МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФГАОУ ВО «Севастопольский государственный университет»
Институт радиоэлектроники и информационной безопасности
Кафедра Информационной безопасности

ВВЕДЕНИЕ В СПЕЦИАЛЬНОСТЬ
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Учебное пособие

Севастополь 2015 г.

УДК 004.732.056

Оформление текстовых работ: учебное пособие/ СевГУ; сост. Костюков А.Д., Люльченко А.Н., Ожиганова М.И., Сафьяник А.О. — Севастополь: Изд-во СевГУ, 2015. —145с.

Учебное пособие раскрывает актуальность проблемы защиты информации, показывает историю развития защиты информации в России, характеризует особенности информационной войны и специальных информационных операций. Рассматриваются вопросы становления и развития проблем защиты информации в мировой практике, особенности современных систем защиты информации в ведущих зарубежных странах, таких как США, страны Евросоюза, КНР, а также основные понятия информационной безопасности Российской Федерации. Для студентов высших учебных заведений, обучающихся по направлению 10.03.01 «Информационная безопасность».

Учебное пособие утверждено на заседании кафедры Информационной безопасности 02.09.2015, протокол № 2.

Рецензент: кандидат технических наук, профессор Кирияченко В.А.

Ответственный за выпуск: кандидат технических наук, заведующий кафедрой Информационной безопасности Ожиганова М.И.

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Жизнь современного общества немыслима без повсеместного применения информационных технологий. Компьютеры обслуживают банковскую систему, контролируют работу атомных реакторов, распределяют энергию, следят за расписанием поездов, управляют самолетами и космическими кораблями. Сегодня компьютерные системы и телекоммуникации определяют надежность систем обороны и безопасности страны, реализуют современные информационные технологии, обеспечивая хранение информации, ее обработку, доставку и представление потребителям.

Однако именно высочайшая степень автоматизации, к которой стремится современное общество, ставит его в зависимость от уровня безопасности используемых информационных технологий. От них зависит благополучие и жизнь людей. Массовое применение компьютерных систем, позволившее решить задачу автоматизации процессов обработки постоянно нарастающих объемов информации, сделало эти процессы чрезвычайно уязвимыми по отношению к агрессивным воздействиям и поставило перед потребителями информационных технологий новую проблему, — проблему информационной безопасности.

Сложившаяся в сфере безопасности информационных технологий ситуация еще раз подтверждает давно известную неприятную особенность технического прогресса порождать в ходе решения одних проблем новые, иногда даже более сложные.

ГЛАВА 1.
АКТУАЛЬНОСТЬ ПРОБЛЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

1.1. Актуальность проблемы защиты информации

Актуальность проблемы защиты информации связана с ростом возможностей вычислительной техники. Развитие средств, методов и форм автоматизации процессов обработки информации, массовость применения персональных электронно-вычислительных машин (ЭВМ) резко повышают уязвимость информации. Основными факторами, способствующими повышению этой уязвимости, являются :

– резкое увеличение объемов информации, накапливаемой, хранимой и обрабатываемой с помощью ЭВМ и других средств автоматизации;

– сосредоточение в единых базах данных информации различного назначения и различной принадлежности;

– резкое расширение круга пользователей, имеющих непосредственный доступ к ресурсам вычислительной системы и находящимся в ней массивам данных;

– усложнение режимов функционирования технических средств вычислительных систем: широкое внедрение мультипрограммного режима, а также режима разделения времени;

– автоматизация межмашинного обмена информацией, в том числе и на больших расстояниях.

В этих условиях возникает возможность несанкционированного использования или модификации информации (т. е. опасность утечки информации ограниченного пользования). Это вызывает особую озабоченность пользователей, в связи с чем защите информации от несанкционированного доступа (чтения) уделяется повышенное внимание.

Совершенно очевидна уязвимость незащищенных систем связи, в том числе вычислительных сетей. Информация, циркулирующая в них, может быть незаконно изменена, похищена, уничтожена.

В последнее время в средствах массовой информации появилось большое количество сенсационных сообщений о фактах несанкционированных преступных воздействий на аппаратуру обработки, хранения и передачи информации с нанесением большого материального ущерба.

Защита информации находится в центре внимания не только специалистов по разработке и использованию информационных систем, но и широкого круга пользователей. В последние годы, в связи с широким распространением и повсеместным применением вычислительной техники, массовостью внедрения персональной ЭВМ, резко повысилась уязвимость накапливаемой, хранимой и обрабатываемой в системах информации. Сейчас четко выделяются три аспекта уязвимости информации:

1) подверженность физическому уничтожению или искажению,

2) возможность несанкционированной (случайной или злоумышленной) модификации;

3) опасность несанкционированного (случайного или злоумышленного) получения информации лицами, для которых она не предназначалась.

Однако, если первый аспект уязвимости информации был известен существует определенная разработанная научно-методическая база для практических рекомендаций, то резкое повышение возможности не санкционированного получения информации оказывается большой опасностью. Эта опасность является тем более острой, что традиционные меры защиты от несанкционированного доступа к информации оказались недостаточными для решения аналогичных задач в системах с применением новых информационных технологий. Как утверждается в зарубежной литературе, преступления с использованием ЭВМ превратились в национальное бедствие.

