Титульный лист

Содержание

Введение

В конце XX – начале XXI в. стремительными темпами развивается глобальная компьютерная сеть, с каждым годом увеличивается численность ее аудитории. В Интернете коммуникация часто выглядит неперсонализированной, обезличенной, поэтому у части пользователей появляется соблазн передачи сообщений, носящих недостаточно достоверный, а иногда и откровенно ложный, провокационный характер. Возникает наличие острой социальной проблемы, заключающейся, с одной стороны, в противоречии между инновационным коммуникативным потенциалом глобальной сети, предоставляемыми возможностями самореализации для активной части интернет-аудитории, а с другой - в отсутствии должного контроля и действенных механизмов социального управления Интернетом. Значительное увеличение масштабов трансляции недостоверной информации в глобальной компьютерной сети может рассматриваться и в качестве источника угроз информационной безопасности. Объем информации, размещенный в сетях, перестает быть контролируемым. Следовательно, возникает необходимость обеспечения информационной безопасности в процессе функционирования глобальных сетей, что обуславливает актуальность данной проблемы и поиск путей ее решения на современном этапе развития общества.

Стоит отметить позитивные и негативные последствия появления и развития глобальной компьютерной сети. Если позитивные аспекты интернет-реальности способствуют социальному прогрессу, то негативные – социальной дезорганизации и развитию дисфункций социума. Особую актуальность в современных условиях приобретают проблемы управления Интернетом и обеспечения информационной безопасности в нем.

За короткое время произошли столь масштабные и беспрецедентные изменения, что узкоспециальные вопросы защиты информации — предмет интереса преимущественно государственных органов и ограниченного

количества технических специалистов, математиков — превратились даже не в междисциплинарные, а в глобальные проблемы информационной безопасности. Но интеграционный период уже сменяется новой дифференциацией: безопасность компьютерных технологий или, в американизированной терминологии, кибербезопасность, становясь в свою очередь предметно-многообразной, обособляется от множества нетехнологических проблем. Активно формируется и выходит на первый план претендующий на интегрирующую функцию юридический аспект.

Всё в большей мере вопросы информационной безопасности обращают на себя внимание широкого круга специалистов гуманитарной сферы. Даже технические аспекты во многих случаях становятся актуальными по гуманитарным мотивам.

Технологический прогресс существенно обгоняет теоретическое осмысление происходящего в области создания и применения информационных технологий, использования новых коммуникационных возможностей. Но такое положение, когда быстро развивающиеся технологии, имеющие тотальный характер, стимулируемые рыночными критериями, слишком долго остаются теоретически неосознанными, чревато непредсказуемыми последствиями. В этих условиях необходимы совместные усилия по выработке национальной политики в области обеспечения информационной безопасности в целом и глобальных сетей в частности.

Целью данной курсовой работы является изучение процесса обеспечения информационной безопасности в условиях функционирования глобальных сетей.

Задачи курсовой работы:

1. Изучение процесса информационной безопасности и общих угроз функционированию глобальных сетей.
2. Исследование проблем информационной безопасности в условиях функционирования глобальных сетей.
3. Анализ государственной политики в сфере информационной

безопасности глобальных сетей.

4. Рассмотрение современных технологий обеспечения информационной безопасности в условиях функционирования глобальных сетей.

Объект курсовой работы – информационная безопасность глобальных сетей. Предметом данной курсовой работы является глобальная сеть как фактор угрозы информационной безопасности.

В ходе написания курсовой работы были использованы научные методы исследования, в том числе и методы анализа, и синтеза информации.

1. Сущность информационная безопасность глобальных сетей

1.1 Понятие информационной безопасности

Для нынешней информационной цивилизации характерен пересмотр образовательных научных концепций на основе достижений кибернетики, информатики, синергетики, психологии, педагогики и ряда других наук, а также бурное развитие науки и наукоемких производств. Основной характеристикой человеческой деятельности наряду с энергией и веществом становится информация как возобновляемый и неистощимый ресурс человечества, как главная ценность общества. Именно это дает основание говорить о том, что человечество вступило в новую эпоху своего развития.

Изучение современной картины мира без привлечения общенаучной категории «информация» оказывается односторонним и неполным, особенно в период перехода общества к безопасному развитию, которое предполагает дальнейшую интеллектуализацию общества, в частности, на основе его информатизации. Процесс информатизации разворачивается во всех областях человеческой деятельности (таких как политика, экономика, образование, культура и др.). Новые информационные технологии и средства коммуникационно-вычислительной техники являются ядром процесса информатизации.

