«Кто владеет информацией - владеет миром»
Ф. Бэкон

Америка является производителем огромного количества информации, но только те, у которых есть определенные коды, некие ключи для дешифровки, способны правильно ею распорядиться.

В.Коровин

Сетецентричная война – это новый вид тотальной войны. Сетецентричная война представляет собой глобальную манипуляцию над всеми участниками исторического процесса в мировом масштабе. Это выигрыш битвы до её начала.

Генерал А.Владимиров

В глобальном киберпространстве человек человеку – «facebook».

Нанокомпьютерный Странник

Раздел I. Проблемы обеспечения информационной безопасности в меняющемся мире

§1. Что такое «информационная модель цивилизации» и «правительство Интернета»?

В условиях глобализации и распада сложившегося после Второй мировой войны мирового порядка произошло резкое падение уровня управляемости международными процессами. Прежние системы и механизмы международной безопасности оказались неэффективными, резко возросла региональная и глобальная нестабильность. **Обшепланетарная ситуация в меняющемся мире стремительно усложняется, геостратегическая ситуация имеет четко выраженную тенденцию к ухудшению, что, естественно, не может не отражаться на состоянии национальной безопасности России.**

Беспрецедентные темпы развития информационных технологий, их стремительное проникновение буквально во все сферы жизни общества, помимо очевидного позитивного эффекта, выраженного в значительном повышении производительности и эффективности человеческого труда, привело к появлению ряда трудно разрешаемых проблем, к возникновению новых, невиданных ранее угроз и уязвимости[1]. Очевидно, что подобная уязвимость весьма привлекательна как в контексте политической и экономической борьбы так и для кибертеррористов, так как потенциально позволяет за счет сравнительно небольших усилий нескольких злоумышленников, действующих в скрытом режиме, вызвать катастрофу, угрожающую жизни многих тысяч, а может быть, и миллионов людей. При этом следует учитывать, что сами технологии нападения на информационные системы, то есть информационное оружие, быстро развиваются и совершенствуются параллельно с развитием самих информационных технологий и с течением времени становятся доступными для всѐ более широкого круга потенциальных злоумышленников.

Понятие информационного терроризма на сегодняшний день имеет по крайней мере два толкования.

Первое направление – манипулирование общественным сознанием путем массированного вбрасывания недостоверной или ложной информации с целью создания напряженности в обществе, неустойчивости, панических настроений, направленное на реализацию политических или экономических задач в своих интересах.

Вторая разновидность – часто термин "информационный терроризм" понимается как кибератаки на информационные системы критического применения, работающие в контурах управления социально важными техническими и технологическими объектами и системами, с целью нарушения их нормальной работы.

На рубеже веков терроризм стал неизбежным спутником противоречивого развития современного мира. Среди разнообразных проявлений терроризма и способов террористической деятельности особое место занимает информационный терроризм. На Западе он получил название "кибертерроризм". Применение террористическими организациями важнейших достижений в области науки и техники стало неотъемлемым фактом современности. При этом терроризм в информационно-культурной среде не только привлекает к себе особое внимание и может шантажировать власть, но и способен увеличивать масштабы и спектр воздействия на сознание человека. Только в 2010 г. сотрудники Федеральной службы безопасности Российской Федерации отразили свыше 1 миллиона 200 тысяч хакерских атак, причем более 280 тысяч из них было направлено на сайт Президента Российской Федерации.

Не меньшую опасность представляет собой распространение информации террористического или подрывного содержания. Посредством сети Интернет распространяются компьютерные игры, пропагандирующие убийства и насилие в отношении лиц других национальностей и религиозных убеждений и оказывающие разрушительное воздействие на психику молодежи. Растет, к сожалению, и количество уголовных дел, связанных с преступлениями в сфере информационных технологий. Эта динамика впечатляет. Если в 2007 году количество таких уголовных дел было 4,5 тысячи, то в 2008 году оно превысило 5,5 тысячи, а в 2010г. уже было около 8 тысяч уголовных дел.

Таким образом, можно констатировать, что в глобальном информационном пространстве ***создается своего рода преступная террористическая культура***, которая живет и распространяется, как раковая опухоль, формируя сетевую террористическую инфраструктуру, способную к самовоспроизводству [1].

Проблема обеспечения информационной безопасности федеральными органами законодательной и исполнительной власти Российской Федерации, политическим руководством страны, учеными и практиками воспринимаются как одна из наиболее злободневных и жизненно важных для современной России. Еѐ актуальность обусловлена следующими обстоятельствами.

1. Качественно новой ролью информации в современном обществе, превращением ее в основной социальный ресурс.
2. Возрастанием политической роли информации, превращением ее в национальный политико-стратегический ресурс и критерий зрелости и

развитости политической системы. Сегодня в научном мире информация вполне обоснованно считается политическим капиталом нации.

3. Превращением информационной безопасности в неотъемлемый компонент общей системы безопасности, состояние которой в условиях трансформации российского общества и государства является достаточно проблематичным.
4. Социальными последствиями низкой отечественной информационной культуры, отставанием информационных технологий России от западных.

Как известно, информация (от латинского informatio – разъяснение, изложение) – в самом общем понимании представляет собой меру распределения материи и энергии в пространстве и во времени, меру изменений, которыми сопровождаются все протекающие в мире процессы.

В исследованиях, связанных с понятием информации, и по сей день много нерешенных вопросов[2]. До сих пор длится дискуссия, является ли информация свойством всего материального, или – только живых организмов, или – исключительно разумных, сознательно действующих существ. Определения информации давали такие широко известные ученые, как Н. Виннер, Р. Хартли, К. Шеннон, Н. Рашевский и другие. Ниже приведены лишь некоторые из наиболее распространенных определений. Информация:

- фундаментальная первооснова и всеобщее свойство Вселенной, которая существует независимо от нас, проявляется в трехмерном процессе взаимодействия микро- и макропроцессов энергии, движения и массы в пространстве и времени;
- результат отражения движения объектов материального мира в системах живой природы;
- свойство материи изменяться и отражать это изменение;
- сообщение, описание фактов;
- новости, новые сведения;
- «отраженное разнообразие»;
- снятие (устранение) неопределенности, где неопределенность – недостаточное знание об объектах и явлениях (отождествляется с неинформированностью субъекта);
- степень модификации структуры входными данными;
- передача, основа связи и управления в живой природе и машинах.

Информация характеризуется формой представления, содержанием и затратами интеллектуального труда человека на ее создание.

Основными свойствами информации являются: способность воздействовать на психику; значимость (полнота); достоверность; целостность; адекватность.

Способность воздействовать на психику – неотъемлемое свойство информации. Фундаментальное свойство информации (применительно к человеку) – оторвавшись от объекта отражения существовать самостоятельно, стать содержимым памяти, то есть самостоятельно участвовать в психических процессах, трансформируясь в представления, знания, умения, навыки.

Значимость информации – свойство информации сохранять свою потребительскую ценность для получателя в течение времени, т.е. не подвергаться моральному старению.
Достоверность информации – соответствие полученной информации действительной обстановке.
Целостность информации – это неизменность информации в условиях случайных или преднамеренных действий в процессе эксплуатации информационной системы.
Адекватность или старение информации – свойство информации утрачивать со временем свою практическую ценность, обусловленное изменением состояния отображаемой ею предметной области.

Общегосударственная система мер по обеспечению информационной безопасности России[3] базируется на **Доктрине информационной безопасности Российской Федерации** [4] (далее — Доктрина), утвержденной Президентом Российской Федерации 9 сентября 2000 года. Доктрина развивает Концепцию национальной безопасности Российской Федерации применительно к информационной сфере и представляет собой совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности Российской Федерации.

Доктрина служит основой для:

- формирования государственной политики в области обеспечения информационной безопасности Российской Федерации;
- подготовки предложений по совершенствованию правового, методического, научно-технического и организационного обеспечения информационной безопасности Российской Федерации;
- разработки целевых программ обеспечения информационной безопасности Российской Федерации**.**

В соответствии с Доктриной, ***под информационной безопасностью Российской Федерации понимается состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью интересов личности, общества и государства***.

Угрозы национальной безопасности подразделяются на следующие категории:

- **Угрозы личности и обществу** —

кибертерроризм;
угрозы нравственности (распространение порнографии, пропаганда насилия, наркотиков, криминализация, разжигание межнациональной розни и т. д.);
неконтролируемые воздействия на подсознание (киберзомбирование);
распространение политических и религиозных взглядов, угрожающих стабильности общества (пропаганда расизма, нацизма, тоталитарных сект);
ведение с различными целями информационной войны в электронных масс-медиа;
фальсификация данных и документов в системах электронного правительства.

- **Угрозы экономике:**

бизнес - разведка иностранных фирм и государств;
распространение негативной информации, влекущей экономические потери для субъектов бизнеса;

киберпротиводействие конкурирующим фирмам;
незаконное использование интеллектуальной собственности (информационных активов);

• **Военные угрозы**:

контроль Интернет-трафика потенциальным противником и сбор статистики по национальному трафику, сбор статистики по вычислительным ресурсам, оценка уровня их использования для национальной обороны;
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;
целевое нарушение или изменение трафика, разрушение системы связи страны в критические моменты;
распространение дезинформации;
поражение ВЦ, центров обработки данных и телекоммуникационных сетей путем применения боевых компьютерных вирусов и других средств;
разведывательно-диверсионная и военная деятельность с применением роботизированных средств и соединений боевых роботов.

С развитием ИКТ многократно возрастают возможности по добыванию, сбору, обработке, хранению, поиску, отображению и передаче информации. Параллельно и столь же интенсивно разрабатываются способы и средства уничтожения, искажения, несанкционированного доступа к информации, ее блокирования, а также нарушения функционирования *информационно-телекоммуникационных систем* (ИТКС), которые относят к наиболее уязвимым элементам инфраструктуры. В связи с этим *многократно повышается роль и значение информационной безопасности ИТКС государственного и ведомственного управления*. Стремительное развитие компьютерных технологий и международных компьютерных сетей как неотъемлемой части международной финансовой и банковской деятельности создало предпосылки, в немалой степени облегчающие совершение преступных экономических деяний внутри страны и на международном уровне. В настоящее время стали появляться преступные формирования «взломщиков» компьютерных средств защиты, которые по заданиям криминальных структур проводят значительные хищения в различных финансовых органах. ***Растет, удваиваясь почти каждые 18 месяцев, число преступлений с использованием аппаратно-программных средств, «взломщики» проникают в атакуемую ИТКС через глобальную сеть Интернет.***

В 2003 году мировой экономический ущерб от хакерских атак — явных и скрытых, — а также от последствий распространения вирусов и «червей» может превысил $150 млрд. Спустя десятилетие, рост ущерба может приблизиться к отметке 700%. Анализ отечественных и зарубежных экспертов свидетельствует, что основным видом компьютерных преступлений стала область финансовой и банковской деятельности.

Структура и рейтинг компьютерных преступлений выглядит следующим образом:

- несанкционированный доступ в информационные системы, перехват информации, кража оплаченного пользователем времени;
- злонамеренные нарушения ИБ в форме всевозможных вирусов и вредоносных программ;
- мошенничества с банкоматами, игровыми автоматами, платежными средствами и т. п.;
- нарушения авторских прав, незаконное копирование программного обеспечения;
- распространение порнографии, в том числе детской, через Интернет;
- неправомочное использование междугородней и международной телефонной связи;
- изготовление и продажа технических средств для незаконного получения доступа в ИКТ-системы и информационные базы;
- сетевой экстремизм и информационный терроризм;
- деятельность подразделений иностранных спецслужб и армий, занимающихся разработкой боевых вирусов и методов информационной войны (например, для проверки результатов НИОКР);
- деятельность органов юриспруденции иностранных государств, несанкционированно вторгающихся в киберпространство России для сбора доказательств преступной деятельности граждан РФ.

Сети международного информационного обмена существенно расширяют возможности использования информационного оружия, которое по своей результативности сопоставимо с оружием массового поражения. *Под* **информационным оружием** *понимается совокупность средств и методов, позволяющих похищать, искажать или уничтожать информацию, ограничивать или прекращать доступ к ней законных пользователей, нарушать работу или выводить из строя телекоммуникационные сети и компьютерные системы, используемые в обеспечении жизнедеятельности общества и государства*. Спектр действия такого оружия простирается от нанесения вреда психическому здоровью людей, негативного воздействия на индивидуальное и общественное сознание до перехвата и уничтожения важной информации. Например, программные вирусы и программные закладки способны полностью или частично вывести из строя базирующиеся на вычислительной технике средства связи, системы государственного и ведомственного управления. К информационному оружию относят разновидности боевых «интеллектуальных агентов» и «логические бомбы», которые вносятся в компьютерные сети потенциального противника, и активизируются специальными командами, подаваемыми в необходимый момент времени, а также различные технические и программные средства преодоления защиты ИТКС, дистанционного нарушения их работоспособности, извлечения данных из информационных массивов и манипулирование потоками информации. Программное воздействие на ИТКС и информационные ресурсы осуществляется путем внедрения элементов информационного оружия (компьютерных вирусов, «программных червей», «Троянских коней», программных закладок, логических бомб) в системы управления с целью разрушения (уничтожения), искажения, съема (перехвата)

информации в процессе ее сбора, обработки, хранения, передачи и распространения.

Объектами общенациональной системы информационной безопасности являются компьютерные технологии и информационные ресурсы в следующих областях:

• *правительственные автоматизированные системы*, включая все государственные учреждения и региональные структуры;

• *объекты критической национальной инфраструктуры*, такие, как транспортные системы, включая трубопроводные, кредитно-денежная система, связь и энергоснабжение;

• *корпоративные автоматизированные информационные системы*;

• *персональные пользователи информационных ресурсов*.

