электронный журнал
МОЛОДЕЖНЫЙ НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК
Издатель ФГБОУ ВПО "МГТУ им. Н.Э. Баумана". Эл No. ФС77-51038.

УДК 004.738.5

Философские проблемы кибербезопасности: свободы и войны в киберпространстве

***Мушиц С.И.**, студент*
Россия, 105005, г. Москва, МГТУ им. Н.Э. Баумана,
кафедра «Программное обеспечение ЭВМ и информационные технологии»

Научный руководитель: Губанов Н.Н., к.ф.н., доцент кафедры «Философия»
Россия, 105005, г. Москва, МГТУ им. Н.Э Баумана
dekan.fsgn@bmstu.ru

С древнейших времен вопросы безопасности, в том числе защиты информации от нежелательного доступа, ее повреждения или изменения являлись предметом исследований, результатом которых стало появление разнообразных методов защиты, специализированных служб и учреждений. Этот процесс продолжается и сейчас, но глобальное распространение компьютеров и интернета, проникающих во все области деятельности общества и государства, ведет к повышению объемов информации, хранящихся на цифровых устройствах и обрабатывающихся с помощью цифровых методов, при этом она быстрее распространяется и скорость этого распространения возрастает. Одновременно происходит объединение автоматизированных и традиционных технологий работы с информацией. Такое быстрое становление информационной составляющей социальных процессов требует развития особой дисциплины - кибербезопасности.

К защите военных и государственных тайн добавляется защита коммерческих, промышленных и банковских секретов; необходимость обеспечить защиту авторского права и права собственности на информацию, персональную информацию и т.д. В связи с этими нововведениями необходимо менять общественную позицию по отношению к вопросам кибербезопасности и качественно улучшать способы, методы и средства ее обеспечения, а также воспитывать информационную культуру современного человека. Большая часть людей в обществе использует компьютер и интернет для учебы, развлечений, работы и коммуникации, но многие из них не имеют достаточно знаний по обращению и защите информации в сетях. Высокая актуальность проблем кибербезопасности диктуется также возможностями, которые Интернет предоставляет

различным агентам влияния для манипулирования общественным сознанием. Манипулирование является одним из способов ментализации – формирования менталитета, а роль менталитета в социально-историческом процессе невозможно переоценить [3; 4; 5].

В сфере кибербезопасности рассматриваются следующие основные вопросы [1]:

- Социальные вопросы, связанные с неуправляемым использованием и распространением конфиденциальных данных, проникновениями в частные сферы жизни, фильтрацией и цензурой информации, а также кражами информации, находящейся в личной собственности.
- Экономические и юридические вопросы, связанные с утечками и кражами коммерческой и финансовой информации, подделыванием брендов и несоблюдением прав интеллектуальной собственности, промышленным шпионажем и клеветой в отношении компаний.
- Политические вопросы, связанные с кибервойнами, информационными войнами, кибертерроризмом и киберразведкой в интересах политических групп и отдельных государств, компрометацией секретных материалов, атак на цифровые системы оборонных, транспортных и промышленных объектов.

Рассмотрим проблемы кибербезопасности, возникающие в социальной и политической сфере и влияющие на государство, общество и граждан, подробнее.

Борьба между свободами граждан и безопасностью общества и государства в киберпространстве.

Если раньше кибербезопасность обеспечивалась защитой отдельных компьютеров посредством антивируса или брандмауэра, то теперь уровень защиты поднимается до национальной безопасности, так как угрозы, идущие от или нацеленные на киберпространство могут легко подвергнуть опасности благосостояние всего общества, а также защиту и безопасность отдельных граждан. В течение последних лет кибербезопасность становится объектом изучения и управления правительств национальных государств и международных объединений (НАТО, ЕС и др.).

Однако вовлечение властей в управление киберпространством не происходит без дополнительной цены, которую необходимо заплатить обществу и которая является новой и еще более усугубленной версией «борьбы между свободами и властями», как называл указанный процесс еще в XIX в. Д.С. Милль [10]. Эта борьба относится к противостоянию между правами индивида и законами, ограничивающими их, принятыми властями и распространяющими свое влияние на гражданское общество.