Проблема технологического и безопасного развития государства в нынешних условиях необходима рассматриваться и как научно-техническая, и как национальная проблема экономического выживания и будущего безопасного развития. Обеспечение безопасности страны в принципе невозможно без перехода на путь безопасного развития государства. А сохранение биосферы и человеческой культуры невозможно без обеспечения их совместной безопасности

Словосочетание «информационная безопасность» в разных контекстах может иметь различный смысл. В Доктрине информационной безопасности

Российской Федерации термин «информационная безопасность» используется в широком смысле. Имеется в виду состояние защищенности национальных интересов в информационной сфере, определяемых совокупностью сбалансированных интересов личности, общества и государства.

В Законе РФ «Об участии в международном информационном обмене» информационная безопасность определяется аналогичным образом - как состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государства.

Таким образом информационная безопасность - защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений, в том числе владельцам и пользователям информации и поддерживающей инфраструктуры[1].

В настоящее время отдельные элементы единой государственной системы информационной безопасности в наших странах созданы и функционируют (органы внешней разведки, информационные службы различных министерств, ведомств и т. д.). Федеральный закон «Об информации, информатизации и защите информации» должен сыграть свою положительную роль в деятельности органов информационной безопасности, которая пока не в полной мере отвечает возложенным на нее задачам.

Формы и способы обеспечения информационной безопасности образуют тот инструмент, посредством которого силы информационной безопасности решают весь комплекс задач по защите жизненно важных интересов личности и общества. Поэтому необходимо четкое юридическое оформление при разработке нормативных актов, регулирующих деятельность органов информационной безопасности.

---

1. [1] Доктрина информационной безопасности РФ // Российская газета. 2000. 29 сентября.

Безусловно, в различных сферах государственной деятельности воздействие информационных угроз может проявляться по-разному. Однако достаточно очевидно, что неадекватное восприятие действительности лицами, принимающими государственные решения, может повлечь за собой самые серьезные последствия.

В отличие от традиционных информационных источников — анализа печатных изданий, опроса граждан и т. п. уровень и качество информации нового информационного канала могут оказать решающее воздействие на выработку активной политики западных государств в отношении российского общества и его граждан. Нейтрализовать воздействие информационных угроз призвана единая государственная система информационной безопасности, которой, к сожалению, в России пока нет. Под государственной системой информационной безопасности страны обычно понимают организационное объединение государственных органов, сил и средств информационной безопасности, осуществляющих свои функции на основе закона и под контролем и защитой судебной власти.

1.2 Возникновение и развитие проблем информационной безопасности в современном мире.

Научно-техническая революция XX в. полностью изменила представления человечества об окружающем мире. Великие открытия в области физики и химии стали толчком к появлению и развитию компьютеров, сотовых телефонов и других высокотехнологичных устройств, без которых невозможно представить сегодняшний мир. Процесс внедрения высоких технологий в повседневную жизнь сказывался на качественном изменении отношений в обществе, информация приобретала все большую значимость. Одновременно с понятием огромной ценности информации возникает потребность и в ее защите. Со временем социальные преобразования привели к необходимости законодательного регулирования новых общественных отношений. Проблема защиты информации и информационных систем сейчас является одной из самых актуальных во всем мире.

История развития законодательства, регулирующего общественные отношения в сфере высоких технологий, неразрывно связана с появлением и совершенствованием компьютеров и глобальной сети Интернет.

В 1958 г. по указанию президента США Д. Эйзенхауэра в рамках Министерства обороны было создано Агентство перспективных исследований (ARPA), которому принадлежит особая роль в истории Интернета. Одной из задач ARPA стала разработка возможности передачи информации между компьютерами по сети, которая могла бы функционировать даже в случае ее частичного повреждения.

Первым исследованием, подтолкнувшим развитие сетевых технологий, стало «Galactic Network» (Галактическая сеть) Джона Ликлайдера (J.C.R. Licklider), написанное в 1962 г. В нем он описал возможность появления в будущем глобальной сети, подключиться к которой сможет любой желающий, и что данная сеть соединит компьютерные системы по всему миру.

Д. Ликлайдер изложил основные принципы построения такой сети - это глобальность, распределенность, анонимность, способность сохранять работоспособность даже после остановки большинства ее узлов. Именно эти принципы сформировали облик современного Интернета. Сегодня можно утверждать о непродуманности многих моментов в архитектуре построения сети. В первую очередь это касается юридического контроля, который сильно затруднен при существующей структуре сети. Много внимания было уделено универсальности, распределенности, надежности, быстроте работы, но большинство вопросов безопасности и правового регулирования остались вне поля зрения, так как возникновения преступности в сфере высоких технологий в то время никто не предвидел[2].

В 1979 г. в Далласе состоялась Конференция Американской ассоциации адвокатов, на которой были определены и сформулированы основные составы компьютерных преступлений, в последующем включенные в состав Уголовного кодекса США.