1.2. Основные понятия информационной безопасности

Информационная система – это система обработки информации и соответствующие организационные ресурсы (человеческие, технические, финансовые и т. д.), которые обеспечивают и распространяют информацию.

Информационная система предназначена для своевременного обеспечения надлежащих людей надлежащей информацией[3], то есть для удовлетворения конкретных информационных потребностей в рамках определенной предметной области, при этом результатом функционирования информационных систем является *информационная продукция* — документы, информационные массивы, базы данных и информационные услуги.

Информация – это сведения (сообщения, данные) независимо от формы их представления.

Основными и наиболее значимыми с точки зрения информационной безопасности являются следующие свойства информации:

- *конфиденциальность* – состояние информации, при котором доступ к ней осуществляют только субъекты, имеющие на него право.
- *целостность* – состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право;
- *доступность* – состояние информации, при котором субъекты, имеющие право доступа, могут реализовывать его беспрепятственно [1].

Вся информация делится на *общедоступную* и *ограниченного доступа*. К общедоступной информации относятся общеизвестные сведения и иная информация, доступ к которой не ограничен.

К информации с ограниченным доступом относится *государственная тайна* и *конфиденциальная информация*.

Ограничение доступа к информации устанавливается федеральными законами в целях защиты основ конституционного строя, нравственности,

здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства [2,3].

Далее представлен перечень конфиденциальной информации согласно законодательству Российской Федерации.

1. *Персональные данные*

Любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу [4].

2. *Коммерческая тайна*

Сведения любого характера (производственные, технические, экономические, организационные и другие), в том числе о результатах интеллектуальной деятельности в научно-технической сфере, а также сведения о способах осуществления профессиональной деятельности, которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, к которым у третьих лиц нет свободного доступа на законном основании и в отношении которых обладателем таких сведений введен режим коммерческой тайны [5].

3. *Банковская тайна (тайна банковских вкладов)*

Сведения об операциях, счетах и вкладах ее клиентов и корреспондентов, а также об иных сведениях, устанавливаемых кредитной организацией [6,7].

4. *Служебная тайна*

Служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами [8,9,10,11].

5. *Тайна кредитной истории*

Информация, которая характеризует исполнение заемщиком принятых на себя обязательств по договорам займа (кредита) и хранится в бюро кредитных историй [12].

6. *Тайна страхования*

Сведения о страхователе, застрахованном лице и выгодоприобретателе, состоянии их здоровья, а также об имущественном положении этих лиц (946 ГК РФ) [9].

7. Тайна завещания

Сведения, касающиеся содержания завещания, его совершения, изменения или отмены (1123 ГК РФ) [9].

8. Налоговая тайна

Любые полученные налоговым органом, органами внутренних дел, органом государственного внебюджетного фонда и таможенным органом сведения о налогоплательщике (за рядом исключением) [13].

9. Тайна усыновления ребенка

Судьи, вынесшие решение об усыновлении ребенка, или должностные лица, осуществившие государственную регистрацию усыновления, а также лица, иным образом осведомленные об усыновлении, обязаны сохранять тайну усыновления ребенка [14].

10.Врачебная тайна

Сведения о наличии у гражданина психического расстройства, фактах обращения за психиатрической помощью и лечении в учреждении, оказывающем такую помощь, а также иные сведения о состоянии психического здоровья [15].

11.Медицинская тайна

Информация о факте обращения за медицинской помощью, состоянии здоровья гражданина, диагнозе заболевания, иные сведения, полученные при обследовании и лечении гражданина, а также сведения о проведенных искусственном оплодотворении и имплантации эмбриона, а также о личности донора. Результаты обследования лица, вступающего в брак (Основы законодательства РФ об охране здоровья граждан, 223-ФЗ Семейный кодекс РФ) [14].

12. Тайна переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений

На территории Российской Федерации гарантируется тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных и иных сообщений, передаваемых по сетям электросвязи и сетям почтовой связи [16,17].

13.Тайна частной жизни (личная тайна)

Право на неприкосновенность частной жизни означает предоставленную человеку и гарантированную государством возможность контролировать информацию о самом себе, препятствовать разглашению сведений личного, интимного характера (Конституция РФ, 150 ГК РФ) [18,9].

14.Аудиторская тайна

Любые сведения и документы, полученные и (или) составленные аудиторской организацией и ее работниками, а также индивидуальным аудитором и работниками, с которыми им заключены трудовые договоры, при оказании услуг (за рядом исключений) [19].

15.Тайна судопроизводства (тайна следствия и судопроизводства)

Данные предварительного расследования не подлежат разглашению… могут быть преданы гласности лишь с разрешения прокурора, следователя, дознавателя и только в том объеме, в каком ими будет признано это допустимым, если разглашение не противоречит интересам предварительного расследования и не связано с нарушением прав и законных интересов участников уголовного судопроизводства. Разглашение данных о частной жизни участников уголовного судопроизводства без их согласия не допускается (241 УПК РФ, 10 ГПК РФ, 11 АПКРФ, 166 УПК РФ, Указ Президента от 6.03.1997 №188) [20,21,22,8]

16.Адвокатская тайна (тайна судебного представительства)

Любые сведения, связанные с оказанием адвокатом юридической помощи своему доверителю [23].