Согласно одной из наиболее известных позиций, власть государственных органов и индивидуальные права прямо противопоставляются друг другу, и чем больше аккумулируется власти, тем меньшими правами наделен гражданин. Пути решения этой проблемы определяются различно: в плюралистических, демократических обществах присутствует «бдительное» гражданское общество и справедливая судебная система, которые ограничивают так называемую «силу закона» и защищают индивидуальные права, в отличие от авторитарных (тоталитарных) обществ.

В век информационной революции борьба не просто возобновилась, она усилилась, принимая во внимание цифровую природу киберпространства [12]. Данные, биты, которые составляют киберпространство, по своей природе могут быть легко изменены [11]. Они могут переноситься, храниться, обрабатываться, к ним может быть получен доступ, их может добыть третья сторона, раскрыв тем самым деликатную личную информацию, что вынуждает прибегать к наблюдательным и контролирующим мерам. Тогда встает вопрос, могут ли персональные данные и информация быть полностью доступны тем, кто применяет эти меры и имеет соответствующие технологии, тем самым подрывая права на частную жизнь, анонимность, прозрачность действий правительства и свободу слова [13]. Скандал, случившийся в 2013 г. с американским Национальным Агентством Безопасности (NSA), является реальным примером того, как технологическая и государственная власть может ощутимо угрожать упомянутым правам.

Отражением противостояния власти государства и свобод граждан является цензура и блокировка Интернет-ресурсов. Наибольшее внимание международных организаций, исследующих свободу в Интернете, привлекает цензура политического контента, которая нарушает основополагающие права – свободы слова и религии (вероисповедания). Фильтрацию политического контента осуществляют не только тоталитарные и авторитарные, но и демократические режимы, прикрываясь формулировками защиты государственной безопасности или борьбой с радикальными движениями в стране. Например, во многих мусульманских странах блокируются популяризирующие христианство сайты. Также под цензуру попадают ресурсы и сервисы, позволяющие получать доступ к заблокированным сайтам или свободно общаться. В результате власти получают еще больший контроль за интернет-активностью своих граждан. В КНР недоступны многие международные ресурсы, такие как Twitter, Google, YouTube, которые не подконтрольны китайскому правительству. Взамен, доступны китайские сервисы, чьи сервера расположены на территории КНР, а, следовательно, могут контролироваться и цензурироваться властями.

Сбор информации в Интернете.

Как было показано выше, сбор информации в Интернете, независимо от того, используется он на благо народа или нет, нарушает свободы граждан. В связи с этим, рассмотрим подробнее наиболее распространенные способы сбора конфиденциальной информации о пользователях сети, применяемых государствами [2].

Одна из них - обязанность Интернет-провайдеров хранить техническую информацию об интернет-активности пользователей, что позволяет в любой момент отслеживать посещаемые человеком ресурсы и его поведение на них. Такая информация может использоваться для поиска и поимки злоумышленников в Сети.

Следующая мера - наблюдение за интернет-кафе, которые могут быть использованы для нелегальной деятельности, так как в данном случае сложнее установить личность злоумышленника. К примеру, для использования интернет-кафе в КНР или Италии необходимо предъявить документ, удостоверяющий личность, а владельцы обязаны хранить записи о действиях пользователей. Во Вьетнаме и Бирме в каждом интернет-кафе должна присутствовать видеокамера наблюдения. Еще один метод сбора информации - установление систем интернет-слежки, возможное применение которых предусмотрено большинством стран мира. В России действует система СОРМ-2, по условиям которой провайдеры должны использовать в оборудовании специальное устройство, позволяющее спецслужбам проверять и изучать трафик конкретных пользователей. В США работает похожая система под названием CALEA.