В 1983 г. в США в штате Милуоки произошел первый арест интернет-преступника, о котором известно общественности. Первый зарегистрированный интернет-взлом был совершен группой из шести подростков, которая называла себя «группа 414» (414 - междугородний телефонный код Милуоки). В течение девяти дней ими было «взломано» 60 компьютеров, среди которых компьютеры Лос-Аламосской государственной лаборатории (центр исследования ядерного оружия).

В 1986 г. в США принят Закон о мошенничестве и злоупотреблении с использованием компьютеров (The Computer Fraud and Abuse Act8). Он образует собой основной нормативно-правовой акт, устанавливающий уголовную ответственность за преступления в сфере компьютерной информации.

К концу 80-х - началу 90-х годов рост интернет-преступности отмечен практически во всех странах. Необходимость создания нормативной базы для

---

[2] Ковалева, Н. Н. Информационное право России: учебное пособие / Н. Н. Ковалева. - 2-е издание, переработанное и дополненное. - Москва: Дашков и К°, 2009. - 349, с.

борьбы с преступлениями в сфере высоких технологий осознали власти большинства развитых стран.

В начале 90-х гг. попытка создать единую классификацию компьютерных преступлений предпринята рабочей группой Международной организацией уголовной полиции Интерпол. В утвержденном кодификаторе компьютерных преступлений выделены: несанкционированный доступ и перехват, изменение компьютерных данных, компьютерное мошенничество, незаконное копирование, компьютерный саботаж и прочие компьютерные преступления. Неоднократно проблема унификации уголовного законодательства поднималась и на конференциях стран Группы Восьми (G-8).

Первоначально, столкнувшись с компьютерной преступностью, органы уголовной юстиции начали борьбу с ней при помощи традиционных правовых норм о краже, присвоении, мошенничестве, злоупотреблении доверием. Однако такой подход оказался не вполне удачным, поскольку многие компьютерные преступления не охватываются составами традиционных преступлений.

Так, например, простейший вид компьютерного мошенничества - перемещение денег с одного счёта на другой путём «обмана компьютера» - не охватывается ни составом кражи, ни составом мошенничества, поскольку обмануть компьютер в действительности можно лишь в том смысле, в каком можно обмануть замок у сейфа.

Одновременно начался поиск путей уголовно-правового регулирования вопросов ответственности за совершение таких преступлений в глобальной сети, который продолжается и по настоящее время. Таким образом, России в целях обеспечения информационной безопасности глобальных сетей необходимо ориентироваться на международный опыт, а также вырабатывать своих технологии и меры по обеспечению безопасных условий функционирования глобальных сетей.

1.3 Угрозы информационной безопасности функционированию глобальных сетей

В настоящее время можно выделить следующие наиболее существенные формы информационно-технических опасностей, обусловленных достижениями научно-технического прогресса в условиях глобализации:

1. Первая форма связана связана с использованием современных информационных технологий (махинации с электронными деньгами, компьютерное хулиганство и др.).

2. Вторая форма связана с использованием современных информационных технологий в политических целях.

3. Третья форма с бурным развитием нового класса оружия - информационного, которое способно эффективно воздействовать и на психику, сознание людей, и на информационно-техническую инфраструктуру общества и армии.

В Доктрине информационной безопасности и специальной литературе определяются и классифицируются виды угрозы информационной безопасности, часть которых представляет потенциальную опасность для личности. К ним можно отнести как минимум три группы угроз:

1) непосредственная угроза, например: намерение препятствовать реализации гражданами названных выше конституционных прав и свобод, охраняемых уголовным законом;

2) самоугроза как потенциальная способность личности оказаться жертвой преступления «в результате отрицательного взаимодействия его личностных качеств с внешними факторами»;

3) уголовно наказуемое применение нетрадиционных методов информационного воздействия прежде всего на индивидуальное сознание (правосознание), индивидуальные чувства, эмоции и др;

4) пропаганда порнографии, секса, проституции, иных нравственно порочных образцов жизнедеятельности определенного социума и др.

5) опосредованная угроза, например: пропаганда криминальной культуры, романтизация преступного мира, привлекающая молодежь, особенно несовершеннолетних на сторону тех, кто живет по законам преступного мира, «тюремного закона»[3].

Данные виды угроз информационной безопасности могут проявляться и в глобальных сетях. Следовательно, возникает необходимость изучения и преодоления данных угроз органами государственной власти и социальными институтами общества.