17.Тайна нотариальных действий (нотариальная тайна)

Нотариус обязан хранить в тайне сведения, которые стали ему известны в связи с его профессиональной деятельностью. Суд может

освободить нотариуса от этой обязанности сохранения тайны, если против него возбуждено уголовное дело в связи с совершением нотариального действия. Поскольку нотариусы предоставляют информацию о совершенных ими нотариальных действиях нотариальным палатам, должностные лица этих палат также обязаны сохранять нотариальную тайну (Основы законодательства Российской Федерации о нотариате).

18.Тайна исповеди

Священнослужитель не может быть привлечен к ответственности за отказ от дачи показаний по обстоятельствам, которые стали известны ему из исповеди [24].

19.Тайна голосования

Подсчет избирательных бюллетеней проводится таким образом, чтобы не нарушалась тайна голосования [25,26,27].

20. Тайна сведений о мерах безопасности в отношении должностного лица правоохранительного или контролирующего органа

Разглашение сведений о мерах безопасности, применяемых в отношении судьи, присяжного заседателя или иного лица, участвующего в отправлении правосудия, судебного пристава, судебного исполнителя, потерпевшего, свидетеля, других участников уголовного процесса, а равно в отношении их близких, если это деяние совершено лицом, которому эти сведения были доверены или стали известны в связи с его служебной деятельностью [28].

21.Журналистская (редакционная) тайна

Редакция не вправе разглашать в распространяемых сообщениях и материалах сведения, предоставленные гражданином с условием сохранения их в тайне. Редакция обязана сохранять в тайне источник информации и не вправе называть лицо, предоставившее сведения с условием неразглашения его имени, за исключением случая, когда соответствующее требование поступило от суда в связи с находящимся в его производстве делом. Редакция не вправе разглашать в распространяемых сообщениях и

материалах сведения, прямо или косвенно указывающие на личность несовершеннолетнего, совершившего преступление либо подозреваемого в его совершении, а равно совершившего административное правонарушение или антиобщественное действие, без согласия самого несовершеннолетнего и его законного представителя [29].

22.Тайна вероисповедания

Сведения об отношении к религии, к исповеданию или отказу от исповедания религии, об участии или неучастии в богослужениях, других религиозных обрядах и церемониях, о деятельности в религиозных объединениях, об обучении религии (125-ФЗ «О свободе совести и о религиозных объединениях»).

23.Тайна сведений о военнослужащих внутренних войск МВД

Сведения о местах дислокации или о передислокации соединений и воинских частей внутренних войск, а также сведения о военнослужащих внутренних войск, принимавших участие в пресечении деятельности вооруженных преступников, незаконных вооруженных формирований и иных организованных преступных групп, а также сведений о членах их семей [30].

Информационная безопасность (ИБ) – это состояние защищённости информации, при котором обеспечиваются её конфиденциальность, доступность и целостность.

Защита информации (ЗИ) – это комплекс организационных, правовых и технических мер по предотвращению угроз информационной безопасности и устранению их последствий.

Понятие информационной безопасности шире, чем понятие защиты информации, т.к. ИБ – состояние, достигаемое комплексом мер и действий, называемых ЗИ, т.е. информационная безопасность – цель, а защита информации средство ее достижения.

Утечки информации – это случайные потери или намеренное хищение информации

Злоумышленник (нарушитель) – лицо или группа лиц, которые в результате предумышленных или непредумышленных действий обеспечивает реализацию угроз информационной безопасности.

Несанкционированный доступ к информации – это доступ к закрытой для публичного доступа информации со стороны лиц, не имеющих разрешения на доступ к этой информации [1].

Как было сказано ранее, защита информации включает комплекс мероприятий, которые должны охватывать следующие аспекты ИБ:

Правовые: нормативно-правовые акты и стандарты в области ИБ

Технические: применение технических, а также инженерно-технических средств защиты информации, в том числе и криптографических и программно-аппаратных средств защиты.

Экономические: включают расчет финансовых затрат на защиту информации, а также расчет экономического ущерба, наносимого несанкционированным доступом к информации.

Организационные: мероприятия, связанные с организацией вышеперечисленных аспектов

1.3. Основные угрозы информационной безопасности

Уязвимость - это недостаток в обеспечении мер защиты информации, который может предоставить злоумышленнику возможность получения несанкционированного доступа к информационным ресурсам компании. Уязвимость - это отсутствие или слабость защитных мер.

Угрозы информационной безопасности – совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации.

Источник угрозы информационной безопасности - это потенциальные антропогенные, техногенные и стихийные угрозы безопасности.

Риск - это вероятность того, что источник угрозы воспользуется уязвимостью, что приведет к негативному воздействию на бизнес.

Воздействие злоумышленника на информационную систему - это действия, приводящие к потерям в связи с действиями источника угрозы. Злоумышленник воздействует на уязвимости, что приводит к возможности нанесения ущерба информационной системе.

Защитные меры - это меры, внедрение которых позволяет снизить уровень потенциального риска.

Взаимосвязь между рисками, уязвимостями, угрозами и мерами защиты показана на рисунке 1.