Россия обладает значительным заделом базовых научно-технических разработок в области программных, аппаратных и криптографических технологий защиты информации. Однако ориентация на использование узко национальных средств безопасности может привести к созданию дополнительных барьеров для интеграции российских организаций в международные системы электронной коммерции и, в конечном счете, привести к снижению темпов развития индустрии информации и телекоммуникаций. **В то же время, преимущественное использование зарубежных технологий обуславливает потенциальную уязвимость информационно-коммуникационной инфраструктуры для дестабилизирующих внешних воздействий со стороны стран-разработчиков, в том числе, в случае возможного применения ими информационного оружия.**

Отдельным аспектом проблемы информационной безопасности России является широкое использование в нашей стране зарубежных программных продуктов, неадаптированных к национально-психологическим особенностям населения, что создает угрозу возникновения системных «пользовательских ошибок» на различных этапах разработки, производства и эксплуатации объектов, и повышению риска техногенных аварий. В настоящее время в России практически отсутствует политика безопасности Интернет-сайтов. Решение проблем обеспечения национальной безопасности не может быть осуществлено исключительно силами государства. *Необходима согласованная и заинтересованная работа органов государственной власти совместно с общественными организациями, представителями деловых кругов, влиятельных политических сил, то есть всего общества*.

Имеющиеся на сегодняшний день организационно-административные и программно-технические решения в области борьбы с компьютерной преступностью и обеспечения информационной безопасности критических компонентов инфраструктуры являются недостаточными, не отвечают требованиям высокой технологичности, слабо учитывают специфику этой сферы деятельности. Внедряемые аппаратные и программные средства зачастую не способны к качественному системному взаимодействию с информационными системами зарубежных государств. *Главной целью государственной политики* в области выявления и пресечения компьютерных преступлений в этих

условиях *становится создание* **эффективной национальной системы борьбы с правонарушениями в сфере компьютерных технологий**.

Система управления информационной безопасностью

В настоящее время **система управления информационной безопасностью России** включает:

• Президента Российской Федерации,
• Совет Федерации Федерального Собрания РФ,
• Государственную Думу Федерального Собрания РФ,
• Правительство РФ,
• Совет Безопасности РФ,
• федеральные органы исполнительной власти,
• межведомственные и государственные комиссии, создаваемые Президентом РФ и Правительством РФ,
• органы исполнительной власти субъектов РФ,
• органы местного самоуправления,
• органы судебной власти,
• общественные объединения,
• отдельных граждан.

Основным органом, на практике отвечающим за обеспечение информационной безопасности РФ, является **Государственная техническая комиссия (ГТК) при Президенте РФ**, созданная в соответствии с Указом Президента РФ № 9 от 5 января 1992 г. в целях обеспечения национальной безопасности народов и территорий РФ в части приоритетов и защиты информации в области обороны, политики, экономики, науки, экологии, ресурсов и противодействия иностранным техническим разведкам.

В действующую систему управления информационной безопасностью РФ входит ряд подразделений по борьбе с высокотехнологическими преступлениями, созданных в рамках силовых ведомств[5]:

• в ФСБ РФ работают 8 и 16-й центры (бывшее Федеральное агентство правительственной связи и информации - ФАПСИ), в Министерстве обороны РФ - Управление криптографии. Эти подразделения заняты обеспечением безопасности каналов связи;
• функции борьбы с киберпреступностью возложены на ФСБ РФ и МВД РФ. В ФСБ РФ — этим занято Управление компьютерной и информационной безопасности, в МВД РФ расширены до федерального уровня функции Управления, ранее занимавшегося собственной технической безопасностью министерства. В структуре ГУВД г. Москвы с 2002 г. действует Управление по борьбе с киберпреступностью;
• в структуру Управления МВД РФ входят:

- отдел по борьбе с компьютерными преступлениями;
- отдел по борьбе с незаконным оборотом радиоэлектронных и специальных технических средств;
- отдел по борьбе с распространением детской порнографии;
- аналитический отдел;
- технический отдел.

Сложившаяся к настоящему времени схема управления информационной безопасностью страны не обеспечивает достаточное противодействие современным киберугрозам и практически не занимается технологиями предотвращения киберпреступности. У перечисленных структур недостаточно сил и средств для серьезной аналитической работы по информационной безопасности, ведению широкомасштабных НИОКР и их координации, а также активному противодействию потенциальным угрозам информационной безопасности.

Главный недостаток *системы управления информационной безопасностью страны* состоит в том, что она не в состоянии проводить единую техническую политику в данной сфере[3]. Каждый регион, каждое министерство, ведомство и государственное учреждение практически самостоятельно проводят мероприятия по информационной безопасности. При этом отсутствуют протоколы связи, и работы проводятся не всегда на должном профессиональном уровне. В результате *национальная информационно-коммуникационная инфраструктура может оказаться незащищенной*, а региональные и ведомственные информационные ресурсы оказываются недоступными и не сводимыми в национальную сеть.

Система управления информационной безопасностью на современном этапе должна как минимум:

• *адекватным образом отвечать характеру компьютерных преступлений и быть готова к отражению угроз информационной войны;*

• *обеспечивать координацию деятельности всех министерств, ведомств и регионов в области информационной безопасности;*

• *обеспечивать безопасность национальных информационно-телекоммуникационных сетей, включая критические корпоративные сети;*

• *сочетать механизмы бюджетного рыночного финансирования развития сферы информационной безопасности.*

С учетом серьезности угроз информационной безопасности и требований, предъявляемых к системе управления информационной безопасности, необходимы:

• *централизация управления сферой обеспечения информационной безопасности*;

• *создание разветвленной региональной системы управления* как для решения региональных проблем обеспечения информационной безопасности, так и для защиты национальных информационно-телекоммуникационных сетей.

Для решения задач обеспечения информационной безопасности страны **целесообразно** создание **Федеральной службы информационной безопасности** (ФСИБ РФ) на базе 8-го и 16-го центров, Управления компьютерной и информационной безопасности ФСБ РФ, Управления по борьбе с киберпреступностью МВД РФ. Соответствующие региональные подразделения должны быть созданы в Федеральных округах. (Как вариант, возможно создание **Центра информационной безопасности** (ЦИБ) с аналогичными функциями в рамках ФСБ РФ). Создаваемая схема управления должна быть также дополнена **подсистемами горизонтальной и вертикальной координации** в виде комиссий, которые в полной мере отвечали бы как характеру программных мероприятий, так и специфике объектов информационной безопасности.

В последние годы объем знаний на планете удваивается каждый год, и темп его прироста определяется экспоненциальным законом. Информация становится стратегическим ресурсом современного общества, важнейшим фактором экономического развития и политической власти. Современное общество становится информационным[6]. Информационное общество определяется как общество, где «развитие компьютеризации предоставит людям доступ к надежным источникам информации и избавит их от рутинной работы, обеспечив высокий уровень автоматизации производства».

Современная стадия общественного развития характеризуется понятием глобализации, означает «смешение» национального и внешнего мира. Основными влияющими факторами глобализации, качественных изменений в современном обществе являются:

- удешевление информации и информационного обмена: во-первых, за счет перехода с бумажных на преимущественно электронные носители, а во-вторых, за счет снижения стоимости самого электронного информационного обмена;
- переизбыток информации. В условиях переизбытка информации все сложнее найти нужную. В этих условиях интенсивно развивается рынок информационных услуг. Информационное посредничество, как и любое другое – это бизнес, который не требует больших капиталовложений

Общегосударственная система мер по развитию информационного общества России базируется на **Стратегии развития информационного общества в Российской Федерации** [7] (Утверждена Президентом Российской Федерации В.Путиным 7 февраля 2008 г., № Пр-212).

Целями развития информационного общества в России являются:

- Повышение устойчивости общественного развития, конкурентоспособности страны, благосостояния и качества жизни граждан.
- Укрепление государственных гарантий реализации конституционных прав человека и гражданина в информационном обществе, создание равных возможностей по доступу к информации и информационно-коммуникационным технологиям.
- Повышение качества образования и здравоохранения.
- Создание условий для сохранения и развития культурного разнообразия и самобытности народов, проживающих на территории Российской Федерации.
- Повышение эффективности государственного управления. Противодействие угрозам использования потенциала информационно-коммуникационных технологий для нанесения ущерба национальным интересам России.

Итак, «информационная модель будущей цивилизации» - это модель общества, к воплощению в жизнь которой следует стремиться. Во многих документах формулируются обобщенные трактовки этого понятия: «новый уровень развития человечества», «концепция постиндустриального общества; новая информационная фаза развития цивилизации, в которой главными продуктами производства являются информация и знания» и выделяют три основных признака: «увеличение роли информации и знаний в жизни общества»; «возрастание доли информационных коммуникаций, продуктов и услуг в валовом внутреннем продукте»; «создание глобального информационного пространства**,**

обеспечивающего (а) эффективное информационное взаимодействие людей, (б) их доступ к мировым информационным ресурсам и (в) удовлетворение их потребностей в информационных продуктах и услугах» и т.п..

Однако эта ярко выраженная сегодня тенденция несет в себе и определенную идеологическую нагрузку, позволяя ей (и ему, т.е. «информационному обществу») стать проводником интересов влиятельных игроков глобальной политической игры. Совершенно очевидно, что многообразные и большие преимущества получают в данном контексте прежде всего США и страны «золотого миллиарда» (т.е. ЕС+Австралия, Канада, Япония, Новая Зеландия).

Реализация этой концепции, вероятно, будет означать формирование *мирового политический порядок в информационной сфере*: «Международный информационный порядок (МИП) (…) включает в себя все процессы межкультурных коммуникаций, происходящие при посредстве в основном технических информационных систем как индивидуального (персональные компьютеры), так и массового характера (пресса, ТВ, Интернет, спутниковые и другие системы передачи и распространения знаний)» [8].

Прогресс средств и каналов информационного обмена рождает качественные изменения в экономической, социальной, культурной, правовой, политической и в других сферах, которые охватывают весь мир. Формируется новый мировой информационный порядок. Он формируется как под воздействием стихийных процессов, так и в результате сознательной и целенаправленной деятельности субъектов. Поэтому мировой информационный порядок следует понимать как совокупность информационных процессов и как институты и нормы, регулирующие деятельность участников этих процессов. Современный мировой информационный порядок – глобальный, и он лежит в основе глобализации всего мирового порядка. Это прежде всего относится к сфере экономики.

К. Келли сформулировал основные тенденции и особенности новой экономики, представив их как «12 законов успеха в бурно меняющемся мире» [9]:

1. «Закон связи» (мир представляется как сеть микрочипов, телекосмос; экономика – это сетевая экономика, «коллективное взаимодействие, связывающее воедино триллионы объектов живой и не живой природы через волокно или воздух»).

2. «Закон полноты» (В сетевой экономике ценность вырастает из изобилия и возрастает от повсеместного распространения («эффект факса»).

3. «Закон экспоненциального роста».

4. «Закон переломных точек» (особенность сетевой экономики в том, что точку перелома определить вовремя практически невозможно, и последствия перелома становятся заметными лишь спустя много времени).

5. «Закон увеличивающихся отдач».

6. «Закон обратного ценообразования» – «самое лучшее дешевеет с каждым годом», постоянное и существенное улучшение качества продукции.

7. «Закон щедрости» (Компания Sun, раздавая Java, очень успешно продавала серверы, а Netscape продавал математическое обеспечение для коммерческих серверов, раздавая бесплатно браузеры для потребителей.

Параллельно существует обратная тенденция, когда продукты, создаваемые как бесплатные, приобретают и наращивают цену. Например, энциклопедия «Британника» начиналась как сборник статей любителей, нечто аналогичное современным подборкам FAQ).

8. «Закон преданности» (традиционное для индустриальной эпохи деление на своих и чужих теряет своѐ значение, «пользователи голосуют за максимальное расширение сети»).

9. «Закон временного спуска» (сеть развивается очень динамично, экономическая деятельность сопряжена с постоянными и очень большими рисками, с неопределенностью).

10. «Закон замещения» (постепенное замещение материальных ценностей в нашей экономике информацией: автомобили и телефоны меньше весят, но функционируют гораздо лучше).

11. «Закон маслобойки» (Маслобойка символизирует креативную силу разрушения. Например, «одновременно с уничтожением старых рабочих мест рождаются новые, при этом превышение постоянно увеличивается. Любая инновация - это всегда разрушение, постоянная инновация - это непрекращающееся разрушение. Отрицательная сторона "сетевой экономики" - постоянная гибель многих компаний, отраслей индустрии и рабочих мест: "сетевая экономика" функционирует на грани хаоса).

12. «Закон неэффективности». (Экономисты полагают, что грядущая эпоха принесет «суперпродуктивность».Главная функция человека в экономике – понять, какую работу следует делать дальше. Новая экономика – это интеллектуальная экономика и экономика идей.)

Далеко не все изменения, описанные Келли, могут быть возведены в разряд устойчивых тенденций. Многие из них обращены в отдаленное будущее, не лишены идеализма и утопизма. Становление нового миропорядка сопровождается широкомасштабными информационными войнами.

В августе 1995 года Национальный институт обороны США опубликовал работу Мартина Либики «**Что такое информационная война?».** В ней автор определил семь форм информационной войны:

1. Борьба с системами управления (C2W – Command and Control Warfare);.
2. Информационно-разведывательные операции (Intelligence-based operations);
3. Психологическая борьба (PSYOPS);
4. «Хакерская» борьба (Hakerwar);
5. Экономическая информационная борьба.
6. Электронная борьба (EW);
7. «Кибернетическая» и «сетевая» борьба (Cyberwar combat in the virtual realm);

Реалии современного мира неопровержимо доказывают, что сегодня между ведущими государствами развернулось геостратегическое информационное противоборство за достижение превосходства в мировом информационном пространстве[10]. Безусловно, что особо важную роль оно стало играть в сфере военной безопасности. В настоящее время наиболее развитые страны располагают мощным информационным потенциалом, который в определенных условиях обеспечивает достижение ими самых различных политических целей. Острота и непредсказуемость информационного противоборства подпитываются тем

обстоятельством, что до сей поры нет разработанных международных юридических норм его ведения. **В современном мире сложилась глобальная система идейно-политической и военно-экономической гегемонии США**. За ними после развала СССР в мире закрепился статус первой и единственной сверхдержавы. Они лидируют в процессе информационной революции. Здесь новые информационные системы и технологии уже стали неотъемлемой частью не только жизни общества, но и отдельных граждан. Прежде всего это касается электронных средств массовой информации, интернета, различного рода телекоммуникационных систем (имеются в виду мобильная связь, глобальная высокоточная навигация, оптико-волоконные и беспроводные сети передачи данных), используемых в профессиональной деятельности и в быту. Словом, информационная эра стала оказывать и прямое, и косвенное воздействие на все стороны жизнедеятельности человека. Бурные события конца XX в. – начала XXI в. показали, что новые технологии еще больше увеличили потенциальные возможности информации в войне, а также подтвердили важность ее роли в обеспечении не только национальной и военной безопасности отдельной страны, но и международной безопасности в целом. Однако именно эти достижения привели к тому, что открылись новые угрозы безопасности государств.