Угрозы можно классифицировать по нескольким критериям:

- по аспекту информационной безопасности (доступность, целостность, конфиденциальность), против которого угрозы направлены в первую очередь;
- по компонентам информационных систем, на которые угрозы нацелены (данные, программы, аппаратура, поддерживающая инфраструктура);
- по способу осуществления (случайные/преднамеренные действия природного/техногенного характера);
- по расположению источника угроз (внутри/вне рассматриваемой ИС).

Отдельную группу угроз составляют угрозы информационной безопасности глобальных сетей. Данные угрозы влияют на все сферы общественной жизни.

В информационной сфере распространено вредоносное программное обеспечение Одним из опаснейших способов проведения атак является внедрение в атакуемые системы вредоносного программного обеспечения. Грани вредоносного ПО:

1) способ распространения;
2) вредоносная функция;
3) внешнее представление.

---

[3] Ищейнов, В. Я. Защита конфиденциальной информации: / В. Я. Ищейнов, М. В. Мецатунян. - Москва : ФОРУМ, 2013. - 254 с.

Выделяют и угрозы экономике.

- Конкурентная разведка западных фирм и государств.
- Распространение негативной информации (в том числе и сети интернет), влекущей для субъектов бизнеса экономические потери.
- Киберпротиводействие конкурирующим фирмам.
- Хищения государственной и корпоративной интеллектуальной собственности.
- Целенаправленное вытеснение России с ряда перспективных рынков за счет скоординированных действий на основе моделей экономики страны и других компьютерных технологий.
- Появление новых компьютерных методов ведения научно-технической разведки.
- Угрозы, вызванные отставанием страны в области ИКТ и критическиих технологий для обеспечения национальной безопасности.

Также существуют военные угрозы

- Контроль Интернет-трафика и сбор статистики по национальному трафику, сбор статистики по вычислительным ресурсам, оценка уровня их использования для национальной обороны.
- Анализ морально-политического состояния населения страны и его демографических особенностей.
- Использование вычислительных и частотных ресурсов России для решения военных задач.
- Несанкционированное использование противником канальной емкости систем связи при проведении военных операций против России или третьих стран.
- Ведение с различными целями информационной войны в электронных масс-медиа.
- Целевое нарушение или изменение трафика, разрушение системы связи страны в критические моменты.
- Распространение дезинформирующей информации с

использованием электронных масс-медиа.

- Поражение ВЦ, центров обработки данных и телекоммуникационных сетей путем применения боевых вирусов и других средств.
- Разведывательно-диверсионная и военная деятельность с применением роботизированных средств и соединений боевых роботов.
- Ведение с различными целями информационной войны в электронных масс-медиа[4].

Основными направлениями обеспечения информационной безопасности России при международном сотрудничестве должны являться:

1) запрещение разработки, распространения и применения "информационного оружия";

2) обеспечение безопасности международного информационного обмена, в том числе сохранности информации при ее передаче по национальным телекоммуникационным каналам и каналам связи;

3) координация деятельности правоохранительных органов стран, входящих в мировое сообщество, по предотвращению компьютерных преступлений;

Это далеко не все угрозы, постоянно появляются различные виду угроз глобальным сетям. В этой связи необходимо изучение и преодоление данных угроз органами государственной власти и социальными институтами общества, опираясь на международный опыт, и проводя международное сотрудничество в целях обеспечения информационной безопасности общества в целом, и глобальных сетей в частности.

---

[4] Юрченко И. В. Вызовы и угрозы национальной и региональной безопасности Российской Федерации в политикоинформационном пространстве: монография. Краснодар: КубГУ, 2009. 281 с.

2. Информационная безопасность в условиях функционирования глобальных сетей

2.1 Государственная политика обеспечения информационной безопасности в условиях функционирования глобальных сетей

Многие исследователи выделяют ряд проблем в области информационной безопасности.

Противоречивые методы и средства системной защиты. Возник совершенно определённый методический и технологический разрыв между механизмами и программно-техническими средствами защиты, функционирующими в реальном масштабе времени в режиме мониторинга, с одной стороны, и возможностями и инструментами комплексной оценки ИБ, её «медленной» составляющей (аудит, экспертиза безопасности), — с другой. Тоже своего рода «расширяющаяся пропасть». В первом случае разрабатываются все более тонкие средства, хотя и реализующие преимущественно «реактивный» подход — защиту от того, что уже случилось; во втором — чаще всего эвристические модели, экспертное оценивание, ориентация на конъюнктурные требования вводимых нормативов, использование которых на практике остаётся проблематичным. Между этими направлениями, в той или иной мере, но необходима интеграция.