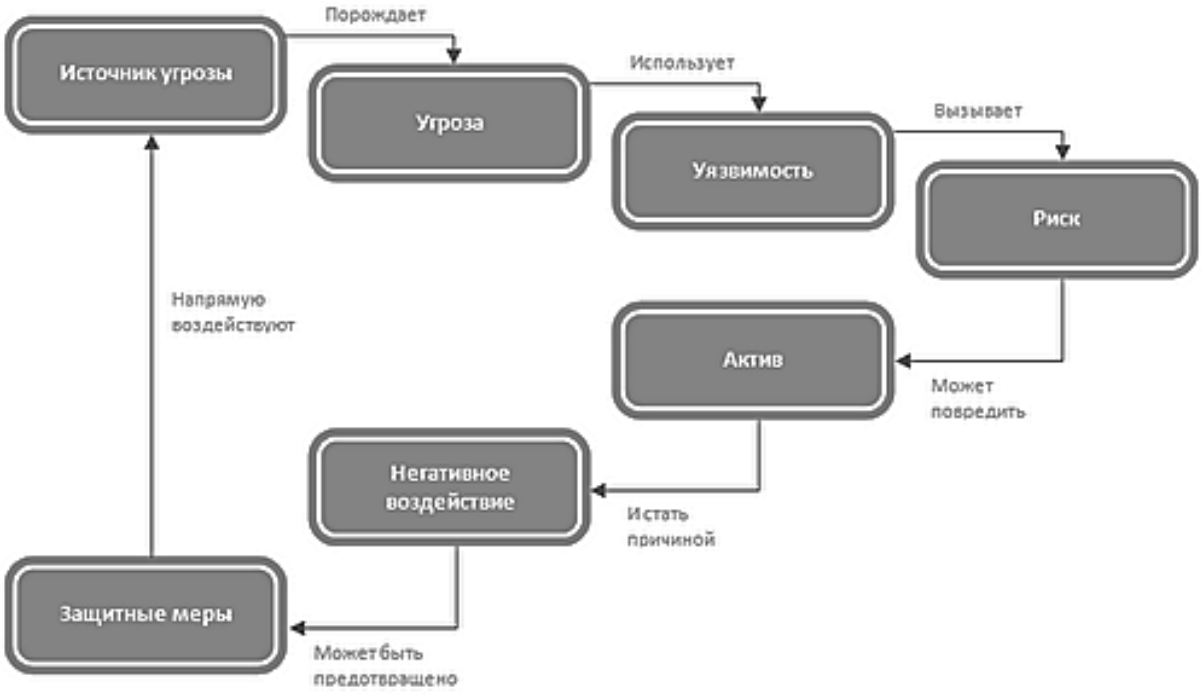

Рис.1. Взаимосвязь элементов системы защиты информации

Угрозы информационной безопасности могут быть классифицированы по различным признакам:

1. *По аспекту информационной безопасности, на который направлены угрозы:*
   - угрозы конфиденциальности (неправомерный доступ к информации);
   - угрозы целостности (неправомерное изменение данных);

– угрозы доступности (осуществление действий, делающих невозможным или затрудняющих доступ к ресурсам информационной системы).

2. *По степени преднамеренности действий:*

– случайные (неумышленные действия, например, сбои в работе систем, стихийные бедствия);

– преднамеренные (умышленные действия, например, шпионаж и диверсии).

3. *По расположению источника угроз:*

– внутренние (источники угроз располагаются внутри системы);

– внешние (источники угроз находятся вне системы).

4. *По размерам наносимого ущерба:*

– общие (нанесение ущерба объекту безопасности в целом, причинение значительного ущерба);

– локальные (причинение вреда отдельным частям объекта безопасности);

– частные (причинение вреда отдельным свойствам элементов объекта безопасности).

5. *По степени воздействия на информационную систему:*

– пассивные (структура и содержание системы не изменяются);

– активные (структура и содержание системы подвергается изменениям).

Меры противодействия угрозам:

1. *Правовые и законодательные.* Законы, указы, нормативные акты, регламентирующие правила обращения с информацией и определяющие ответственность за нарушение этих правил.

2. *Морально-этические.* Нормы поведения, которые традиционно сложились или складываются в обществе по мере распространения вычислительной техники. Невыполнение этих норм ведет к падению авторитета, престижа организации, страны, людей.

3. *Административные или организационные*. Меры организационного характера, регламентирующие процессы функционирования АС, деятельность персонала с целью максимального затруднения или исключения реализации угроз безопасности:

- организация явного или скрытого контроля за работой пользователей
- организация учета, хранения, использования, уничтожения документов и носителей информации.
- организация охраны и надежного пропускного режима
- мероприятия, осуществляемые при подборе и подготовке персонала
- мероприятия по проектированию, разработке правил доступа к информации
- мероприятия при разработке, модификации технических средств

4. *Физические*. Применение разного рода технических средств охраны и сооружений, предназначенных для создания физических препятствий на путях проникновения в систему.

5. *Технические*. Основаны на использовании технических устройств и программ, входящих в состав АС и выполняющих функции защиты:

- средства аутентификации
- аппаратное шифрование
- другие

Принципы построения систем защиты:

1. *Принцип системности* - системный подход предполагает необходимость учета всех взаимосвязанных и изменяющихся во времени элементов, условий и факторов, существенно значимых для понимания и решения проблемы обеспечения безопасности.