Дело в том, что ***прозрачность государственных границ для информационных потоков создала принципиально иную ситуацию в функционировании институтов государственной власти, а интеграция инфраструктур государства на основе информационных систем (банковско-финансовой, транспортной, электрических сетей, нефте- и газопроводов) сделала их потенциальными объектами средств информационного противоборства.*** Более того, стало очевидным, что фактическая неуправляемость информационным пространством собственной страны приводит к значительному ограничению ее суверенитета, а то и даже ставит под вопрос возможностью дальнейшего существования самого государства.

Если коммерческая организация допускает утечку более 20% важной внутренней информации, то в 60 случаях из 100 она – банкрот. 93% компаний, лишившихся доступа к собственным данным на срок более 10 дней, покидают бизнес[11]. Ущерб, нанесенный мировой экономике IT-угрозами (вирусами, атаками хакеров, сетевыми мошенничествами и спамом), огромен. По данным Computer Economics, убытки только от одних «вредоносных» программ составили в прошлом году более 14 миллиардов долларов. Ежегодный ущерб от киберпреступлений во всем мире превышает 40 млрд. долларов! В России их количество увеличивается с каждым годом. У всех до сих пор на слуху истории с крупнейшими мобильными операторами России (МТС, БИЛАЙН), у которых неизвестные похищали личные сведения об абонентах, а компакт диски с этой информацией можно было свободно купить на рынках Москвы. Продолжаются скандалы с утечкой государственных баз данных.

Проблема информационной безопасности, представленная сегодня в виде новых рисков и угроз, также является особенностью современного мирового информационного порядка. Информационная безопасность определяется как состояние защищенности информации и поддерживающей ее инфраструктуры,

обеспечивающее ее формирование и развитие в интересах определенных структур (владельцев и пользователей).

К основным видам угроз информационной безопасности можно отнести:

Появление и стремительное развитие различных способов контроля над информацией и информационно-технологическими системами со стороны их разработчика. Современные технологии связи позволяют перехватывать все телефонные сообщения на территории всего мира (посредством полной компьютерной обработки всего объема телефонных сообщений и перехвата всех сообщений в сети Интернет), и т.п. [12] Сегодня в США в соответствующей государственной структуре заняты более 350 тыс. человек.

1. Современные информационные технологии являются эффективным средством распространения различных организационных и управленческих технологий, которые позволяют разработчику определенном образом структурировать политические и бизнес-процессы клиента (например, MRP, ERP и APS-системы), а также контролировать и управлять ими.

Современные информационные технологии становятся инструментом контроля корпоративных субъектов в обществе, что ущемляет права личности. Об этом говорит Р. Барбер, оценивая демократический потенциал современных технологий[13]. **Он предлагает понятие «мягкой тирании», которая «не требует постоянного физического контроля над субъектом», а выражается в контроле над «сердцами и умами через контроль над образованием, информацией и коммуникацией и, таким образом, превращает субъектов в союзников рабства»**. По его мнению, «новые технологии могут стать опасным катализатором для *нового вида* тирании» - мягкой, а «нет более опасной тирании, чем невидимая и мягкая» [13]. Для РФ «идея» более, чем актуальная!

Источником угроз информационной безопасности признается «цифровое неравенство». Угроза видится в возникновении «элиты, обладающей неограниченным доступом к информации и коммуникационным сетям как на внутригосударственном, так и на международном уровнях, использующей преимущество владения базами данных и связью в своих узких групповых целях и осуществляющей селективное распределение информации. В результате резко возрастают возможности манипулирования общественным мнением, базирующиеся на разных уровнях доступа отдельных людей, социальных групп, государств и т.д. к информации» [12].

Еще одна группа угроз информационной безопасности связана с понятием «информационной милитаризации» [14]. Появляются новые формы конфликтов и противодействия, среди которых выделяют три основных вида: кибервойна, информационная война и сетевая война. В XXI веке ***информационная война*** станет основным средством современной мировой политики, доминирующий способ достижения духовной, политической и экономической ***власти.***

Кибервойна характеризуется применением новых информационных технологий в создании боевых единиц, высокой степенью их автоматизации. Современная боевая единица может быть невидимой и неуязвимой, самостоятельно и с высокой точностью определять и поражать цель.

Угроза информационной войны более актуальна и вероятна, и существует в двух основных измерениях:

- Это угроза дестабилизации и вывода из строя информационно-технологических систем, например, различные вирусные атаки. При информационно-техническом противоборстве главными объектами воздействия и защиты являются информационно-технические системы (системы связи, телекоммуникационные и компьютерные системы, радиоэлектронные средства и т.д.).
- При информационно-психологическом противоборстве главными объектами воздействия, а, следовательно, и защиты являются психика военно-политического руководства, личного состава вооруженных сил, спецслужб и населения, а также системы формирования общественного мнения и принятия решений. Активным субъектом информационных атак такого рода и источником угроз являются США. Уже к концу 20 века Соединенные Штаты контролировали более 80% всего объема информации, распространявшейся в мире, и могли оперативно воздействовать на общественное мнение планеты.

Сетевые войны – это социальные невооруженные конфликты низкой эффективности, отличающиеся от традиционных вооруженных военно-политических конфликтов прежде всего характером и структурой участников. Источником угроз в данном случае являются отдельные организации или теневые сети организаций (например, «Аум Сен Рике», масонские «братства», «ваххабиты», «аль-Каида»). В новых войнах исчезают традиционные географические измерения, такие как тыл, линия фронта и т.п. Участники четко не определены [15].

"Сетевая война" является более сложной формой будущего военно-политического конфликта, в ходе которого борьба за информационное доминирование затронет социальные и национальные особенности сторон, вовлеченных в конфликт.

Иначе говоря, новые информационные технологии позволят "сражаться" непосредственно с сознанием противника, активно используя информационные сети и различные СМИ для ведения адаптированной пропаганды и создания у противника искаженной картины мира. Сами информационные технологии рассматриваются в данной концепции только как средство, облегчающее стратегическое информационное доминирование, под которым в данном случае понимается создание таких информационных условий, в которых действия противника в конечном итоге неизбежно окажутся выгодными или будут направлены на обслуживание интересов противоположной стороны.

Институты и модели управления современными информационными процессами: Основные модели управления современными информационными процессами:

1. Европейская модель, в которой значительная роль отводится государству и правительственным структурам в вопросах контроля и решения ряда проблем в информационной сфере.

2. Американская модель информационного общества предполагает сведение к минимуму роли государства и делает акцент на рыночных механизмах развития.
3. Восточная модель – это попытка разработать альтернативный западному подход к развитию информационного общества. В основе этой модели лежит сотрудничество государства и рынка с учетом собственных культурно-цивилизационных особенностей и традиций.

Мировые глобальные институты управления современными информационными процессами:

1. Международный союз электросвязи (International Telecommunication Union (ITU)) - структурное подразделение ООН, разрабатывающее международные стандарты для телекоммуникаций и документацию многих сетевых стандартов. В настоящее время его основными функциями являются разработка международных стандартов информатизации, координация деятельности государств в данной сфере, обеспечение международного сотрудничества между государствами и негосударственными организациями по вопросам информатизации, экспертная деятельность, разработка стратегий развития информационного общества и др.

В начале 90-х гг. Альберт Гор-младший выдвинул новую сетевую инициативу NREN (National Research and Education Network — Национальная сеть для исследований и образования). В 1991 г. внесенный им билль стал законом — High Performance Computing Act, 194-м законом Конгресса 102-го созыва (Public Law — 102-194) [16].

2. С середины 90-х гг. в решение задач глобального управления информационной сферы включается бизнес и экспертное сообщество. В феврале 1995 г. в Брюсселе состоялась встреча министров, ответственных за развитие проектов информационного общества. Министры определили одиннадцать глобальных проектов информационного общества.

В марте 2000 года Европейская Комиссия приняла новую десятилетнюю программу «Электронная Европа» (e-Europe), основными задачами которой стали обеспечение компьютерами и Интернетом всех предприятий и образовательных, культурных учреждений, финансирование развития новых технологий. Отличием западных программ является нацеленность на продвижение западной культуры посредством ИКТ, о чем открыто говорится в планах и концепциях. Так, например, одной из целей программы «Электронная Европа» является «поддерживать распространение европейской культуры через создание «цифровой» литературы» [17].

Была принята Окинавская Хартия глобального информационного общества [18] (22 июля 2000г.) – рамочный документ, в основном посвящена проблеме «цифрового разрыва» (digital divide) и призывает государства к сотрудничеству: «Настоящая Хартия является прежде всего призывом ко всем как в государственном, так и в частном секторах, ликвидировать международный разрыв в области информации знаний. Эффективное партнерство среди участников, включая совместное политическое сотрудничество, также является ключевым элементом рационального развития информационного общества» [6].

По итогам международных обсуждений, разработкой национальных концепций информационного общества начинают заниматься другие страны. Пока

это страны «Большой восьмерки»: с ноября 2000 года Япония, а несколько позже – и Россия, где были приняты соответствующие программы, и на федеральном уровне (ФЦП «Электронная Россия» [19], 2002-2010 гг.), и на региональном уровне («Электронная Москва», «Электронный Санкт-Петербург» и др.).

16-18 ноября 2005 г. была принята Тунисская программа информационного общества (Tunis Agenda for the Information Society) [20] и были выработаны решения основных спорных вопросов по управлению информационной сферой. В результате рассмотрения нескольких моделей управления Интернетом, было решено, что **правительство США будет осуществлять односторонний контроль за всемирной сетью, «по историческим причинам».** ИКАНН будет по-прежнему обеспечивать техническое управление Интернет (Весьма примечательно, что волна дестабилизации и хаотизации, охватившая весь Арабский Восток в 2011 г., началась именно с Туниса: роль интернет-технологий в «раскачивании» ситуации в регоине, по оценкам специалистов, была огромна. - Прим.авт.).

Основными субъектами, управляющими информационными процессами в глобальной информационной политической игре, являются:

I.Государства.

Главной особенностью государства как участника международных отношений является его суверенитет, что закрепляется международным правом. Суверенитет государства означает «верховенство государства в пределах собственных границ и независимость в международных отношениях» [21]. Сегодня все больше проявляется тенденция «размывания суверенитета» государств, о чем говорят многие исследователи.Оно испытывает давление со стороны других – финансовых, экономических, социальных, политических – субъектов международных отношений» [22].

Сильнейшим игроком среди государств являются США. Сегодня США лидируют и в информационной сфере. Это крупнейший поставщик информации и информационных технологий в мире. Это дает США значительные преимущества и в других сферах, в первую очередь, в экономике (так как информационная сфера является передовой отраслью в экономике, наиболее прибыльной и быстро развивающейся) и культуре (расширяет возможности культурной интервенции и идеологического воздействия). Главной целью государства во внешней политике является отстаивание национальных интересов [23]. Добавим, что интересы нации не всегда едины. Точнее, всегда есть противоречие, конфликт интересов внутри государства. В случае конфликта реализуются интересы наиболее влиятельных групп, как во внутренней, так и во внешней политике.

II.Корпорации

Концепция социально ответственного бизнеса позволяет корпорациям добиться легитимности своего участия в процессе управления информационными процессами. Процесс монополизации информационных рынков начался в США. Со временем американские корпорации вышли на глобальный рынок и стали претендовать на монополию в глобальном масштабе. В первую очередь монополии контролировали производство контента. Бизнес, таким образом, набирает силу, объединяя 2 вида ресурсов: экономические и информационные.

Транснациональные корпорации стали крупнейшими игроками в глобальной информационной политической игре. В информационной сфере у бизнеса особые притязания на власть. В первую очередь это связано с особым положением СМИ в обществе, с их возможностью влиять на важнейшие политические решения, управлять массовым сознанием. ***Синтез финансовых, информационных и организационных ресурсов способствовал появлению на глобальной арене нового сверхмонстра – наднациональной олигархии.***

III.Некоммерческие организации

Это самый сложный тип игроков. Они одновременно являются и самостоятельными участниками международных отношений, и инструментами, которые используют первичные игроки для реализации своих интересов.

IV.Экспертные группы.

Экспертные группы в наименьшей степени ориентированы на широкую общественность, они ориентированы на заказчика. Также как и некоммерческие организации, они могут рассматриваться и как игроки, и как инструменты согласования интересов, используемые другими игроками.

V.Научное сообщество

Оно представлено, как правило, университетами, научно-исследовательскими институтами, ассоциациями. Они являются участниками различных организаций, наряду с государством и бизнесом, благодаря своему авторитету способны влиять на общественное мнение и таким образом влиять на других участников.

VI.Межправительственные институты

1. Главным институтом глобального управления является Организация объединенных наций.

ЮНЕСКО (United Nations Educational Scientific and Cultural Organization) [24] – агентство в составе ООН, которое заниматься проблемами образования, науки и культуры. Одной из 5 групп проблем («тематических сфер»), которыми занимается организация, является раздел «Коммуникация и информация» [25].

VII.Смешанные институты

Главной организацией в сфере управления Интернет является **ICANN** (Internet Corporation for Assigned Names and Numbers)[26], которую некоторые иногда называют **«Верховным судом Интернета», «Правительством Интернета»**. ICANN – это некоммерческая полугосударственная организация, которая по контракту с правительством США занимается координацией политики и техническими протоколами, связанными с доменными именами. ICANN изначально была полностью частная организация, в задачи которой входило решение спорных ситуаций вокруг домена **.US** и координация действий сетевого общества. **Она финансировалась Пентагоном и осуществляла повседневный контроль за системой адресации и обмена данными между серверами.** Постепенно круг ее функций расширялся, и в настоящее время ICANN занимается распределением доменных имен во всем Интернете и включает 3 комитета: доменных имен, IP-адресов и протоколов. ICANN сотрудничает с другими организациями и частными лицами, государствами и межправительственными организациями. ICANN наделена властными полномочиями по контракту с правительством США. Министерство торговли США обладает правом продления

соглашения сторон. Членом ICANN является некоммерческая организация IANA - Internet Assigned Numbers Authority [27].