Противоречиво техническое нормотворчество. Понятийный аппарат и терминология семантически размываются и американизируются, теряется однозначность и устоявшиеся понятия, возникают логические неполнота и противоречия. Корпоративный подход к обеспечению информационной безопасности, который к тому же особо подвержен иноязычному влиянию, еще больше способствует размыванию понятий в этой сфере. В результате вместо некоторой междисциплинарной смысловой противоречивости и неоднозначности в недавнем прошлом возникло новое явление: многие

понятия, легко и повсеместно теперь употребляемые, виртуализируются, едва ли не теряя смысл. Следование в русле чужого понятийного аппарата, каким бы универсальным и интернациональным он не казался, по сути, есть акт разоружения в информационном противоборстве.

Противоречива ситуация с подготовкой кадров: специальностей много, а специалистов не хватает. Структура специальностей, содержание образования не могут сформироваться, сохраняется дублирование, при нехватке специалистов многие выпускники идут работать в другие области ИКТ. В то же время не заметно успехов в просвещении гуманитариев — сужать понятие «информационная безопасность» до технической проблематики в образовании в настоящее время уже недопустимо. Любому современному человеку, особенно будущим педагогам, крайне необходимы знания хотя бы в области информационно-психологической защиты от агрессивных и деструктивных воздействий на его сознание. Знание основных технических вопросов безопасности в условиях сплошной компьютеризации и «интернетизации» также не будет вредным, а оно сейчас у гуманитариев, как показывает опыт, не простирается далее элементарной осведомленности о компьютерных вирусах и «спаме» и, может быть, еще каких-нибудь туманных сведений об ЭЦП.

Отдельный вопрос — подготовка и воспитание специалистов в области информационного права. Хотя среди юристов существует мнение, что достаточно переформулировать или свести вопросы, связанные с информационноправовыми отношениями, к терминам и процедурам традиционного материального права и проблемы не будет, в общем случае такое вряд ли возможно без ущерба для существа дела — информация это «материя» особая и попытка редукции проблемы здесь неправомерна. Поэтому специалисты нужны, но задача их подготовки оказалась непростой из-за своей противоречивости: будущим ИТ-инженерам просто не хватает времени для получения достаточного, чтобы считаться квалифицированным правоведом, юридического базиса, а студенты-юристы, видимо по складу ума,

не воспринимают необходимый инженерный минимум.

Существует и ряд других проблем в области обеспечения информационной безопасности, поэтому возникает необходимость выработки комплекса мер со стороны государства по обеспечению информационной безопасности.

Для защиты интересов субъектов информационных отношений необходимо сочетать меры следующих уровней:

1) законодательного;

2) административного (приказы и другие действия руководства организаций, связанных с защищаемыми информационными системами);

3) процедурного (меры безопасности, ориентированные на людей);

4) программно-технического.

Законодательный уровень является важнейшим для обеспечения информационной безопасности. На законодательном уровне различаются две группы мер:

1) меры, направленные на создание и поддержание в обществе негативного (в том числе с применением наказаний) отношения к нарушениям и нарушителям информационной безопасности (назовем их мерами ограничительной направленности);

2) направляющие и координирующие меры, способствующие повышению образованности общества в области информационной безопасности, помогающие в разработке и распространении средств обеспечения информационной безопасности (меры созидательной направленности)[5].

Важнейшим правовым актом, определяющим направления государственной политики в области обеспечения информационной безопасности Российской Федерации, является Доктрина информационной безопасности Российской Федерации. Основной целью создания этого концептуального документа является определение основных направлений

[5] Безопасность в Интернете: приоритеты государства [Текст] // Университетская книга. - 2013. - № 4. - С. 32-35

деятельности органов государственной власти по обеспечению безопасности государства в информационной сфере, а также конкретизация общецелевых установок по противодействию угрозам информационной безопасности в различных сферах жизнедеятельности личности, общества и государства.

В Доктрине не представлены конкретные программы действий, но определены основные направления и изложены общие методы обеспечения информационной безопасности России.

Среди этих основных направлений можно выделить:

1) развитие и совершенствование системы обеспечения информационной безопасности;

2) совершенствование нормативно-правовой базы обеспечения информационной безопасности;

3) разработка федеральных и региональных программ обеспечения информационной безопасности;

4) координация деятельности федеральных органов власти, органов государственной власти субъектов Российской Федерации, предприятий, учреждений и организаций независимо от формы собственности в области обеспечения информационной безопасности;

5) создание систем и средств предотвращения несанкционированного доступа к информации, а также разработка и принятие нормативно-правовых актов, устанавливающих ответственность юридических и физических лиц за несанкционированный доступ к информации или ее неправомочное применение;

6) развитие и совершенствование государственной системы защиты информации и системы защиты государственной тайны;

7) создание и развитие единой системы подготовки кадров в области информационной безопасности и информационных технологий;

8) определение порядка финансирования программ обеспечения информационной безопасности;

9) совершенствование законодательства, регулирующего отношения

в области науки и техники;

10) защита конституционных прав и свобод человека и гражданина в процессе обеспечения информационной безопасности[6].