2. *Принцип компетентности* - предполагает построение системы из разнородных средств, перекрывающих все существующие каналы реализации угрозы безопасности и не содержащих слабых мест на стыке отдельных компонентов.

3. *Принцип непрерывной защиты* - защита должна существовать без разрыва в пространстве и времени. Это непрерывный целенаправленный процесс, предполагающий не только защиту эксплуатации, но и проектирование защиты на стадии планирования системы.

4. *Принцип разумной достаточности*. Вложение средств в систему защиты должно быть построено таким образом, чтобы получить максимальную отдачу.

5. *Принцип гибкости управления и применения*. При проектировании системы защита может получиться либо избыточной, либо недостаточной. Система защиты должна быть легко настраиваема.

6. *Принцип открытости алгоритмов и механизмов защиты*. Знание алгоритма механизма защиты не позволяет осуществить взлом системы.

7. *Принцип простоты применения защитных мер и средств*. Все механизмы защиты должны быть интуитивно понятны и просты в использовании. Пользователь должен быть свободен от выполнения малопонятной многообъемной рутиной работы и не должен обладать специальными знаниями.

Обеспечение информационной безопасности является сложной задачей, для решения которой требуется комплексный подход. Выделяют следующие **уровни защиты информации**:

1. законодательный – законы, нормативные акты и прочие документы РФ и международного сообщества;

2. административный – комплекс мер, предпринимаемых локально руководством организации;

3. процедурный уровень – меры безопасности, реализуемые людьми;

4. программно-технический уровень – непосредственно средства защиты информации.

Законодательный уровень является основой для построения системы защиты информации, так как дает базовые понятия предметной области и определяет меру наказания для потенциальных злоумышленников. Этот

уровень играет координирующую и направляющую роли и помогает поддерживать в обществе негативное (и карательное) отношение к людям, нарушающим информационную безопасность.

Государственные органы РФ, контролирующие деятельность в области защиты информации:

- Комитет Государственной думы по безопасности;
- Совет безопасности России;
- Федеральная служба по техническому и экспортному контролю (ФСТЭК России);
- Федеральная служба безопасности Российской Федерации (ФСБ России);
- Федеральная служба охраны Российской Федерации (ФСО России);
- Служба внешней разведки Российской Федерации (СВР России);
- Министерство обороны Российской Федерации (Минобороны России);
- Министерство внутренних дел Российской Федерации (МВД России);
- Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор);
- Центральный банк Российской Федерации (Банк России).

1.4. Статистика нарушения информационной безопасности по различным критериям

Аналитический центр компании InfoWatch представляет глобальное исследование утечек конфиденциальной информации за 2014 год [31].

По данным отчета, по сравнению с прошлым годом число утечек информации в мире выросло на 22%, в России – на 73%**.**

По сравнению с 2013 годом, доля случайных утечек увеличилась на 10%

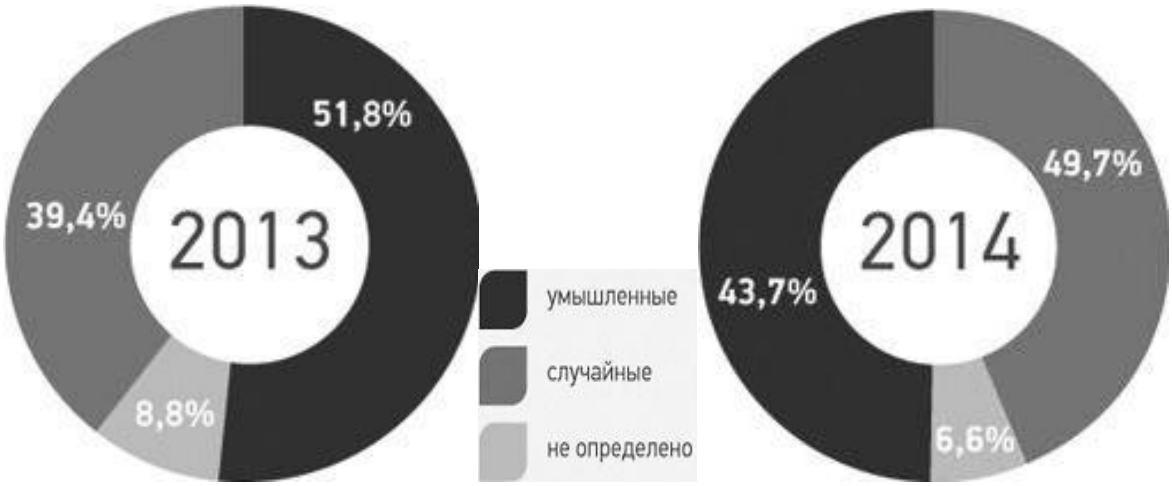

Рис. 2. Сравнительная диаграмма случайных утечек

В 55% виновниками утечек информации были настоящие или бывшие сотрудники – 54% и 1% соответственно. Велика доля утечек, случившихся на стороне подрядчиков, чей персонал имел легитимный доступ к охраняемой информации (4%). Более чем в 1% случаев зафиксирована вина руководителей организаций (топ-менеджмент, главы отделов и департаментов); пользователей с расширенными правами доступа к информации (системных администраторов).

Рис.3. Статистика виновников утечек информации

Доля утечек персональных и платежных данных в распределении утечек по типу информации выросла на 7% к данным 2013 года, составив 92%.

