овеществленный труд, являются одновременно и овеществленной информацией.

Формирование информационного общества является закономерным этапом эволюции современного социума, характеризующегося, в первую очередь, масштабным внедрением информационных технологий и развитием глобального информационного пространства. Процесс становления нового общества, обусловленный внедрением информационных технологий, нуждается в верном осознании его информационной специфики и конструктивном развитии заложенного в нем потенциала.

Проблема защиты от проявившихся в третьем тысячелетии новых видов опасностей и угроз, порожденных информатизацией, беспокоит исследователей современного общества.

Сложность освещения проблемы информационной безопасности до настоящего времени, как отмечают специалисты[1], связана с отсутствием общепринятого толкования терминов, описывающих рассматриваемую предметную область. Наряду с термином «информационная безопасность» активно используется термин «безопасность информации». Не вызывает сомнений тот факт, что данные понятия взаимосвязаны.

Информационная среда определяет качество функционирования жизнедеятельности общества, его уровень развития и безопасность. Информационное взаимодействие, его своевременность, полнота и интенсивность регулируют все процессы жизнеобеспечения общества. Оттого информационная инфраструктура - основная цель информационного оружия. Как отмечает Г. Рэттрей, мишенью «асимметричной» войны являются жизненно важные точки государства[2]. Эти точки называются критическими инфраструктурами, потому что их дееспособность или уничтожение будет иметь пагубные последствия для национальной безопасности и экономического и социального благополучия нации[3] [4].

В свое время Н. А. Бердяев отмечал, что изобретательность человека в орудиях разрушения превышает изобретательность в технике, например, медицинской, а также то, что «небольшая кучка людей, обладающая секретом технических изобретений, сможет тиранически держать в своей власти все человечество»[5]. Рост модификации информационного оружия далеко опередил развитие технологий защиты, в результате чего нейтрализация данного оружия становится приоритетной задачей национальной безопасности государства.

Информационная революция начинается с создания электронно-вычислительных машин в конце 40-х годов XX века, с того времени исчисляется эра развития информационной технологии, материальное ядро которой образует микроэлектроника. Процесс развития современных технологий

отражает качественную перестройку информационной среды человека и все возрастающее на этом фоне значение информации - главной общественной ценности, специфически человеческой и сущностно-центральной для информационной технологии.

Информационные технологии повлияли на сознание человека и возможности, изменили его образ жизни. Современные информационные технологии поменяли приоритеты и ценности. Сегодня используемые в обществе информационные технологии рассматриваются как фактор, оказывающий огромное влияние на глобальное развитие социума и формирование информационной реальности. В настоящее время информационная сфера оказалась сердцевиной экономических, социальных, политических и других конфликтов в обществе. Проявившиеся впоследствии использования современных технологий основные опасности и угрозы систематизированы в зависимости от сфер жизнедеятельности общества.

Так, в социальной сфере возникла опасность нового неравенства в обществе: реальная угроза «информационного расслоения», ведущая к потенциальной угрозе формирования информационной элиты общества. Кроме того, растущую тревогу для общества и государства вызывает появление нового вида преступности - компьютерной.

В духовно-культурной сфере общества опасность применения в противоправных целях информационных технологий привела к угрозе манипулирования человеческим сознанием, психической и социальной дезадаптации человека. Опасность причинения вреда здоровью человека в результате использования информационных технологий породила угрозу развития различных видов заболеваний.

Экономическое состояние государства сегодня прямым образом зависит от ситуации, складывающейся в области создания и применения информационных технологий, вследствие чего как положительные решения в данной области, так и экономические кризисы приобретают глобальный характер. Кроме того, широкое внедрение технологий в процессы производства вызывают опасность изменения характера труда, сверхрационализацию и отчуждение рабочей силы, что несет в себе разрушительную реакцию на человека,потенциальную угрозу дегуманизации труда и реальную угрозу техностресса.