Также ряд авторов выделяют основные элемента государственной политики в области обеспечения информационной безопасности:

1) развитие и совершенствование системы обеспечения информационной безопасности Российской Федерации, реализующей единую государственную политику в этой области, включая совершенствование форм, методов и средств выявления, оценки и прогнозирования угроз информационной безопасности Российской Федерации, а также системы противодействия этим угрозам;

2) выявление технических устройств и программ, представляющих опасность для нормального функционирования информационно-телекоммуникационных систем, предотвращение перехвата информации по техническим каналам, применение криптографических средств защиты информации при ее хранении, обработке и передаче по каналам связи, контроль за выполнением специальных требований по защите информации;

3) координация деятельности федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, предприятий, учреждений и организаций независимо от формы собственности в области обеспечения информационной безопасности Российской Федерации.

4) исключение несанкционированного доступа к обрабатываемой или хранящейся в технических средствах информации;

5) создание систем и средств предотвращения несанкционированного доступа к обрабатываемой информации и специальных воздействий, вызывающих разрушение, уничтожение, искажение информации, а также изменение штатных режимов функционирования систем и средств информатизации и связи;

---

[6] Безопасность в Интернете: приоритеты государства [Текст] // Университетская книга. - 2013. - № 4. - С. 32-35

6) предотвращение утечки информации по техническим каналам, возникающей при эксплуатации технических средств ее обработки, хранения и передачи;

7) разработка эффективной системы мониторинга объектов повышенной опасности, нарушение функционирования которых может привести к возникновению чрезвычайных ситуаций, и прогнозирования чрезвычайных ситуаций.

В Национальном плане США одним из направлений обеспечения информационной безопасности является подготовка общественного мнения о необходимости принятия самых строгих мер, направленных на совершенствование всей государственной системы защиты информации, то в Доктрине информационной безопасности Российсмкой Федерации эта деятельность, по нашему мнению, должного отражения не нашла. Этим, очевидно, в значительной степени объясняются и спекуляции вокруг Доктрины, появившиеся сразу после ее принятия в некоторых средствах массовой информации.

Следовательно, возникает необходимость в совершенствовании государственной системы информационной безопасности. Под государственной системой информационной безопасности страны обычно понимают организационное объединение государственных органов, сил и средств информационной безопасности, осуществляющих свои функции на основе закона и под контролем и защитой судебной власти. Задачами такой системы являются:

а) выявление и прогнозирование появления дестабилизирующих факторов и информационных угроз жизненно важным интересам личности, общества и государства;

б) осуществление комплекса долговременных и оперативных мер по их предупреждению и устранению;

в) создание и поддержание в готовности сил и средств обеспечения информационной безопасности.

Конечно, органы информационной безопасности могут и должны создаваться и в негосударственных структурах для защиты своих потребностей в обеспечении необходимой информацией, ее сохранности и т. п., но на законодательной основе (более того, эти органы путем заключения договоров могут быть включены в единую государственную систему информационной безопасности).

В основу единой государственной системы информационной безопасности в соответствии с законом Российской Федерации «О безопасности» должны быть положены следующие принципы:

1) законность, соблюдение баланса интересов личности, общества и государства;
2) взаимная ответственность субъектов обеспечения безопасности;
3) интеграция систем национальной и международной безопасности[7].

Специфическими принципами обеспечения информационной безопасности являются:

— превентивный характер проведения ее мероприятий по отношению к мероприятиям других видов безопасности;

— адекватная информированность объектов безопасности, в том числе и международных.

Таким образом, органы государственного управления принимают усилия по выработке национальной политики в области обеспечения информационной безопасности и принимают соответствующие директивные документы, регулирующие процесс информатизации всех сфер жизни общества.

[7] Безопасность в Интернете: приоритеты государства [Текст] // Университетская книга. - 2013. - № 4. - С. 32-35

2.2 Современные технологии обеспечения информационной безопасности в условиях функционирования глобальных сетей

Зависимость страны от импортируемых компонентов ставит особые задачи по обеспечению безопасности. Речь идет о необходимости приобретения западных технологий и организации производства критических компонентов и продуктов на территории России.

К их числу в первую очередь следует отнести:

- Технология производства заказных СБИС (сверх большие интегральные схемы), например, процессоров, ПЛМ (программируемые логические матрицы), и т.п.;
- Технология производства многослойных печатных плат;
- Технология производства кристаллов памяти;
- Технология производства герметичных электроаккумуляторов;
- Технология производства магнитных и оптических накопителей;
- Технология производства систем маршрутизации и сетеобразования.