Существуют еще более масштабные системы, которые могут обрабатывать и исследовать трафик всей страны с помощью технологии глубокого анализа пакетов (Deep Packet Inspection). Такие системы позволяют спецслужбам производить слежение за Интернет-активностью пользователей, за тем, какие приложения, сайты и сервисы они используют и какие данные пересылают. Использование этих систем запрещено в Европейском Союзе и России, так как они идут вразрез с правом человека на частную жизнь. Несмотря на это, в данный момент ведутся дебаты на международном уровне о возможности их использования для борьбы с терроризмом и несоблюдением авторских прав. Так как такие системы массового наблюдения за интернет-активностью целой страны требуют колоссальных вычислительных мощностей, они присутствуют не во всех странах, а только в тех, которые могут себе это позволить. В США АНБ в рамках «Патриотического акта» 2002 г. отслеживает действия в Интернете с помощью суперкомпьютеров, китайские власти применяют глубокий анализ пакетов в целях сетевой цензуры, некоторые другие страны также используют похожие технологии.

Информационные и кибервойны.

Другая основная философская проблема кибербезопасности связана с политической сферой и наиболее ярко представляется явлением под названием Информационная война.

Информация в каждой эпохе истории человечества представляла собой объект борьбы. В современном мире оправдано утверждение: чем больший информационный потенциал имеет государство, тем у него больше шансов завладеть стратегическими геополитическими преимуществами. Очевидно, что большинство государств рассматривают информацию в качестве стратегического ресурса и стремятся ее защищать.

Многие государства желают захватить лидерство в международном киберпространстве, а также разрабатывают идеи и планы информационных войн, которые представляют потенциальную угрозу для киберпространства других государств мира, нормального функционирования их информационных и телекоммуникационных сервисов, безопасности чужих информационных ресурсов, соблюдению конфиденциального доступа к ним.

Информационная война, как следует из названия, отличается от противостояний армий, погибающих на полях сражений. Конфликт в зоне Персидского залива 1990-1991 гг. ознаменовался невиданным доселе размахом применения «умного» и высокоточного оружия, а также самым широким освещением происходящих боевых событий в СМИ по всему миру. Отсюда, по мнению многих экспертов, эту войну можно характеризовать как первую полномасштабную информационную войну. Кроме того, в международных отношениях в качестве способов воздействия в новом тысячелетии начинает распространяться и превалировать глобальный экстремизм, что еще больше обостряет проблему информационной войны. Характерной чертой этого явления является применение на международной арене террористами технологий «стравливания» стран, особенно имеющих большое мировое влияние на крупные державы. Наиболее явно описанное явление начало проявляться в последнем десятилетии XX в. в виде обострения информационно-экономической борьбы между «западным лагерем», представленным США и Европейскими странами – с одной стороны, Россией с союзными государствами – с другой. Это противостояние являлось информационной войной, и в ней использовалось информационное оружие, чье распространение ведет к ухудшению отношений между разными странами, усилению раздробленности (дезинтеграции) мирового сообщества, делению на противоборствующие «лагеря», деформации оценки и восприятия одними народами других, размыванию традиционных культур и национальных обычаев,

возникновению агрессии колоссальных размеров, распространению экстремистских настроений.

С приходом в обыденную жизнь Интернета и других компьютерных технологий, большая часть общества, включая как людей, так и целые организации, становится зависимой от них. Использование сети для атак компьютеров и оборудования другой страны способно причинить значительный ущерб ее геополитическому положению и создать духовный раскол в данном социуме (вспомним события «арабской весны» 2011 г.). Современные кибератаки превращаются из отдельных инцидентов в кибервойны между странами и объединениями, что несет глобальную опасность для государственной безопасности и спокойствия.

Далее, структуры разведки ряда государств используют интернет для шпионажа, а именно: аккумулирования секретных данных, проникновения в компьютерные системы, проведения диверсий и разведки секретной экономической и политической информации. Например, КНР неоднократно обвиняли в проведении кибератак на компьютерные системы США, ФРГ, Индии, но причастность его государственных учреждений к данным акциям не доказана. Другим известным применением наступательного кибероружия является до настоящего момента официально не подтвержденная секретная операция, проведенная США, и, возможно, Израилем под названием «Олимпийские игры», направленная против иранских ядерных объектов.