Военно-политическая сфера жизнедеятельности современного общества отличается низкой степенью защиты информации о личности человека, содержащейся в государственных системах и компьютерных сетях. Опасность контроля над человеком, манипулирование, распространение конфиденциальной информации ведут к потенциальной угрозе информационного тоталитаризма. Опасность информационно-технологической зависимости государств послужила почвой для зарождения потенциальной угрозы информационного колониализма. Отрицательным эффектом применения современных технологий в военно-политической сфере служат открывшиеся возможности производства новых видов информационного оружия.

Корни информационного противоборства лежат глубоко в истории, оно наиболее ярко проявляется в моменты политического и военного противостояния. В VI-V веках до нашей эры древнекитайский полководец Сунь-Цзы изложил ряд информационно-интеллектуальных приемов ведения военных действий, которые сохранили свою актуальность сегодня и стали определенным методическим базисом, заложенным в основу современной политики и дипломатии. В основе концепции Сунь-Цзы лежит теория управления врагом: «его заманивают в ловушки выгодой, лишают храбрости, ослабляя и изматывая перед атакой»[6] [7]. В XVI веке итальянский мыслитель Николо Макиавелли сформулировал информационно-психологическую концепцию государственной власти, где изложил основополагающие принципы внедрения информационного противоборства в политической сфере. Кроме того, история богата примерами проведения крупных информационно-пропагандистских акций, классических вариантов дезинформации народа глобального масштаба, сыгравших свою роковую роль.

Наиболее активное развитие информационные экспансии и информационное оружие получили в XX веке, здесь особое место в приемах атакующего воздействия приобретает информационная пропаганда. Первым в мире лидером по созданию и применению информационных средств поражения становятся Соединенные Штаты Америки: вторжения в Гренаду, в Панаму, война в Югославии, боевые действия в районе Персидского залива, борьба с терроризмом. На мой взгляд, уже неопровержимо мнение, что в XXI веке приоритет в вооружении стран будет направлен на приобретение информационного превосходства, нежели на увеличение количества авиа- и бронетанковой техники, как когда-то в XX веке. Информационно-компьютерные системы, коммуникационные технологии теперь основные поражающие методы и средства в современной войне.

В настоящее время в научной литературе сформировалось два методологических направления, изучающих возникновение феномена информационная безопасность. Одна группа специалистов тесно связывает развитие информационной безопасности с информационными революциями в истории человеческой цивилизации[8] [9]. Данный подход подразумевает, что уровень безопасности общества определен качеством и объемом информации, доступной социуму, а так же альтернативой ее непосредственного приложения.

Второй подход, предложенный в свое время В. Н. Лопатиным, предполагает, что в истории человеческой цивилизации появление категории «информационная безопасность» связано с возникновением средств информационных коммуникаций и осознанием человеком возможности нанесения ущерба собственным интересам или интересам социальной системы посредством информационного обмена . В рамках этого подхода, становление информационной безопасности с точки зрения развития технологий защиты разделяют на несколько этапов.

Первый этап определяется периодом до 1816 года, он связан с естественным стремлением человека и общества защитить информацию о каких-либо данных, обладающих уникальным значением. Второй этап применения информационно-коммуникационных технологий в процессе обеспечения информационной безопасности начинается с 1816 года, он характеризуется движением от физической защиты информации к созданию технических средств. Третий этап в создании технических методов информационной безопасности начинается с 1935 года, он связан с применением радиолокационных и гидроакустических средств. С 1946 года начинается четвертый этап решения задач информационной безопасности с помощью электронно-вычислительных машин. Пятый шаг в развитии технических средств информационной безопасности связан с созданием локальных информационных сетей в период с 1965 года. Следующий этап развития информационной безопасности (с 1973 года) характеризуется применением сверхмобильных коммуникационных механизмов, решающих высокотехнологичные задачи. Седьмой этап начинается с 1985 года прошлого столетия, он связан с развитием глобальных информационных сетей и космических разработок. Очередной этап информационной безопасности, как показывает практика, будет протекать на базе новейших информационно-коммуникационных технологий с широким спектром возможностей, осуществляемым посредством глобальной сети и космических систем[10]. Полагаю, что данный этап потребует формирования глобальной системы информационной безопасности для решения задач человечества под эгидой международного взаимодействия.