Еще одна организация, которая играет значительную роль в управлении Интернет - World Wide Web Consortium W3C [28] (дословный перевод: Консорциум Всемирной Паутины). Это международное объединение компаний, связанных с развитием Интернет. W3C был основан в 1994 году Тимом Бирнерсом-Ли (Tim Berners-Lee). Цель организации состоит в разработке открытых стандартов для развития всемирной сети (WWW), чтобы она развивалась в едином направлении, а не раскалывалась на конкурирующие фракции. W3C утвердил, в частности, стандарты на язык HTML и протокол обмена HTTP.

Кроме ICANN и W3C, существует около 10 международных организаций, цель деятельности которых - управление, руководство и обслуживание Интернет. и принимаются группой, в которую входят Internet Society (ISOC) [29] и несколько структур под покровительством ISOC. История Internet Society (ISOC) начинается в 1991 году. Интенсивное развитие Интернет в коммерческом секторе (и везде - благодаря коммерческому сектору) в начале 90-х вызвало необходимость создания формальной организации для обеспечения правового существования структур, которые занимались разработкой сетевых стандартов (IETF и др.). Была создана Internet Society (ISOC), зарегистрированная как некоммерческая компания в округе Колумбия (США).

Подводя итоги, заметим, что большинство глобальных институтов по управлению Интернетом родились в США и не торопятся становиться космополитами. Они по-прежнему контролируются правительством США и в их глобальной сетевой структуре все же есть вершина. А это означает возможность контроля над Интернет-коммуникациями во всем мире. Предложение ICANN перевести свою штаб-квартиру в Женеву не вызвало восторга у американского правительства, эта инициатива была отвергнута без обсуждений.

Юридическая природа ИНТЕРНЕТА [30]**.**Что такое Интернет – субъект права, вступающий в правоотношения со своими пользователями, или объект правоотношений, правового регулирования?

Как известно, не существует организационной структуры, выступающей собственником или владельцем этой компьютерной сети. Интернет не имеет собственного обособленного имущества, его ресурсы принадлежат на праве собственности разным субъектам: каналы связи – телекоммуникационным компаниям; компьютерное оборудование – пользователям; информация – ее собственникам; техника и программное обеспечение поддержки магистральных сетей – их владельцам.

Интернет не может иметь какие-то самостоятельные права и нести обязанности; за каждым возникающим в процессе работы в Интернете правоотношением стоит конкретный правоспособный субъект: при подключении к сети – провайдер, при покупке через сеть товара – организация-продавец, при платеже по сделке через сеть – специализированная финансовая фирма (виртуальный банк).

Таким образом, Интернет не является ни зарегистрированной организацией, ни юридическим лицом. Интернет – это не средство массовой информации. Интернет – это средство массовой коммуникации

В юридической литературе предлагается рассматривать его субъектом права нового типа как организационное единство, введя для этого новое понятие «множественности субъектного состава» Интернета, и наделяя последний характеристикой нового субъекта права.

Представляется безосновательным такое выделение, поскольку организации, вступающие в правоотношения, самостоятельно осуществляют свои права и несут обязанности, и нет никакой необходимости объединять их в такой «множественный субъект».

Таким образом, Интернет не является участником правоотношений, субъектом прав. Является ли Интернет тем, по поводу чего возникают правоотношения, объектом права? Интернет как компьютерная сеть не создает новых объектов и товаров, а лишь предоставляет возможности для их создания, размещения и доступа к ним пользователей сети.

Отношения же, возникающие в связи с функционированием Интернет как сети компьютеров, относятся больше к сфере технических стандартов и практически не носят правового характера.

Если Интернет не является ни субъектом, ни объектом права, то, возможно, и нет юридической специфики его функционирования?

Это не так. Юридическая особенность отношений в Интернете состоит в специфическом способе реализации прав и обязанностей пользователей сети. С появлением сетевых услуг возникает новый характер взаимоотношений между людьми и организациями. Подавляющее большинство сделок в сети осуществляется между лицами, физически находящимися в разных странах, и не ясно, какое право подлежит применению.

Таким образом, можно говорить о специфическом способе возникновения правоотношений между физическими и юридическими лицами посредством компьютерной сети.

Глобальный характер Всемирной сети создает проблемы в определении того, какие правоприменительные органы должны рассматривать споры по правоотношениям.Сам Интернет, не имея территориальных границ, позволяет получить доступ к информации, распространение которой каким-либо иным способом запрещается.

Система доменных имен в Интернет. При создании системы доменных имен в Интернет не было учтено, что в мире уже давно существуют средства индивидуализации в виде товарных знаков и фирменных наименований. Правообладателей товарных знаков, владельцев компаний с фирменными наименованиями не устраивает существование в Интернете наименований, совпадающих с их именами, но не принадлежащих им. Существуют две группы плагиаторов: первые регистрируют сетевые адреса для личного употребления, вторые – для продажи заинтересованному покупателю. С ростом популярности Интернета более масштабными могут быть спекуляции и злоупотребления, связанные с Интернет-адресами. Кроме конфликтов по поводу использования

зарегистрированных товарных знаков и фирменных наименований уже известны случаи споров об использовании названий городов и имен известных лиц.

Основная особенность регистрации доменного имени в том, что оно дает обладателю адреса исключительное право пользования и распоряжения. Никто не может создать и публично эксплуатировать доменное имя в сети, идентичное уже зарегистрированному.

Причиной тому - уникальная система иерархий доменных имен, являющихся надгосударственным образованием и стержнем Интернета.

В практике арбитражных судов уже возникла проблема защиты прав владельцев товарных знаков при использовании их в доменном имени. Это объясняется широким коммерческим использованием ресурсов сети Интернет для привлечения покупателей товаров и услуг.

Можно констатировать, что специального законодательства о защите интеллектуальной собственности в Интернете нет ни в одном государстве. Защита прав владельцев товарного знака происходит на основании специальных законов о товарных знаках, где закреплено исключительное право на его использование в коммерческих целях. Нарушением признается использование подобного знака без разрешения владельца в отношении идентичных или сходных товаров или услуг, если это создает опасность (возможность) их смешения.

Судебная практика зарубежных стран признает нарушением прав владельца товарного знака несанкционированное использование таких доменных имен. Международные конвенции определяют основные принципы защиты прав на интеллектуальную собственность, в том числе на товарный знак при его использовании в Интернете:

- Парижская конвенция по охране промышленной собственности;
- Соглашение по торговым аспектам прав интеллектуальной собственности.

Таким образом, согласно международному праву действия, приводящие к смешению товаров и услуг, нарушают права на товарный знак, в частности, связанные с использованием его в доменном имени.В УК РФ действует ст. 180 «Незаконное использование товарного знака», предусматривающая наказание в виде штрафа либо обязательных работ, либо исправительных работ на срок до двух лет.

Электронный документооборот. В результате создания глобальных компьютерных сетей произошел настоящий переворот в области передачи информации. С использованием средств удаленного доступа стали проводиться торги, осуществляться расчеты с банками, оформляться таможенные декларации и т.п.

В этих случаях речь идет об электронном документообороте (ЭДО) в узком смысле, когда идет передача электронным способом структурированных в соответствии с согласованными стандартами данных. Этим требованиям удовлетворяют банковские системы, автоматизированные системы проведения торгов, где автоматически проверяется аутентичность документа, его соответствие стандарту. В широком смысле ЭДО – любой обмен компьютерными данными между различными субъектами (например, частная переписка с использованием электронной почты).

В последнее время в нашей стране прият ряд нормативных актов, которые регулируют отношения, связанные с использованием систем ЭДО. ГК РФ разрешает использование электронных документов, заверенных электронной цифровой подписью при совершении сделок во всех случаях и порядке, предусмотренном законом и иными правовыми актами и соглашениями сторон за исключением тех, когда предъявляются специальные требования к форме документа (специальная бумага, мастичная печать и т.п.).

Правовое поле «информационного противоборства» РФ.В настоящее время государства, а именно они обладают прерогативой издания общеобязательных законов, все больше стремятся упорядочить динамично развивающиеся информационные процессы посредством правового регулирования, и на международном, и на региональном, и на государственном уровне. Появление нового – виртуального – сегмента общественных отношений создает вакуум в правовом регулировании, который стремятся заполнить государства, распространяя свой контроль на новые отношения. Тем не менее, пока многие новые отношения, порожденные современными информационными процессами, не урегулированы нормами права.

В сфере правового регулирования информационной сферы существует множество дискуссионных вопросов. Это и неоднозначная оценка состава новых виртуальных преступлений (например, судить ли за спам? что понимать под хакерством? где совершено преступление, если оно совершено в Интернет?), и недостаточная определенность статусов участников отношений. В том числе спорные вопросы касаются роли и места государственных органов в регулировании информационных систем.

Россия и всё постсоветское пространство являются одним из основных объектов информационного воздействия, которое проводится через глобальное информационное поле [31]**.** Следствием такой ситуации являются вызовы и угрозы, которые угрожают не только информационной безопасности России, но и ее национальной безопасности.

Одним из ярких примеров этого явилась активная информационная атака Запада в лице Грузии на Россию в ходе августовского конфликта 2008 года, а также агрессивных нападений атлантистов на Ирак и Ливию. США и НАТО имеют геополитические интересы в Закавказье, Центральной Азии, на Ближнем и Среднем Востоке, и их реализация возможна при условии распространения в регионе своего массированного влияния и одновременно ограничения влияния России.

Сейчас Россия в сфере информационной безопасности продолжает отставать от наиболее развитых стран. Поэтому разработка оперативных и долгосрочных мер по предотвращению и нейтрализации негативного, нарушающего баланс интересов информационного воздействия крайне необходима. Во многих странах с этой целью ограничивается участие иностранного капитала в национальных СМИ. Это способствует обеспечению информационного суверенитета государства, безопасности его информационного пространства, своевременному принятию эффективных мер по выявлению, предупреждению, предотвращению и пресечению подрывной и разлагающей деятельности иностранных спецслужб, враждебных объединений, сект внутри

страны, нарушающих баланс интересов государства, общества и человека в информационной сфере, информационной безопасности государства.

России крайне важно усилить свои позиции в информационной сфере с тем, чтобы обеспечить ее национальную безопасность. Однако, юридическая база по информационной безопасности России крайне скудна. В сентябре 2000 года Президентом РФ была подписана Доктрина информационной безопасности РФ [32]. ***За 10 лет, прошедших со времени ее принятия, не было принято ни одного обновленного документа по этой проблематике, в то время как информационный «нажим» на Россию только нарастал.*** Впоследствии были упоминания о противодействии угрозе развязывания противоборства в информационной сфере в Концепции национальной безопасности РФ [33], об активном информационном противоборстве, дезориентации общественного мнения в отдельных государствах и мирового сообщества в целом в Военной доктрине РФ [34]; об усилении глобального информационного противоборства, возрастании угрозы стабильности индустриальных и развивающихся стран мира, их социально-экономическому развитию и демократическим институтам в Стратегии национальной безопасности РФ до 2020 года [35].

Однако, например, в США, первые официальные документы Пентагона по этой проблеме появились в начале 90-х гг. (директива Министерства Обороны США TS3600.I под названием «Информационная война» от 21 декабря 1992 года). В 1993 году в директиве Комитета начальников штабов № 30 уже были изложены основные принципы ведения информационной войны. Эти концептуальные документы США были подготовлены благодаря обобщению значительного опыта американского военно-политического руководства в области осуществления психологических операций и дезорганизации систем управления, приобретенного в Панаме, Гренаде, на Гаити, в Сомали, Косово, Ираке.

В Российской Федерации на данный момент отсутствует координирующий центр по осуществлению единой информационной политики государства [36]. ***Складывающаяся вокруг России обстановка требует принятия адекватных мер противодействия информационной экспансии.*** Основные пути решения данных проблем заключаются в следующих основных направлениях:

- систематической деятельности по выявлению угроз в информационной сфере и их источников, структуризации целей и задач обеспечения информационной безопасности в области обороны, их реализации;
- активном противодействии влиянию на сознание населения с целью изменения национальных идеологических установок;
- развитии отечественной технологической и производственной базы в области информационных технологий;
- повышение безопасности информационных и телекоммуникационных систем, а также систем и средств информатизации вооружения и военной техники, систем управления войсками и оружием;
- совершенствовании структуры обеспечения информационной безопасности в сфере обороны;

- подготовке специалистов в области обеспечения информационной безопасности.

Поэтому, от политической и научной элиты требуется немедленное принятие решений по формулированию государственной стратегии, основанной на подлинных интересах общества, созданию системы реализации информационной политики и проведения конкретных информационных мероприятий.

Институт копирайт (авторское право). Важнейшим правовым институтом в управлении информационными процессами является институт копирайт (авторское право). На международном уровне проблемами интеллектуальной собственности занимается Всемирная организация интеллектуальной собственности / World Intellectual Property Organization (ВОИС/WIPO) [37] (специализированная организация ООН).

В 1998 году в США был принят Закон "Об авторском праве в цифровом тысячелетии" (DMCA Digital Millennium Copyright Act) [38]. Он вызвал противоречивые споры не только в США, но и во всем мире.Например, многие считают закон «наносящим удар по свободе самовыражения, поскольку закон ограничивает возможность потребителей электронных продуктов на пользование ими - это проявилось, в частности, в запрете на копирование и на отправление по почте купленных электронных книг» [39].

«США, а точнее крупнейшие корпорации, расположенные на их территории, оказывают сильное давление на остальной мир, стремясь заставить другие страны принять не менее жесткое законодательство в области защиты цифровых авторских прав» [40]. Политическое давление американских корпораций при поддержке правительства США на другие страны - это лишь одна из проблем, связанных с современным развитием института копирайт. Другая – это **распространение национального законодательства США на лиц, не являющихся резидентами штатов и находящихся на территории других государств в момент нарушения DMCA. Первыми лицами, привлеченными к суду за нарушение этого закона стали российский гражданин, программист Дмитрий Скляров и его компания-работодатель "Элкомсофт"**[41]**.**

Транснациональные корпорации, рожденные в США, хотят работать на рынках других государств по национальным законам Америки. И им это удается. Такая практика правового регулирования является специфичной для информационной сферы. Ведущие игроки стремятся установить не только политический, но и правовой институциональный контроль в информационной сфере, определяя нормы глобального правового режима. **Это яркий пример англосаксонского информационно-компьютерного шовинизма.**

Механизмы и институты управления информационной сферой в РФ.