Рис.4. Диаграмма типов утечек информации

В распределении по характеру действий нарушителя в 81% случаев зафиксирована «классическая» утечка – потеря контроля над информацией.

7,8% зарегистрированных инцидентов классифицированы как нарушения, сопряженные с получением несанкционированного доступа к информации.

Рис.5. Диаграмма утечек по характеру действий нарушителя

Чаще всего утечки фиксировались в медицине (25%), реже всего в муниципальных учреждениях (2%). При этом по объему скомпрометированных записей пальму первенства удерживает банковская вертикаль – 41%**,** вдвое меньше данных утекло в высокотехнологичных компаниях – 17%**,** торговых компаниях – 15%.

Рис. 6. Статистика утечек по отраслям деятельности

В распределении утечек по регионам в 2014 году США традиционно вышли на первую строчку по числу утечек (906). Россия заняла уже привычное второе место (167), которое досталось нашей стране еще по итогам 2013 года. На третьем месте оказалась Великобритания (85).

Приведенные факты показывают, что опасность насанкционированных злоумышленных действий в информационных системах является весьма реальной. И с дальнейшим развитием вычислительной техники, угроза утечки информации, несмотря на все усилия по ее защите, неизменно растет. Все это обуславливает необходимость углубленного анализа опыта защиты информации и комплексной организации методов и механизмов защиты.

Контрольные вопросы

1. Дайте определение понятию «информация»
2. Дайте определение понятию «информационная безопасность»
3. Дайте определение понятию «защиты информации».
4. Перечислите наиболее значимые свойства информации
5. Назовите меры противодействия угрозам безопасности информации
6. Назовите уровни защиты информации.
7. Какие бывают принципы построения системы защиты информации
8. Перечислите государственные органы, контролирующие деятельность в области информационной безопасности.
9. В каких учреждениях было зафиксировано наибольшее количество утечек информации?
10. Какие страны лидируют по количеству утечек информации?

ГЛАВА 2
ИСТОРИЯ РАЗВИТИЯ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

Проблема защиты информации имеет многовековую историю. С момента возникновения человечества всегда существовали сведения, которые человеку или группе людей необходимо было скрыть от своих недругов. Даже в первобытных племенах утечка информации об убитом мамонте могла оставить без пищи охотников. С развитием общества совершенствовались и способы добывания необходимой информации. К 400 году до н.э. Восток значительно опередил Запад в искусстве разведки. Сунь Цзы писал: «То, что называют предвидением, не может быть получено ни от духов, ни от богов, ни посредством расчетов. Оно должно быть добыто от людей, знакомых с положением противника».

С этого начался шпионаж, в том числе промышленный. Очень преуспели в нем многие государи и частные лица. Прекрасно поставленная служба разведки помогала купцам Венеции и банкирскому дому Фуггеров, фирме Круппа и дому Ротшильдов. Методы практически не менялись столетиями: подкупали, шантажировали, посылали послов-шпионов, перехватывали письма, читали пергаменты (позже книги и газеты) в библиотеках и монастырях. Когда удавалось, подсматривали и подслушивали. Трудности возникали и тогда, надо было передавать полученную информацию в центр сбора и обработки. Для этого приходилось гнать не всегда надежных гонцов, лично пробегать марафонскую дистанцию или пользоваться голубиной почтой. А чтобы не забыть по дороге, о чем шла речь, содержание перехваченных переговоров записывали, а иногда и шифровали. Таким образом, мы видим прообраз технической системы съема информации:

- микрофон, фотоаппарат, камера – ухо или глаза шпиона;
- диктофон или система накопления информации – записки;

– радиоканал, провода и т.д. – гонец;

– приемник – лицо, принявшее сообщение у гонца.

Что касается анализа полученной информации, то все осталось без изменений – нужен человек или группа людей, умеющих думать. Их работу сейчас несколько облегчила вычислительная машина. Развитие техники вплоть до начала XX века не влияло на средства несанкционированного съема информации: сверлили дырки в стенах и потолках, использовали потайные ходы и полупрозрачные зеркала, устраивались у замочных скважин и под окнами. Появление телеграфа и телефона позволило использовать технические средства получения информации. Гигантское количество сообщений стало перехватываться, влияя на ведение войн и положение на бирже. В 30–40 годы появились диктофоны, действительно миниатюрные фотоаппараты и микрофоны. В дальнейшем все большее значение приобретает перехват данных, обрабатываемых в компьютерах, но совершенствуются и традиционные средства.

Желание добывать конфиденциальную информацию всегда сопровождалось не меньшим желанием противоположной стороны защитить эту информацию. Поэтому история развития средств и методов разведки – это также и история развития средств и методов защиты информации. Причем, появившиеся в древние времена способы защиты информации по сути своей не изменились до настоящего времени, совершенствовалась лишь техника их реализации. Например, такой способ защиты, как маскировка содержания информации, прошел в своем развитии несколько этапов. В древнем Риме сообщение, написанное на доске, заливали от посторонних глаз воском. В древней Греции обривали раба, писали на его голове и, когда волосы отрастали, отправляли с поручением к адресату. В средние века придумали тайнопись и сообщения скрывали с помощью невидимых химических средств. Параллельно развивались методы шифрования и кодирования, история возникновения которых начинается со времен возникновения письменности в древнем Египте и Китае.