На мой взгляд, описываемый подход к изучению проблемы развития информационной безопасности наиболее глубоко и точно передает историю ее становления. Представленная классификация детально отражает процесс совершенствования информационных воздействий, угроз потенциального и реального характера, который вызвал в человеческом обществе трансформацию идей информационной безопасности, развитие методов и средств обеспечения информационной защиты от возникающих опасностей.

При функционировании мирового информационного пространства информационная

безопасность в полной мере может быть обеспечена только усилиями всех стран мирового сообщества, поэтому возникает потребность в формировании общемировой информационной безопасности. Система глобальной информационной безопасности отражает важный фактор перехода к устойчивому развитию.

На мой взгляд, необходимо определить основные направления развития информационной безопасности глобального масштаба:

- обеспечение состояния защиты глобальной информационной среды от угроз и опасностей реального и потенциального характера;

- развитие в безопасном направлении для общества, человека и биосферы информационного пространства;

- справедливое распределение благ и ресурсов глобальной информационной среды между народами и всеми мировыми государствами;

- содействие процессу перехода к устойчивому развитию формирующейся общемировой информационной среды.

На пути реализации указанной стратегии важно не забывать, что мировое информационное пространство не имеет географических и государственных границ, в результате чего его защита и укрепление зависят одновременно от всего мирового сообщества, равнозначно как уязвимость и ущерб его развитию отражается на разных странах. В этой связи, необходимо рассмотреть вопросы согласования стандартов и национальных законов, а также задачи сотрудничества в их реализации, принятие международных договоров по функционированию международного информационного пространства в социальных, политических, культурных, юридических и т. д. аспектах, разработать адекватные меры противодействия информационному противоборству.

И так на рубеже XX и XI века человечество шагнуло на ступень кардинальных технологических преобразований, связанных с возникновением нового ряда значительных опасностей и угроз. Пройти путь по восходящей лестнице к новой информационной цивилизации, основанной на колоссальных возможностях технологий, не сорваться вниз, способно общество с высокими нравственными идеалами и ясным пониманием всей глубины ответственности за каждый свой шаг. Сегодня информационные технологии, рассматриваемые как фактор, оказывающий огромное влияние на глобальное развитие социума и формирование информационной реальности, повлияли на сознание человека и его возможности, изменили жизнь общества, трансформировали приоритеты и ценности. Как эти высокие технологии, являясь средством осуществления жизнедеятельности человека, будут применены в будущем, зависит от общества и его выбора.

В свое время основатели концепции информационного общества справедливо отмечали, что информация и знания станут ключевым фактором развития, превосходящим по значимости все виды материального производства, энергии и услуг. В этой теории информационные технологии и телекоммуникации представлены основным агентом экономических, социальных и политических изменений в современном мире. Вместе с тем, прогнозы ближайшего будущего социального строя в сравнении с нынешними реалиями оказываются несколько утопическими. Концептуальный анализ позволил выявить относительно невысокую степень критичности исследователей к феномену информационного общества, в силу чего оказывались слабо принятыми в расчет возникающие в современном социуме новые виды опасностей и угроз.

В заключение остается добавить, что формирование информационного общества является закономерным этапом эволюции современного социума. Информационная среда определяет качество функционирования жизнедеятельности общества. Информационные технологии повлияли на сознание человека и возможности, изменили его образ жизни. Современные информационные технологии поменяли приоритеты и ценности. Сегодня используемые в обществе информационные технологии рассматриваются как фактор, оказывающий огромное влияние на глобальное развитие

социума и формирование информационной реальности.