1. Центральным органом управления информационными процессами является Министерство информационных технологий и связи.
2. Важную роль в управлении информационной сферой играет РИО-Центр (Российский центр развития информационного общества). РИО-Центр является независимой некоммерческой организацией, созданной по инициативе научного сообщества.

Региональный общественный центр Интернет-технологий РОЦИТ (общественная организация, созданная в марте 1996 года, главная миссия которой - облегчить включение России в мировое сообщество Интернета) [42].

3. Союз Операторов Интернет СОИ (Основан в 1999 г. в Москве).
4. Ассоциация документальной электросвязи АДЭ (Общественно-государственное объединение "Ассоциация документальной электросвязи" образовано в соответствии с Распоряжением Правительства Российской Федерации).
5. Национальная ассоциация участников электронной торговли НАУЭТ (Российская некоммерческая негосударственная организация, включает «организации различных форм собственности, объединенные общей сферой деятельности, связанной с использованием современных инфокоммуникационных технологий и глобальной сети Интернет в предпринимательской деятельности»).

Что касается управления Интернет в России, здесь также реализуется западная (глобальная) модель регулирования. С 2000 года распределением адресного пространства в сети занимается аккредитованная при ICANN Автономная некоммерческая организация АНО «Региональный Сетевой Информационный Центр» (RU-CENTER) [43].

Сейчас Россия активно работает над «включением» в «информационное общество». Министерство информационных технологий и связи охотно участвует в глобальных и региональных конференциях. В целом официальная Россия откликается на призывы запада, принимает глобальные правила игры, даже если они не вполне соответствуют национальным интересам.

Новое государственное управление. Сегодня наиболее популярной концепцией реформирования государственной службы является «электронное правительство».Под электронным правительством понимается внедрение ИКТ в сферу государственного управления и последствия этого внедрения, в первую очередь, реинжениринг управленческих процессов."Электронное правительство" - не дань моде, а необходимость, условие успешного развития всех сторон социально-экономической жизни в нашей стране. Остаться в стороне от происходящих в сфере мировой информатизации процессов нам уже просто не удастся. **Но с другой стороны, перевод информационных потоков в электронный вид требует и новых подходов к защите информации.** Несанкционированное копирование и хищение значительных объемов представляющих интерес данных в электронном виде в отсутствие специальных защитных систем осуществить тоже намного проще. Таким образом, эффективность внедряемых вычислительных информационных систем, целесообразность затрат на их создание во многом зависят от уровня безопасности, который они обеспечивают. В целом использование ИКТ государственными ведомствами повышает качество их услуг, предоставляемых бизнесу и населению, способствует дебюрократизации государственного управления. Также повышается эффективность коммуникаций и качество управленческих процессов внутри ведомств, и в межведомственных отношениях, в связи с чем «электронное правительство» трактуется шире, чем просто внедрение информационных технологий в сфере государственного управления.

Это понятие включает также изменения характера деятельности государственных служб на основе ИКТ. Анализ нормативных актов в области использования ИКТ органами государственной власти РФ показывает, что ***на федеральном уровне отсутствует единое видение приоритетов информатизации государства, основные проекты реализуются в рамках отдельных федеральных и ведомственных программ и недостаточно скоординированы и увязаны между собой.*** Ни на теоретическом, ни на нормативном уровне не определен характер и степень взаимодействия законодательства в информационной сфере и других отраслей права, в первую очередь гражданского[3].

Для упорядочения сложившейся ситуации необходимы:

- принятие единого нормативного акта, раскрывающего основные права граждан в области информации (включая порядок осуществления доступа к информации) и механизм их реализации;
- законодательная регламентация прав и обязанностей государственных органов при формировании государственных информационных ресурсов и обеспечения доступа граждан к соответствующим данным;
- выработка предметного перечня открытой информации, содержащейся в государственных информационных ресурсах;
- законодательное закрепление в едином нормативном акте принципов предоставления информации;
- формирование единого порядка информационного взаимодействия государственных органов с гражданами и организациями.
- систематизация и должная детализация регулирования института конфиденциальной информации.

Информационная безопасность для бизнеса. В настоящее время деятельность любой компании тем либо иным образом связана с получением и передачей информации, которая в современном постиндустриальном обществе является стратегически важным товаром. При этом потеря информационных ресурсов, особенно это касается организаций финансовой отрасли, или завладение секретной информацией конкурентами, как правило, наносят компаниям серьезный ущерб[44]. По оценкам компании SearchInform, одного из ведущих игроков российского рынка средств защиты и контроля информационных потоков, в 2010 г. затраты российских компаний на обеспечение информационной безопасности выросли в 3 - 4 раза по сравнению с 2009 г., а в нынешнем году ожидается двукратный рост по сравнению с 2010 г.

Все угрозы в сфере информационной безопасности (ИБ) для организации можно подразделить на две категории: внутренние и внешние[45]. Внешние исходят извне организации, например от тех, кто пытается перехватить ее электронную почтовую корреспонденцию. С момента своего появления информационная безопасность в основном была ориентирована на защиту сведений компании от внешних посягательств. Развивались методы антивирусной защиты, защиты от несанкционированного доступа, защиты каналов связи, методы шифрования и другие методы, призванные обезопасить информацию от предположительного внешнего злоумышленника. Именно внешние угрозы, как

правило, являются приоритетом в плане защиты для большинства организаций в мире.

Однако есть и другая категория угроз - это те, которые исходят от самих сотрудников организации. Главная из них - это, конечно, угроза утечек информации за пределы организации. Утечки могут быть как следствием стечения обстоятельств или халатности персонала, так и результатом целенаправленных действий имеющих доступ к конфиденциальной информации сотрудников-инсайдеров. Защитой от них многие организации почему-то пренебрегают, хотя инсайдер может принести намного больше вреда, чем, например, хакер, взломавший корпоративный сайт. ***Давно известно, что в 6 случаях из 10 для банкротства организации достаточно утечки всего лишь 20% ее коммерческих секретов.***

Сегодня наиболее заметно влияющей на непрерывность бизнеса является защита от внутренних угроз. Для предотвращения утечек информации недостаточно контроля только на "входе-выходе" информации в организации и требуется контроль внутренних информационных потоков, поэтому это может повлиять и на внутренние бизнес-процессы.

Важную роль в борьбе с похитителями информации должен сыграть и вступивший в силу 27 января 2011 г. Федеральный закон "О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком и о внесении изменений в отдельные законодательные акты Российской Федерации", в котором определены действия, признаваемые манипулированием рынком. За нарушение Закона об инсайде установлена административная и уголовная ответственность.

Технические аспекты. В последние годы для защиты от утечек информации в организациях используются специальные системы, называемые DLP-системами (от англ. Data Leak Prevention - предотвращение утечек данных). Под DLP-системой понимают программный комплекс, который позволяет анализировать потоки данных, "пересекающие" периметр защищаемой информационной системы, и предотвращать утечки конфиденциальных сведений из нее. Достаточно определить перечень защищаемых документов, заложить данные документы в систему и определить политики работы системы с различными видами выявленных инцидентов: блокировка сообщения, отправка с уведомлением офицера безопасности, получение подтверждения отправки от отправителя или его начальника и другие. Внедрение подобных систем позволяет значительно повысить уровень реальной защищенности.

По данному критерию (распознавании конфиденциальных данных в перехваченном ею трафике) все DLP-системы можно подразделить на два больших класса: системы с активным контролем трафика, или блокирующие, и системы с пассивным контролем трафика, или неблокирующие.

Практика показывает, что неблокирующие системы являются эффективным средством борьбы с систематическими утечками, которые вызваны злым умыслом виновного в них сотрудника или просто отсутствием у него даже базовых знаний в области информационной безопасности. Системы с активным контролем эффективны также в борьбе со случайными утечками информации, однако именно такие системы представляют собой наибольшую угрозу для внутрикорпоративных

бизнес-процессов, которые могут быть остановлены по причине блокировки информации. В работе современных DLP-систем всегда присутствует определенный процент ложно распознанных утечек.

Цена защиты. Защита имеет свою цену, которая должна быть ниже цены утечки информации, только в таком случае защита будет являться целесообразной.

Практические аспекты. Конфиденциальная информация - это информация, доступ к которой ограничивается в соответствии с законодательством РФ, и представляет собой коммерческую, служебную или личную тайны, охраняющиеся ее владельцем[46].

Информация, которой обладает организация, может быть интересна для:

1. Средства массовой информации.
2. Проверяющие и контролирующие госорганы по долгу службы.
3. Недовольные сотрудники.
4. Злонамеренные лица.
5. Конкуренты.

Информация из организации может похищаться разными способами и методами. Закрыть возможность утечки информации в развивающейся организации можно применением комплексного подхода при построении современной системы защиты информации компании:

1. Для начала в организации необходимо провести аудит информационной безопасности, который позволит получить четкое понимание нынешнего состояния дел с защитой информации.

2. Использовать современные средства защиты:

- антивирусные системы (Antivirus);
- системы контроля доступа в помещение (СКД);
- средства межсетевого экранирования (FireWall);
- продукты контроля доступа в сети (Network Access Control-NAC);
- средства контроля почтовых сообщений (Email Security);
- средства контроля интернет-активности (Web Security);
- инструменты обнаружения вторжения (Intrusion Prevention Systems-IPS);
- сканеры уязвимостей (Vulnerabilities Scanners);
- системы контроля утечки данных (Data Loss Prevention-DLP);
- программно-аппаратные средства контроля целостности и доступа к информации на локальном компьютере (ПАК СКЦ);
- средства защиты баз данных (Database security);
- средства построения защищенного соединения (Virtual Private Network-VPN);
- решения резервного копирования (Backup);
- и другие.

Каждая система генерирует события безопасности, на которые администратору стоит обратить внимание, и таких событий зачастую бывает более тысячи в минуту. Для их анализа можно использовать Центр мониторинга и Управления Информационной Безопасностью – ЦУИБ. На рынке представлено множество ЦУИБ, и все они имеют свои плюсы и минусы. Среди наиболее известных можно назвать ArcSite, Enterasys Security Information and Event Manager (SIEM), RSA nVision, Security Vision (SV2010), Symantec Security Information Manager (SIM).

3. Наладить процесс регулярной проверки состояния систем защиты на работоспособность с учетом появления и установки свежих программных продуктов и публикации новых обнаруженных уязвимостей.

4. При выявлении несоответствий Политике информационной безопасности и новых уязвимостей следует найти инструменты усовершенствования вашей системы комплексной защиты и залатать обнаруженные в ней прорехи, усилить слабые места.

Обеспечение выполнения правил информационной безопасности невозможно без поддержки высшего руководства

Существует системное противоречие между бизнес-подразделениями и подразделениями ИБ в вопросе доступности информации[47]. Бизнес стремится убрать все границы в работе с информацией и сделать ее максимально доступной для большинства сотрудников компании для быстрой и эффективной работы. Подразделения ИБ, наоборот, стремятся как можно больше разграничить доступ к информации, сократить до минимума количество лиц, имеющих доступ к конфиденциальным сведениям. Именно для нахождения разумного компромисса в данном вопросе необходимо подключение в качестве арбитра одного из топ-менеджеров компании.

Современная эффективная система ИБ представляет собой сложный организационно-технический комплекс, состоящий не только из технических средств защиты, но и серьезного набора организационно-распорядительной документации: соответствия политике компании, регламентов, инструкций, описывающих правила работы с информацией и требования ко всем сотрудникам компании. Именно на оценке рисков должна базироваться работа службы ИБ. Но такая оценка будет невозможна без поддержки руководства бизнес-подразделений компании, т.к. именно они должны стать источником информации о важности тех или иных информационных активов и о возможных последствиях в случае нарушения их конфиденциальности, целостности и доступности.

Закон "О персональных данных". На протяжении всего своего существования российское законодательство не налагало никаких особых требований на обеспечение ИБ в коммерческих компаниях. Все законодательные требования относились только к государственным структурам. Однако все изменилось в 2006 г., когда был принят Федеральный закон 152-ФЗ "О персональных данных". Этот Закон стал первым законодательным актом, определившим требования по информационной безопасности практически для всех юридических лиц, работающих на территории России.

Расследования компьютерных преступлений. Еще одной совершенно новой тенденцией рынка информационной безопасности стало появление нового вида профессиональных услуг по аутсорсингу расследования компьютерных преступлений. Информация в компании не может быть на 100% защищена. Современные киберпреступники давно перестали быть талантливыми одиночками - теперь бизнесу противостоят хорошо организованные группировки с серьезным техническим оснащением.

Внутренний аудит (ревизия) информационной безопасности.

Методика ревизии информационной безопасности в организации, включает такие основные направления проверки, как обработка персональных данных,

защита конфиденциальной информации и локально-вычислительной сети, использование программного обеспечения и представляет собой процесс проверки наличия реализации в существующей системе установленных требований [48].

Рекомендациями по стандартизации Р 50.1.053-2005 "Информационные технологии. Основные термины и определения в области технической защиты информации" **понятие безопасности информации раскрывается как состояние защищенности информации, при котором обеспечиваются ее конфиденциальность, доступность и целостность.**

Конфиденциальность - свойство информационных ресурсов, в том числе информации, связанное с тем, что они не станут доступными и не будут раскрыты для неуполномоченных лиц. Целостность - неизменность информации в процессе ее передачи или хранения. Доступность - свойство информационных ресурсов, в том числе информации, определяющее возможность их получения и использования по требованию уполномоченных лиц.

Объектами защиты информации являются информация, данные, ресурсы, носители информации, аппаратное обеспечение, программное обеспечение и коммуникации. Методы защиты: правовые, технические и организационные (регламентация взаимодействия на нормативно-правовой основе организации). Обратим внимание в первую очередь на организационно-правовую защиту, так как она менее затратная.