Наиболее интенсивное развитие этих методов приходится на период массовой информатизации общества. Поэтому история наиболее интенсивного развития проблемы защиты информации связывается с внедрением автоматизированных систем обработки информации и измеряется периодом в 30 с лишним лет. В 60-х годах на Западе стало появляться большое количество открытых публикаций по различным аспектам защиты информации. Такое внимание к этой проблеме вызвано было в первую очередь все возрастающими финансовыми потерями фирм и государственных организаций от преступлений в компьютерной сфере.

В нашей стране также давно и небезуспешно стали заниматься проблемами защиты информации. И не зря советская криптографическая школа до сих пор считается лучшей в мире. Однако чрезмерная закрытость всех работ по защите информации, сконцентрированных главным образом в отдельных силовых ведомствах, в силу отсутствия регулярной системы подготовки профессионалов в этой области и возможности широкого обмена опытом привела к некоторому отставанию в отдельных направлениях информационной безопасности, особенно в обеспечении безопасности компьютерной. Тем не менее, к концу 80-х годов бурный рост интереса к рассматриваемым проблемам не обошел и нашу страну. В данное время есть все основания утверждать, что в России сложилась отечественная школа защиты информации. Ее отличительной особенностью является то, что в ней наряду с решением сугубо прикладных проблем защиты большое внимание уделяется формированию развитого научно-методологического базиса, создающего объективные предпосылки для решения всей совокупности соответствующих задач на регулярной основе.

Естественно, что за истекшее после возникновения проблемы защиты информации время, существенно изменилось как представление о сущности, так и методологические подходы к решению. Указанные изменения происходили постепенно и непрерывно, поэтому всякая периодизация этого процесса в значительной мере будет носить искусственный характер [32].

2.1. Организация защиты информации в Древней Руси

В IX в. в результате объединения новгородских и киевских земель образовалось единое русское государство – Киевская Русь. Эффективное управление весьма обширной территорией было невозможно без организации надежной связи между столицей Киевом с подчиненными территориями и войсками, несущими сторожевую службу на границах Руси, а также находящимися в походе. Основным средством связи в то время были специальные княжеские гонцы – «люди пешие и конные» – и «верные головы» (люди из княжеской дружины), которые со скоростью 200 и более верст в сутки передвигались от одного пункта до другого, передавая как устные, так и письменные сообщения. Использовались и другие способы связи: оптическая сигнализация с помощью костров и дымов, почтовые голуби, на поле боя управление осуществлялось с помощью сигнальных труб и свистков.

Для обеспечения конфиденциальности передаваемой информации использовались различные методы. Наиболее важные сообщения заучивались гонцом наизусть. При этом часто использовались намеки, иносказания условные слова. Суть данного метода заключается в том, что смысл передаваемого сообщения мог понять только посвященный человек. В последствии в криптографии такой способ обеспечения секретности получил название «жаргонного кода» и применяется до сих пор. Использовался и так называемый «тарабарский язык», когда в устное сообщение вставлялись частицы-паразиты так фраза «возьми суму» звучала так: «тараВОбараЗЬМИтараСУбараМУ». Причем фраза произносилась как можно быстрее, человеку непривычному к такому способу общения понять смысл сказанного было крайне затруднительно. Подобные способы защиты информации с древних времен были распространены не только у государственных служб, но и среди представителей криминального мира в различных странах, в том числе и в России.

Для защиты письменных сообщений использовалась физическая защита, стеганография и шифрование. В качестве гонцов использовались физически крепкие люди, они были хорошо вооружены, нередко гонец следовал в сопровождении охраны. Сами письма скручивались в свитки, которые опечатывались специальными печатями, содержащими надпись « ДЬНЕСЛОВО», что переводится как «скрытое, тайное слово». Такие печати были у многих русских князей, в том числе и у Александра Невского.

Стеганографический метод заключался в запрятывании сообщений. Депеши зашивались в одежду, помещались в подошвы и каблуки обуви и другие места.

2.2. Организация защиты информации в Средневековье

Во время царствования Ивана IV Грозного (1530–1584 гг.) осуществлялись крупные дипломатические и военные акции – покорение Астраханского и Казанского ханств, Ливонская война, установление торговых связей с Англией и некоторыми другими государствами, присоединение Сибири. Все это, естественно, оказало влияние на дальнейшее развитие конфиденциальной государственной и военной связи.

Этой же цели служило и упорядочение несения службы на границах Московского государства. 16 февраля 1571 г. был утвержден Приговор (устав) «О станичной и сторожевой службе», установивший расписание доставки гонцами и сторожами имеющих государственное значение вестей из столицы на места и обратно.

Доставка ратных вестей в большие города и центры государства кроме гонцов и сторож осуществлялась также с помощью ямской гоньбы, которая получила дальнейшее развитие и была независима от разведки и сторож. В 1550 г. был основан Ямской приказ – центральное учреждение в России, ведавшее почтовыми сообщениями. К важным центрам государства и пограничным городам были проложены ямские тракты.