Библиографический список

1. Артамонова Я. С., Артамонов П. А. Информационная безопасность и информационные коммуникации // T-Comm - Телекоммуникации и Транспорт. - 2012. - № 4; Шамсуев М.-Э. Х. Теоретические аспекты изучения информационной безопасности // Теория и практика общественного развития. - 2010. - № 2. - С. 322

2. Бердяев Н. А. Человек и машина (проблема социологии и метафизики техники) // Путь. - 1933. - № 38. - Май.

3. Лопатин В. Н. Информационная безопасность России: Человек, общество, государство. - Москва: Фонд «Университет», 2000. - Серия: Безопасность человека и общества.

4. Малюк А. А., Пазизин С. В., Погожин Н. С. Введение в защиту информации в автоматизированных системах. - Москва: Горячая линия-Телеком, 2001. - С. 7.

5. Манойло А. В. Государственная информационная политика в особых условиях. - Москва: МИФИ, 2003.

6. Николо Макиавелли. Государь / под ред. В. П. Бутромеева. - Москва: Олма Медиа Групп, 2011.

7. Сунь-Цзы. Искусство войны / пер. Н. И. Конрад. - Москва: Эксмо, _2011. - С. 10.

8. Хитарова И. Ю. Философско-культурологический анализ информационной безопасности культурного наследия: автореф. дис. ...д-ра филос. наук: 24.00.01. - Санкт-Петербург, 2008.

9. Abele-Wigert I., Dunn M. The International CIIP Handbook 2006. An Inventory of Protection Policies in 20 Countries and International Organizations. - Zurich: Center for Security Studies, 2006

10. Cavelty M., Kristensen K. Introduction: Securing the Homeland: Critical Infrastructure, Risk, and (In)Security. In Securing the Homeland: Critical Infrastructure, Risk, and (In)Security, edited by M. D. Cavelty and K. S0byKristensen. - London: Routledge, 2008.

11. Rattray G. Strategic Warfare in Cyberspace. - Cambridge: MIT Press, 2001.

[1] Малюк А. А., Пазизин С. В., Погожин Н. С. Введение в защиту информации в автоматизированных системах. - Москва: Горячая линия-Телеком, 2001. - С. 7.

[2] Rattray G. Strategic Warfare in Cyberspace. - Cambridge: MIT Press, 2001.

[3] Abele-Wigert I., Dunn M. The International CIIP Handbook 2006. An Inventory of Protection Policies in 20 Countries and International Organizations. - Zurich: Center for Security Studies, 2006; Cavelty M., Kristensen K. Introduction: Securing the Homeland: Critical Infrastructure, Risk, and (In)Security. In Securing the Homeland: Critical Infrastructure, Risk, and (In)Security, edited by M. D. Cavelty and K. S0byKristensen. - London: Routledge, 2008.

[4] Бердяев Н. А. Человек и машина (проблема социологии и метафизики техники) // Путь. - 1933. - № 38. - Май.

[5] Там же. - С. 24.

[6] Сунь-Цзы. Искусство войны / пер. Н. И. Конрад. - Москва: Эксмо, _2011. - С. 10.

[7] Николо Макиавелли. Государь / под ред. В. П. Бутромеева. - Москва: Олма Медиа Групп, 2011.

[8] Артамонова Я. С., Артамонов П. А. Информационная безопасность и информационные коммуникации // T-Comm - Телекоммуникации и Транспорт. - 2012. - № 4; Шамсуев М.-Э. Х. Теоретические аспекты изучения информационной безопасности // Теория и практика общественного развития. - 2010. - № 2. - С. 322; Хитарова И. Ю. Философско-культурологический анализ информационной безопасности культурного наследия: автореф. дис. ...д-ра филос. наук: 24.00.01. - Санкт-Петербург, 2008.

[9] Лопатин В. Н. Информационная безопасность России: Человек, общество, государство. - Москва: Фонд «Университет», 2000. - Серия: Безопасность человека и общества.

[10] Манойло А. В. Государственная информационная политика в особых условиях. - Москва: МИФИ, 2003.