В ходе аудита осуществляется проверка по следующим направлениям.

- Контроль за обработкой персональных данных
- Оценка текущего состояния защиты конфиденциальной информации в организации
- Текущее состояние использования программного обеспечения (ПО), защищенного законом об авторском праве

На основании анализа полученных данных разрабатываются мероприятия для устранения выявленных нарушений. Главная задача аудита - обратить внимание клиента на проблемные участки и предложить план совершенствования работы.

При анализе информационной безопасности рекомендуется отдельно рассматривать следующие направления защиты информационной системы:

- защиту объектов (информация) информационной системы;
- защиту процессов, процедур и программ обработки информации;
- защиту каналов связи;
- подавление побочных электромагнитных излучений;
- управление системой защиты.

Защиты информационного пространства от наличия в нем контрафактной продукции. Контроль за установленным в организации ПО может осуществляться в том числе с помощью автоматизированного инструмента выявления контрафактного ПО, которое позволяет провести инвентаризацию ПО, более отчетливо и точно представить положение дел, убедиться в существовании в организации контрафактной продукции.

Важно иметь в виду, что наличие контрафактной продукции у руководителя организации создает риск привлечения к уголовной ответственности, предусмотренной ч. 2 ст. 146 УК РФ. Незаконное использование объектов авторского права или смежных прав наказывается штрафом в размере до 200 тыс.

руб., или в размере заработной платы либо иного дохода осужденного за период до 18 месяцев, или направлением на обязательные работы на срок от 180 до 240 часов, или лишением свободы на срок до двух лет. Для организации возникают риски применения административных мер, предусмотренных п. 1 ст. 7.12 КоАП РФ, а именно привлечения к административной ответственности с конфискацией контрафактных экземпляров произведений и фонограмм, а также материалов и оборудования, используемых для их воспроизведения, и иных орудий совершения административного правонарушения.

Информационная безопасность в банковской сфере

Информационное обеспечение деятельности банка[49] осуществляется путем использования общедоступной информации и информации (сведения, составляющие банковскую, коммерческую, налоговую и иную тайну, а также персональные данные физического лица), доступ к которой ограничен федеральными законами. Преступные посягательства на принадлежащую банкам информацию ограниченного доступа (конфиденциальную информацию) в подавляющем большинстве случаев совершаются с целью подготовки хищения денежных средств банков (и их клиентов). Основными видами нарушений законодательства о банковской тайне, влекущими правовые последствия, являются незаконное получение, разглашение или использование сведений, составляющих коммерческую (банковскую) тайну. Ответственность за совершение указанных действий предусмотрена системой норм уголовного, гражданского, трудового и административного законодательства. Уголовно-правовая ответственность за преступные посягательства на отношения в сфере компьютерной информации установлена ст. 272 УК РФ "Неправомерный доступ к компьютерной информации", ст. 273 УК РФ "Создание, использование и распространение вредоносных программ для ЭВМ" и ст. 274 УК РФ "Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети". Согласно упоминавшимся выше официальным данным МВД России, число преступлений в сфере компьютерной информации, совершенных в 2010 г., имеет стойкую тенденцию к росту и увеличилось в октябре с.г. по сравнению с январем 2010 г. почти в 6 раз. **Нередко в преступных аферах и хищениях соучаствуют сами работники банковской сферы.**

Типичными способами использования компьютерных технологий при совершении хищений с использованием систем удаленного управления счетом являются:

- создание и авторизация платежной информации (платежного документа), проведение с использованием систем удаленного доступа несанкционированных операций по списанию денежных средств с банковских счетов;

- передача банку по системе интернет-банкинг поддельного платежного поручения о перечислении денежных средств физического лица на счет подконтрольной преступникам организации (фирмы-однодневки);

- списание денежных средств со счетов клиента банка на счета соучастника преступления путем фальсификации (изготовления несуществующих) электронных платежных сообщений;

- списание денежных средств со счета клиента банка на счета соучастника преступления путем искажения реально существующих электронных платежных сообщений.

Для получения охраняемой законом тайны в целях хищений денежных средств со счетов клиентов с использованием систем удаленного управления счетом преступники, как правило, выполняют следующие подготовительные действия:

- незаконное завладение паролем-ключом к электронной системе "банк-клиент" путем копирования данных (завладение может быть совершено работником организации либо посторонним лицом;

- создание и использование вредоносных программ для банковских ЭВМ с целью незаконного получения информации о ключах и паролях банковских систем управления счетами;

- создание и использование вредоносных программ для банковских ЭВМ с целью их внедрения в компьютеры клиентов для незаконного получения информации о ключах и паролях доступа к системе дистанционного обслуживания счета;

- незаконное получение информации о паролях клиентов системы интернет-банкинг от так называемых информационных брокеров (путем личного контакта либо безличного общения через Интернет).

Условия, способствующие совершению преступных посягательств на безопасность информационного обеспечения банковской деятельности.

Наиболее значимым фактором, способствующим совершению этой разновидности преступлений, как и преступлений в других сферах банковской деятельности, является причастность к противоправной деятельности персонала банков.

Среди других весомых обстоятельств следует назвать неспособность банков и их клиентов организовать систему защиты охраняемой законом информации, в том числе просчеты организационного характера со стороны банков:

- недостатки организации системы защиты сведений о ключах и паролях банковских систем управления счетом, а также о коде настройки компьютерной системы банкомата, позволяющей мошенникам произвольно завышать обменный курс одной из валют. В одном из случаев код настройки банкомата сообщил соучастникам хищения инкассатор банка за плату в размере 2/3 от суммы похищенных средств. При этом сам инкассатор официального допуска к указанным сведениям не имел;

- недостатки физической защиты компьютера банка от неправомерного доступа;

- недостатки организации системы информационной защиты процессингового центра от несанкционированного доступа к операциям по счету.

В апреле 2010 г. в одном из крупных московских банков деньги со счета клиента в сумме более 1 млн руб. были сняты в два приема с использованием временного (динамического) IP-адреса, в то время как по условиям договора управление счетом могло осуществляться только с постоянного статического IP-адреса;

- отсутствие автоматизированных средств контроля за деятельностью сотрудников, обладающих максимальными возможностями доступа к информационным ресурсам и средствам их обработки (программисты, администраторы);

- просчеты в организации деятельности подсистем сбора и обработки информации из банкоматов и процессингового центра в соответствии с п. 2.9 Положения Банка России от 24.12.2004 N 266-П "Об эмиссии банковских карт и об операциях, совершаемых с использованием платежных карт", в том числе в сопоставлении записей и идентификации транзакций;

- отстраненность службы безопасности от участия в контроле за безопасностью аппаратно-программного сегмента информационной системы банка.

К типичным недостаткам защиты информации в сфере обслуживания держателей банковских карт относятся:

- недостатки системы физической защиты банкоматов от несанкционированного доступа к компьютерной информации и заражения вирусом (в т.ч. от проникновения в компьютерный отсек банкомата с использованием дубликата ключа, подключения к компьютеру через USB-порт);

- просчеты организационного и технического характера при создании системы защиты банкоматов от несанкционированного получения информации с использованием скиммера;

- отсутствие системы мониторинга подозрительных операций с банковскими картами с целью выявления и предупреждения типичных способов мошенничества. Эффективность указанной системы подтверждена фактами успешного выявления мошеннических действий и их пресечения (во взаимодействии с милицией). В то же время отсутствие системы позволяло оставаться вне поля зрения банковских служб безопасности мошенникам, совершавшим до нескольких сотен операций с поддельными картами;

- отсутствие в службах безопасности банков структурных единиц, предназначенных для выявления и предупреждения преступных посягательств методами и средствами защиты информации и криминалистики: по данным Главного управления безопасности и защиты информации ЦБ РФ за 2009 г., **в 50% российских банков нет специалистов по информационной безопасности.**

В целях выполнения в организациях банковской системы Российской Федерации требований Федерального закона от 27.07.2006 N 152-ФЗ "О персональных данных" (далее - Закон N 152-ФЗ) Центральный банк Российской Федерации при участии Ассоциации российских банков (далее - АРБ) и Ассоциации региональных банков России (Ассоциации "Россия") разработал отраслевые документы[50] по приведению деятельности кредитных организаций в соответствие с требованиями законодательства в области персональных данных и информационной безопасности

Концепция «корпоративной информационной безопасности» [51]. Создание корпоративной информационной системы (КИС) предприятия всегда связано с удовлетворением требований четко очерченной нормативно-правовой базы, жестко прописанной в проектных документах по ее созданию. Порядок

утверждения и согласования ТЗ на информационную систему и ее подсистемы установлен в ГОСТ 34.602-89, который является неотъемлемой частью упомянутой нормативно-правовой базы.

Как видно, вопрос о том, как создавать КИС, достаточно изучен и даже стандартизован. Это относится прежде всего к ее функциональному наполнению и к работе прикладных процессов.

Однако не менее важным моментом в решении вопроса функционирования будущей КИС является проблема обеспечения ее информационной безопасности. Создание защищенной информационной системы заключается в выполнении совокупности мероприятий, направленных на разработку и/или практическое применение таких информационных технологий, которые бы реализовали функции по защите информации в соответствии с требованиями стандартов и нормативных документов, как во вновь создаваемых, так и в действующих системах.

Основные принципы и положения по созданию и функционированию защищенных систем изложены в требованиях ГОСТ 29339, ГОСТ Р 50543, ГОСТ Р 50739-95, ГОСТ Р 50972, ГОСТ Р 51275, ГОСТ РВ 50797 и других нормативных документах.

Работы по созданию, производству и эксплуатации информационной системы с использованием криптографических (шифровальных) средств для защиты информации ограниченного доступа ведутся ФСБ России. Если в системе обрабатывается информация, относящаяся к государственной тайне Российской Федерации, то необходимо наличие лицензии, подтверждающей возможность работы предприятия с этими сведениями. Для создания КИС могут применяться как серийно выпускаемые, так и вновь разработанные программные, программно-аппаратные, технические, криптографические СЗИ, которые должны иметь сертификаты соответствия требованиям по защите информации, полученные в соответствующих системах сертификации по требованиям безопасности информации (ФСТЭК России, ФСБ России, ФСО, Минобороны России). Таким образом, вопросы информационной безопасности находятся под постоянным контролем и регулированием как со стороны государства, так и со стороны структур управления предприятий.

Ответственность за несоблюдение указанных требований несет прежде всего руководитель распределенной структуры. Она определена в таких российских законодательных актах, как Конституция Российской Федерации, Гражданский кодекс Российской Федерации, Уголовный кодекс Российской Федерации, Федеральные законы "О безопасности", "О государственной тайне", "Об информации, информатизации и защите информации", "О коммерческой тайне", "О связи", "Об участии в международном информационном обмене", "О техническом регулировании", "Об электронной цифровой подписи", "Об информации, информационных технологиях и о защите информации", указы Президента Российской Федерации, постановления Правительства Российской Федерации, Доктрина информационной безопасности Российской Федерации, международные договоры и соглашения, заключенные или признанные Российской Федерацией, а также в других нормативных правовых актах.

Исходя из общих соображений можно определить ряд подсистем, которые должны входить в систему комплексной защиты информации КИС и практически обязательны к проектированию.

Подсистема авторизации. Данная подсистема обеспечивает доступ пользователя информационной системы (в том числе удаленного) к защищаемым ресурсам на основе анализа предъявляемых им своих учетных данных с использованием средств идентификации и аутентификации. Она строится на принципах реализации мандатного и дискреционного методов доступа, имеет возможность отказать пользователю в доступе, если его данные будут признаны неподлинными, сигнализировать об этом администратору безопасности и зарегистрировать неудачную попытку доступа для проведения расследования коллизий информационной безопасности.

Подсистема контроля целостности. Эта подсистема обеспечивает надлежащее функционирование прикладных процессов в информационной системе и неизменность программной среды на основе контроля за идентичностью необходимых файлов операционных систем, функционального и специального программного обеспечения. Кроме того, она позволяет контролировать целостность данных при их передаче по каналам связи посредством применения криптографических СЗИ (симметричное и несимметричное шифрование).

Подсистема межсетевого экранирования. С помощью этой подсистемы можно осуществлять защиту объектов от несанкционированного доступа и сетевых воздействий (атак) с целью вывода из строя отдельных функций защиты информации, узлов сети или нарушения функционирования информационной системы в целом. Она используется также для разграничения доступа по сети к защищаемой информации системы как на уровне адресов отдельных узлов, так и на уровне приложений.

Подсистема антивирусной защиты. Данная подсистема осуществляет защиту информационной системы при взаимодействии со смежными информационными комплексами и системами от вредоносных программ (вирусов, троянских коней, spyware и пр.).

Подсистема контентного анализа и защиты от нежелательной почты (спама). В подсистеме предусмотрена защита информационной системы при взаимодействии со смежными информационными комплексами и системами от нежелательной (рекламной) информации.

Подсистема обнаружения вторжений. Эта подсистема позволяет производить анализ сетевого трафика и передавать сообщения о возможном нападении на централизованную консоль управления, а также уведомлять администратора безопасности о несанкционированной сетевой активности, регистрировать эти сведения и блокировать доступ нежелательных источников к защищаемой информации в информационной системе.

Подсистема мониторинга уязвимостей и аудита информационной безопасности. Подсистема обеспечивает анализ настроек и оценку эффективности функционирования СЗИ, предоставляя администратору безопасности информацию о сбоях в работе СЗИ и наличии узких мест, которые могут быть использованы потенциальным злоумышленником для получения несанкционированного доступа к данным.

Подсистема управления информационной безопасностью. Подсистема предоставляет возможность централизованного управления конфигурацией всех служб и сервисов комплексной системы защиты КИС. Управление конфигурацией СЗИ позволяет администратору безопасности получать полный доступ к настройкам средств безопасности серверов, рабочих мест, баз данных и средств межсетевого экранирования с использованием защищенных протоколов передачи данных, методами, устойчивыми к пассивному и активному прослушиванию. Кроме того, система обеспечивает обнаружение и устранение причин неисправностей и ошибок авторизации и доступа к данным.

2. Коммерческая разведка и стратегии информационного противоборства США в глобальном пространстве.