Из-за экспоненциального совершенствования компьютерных технологий масштаб кибервойн постоянно растет. Ряд стран начинает проявлять заботу о национальной кибербезопасности посредством выделения нужных ресурсов для установления специальных систем защиты и организации специальных подразделений, чьей задачей является обеспечение кибербезопасности страны и ее жителей.

В связи с этим возрастающим влиянием государства на Интернет, его стремлением контролировать информацию, становится очевидным, что новые технологии и способы взаимодействия с ними, в том числе и кибербезопасность, могут стать источником авторитаризма и тирании [9]. Эти технологии могут позволять вторгаться в частные сферы жизни и нарушать личные свободы даже без намеренного стремления к этому государства. Как показывает история, самый грозный вид тирании – это незаметная и мягкая тирания, при которой граждане сами участвуют в усугублении своего состояния, где повсеместный контроль возник под давлением обстоятельств, а не намеренной воли людей. Описанные технологии дают возможность правомерно следить и контролировать

действия людей в киберпространстве, что может явиться опаснейшим орудием на службе политической и экономической элиты.

Тирании отличаются друг от друга, и если раньше они требовали грубой физической силы для удержания контроля и власти (нацистская Германия), то теперь «мягкая тирания» захватывает и подчиняет умы, взгляды и действия людей посредством контролирования информации всюду, где возможно, начиная от школы и заканчивая Интернетом и телевидением. Государства, ведущие информационную и кибер-войну с собственными гражданами, используют кибербезопасность как средство правомерно устанавливать тотальную слежку даже на уровне повседневной жизни любого человека, еще больше расширяя возможности контроля властей над людьми. И мы должны ответить на вопросы: где находится и как контролировать баланс обеспечения кибербезопасности властями страны? Как предотвратить посягательства на права и свободы граждан государства в сфере кибербезопасности? В целом же проблема кибербезопасности влияет на уровень общественного прогресса, корректирует представления о нем [6], требует моделирования потенциальных вариантов социального развития относительно конкретных исторических ситуаций [7], перестройки мышления государственных деятелей для отражения киберугроз [8].

Список литературы.

1. Алиева М.Ф. Информационная безопасность как элемент информационной культуры // Вестник Адыгейского государственного университета. 2012. № 4. С. 97–102.
2. Апетьян С., Ковалев А., Файб А. Фильтрация контента в Интернете. Анализ мировой практики // Фонд развития гражданского общества. Режим доступа http://civilfund.ru/Filtraciya_Kontenta_V_Internete_Analiz_Mirovoy_Praktiki.pdf (дата обращения: 10.11.2014 г.).
3. Губанов Н.Н. Роль менталитета в развитии общества // Вестник Тюменского государственного университета. 2007. № 1. С. 99–105.
4. Губанов Н.Н. Образование и менталитет в составе движущих сил развития общества // Социология образования. 2010. № 1. С. 22–29.
5. Губанов Н.Н. Формирование глобалистского менталитета и образование // Социология образования. 2011. № 6. С. 74–82.
6. Нехамкин В.А. Теория общественного прогресса: достижения и пределы // Вестник Российской академии наук. 2013. Т. 83. № 8. С. 711-719.

7. Нехамкин В.А., Нехамкин А.Н. Если бы победили декабристы… // Вестник Российской академии наук. 2006. Т. 76. № 9. С. 805-813.
8. Нехамкин В.А. Роль образования руководителя государства в процессе исторического развития // Социология образования. 2012. № 2. С. 82-97.
9. Ревко П.С. Безопасность частной жизни человека в инфокоммуникационном мире // Фонд развития интернет. Режим доступа http://www.fid.ru/projects/internetworld/security2/ (дата обращения: 15.11.2014 г.).
10. Mill J.S. On Liberty // N.Y.: Dover Publications. 2002. P. 98.
11. Moor J.H. Towards a Theory of Privacy in the Information Age // ACM SIGCAS Computers and Society. 1997. № 27 (3). P. 27–32.
12. Taddeo M. Cyber Security and Individual Rights, striking the right balance // Philosophy and Technology. 2013. № 26 (4). P. 353–356.
13. Taddeo M. Information Warfare: a Philosophical Perspective // Philosophy and Technology. 2012. № 25 (1). P. 27–32.