Концепция распространения программного обеспечения (ПО) с открытым кодом (Open Source), обозначающая поставку программ с полным комплектом исходных текстов очень важна в решении проблем информационной безопасности. Главное ее преимущество - заказчик получает возможность протестировать исходные тексты программ и убедиться в отсутствии закладок, побочных эффектов, недокументированных возможностей и т. д. Поэтому во многих странах приняты специальные постановления, регламентирующие использование ПО для различных государственных, оборонных и стратегически важных приложений, и в этих постановлениях существенная роль отводится ПО с открытым кодом.

Сейчас в рамках концепции ПО с открытым кодом следует выделить три основные подхода:

- Свободно распространяемое ПО, коды которого находятся в открытом доступе, и каждый желающий может модифицировать его для собственных нужд. Этот подход применяется при распространении массовых программ. Его недостаток с точки зрения информационной безопасности - коды используемого ПО доступны всем, в том числе потенциальным нарушителям. Достоинство - на основе модификации ПО с открытым кодом можно быстро разрабатывать специализированные версии сложных систем. Таким путем, например, был разработан "красный Linux" - операционная система для государственных служб Китая.
- Свободно распространяемое ПО с единым центром учета модификаций. Каждый желающий может получить код и модифицировать его, однако обязан сообщить обо всех модификациях в некоторую координирующую организацию. Этот подход применяется, например, при создании и развитии антивирусного и защитного ПО, когда исследователи обмениваются между собой данными о новых вирусах и типах атак. К данному типу ПО относится, например, средство обнаружения вторжений SNORT.
- Фирменное ПО, поставляемое разработчиком "как есть" без права модификации со стороны пользователя, но с предоставлением пользователю исходных кодов. Этот подход сейчас усиленно продвигает фирма Microsoft при работе с государственными структурами разных стран.

С точки зрения информационной безопасности страны целесообразно использовать каждый из этих подходов - для решения определенных видов задач лучше подходит первый из них, для других - второй или третий.

Критическое ПО в военной сфере.

Одним из важнейшем направлений, определяющим на ближайшие десять лет развитие информационных технологий является реализуемая руководством США концепция дистанционной войны. В рамках этой концепции в США создается беспилотная авиация, мобильные подводные и сухопутные роботы, цифровое обеспечение дистанционно управляемых

боевых действий в любой точке планеты (цифровая карта мира, системы разведки, связи и управления).

С точки зрения национальной безопасности адекватным ответом на эти вызовы должна стать разработка систем интеллектуального оружия и систем противодействия ему. Одним из ведущих направлений должна стать робототехника и программное обеспечение, составляющее ее начинку, а именно: системы машинного зрения, системы искусственного интеллекта, системы планирования действий больших групп робототехнических средств. Развитие этого направления потребует проведения НИОКР и развития самых разных областей микроэлектроники, нанотехнологий, микро-наноэлектромеханических систем (MEMS, NEMS), нейрокомпьютеров и нейрочипов (по которым также нужна отдельная целевая программа).

Критические технологии, обеспечивающие экономический рост.

Расширение экспортной составляющей рынка ИКТ следует рассматривать, как один из компонентов экономического роста страны и диверсификацию экспорта в направлении увеличения объемов производства и экспорта наукоемкой продукции.

Структура экспорта не является некоей константой. Она претерпевает изменения в соответствии меняющимися требованиями рынка и необходимо быть готовыми к таким изменениям и к интервенциям новых продуктов. Как правило такие интервенции требуют существенных затрат, которые российские компании самостоятельно осуществить не могут, и здесь требуются соответствующие государственные субсидии и субвенции[8].

Реалии настоящего времени таковы, что в России в сфере использования систем связи и телекоммуникаций доминируют иностранные производители. Достаточно эффективна деятельность в России финской фирмы Nokia, которая заняла одно из ведущих мест на российском рынке радиотелефонов, пользуется услугами обширной дилерской сети, реализует проекты по созданию телефонных станций, телекоммуникационных линий и

[8] Кесслер, Г. Информационная безопасность: новые технологии и старые принципы [Текст] / Г. Кесслер // Открытые системы. СУБД. - 2012. - № 2. - С. 44-48 .

систем сотовой связи, поставляет приборы для российских научно-исследовательских институтов.

В настоящее время вопрос обеспечения безопасности информационных систем сверхактуален, так как угроза нападения или вторжения в них весьма реальна. Сегодня эта проблема волнует практически всех.

В этих условиях органы государсьвенного управления принимают усилия по выработке национальной политики в области обеспечения информационной безопасности глобальных сетей.