Коммерческая разведка. Генеральную цель коммерческой разведки любого актора (будь то государство, альянс или организация) можно сформулировать одной фразой[52] - ***это информационно-аналитическое обеспечение возможностей достижения ее стратегических целей при удержании должного уровня конкурентоспособности, рентабельности и высокоэффективности субъекта в целом.*** Разведывательно-сетевые структуры являются наиболее гибким и скрытым инструментом манипулирования и установления контроля над общепланетарным глобальным пространством. Сегодня глобалистский Спрут, штаб-квартира которого располагается в США, раскинул щупальца по всему миру, стремясь опутать своими сетями все страны, народы и континенты. И, если подчинение и порабощение одних осуществляется при помощи вторжений, бомбардировок, оккупации (Ливия, Ирак, Югославия, Афганистан), то закабаление других может успешно осуществляться посредством информационно-культурной экспансии, финансовой комбинаторики, экономических махинаций и афер (Россия 80-90-х гг. – наглядное тому подтверждение). Практически все ТНК (транснациональные корпорации), структуры мирового наднационального олигархата, международной наркомафии, криминальные бизнес-сообщества имеют хорошо организованные информационно-аналитические, разведывательные службы и агентурные сети.

Современная бизнес-среда пропитана информацией буквально насквозь. Главная задача заключается в том, чтобы знать, где искать сведения, наиболее соответствующие (релевантные) информационным запросам руководства компании. Во многих случаях сделать это можно абсолютно бесплатно или в крайнем случае без особых финансовых и временных затрат. Главной особенностью исследований объектов коммерческой разведки является то обстоятельство, что ***они свободно обращаются на рынке или готовятся к такому обращению***, то есть их владельцы заинтересованы в самом широком обнародовании и распространении информации о новых товарах и услугах, "выбрасываемых" на рынок, об их ценах. Именно поэтому **получить такую информацию можно вполне легально, не прибегая к нарушениям этических норм или действующего законодательства.**

Наконец, кто выступает субъектом ведения коммерческой разведки? Как показывает российский и зарубежный опыт, это могут быть любые коммерческие компании (или стоящие за ними «интересанты»), независимо от сферы бизнеса, его размеров или особенностей рыночных условий.

Без малого 30 лет в развитых странах Европы технологии коммерческой, а по их классификации конкурентной разведки (competitive intelligence) используют в своем арсенале от 27 до 60 процентов всех коммерческих организаций, осуществляющих деловую активность как на внутренних, так и на международных рынках. **Наиболее передовые позиции в западном мире удерживают США, где доля таких компаний приближается к 82 процентам. Если же говорить о мировых тенденциях, то первенство, без сомнения, принадлежит Японии - 99 процентов всех коммерческих организаций, в которых в той или иной мере используют возможности специальных исследований в бизнесе. Не здесь ли кроется секрет успешности и конкурентоспособности бизнеса этих стран?**

В этих условиях методы получения информации часто ограничиваются сбором сведений, например, из различных источников в Интернете с последующим циклом информационно-аналитической обработки. Причем при решении разведывательных задач сотрудникам коммерческой разведки нет никакой необходимости прибегать к приемам промышленного шпионажа.

Главная задача коммерческой разведки - выявить риски, угрозы и возможности рыночной среды (перемены конъюнктуры рынка), имеющие высокие шансы реализации в будущем, и заблаговременно предупредить об этом руководство компании, предоставив в качестве дополнительного бонуса рекомендации по возможному реагированию на изменения обстановки. Такая информация, полученная до фактической реализации угрожающих событий или обстоятельств, оставляет руководству компании необходимый запас времени для выработки конкретных решении и адекватного реагирования на изменение существующих условий. Вот почему система коммерческой разведки осуществляет информационно-аналитическое обеспечение именно долгосрочных стратегических целей бизнеса компании, реализация которых - дело завтрашнего дня, а вовсе не текущей обстановки, в чем уверены многие бизнесмены, не понимающие, для чего им разведка, когда уже имеющиеся отделы хорошо справляются с поставленными задачами и владеют необходимой информацией.

Сравнительный анализ проведенный японскими экспертами показал:

- финансовые затраты на обеспечение эффективной безопасности компании (деятельности службы безопасности) могут составлять от 15 до 30 процентов прибыли предприятия;

- в то же время финансирование правильно организованной коммерческой разведывательной деятельности обходится в 1,5 - 2 процента от прибыли предприятия.

Что же до окупаемости специальных исследований рынка, то, по мнению тех же специалистов, практические результаты разведывательной деятельности в бизнесе способны принести своей компании до 30 - 40 процентов дополнительной прибыли. Впрочем, это не прямая, а косвенная прибыль, выражающаяся в таких критериях, как:

- экономия времени (к примеру, на новые разработки, принятие управленческих решений, адекватное реагирование на изменения внешней среды);

- экономия материальных, производственных и прочих ресурсов и снижение издержек (из-за наличия превентивной информации о рисках и возможностях рынка);

- увеличение доходов (за счет активного использования потенциала выявленных возможностей для бизнеса);

- предотвращение, минимизация и снижение затрат.

Между тем основные цели разведки в бизнесе - прогнозирование рисков; экономия средств и времени: создание возможностей для эффективной адаптации бизнеса компании к изменениям внешней среды. Вес это в полной мере востребовано малым и средним бизнесом.

В практическом выражении небольшой компании достаточно осуществлять мониторинг:

- негативных (или позитивных) изменений рыночной обстановки;

- планов конкурентного окружения и их кадровую ситуацию;

- появления новых конкурентов и новых конкурирующих продуктов на рынке;

- цен на конкурирующую продукцию;

- изменений законодательства и новых законодательных инициатив,

чтобы оставаться на плаву и чувствовать себя уверенно в конкурентной среде.

Организация такого мониторинга не требует заоблачных бюджетов или какого-либо специального оборудования.

Стратегии информационного противоборства США. Одним из основных направлений современной стратегии национальной безопасности США, и это эксплицитно закреплено в соответствующих доктринальных документах, на настоящее время является наращивание информационной мощи, главными составляющими которой считаются ***системы военной разведки, связи и управления.*** При этом такое наращивание будет проводиться в условиях, когда общую численность вооруженных сил США, в соответствии с принципами новой американской оборонной политики (передовое присутствие, реагирование на кризисные ситуации, коллективная безопасности и др.), в рамках концепции «минимальных сил» предполагается сократить в начале XXI века примерно на 25%.

Ключевым понятием, введенным в отчете MR-964-OSD, является классификация стратегического противоборства на первое и второе поколение. При этом стратегическое ИП первого поколения рассматривается наряду с традиционными средствами противоборства (ядерными, химическими, биологическими и другими). Подчеркивается, что оно больше ориентировано на дезорганизацию деятельности систем управления и проводится скорее как обеспечение действий традиционных сил и средств. Такое восприятие информационного противоборства свойственно начальному этапу осмысления проблемы. Стратегическое ИП первого поколения можно определить как «…один из нескольких компонентов будущего стратегического противоборства, применяемый совместно с другими инструментами достижения цели». Таким образом, понятие «стратегическое информационное противоборства первого поколения» фактически вобрало в себя основные методы информационной войны,

которые США реализуют в настоящее время на государственном и военном уровнях и от которых не намерены отказываться в обозримом будущем.

Дальнейшее изучение проблемы привело к введению понятия **«стратегического информационного противоборства второго поколения» (2nd Generation Strategic Information Warfare)**. Это понятие можно определить как «принципиально новый тип стратегического противоборства, вызванный к жизни информационной революцией, вводящий в круг возможных сфер противоборства информационное пространство и ряд других областей (прежде всего экономику) и продолжающийся долгое время: недели, месяцы и годы». Отмечается, что развитие и совершенствование подходов к ведению стратегического ИП второго поколения в перспективе может привести к полному отказу от использования военной силы, поскольку скоординированные информационные акции могут позволить обойтись без этой крайней меры. Стоит заметить, что если последствия стратегического ИП первого поколения еще могут быть прогнозируемы с использованием существующих методик, то второе поколение противоборства на текущий момент весьма трудно формализуемо, и существующие методики прогноза могут быть применены к анализу последствий весьма условно.

Среди предлагаемых новых концепций применения в ходе ведения войны высоких информационных технологий особое внимание обращает на себя **концепция «информационного господства»** ("Единые перспективы 2010" и "Единые перспективы 2020" , а также в документах МО США "Четырехлетний обзор состояния вооруженных сил" от 2001 и 2006 годов).

В рамках этой концепции, предусматривающей широкое использование имеющегося перспективного технологического задела и методов моделирования под «информационным господством» понимается возможность «опережающего» получения необходимых сведений и данных о тактической или стратегической ситуации, позволяющих принимать своевременные решения (в соответствии с принципами американской концепции «кризисного управления») по нейтрализации и сдерживанию действий противоборствующей стороны. Отражением идей данной концепции является использование возможностей СМИ в локальных вооруженных конфликтах. Ведущие мировые державы благодаря наличию отлаженного механизма государственного контроля за проведением информационной политики располагают широкими и разнообразными возможностями для достижения своих политических целей и защиты государственных интересов посредством влияния через СМИ на общественное сознание как внутри своих стран, так и за рубежом.

Стратегическая информационная война[10]**.**Понятие стратегической информационной войны (СИВ) включает в себя не столько использование информационных технологий для обеспечения традиционных военных действий, сколько асимметричное воздействие на те сегменты национальной информационной инфраструктуры противника, нарушение работоспособности которых может вызвать последствия, сопоставимые с результатами традиционных военных действий. Возможными последствиями СИВ могут явиться политический и экономический коллапс страны, выход из строя объектов энергоснабжения, остановка транспорта и т.д.

К числу характерных признаков (критериев), позволяющих говорить о начале стратегической информационной войны, относятся:

- наличие угрозы экономической безопасности государства;
- возникновение угрозы для проведения в жизнь национальной военной стратегии государств.

Так, например, России (в контексте СИВ) якобы «для предотвращения грядущего краха» подсовывается «плодотворная идея» - интернационализации мировых ресурсов, естественно, главным образом нефти и газа. Так, бывшая «госсекретарша» США М.Олбрайт уже проговорилась вслух о том, что «несправедливо де, когда столь богатая углеводородами Сибирь принадлежит только одной России». По мнению пенсионера американской большой политики, эти русские уникальные ископаемые должны «принадлежать всему человечеству». **Для этого и навязывается нам концепция интернационализации природных ресурсов. А главным средством её реализации призвано служить информационно-организационное и психополитическое оружие.**

Ниже рассматриваются основные принципы, которым должна соответствовать стратегия сдерживания в информационной сфере:

- воля к ответным действиям;
- вероятность и уверенность;
- гарантированное взаимное уничтожение;
- недопущение СИВ;
- определение потенциального агрессора;
- система «раннего предупреждения» в информационном контексте;
- использование наступательных технологий.

По мнению американских экспертов, **сегодня необходима новая парадигма – «ноополитика».** Это форма политического руководства, которая взаимодействует с ноосферой – самым широким информационным пространством сознания, в котором объединено киберпространство. Ноополитика – это метод реализации внешней политики в информационную эпоху, подчеркивающий первенство идей, духовных ценностей, моральных норм, законов и этики, основанный на применении «мягкой», а не «грубой» силы. ***Особо подчеркивается, что руководящим мотивом ноополитики не могут быть национальные интересы, определенные в терминах государственности.*** Национальные интересы по-прежнему будут играть важную роль, но они должны быть определены больше в «общечеловеческом» (т.е. в горбиообразной трактовке, а, может быть, главный «перестройщик-катастройщик» и получил сию «интеллектуальную креативную заготовку» из заокеанского мозгового треста. – Прим.авт.), а не государственном масштабе и быть интегрированы с более широкими, даже глобальными, интересами в расширяющуюся транснациональную сетевую «структуру», в которую внедрены участники международных отношений.

Таким образом, можно констатировать факт начала проведения изменений в области внешней и внутренней политики США в информационную эпоху. Основной концепцией является информационная стратегия, а одним из ее компонентов будет Стратегическая информационная доктрина, как главный концептуальный документ реализации принципов информационного противоборства на поле боя в конфликтах новой эпохи.

В результате проведенного исследования А.В. Деньщиков пришел к следующим выводам:

1. Современные идеи и материальные основы информационного противоборства формировались одновременно с развитием глобальной информационной среды, информационной сферы общества еще в 80-е гг. Руководству США к середине 90-х годов стала очевидна необходимость разработки единой национальной информационной стратегии, которая получила воплощении в создании ряда структур, чья деятельность состояла в выработке предложений, позволяющих принимать контрмеры против угроз в быстро меняющейся информационной и технологической средах.

2. На межгосударственном уровне, США, имеющие богатый опыт и отработанную систему осуществления информационно-психологического воздействия (управления восприятием), проверенную в годы «холодной войны» и отработанную в ходе локальных войн и вооруженных конфликтов стали адаптировать ее в новых международных условиях. Параллельно с этим реализовывались информационно-технические аспекты воздействия на информационные ресурсы и информационные системы, не позволяющие потенциальным противникам использовать технологические инновации в конкурентных целях.

3. **Появление и динамичное развитие глобальных информационных сетей основанных на передовых электронных технологиях позволили США использовать их потенциал в решении различного рода государственных задач. Управляемое формирование глобального информационного пространства на основе новейших технологий в максимальной степени отвечало интересам США.** Одновременно растущая зависимость США от информации и информационных систем и связанная с этим их уязвимость стали создавать широкий спектр угроз для национальной безопасности. С учетом этих угроз получили развитие оборонительные аспекты информационного противоборства. Масштабное внедрение достижений информационных и телекоммуникационных технологий во все сферы жизнедеятельности государства и общества в США подтолкнуло к разработке государственных и военных программ по защите своих национальных интересов в информационной сфере. К началу XXI века в США насчитывалось более 40 специально созданных организаций, участвующих в информационном противоборстве.

4. Итоги военных операций на Балканах, в Персидском заливе, Средиземноморье и Афганистане подтвердили важность формирования в интересах вооруженной борьбы необходимого информационного пространства. Главным уроком названных выше операций стало понимание, что информационное противоборство может и должно быть неотъемлемой составляющей эффективной государственной политики. Эта идея в политически корректных выражениях стала реализовываться на всех государственных уровнях США уже в 90-х годах XX века.

5. Важный фактор, обеспечивающий превалирующее положение США в военной области, - это превосходство американских вооруженных сил над потенциальными противниками или союзниками на ключевых направлениях военно-технического прогресса. Значительный прорыв науки в развитии новых

перспективных технологий, а также успех промышленности в воплощении этих достижений уже сегодня ставят вооруженные силы США по их военно-техническому оснащению на уровень требований XXI. Военно-политическое руководство, осознав значение потенциала новейших систем боевого управления, связи, компьютеров и разведки, сделало приоритетным достижение информационного превосходства над противниками в вооруженных конфликтах любой интенсивности и любого уровня. **Под информационным превосходством стали понимать способность к сбору, обработке и распространению непрерывного потока исчерпывающей и достоверной информации, одновременно затрудняя или воспрещая аналогичные действия противника.** Для достижения информационного превосходства было сформулировано два условия: во-первых, стремительно развивающиеся коммерческие технологии необходимо использовать и адаптировать их для нужд обороны быстрее, чем это делают военные конкуренты США; во-вторых, государству необходимо иметь эффективные наступательные и оборонительные информационные возможности, которые должны защищать информационные ресурсы и системы от нападения и обеспечивать соразмерные ответные действия.

6. На рубеже XX и XXI веков информационное противоборство в сфере обеспечения национальной безопасности Соединенных Штатов Америки, особенно в вооруженных силах, выходит на первый план в общей системе различных видов борьбы, в том числе вооруженной. Используя весь предшествующий опыт подготовки и ведения локальных войн и вооруженных конфликтов, США в 90-е годы осуществили прорыв в теории и практике комплексного применения сил и средств психологических операций, радиоэлектронной борьбы, введения противника в заблуждение, противодействия разведке противника, специальных операций нападения на компьютерные сети, а также в разработке способов эффективного применения службы по связям с общественностью и службы по работе с гражданской администрацией, объединив их усилия для практической реализации современной концепции информационного противоборства – концепции информационных операций (документы КНШ МО США "Единые перспективы 2010" и ***"Единые перспективы 2020***" , а также документы МО США "Четырехлетний обзор состояния вооруженных сил" от 2001 и 2006 годов). Участие вооруженных сил США в локальных войнах и вооруженных конфликтах в конце XX века позволило им накопить опыт использования современных технологий информационного противоборства.

7. Как показал анализ, современный потенциал системы информационного противоборства американских вооруженных сил является воплощением развития теоретических взглядов, всего исторического опыта совершенствования ее информационно-психологических и информационно-технических компонентов, применения самых разнообразных форм и способов воздействия на важнейшие информационные ресурсы и системы вооруженных сил и государств потенциального противника. Исследование зарождения и развития концепции информационных операций американских войск на протяжении более чем пятидесяти лет позволяют проследить совершенствование теории и практики указанных компонентов, дать объяснение существующей ныне структуры

аппарата, механизма и специфики системы проведения информационных операций вооруженных сил США, тенденции их дальнейшего развития. **Уже в начале 90-х годов на примере опыта войны в Персидском заливе стало очевидно, что произошло слияние информационно-психологической и информационно-технической составляющих информационного противоборства.** Достижение информационного превосходства потребовало особых инструментов, позволяющих воздействовать на всю информационную сферу противника. В свою очередь они получили развитие в рамках концепции информационных операций, основанной на полученном опыте информационного противоборства при проведении военных действий вооруженными силами США в конце XX века. Структура и механизм проведения информационных операций окончательно сформировались в вооруженных силах США только во второй половине 90-х годов. Информационные операции стали неотъемлемой частью деятельности вооруженных сил США как в мирное время, так и при проведении военных действий.

8. **В настоящее время США по сравнению с другими странами обладают значительным преимуществом в области разработки и использования информационных, телекоммуникационных технологий, а также различного рода радиоэлектронных систем.** Основываясь на концепции информационных операций, военно-политическое руководство США стремится всячески закрепить за собой доминирующую роль не только в политической, экономической и военной сферах, но и в мировой информационной инфраструктуре. Об этом свидетельствует характер и специфика ведения информационного противоборства в деятельности американских войск последнего десятилетия XX века.

9. Изучение опыта информационного противоборства американских вооруженных сил в конце XX века, а также руководящих документов военно-политического руководства США позволяет утверждать, что **достижение информационного превосходства – это главный ориентир на перспективу до 2020 г. Сегодня военно-политическое руководство США делает ставку не столько на современные системы огневого поражения и высокоточное оружие, сколько на сохранение и использование в полном объеме своего информационного превосходства.**

10. Анализ содержания, форм и методов информационно-психологического и информационно-технического воздействия на войска и население противника, мировую общественность и население своей страны, а также обобщение теоретического и практического опыта информационных операций американской армии в конце XX века имеют важное значение и для творческого осмысления этих проблем в Российской Федерации.

11. Как выяснилось в процессе исследования, концепция информационного противоборства в том виде, в каком она реализуется в вооруженных силах США, для отечественного военного искусства не является чем-то новым. Теоретические основы информационно-психологического и информационно-технического противоборства довольно полно разработаны в нашей военной науке. Они раскрываются через такие понятия, как «борьба с системами управления противника», «радиоэлектронная борьба», «завоевание господства в эфире»,

«психологическая борьба», «оперативная и стратегическая маскировка войск», «дезинформация» и другие.

Оригинальность американского подхода к теории и практике информационного противоборства состоит в комплексном использовании прежних, в том числе и русско-советских, военно-теоретических разработок по данной проблематике и новейших достижений в области информационных технологий, психологии, социологии, этнологии и других наук, возможностях их применения на всех уровнях государственного и военного управления. **Концептуальный анализ научно-исследовательской и специальной литературы**[10] **по вопросам информационной безопасности государства позволяет классифицировать её по нескольким основным направлениям:**

Отечественную литературу по вопросам информационного противоборства можно разделить на несколько профильных подгрупп:

I.К первой группе следует отнести руководящие документы, регламентирующие деятельность высших органов государственной власти и управления в области информационной политики [53-57]. В них изложены концептуальные основы и целевые установки, однако в прямой постановке проблемы информационно-психологической безопасности практически не раскрыты, к тому же отсутствует анализ возможных последствий использования методов ИП против населения и войск.

II.Вторую группу источников составляют фундаментальные исследования отечественных ученых по общим проблемам теории безопасности и национальной безопасности Российской Федерации: Баришполец В., Возженников А.В., Дзлиев М.И., Золотарев В.А., Косолапов Н., Ладыгин Ф., Лузинян В., Пионтковский А.А., Прохожев А.А., Ромашкин П., Смульский С.В., Турко Н.И., Урсул А.Д., Цыганков П.А., Цыгичко В.Н., Чебан В.В. и др. [58-66], имеющие общеметодологический характер.

Особое место здесь занимают труды, в которых теоретико-методологические обобщения развиты и конкретизированы применительно к проблемам информационной безопасности: Андреев Э.М., Василенко И.А., Корнеев И.К., Крутских А., Поздняков А.И., Степанов Е.А., Турко Н.И., Шевченко А.В., Ярочкин В.И[67-71]. и военной безопасности: Барынькин В.М., Булгаков В., Велесов С.Л., Громов Б.В., Дмитриев А.П., Золотарев В.А., Лутовинов В.Н., Манилов В.А., Панарин И.Н., Рогов С.М., Серебрянников В.В. и др[72-79].

В некоторые из этих работ рассматриваются и различные аспекты информационно-психологической безопасности, содержится характеристика информационного противоборства.

III.Третья группа работ непосредственно включает научные труды по проблемам информационной политики, информационного противоборства и информационно-психологической борьбы: Борисенко М.В., Вепринцев В.Б., Винокуров И.Н., Володенков С.В., Волковский Н.Л., Грачев Г.В., Грешневиков А., Гриняев С.Н., Забарин А.В., Зимичев А.М., Иванов О.В., Кара-Мурза С.Г., Караяни А.Г., Комов С.А., Костин Н.А., Крысько В.Г., Лисичкин В.А., Манойло А.В., Мельник И.К., Модестов С.А., Мухин А.А., Назаретян А.П., Некляев С.Э., Ососков В.П., Павлова Е.К., Панарин И.Н., Петренко А.И., Попов В.Д., Поченцов Г.Г., Пригожин А.И., Прокофьев В.Ф., Расторгуев С.П., Тавокин Е.П., Фролов

Д.Б., Шелепин Л.А., Цуладзе А., Цымбал В.И., Яковлев И.Г. и др[80-89]. Данные работы содержат анализ чрезвычайно широкого спектра вопросов противоборства в информационной сфере, в т.ч. и некоторые аспекты содержания и технологий применения ИП в политических целях.

Основу зарубежной источниковой базы составляют различные исторические документы, а также объединенные доктрины, полевые уставы и директивы министерства обороны США, регламентирующие деятельность системы информационных операций. Всю данную базу также можно разделить на несколько подгрупп:

I.Первая группа – это открытые документы администрации президента США, конгресса и соответствующих правительственных ведомств Соединенных Штатов, в которых рассматриваются вопросы, касающиеся информационных операций, информационного обеспечения, защиты важной государственной инфраструктуры. К ним в первую очередь относятся: «Доклад Президентской комиссии по защите критической инфраструктуры», «Президентская директива по защите критической инфраструктуры», президентский доклад «Стратегия национальной безопасности в новом веке», «Национальный план защиты информационных систем», «Отчет президента США о действиях по защите критической инфраструктуры» и др. [90-93]

1. *II.Вторая группа* – это руководящие и доктринальные[1] документы министерства обороны США, Комитета начальников штабов, министерств и штабов видов вооруженных сил, в той или иной степени касающиеся различных аспектов информационного противоборства. Это прежде всего «Объединенная перспектива 2010», «Концепция будущих объединенных операций: расширенная объединенная перспектива 2010», «Объединенная перспектива 2020», ежегодные доклады министра обороны США Президенту и Конгрессу, «Четырехлетние оборонные обзоры», «Объединенная доктрина информационных операций», «Объединенная доктрина борьбы с системами управления», полевой устав FM-106 «Информационные операции», устав ВВС AFD 2-5 «Информационные операции», полевой устав FM-3-0 «Операции» и др. [94-103]

III.Третья группа – это основополагающие научные труды американских авторов по различным аспектам исследуемой темы. Среди них особо стоит выделить работы следующих авторов: Тоффлер О. – «Третья волна», «Перераспределение власти», «Война и антивойна: выживание в XXI веке»; Агуилла Д. и Ронфельд Д. – «Кибервойна приближается», «Информация, власть и великая стратегия» ; Альбертс Д. – «Оборонная информационная борьба»; Штейн Дж. – «Информационная борьба»; Шафрански Р. – «Теория информационной войны: подготовка 2020»; Швартау В. – «Информационная борьба: хаос на информационной автостраде»; Либики М. – «Что такое информационная война»; Томас Т. – «Российские взгляды на борьбу на основе информации» и др. [104-112]

IV.Четвертая группа – это разработки американских научно-исследовательских центров и военно-учебных заведений, а также

[1] Под доктриной в Соединенных Штатах подразумевают фундаментальные принципы, направляющие действия военной силы или ее элементов в поддержку национальных целей. Под «объединенными доктринами» (joint doctrine) понимаются фундаментальные принципы, регулирующие использование двух или более видов вооруженных сил в скоординированной деятельности для достижения общей цели.

западноевропейские и китайские исследования по проблеме информационного противоборства. В первую очередь это ряд отчетов корпорации РЭНД, сделанных по заказу министерства обороны США: «В лагере Афины: подготовка к конфликтам в информационном веке», «Появление ноополитики: к американской информационной стратегии», «Стратегическая информационная борьба: новое лицо войны», «Усиливающаяся стратегическая информационная борьба», «Появление сетевых войн», «На следующий день … в киберпространстве», «Глобальная технологическая революция» и другие, а также разработки Национального университета обороны, Института оборонного анализа, Центра международных и стратегических исследований, различных научно-исследовательских групп, занимающихся исследованием тех или иных аспектов информационного противоборства и использования информации[113-121].

На основании проведенного анализа, а также исходя из практики боевых действий НАТО в Ливии, Афганистане, Ираке и Пакистане, представляется возможным сделать несколько конкретных предложений по укреплению национальной информационной безопасности РФ:

Первое – внедрение самых передовых стандартов информационной безопасности. Необходимо разработать и реализовать меры государственного стимулирования процессов внедрения и использования перспективных (причем внедрения и использования – это не только довести и дать всем, а именно создать стимулы для их реального внедрения всеми организациями), т.е. не только современных, но и «опережающих» стандартов информационной безопасности, разработанных с учетом развития общемировых тенденций в данной сфере, а также «наработок», достигнутых наиболее авторитетными органами международной стандартизации, такими как ИСО, ИТУ и так далее.

Второе – подготовка кадров для работы в области безопасных информационных технологий. Поручить Минобрнауки и Минобороны развернуть на базе ведущих университетов и академий подготовку кадров для работы в области безопасных информационных технологий с учетом комплексности указанной тематики по специальностям, включающим наряду с углубленным изучением математических и технических дисциплин также изучение соответствующих разделов юридических и экономических наук.

Третье – меры государственного стимулирования разработки и создания отечественных безопасных информационных технологий. Следует разработать финансируемую государством программу исследований и разработки безопасных информационных технологий, включая работы по созданию безопасной отечественной вычислительной платформы и соответствующих средств программирования.

Четвертое – создание общенационального надведомственного органа по координации, мониторингу и контролю всей деятельности в области обеспечения информационной безопасности при Президенте РФ (возможно, в виде особого структурного подразделения Совета Безопасности России).

Пятое - создание специального (элитного) вида войск для ведения различных операций информационно-организационного, психополит-технологического, социоэкономического и военно-технического характера в глобальном киберпространстве.

Шестое - нейтрализация попыток «агентов влияния», сценаристов и фигурантов «информационной войны» (иностранные лоббисты, компрадоры-властедержатели, «грантососы», подкрышные фонды, транснациональные корпорации, местечковые сепаратисты, «активисты-псевдоправозащитники») расшатать устои державной государственности, подменить национальные институты, выступать и действовать от имени всего «гражданского общества», дабы стать «самостийными» субъектами глобальной политики.