Заключение

Для нынешней информационной цивилизации характерен пересмотр образовательных научных концепций на основе достижений кибернетики, информатики, синергетики, психологии, педагогики и ряда других наук, а также бурное развитие науки и наукоемких производств. Основной характеристикой человеческой деятельности наряду с энергией и веществом становится информация как возобновляемый и неистощимый ресурс человечества, как главная ценность общества. Именно это дает основание говорить о том, что человечество вступило в новую эпоху своего развития.

Пройдя за последние время путь развития в качестве общенаучной, категория «информация» является вершиной информационного подхода к познанию действительности личностью. Данный подход в особенности расширился и углубился в процессе развития автоматизированных информационных технологий. Общенаучное понятие информации, которое отражает структуру материи, конкретизирует в информатике как данные и знания, существующие, в частности, в виде различных алгоритмов, моделей и программ.

Проблема технологического и безопасного развития государства в нынешних условиях необходима рассматриваться и как научно-техническая, и как национальная проблема экономического выживания и будущего безопасного развития. Обеспечение безопасности страны в принципе невозможно без перехода на путь безопасного развития государства. А сохранение биосферы и человеческой культуры невозможно без обеспечения их совместной безопасности.

В настоящее время вопрос обеспечения безопасности информационных систем сверхактуален, так как угроза нападения или вторжения в них весьма реальна. Сегодня эта проблема волнует практически всех.

В этих условиях органы государсьвенного управления принимают усилия по выработке национальной политики в области обеспечения

информационной безопасности. Органы государственного управления принимают усилия по выработке национальной политики в области обеспечения информационной безопасности и принимают соответствующие директивные документы, регулирующие процесс информатизации всех сфер жизни общества.

России необходимо изучение и разработка мер в области информационной безопасности функционирования глобальных сетей органами государственной власти и социальными институтами общества, опираясь на международный опыт, и проводя международное сотрудничество в целях обеспечения информационной безопасности общества в целом, и глобальных сетей в частности.

Список литературы

1. Доктрина информационной безопасности РФ // Российская газета. 2000. 29 сентября.
2. Концепция государственной информационной политики РФ 1998 г. [Электронный ресурс]. URL: http://www.nbuv. gov.ua/law/98ru-gip.html
3. Закон Российской Федерации от 5.03.1992. № 2446-1 «О безопасности» // Российская газета. 1992. 6 мая. № 103.
4. Безопасность в Интернете: приоритеты государства [Текст] // Университетская книга. - 2013. - № 4. - С. 32-35
5. Васильев, В. И. Безопасность в Интернете: пути достижения [Текст] // Университетская книга. - 2012. - № 3. - С. 50-51
6. Зети П. П. Информационно-коммуникационные процессы на Юге России: идеологический аспект // Политическая наука: состояние и перспективы развития в XXI веке: материалы международной научно-практической конференции. Краснодар: КубГУ, 2011. С. 458-462.
7. Интеллектуальные системы защиты информации: / В. И. Васильев. - Издание 2-е, исправленное. - Москва: Машиностроение, 2013. - 171с.
8. Ищейнов, В. Я. Защита конфиденциальной информации: / В. Я. Ищейнов, М. В. Мецатунян. - Москва : ФОРУМ, 2013. - 254 с.
9. Кесслер, Г. Информационная безопасность: новые технологии и старые принципы [Текст] / Г. Кесслер // Открытые системы. СУБД. - 2012. - № 2. - С. 44-48 .
10. Ковалева, Н. Н. Информационное право России: учебное пособие / Н. Н. Ковалева. - 2-е издание, переработанное и дополненное. - Москва: Дашков и К°, 2009. - 349, с.
11. Колисниченко, Д. Н. Анонимность и безопасность в Интернете : от "чайника" к пользователю / Денис Колисниченко. - Санкт-Петербург: БХВ-Петербург, 2012. - 232 с.

12. Литвинова, Т. Н. "Информационный джихад" в глобальной сети [Текст] / Т. Н. Литвинова // Власть. - 2010. - № 9. - С. 116-119.

13. Парфенов, Б. А. Все - на защиту информационной безопасности [Текст] / Б. А. Парфенов // Вестник связи. - 2011. - № 12. - С. 22-26

14. Пасхин Е.Н., Тупало В.Г., Урсул А.Д. Устойчивое развитие и информатизация образования: Монография. М., 2009.

15. Самохвалова, В. И. Глобальный мир как пространство современных информационных войн [Текст] / В. И. Самохвалова // Философия и общество. - 2011. - № 4. - С. 33-49 .

16. Юрченко И. В. Вызовы и угрозы национальной и региональной безопасности Российской Федерации в политикоинформационном пространстве: монография. Краснодар: КубГУ, 2009. 281 с.