Следует подчеркнуть, что ямская гоньба в Российском государстве была учреждена исключительно для нужд правительства и для проезда послов иностранных государств. Право пользования ямскими подводами определялось особыми грамотами, называвшимися подорожными, которые появились еще до учреждения ямской гоньбы и выдавались обычно только княжеским гонцам или другим должностным лицам, выполнявшим аналогичные поручения. Наличие подорожных грамот у гонцов способствовало более успешному выполнению возложенных на них обязанностей по срочной доставке особо важной правительственной корреспонденции. Тем более, что подписывались такие грамоты, как правило, великими князьями, а в дальнейшем царями. Роль правительственных гонцов в рассматриваемый период могли выполнять не только ответственные должностные лица ямского приказа, но и военные курьеры военного ведомства (разрядного приказа).

Кроме основных ямских направлений в X VI в. существовали и другие, второстепенные направления к городам, имевшим политическое, военное и экономическое значение.

Ямская гоньба использовалась также для связи с появившимися в середине XIV в. на восточной и юго-восточной окраинах государства казачьими войсками (запорожскими, донскими, кубанскими, терскими).

Ко времени правления Ивана Грозного, понимавшего, что ведение «большой политики» немыслимо без соблюдения государственной тайны, относится и начальный этап становления криптографии в России как явления государственного.

Образованный в 1549 г. Посольский приказ, отвечавший, в числе прочего, за организацию посольской и внутриполитической шифрованной переписки, обеспечивал весьма высокий уровень ее конфиденциальности.

Таким образом, в XVI в. в России впервые сложилась довольно стройная система связи высших органов управления централизованным

государством, обеспечивавшаяся специальными категориями служилых людей следующих структур исполнительной власти:

– ямского приказа (почтового ведомства) – организационное обеспечение системы ямской гоньбы и доставка корреспонденции второстепенного значения;

– разрядного приказа (военного ведомства) – доставка особо важно правительственной корреспонденции военными курьерами (гонцами);

– посольского приказа (внешнеполитического ведомства) – организация и обеспечение криптографической защиты внешне- и внутригосударственной переписки.

При царе Алексее Михайловиче, втором царе из династии Романовых, был создан приказ тайных дел (1654 г.). В ведении Приказа находилась и шифровальная служба государя. При Алексее Михайловиче бежал за границу один из служащих, имевших доступ к материалам тайного приказа. Он кормился за рубежом за счет продажи своих сенсационных «откровений». В частности, он сообщил следующее: «А устроен тот приказ при нынешнем царе для того, чтобы его царская мысль и дела исполнялись все по его хотению, а бояре б и думные люди о том ничего не ведали». Таким образом, шифровальное дело находилось под личным контролем царя, и никто из его окружения доступ к нему не мог иметь. Так сохранялась тайна секретной переписки государства. К ней не допускались даже члены боярской думы. И это было вполне оправдано.

В это же время была организована система регулярного перехвата и перлюстрации (тайное вскрытие и копирование) корреспонденции зарубежных представителей, находившихся в России. Здесь стоит высказать гипотезу, что уничтожались как раз шифрованные письма, которые в приказе тайных дел прочитать не могли и действовали по принципу: «так не доставайся ж ты никому».

После кончины царя Алексея Михайловича в 1676 г., тайный приказ, ведавший секретной перепиской, был упразднен. По вполне понятным

причинам среди бояр было немало людей, которые спешили ликвидировать и его архив.

Тем не менее, один из бывших руководителей приказа дьяк Д. Башмаков сумел сохранить для потомков мешок с «тайными азбуками» – шифрами. Он передал его наследнику – будущему царю Петру I. Петр I очень внимательно отнесся к этим бумагам. Опыт отца в защите информации он эффективно использовал.

Петр сам изобретал шифрсистемы, заставлял заниматься этим своих соратников, и даже лично проводил криптоанализ некоторых русских шифров для оценки их стойкости.

Заметим, что Петр I считал шифры монополией царя российского. Он строго наказывал своих подданных за использование «негосударственных» шифров («цифирей»). Однако частные лица все же пользовались собственными шифрами. Среди них можно указать царевну Софью Алексеевну, которая использовала шифр в переписке со своим фаворитом князем В. В. Голицыным.

Другим способом защиты информации было введение цензуры. Предпоследнее десятилетие XVII в. в России сложилась весьма тяжелая внутриполитическая обстановка. Три человека считались главой государства – царевна Софья и два царя (среди них – будущий император Петр I), наводили свои порядки стрельцы, поговаривали о будущей войне с Крымом. Все слухи могли проникнуть за границу и вызвать там нежелательный резонанс. Поэтому правительство приняло решение о введении гласной почтовой цензуры писем, отправленных в западноевропейские страны, цензуры явной, а не тайной перлюстрации, которая широко применялась на почтовых дворах Западной Европы.

XVII, XVIII и первая половина XIX вв. вошли в историю криптографии как эра «чёрных кабинетов» – специальных государственных органов по перехвату и дешифрованию переписки. В штат « чёрных кабинетов» входили криптографы-дешифровальщики, агенты по перехвату почты, специалисты

по вскрытию пакетов, писцы-копировальщики, переводчики, граверы, специализировавшиеся на подделке печатей, химики, их наличие было необходимо из-за активного использования стеганографических методов защиты информации, так называемых невидимых чернил, специалисты по имитации почерков и так далее.

Таким образом, чёрные кабинеты состояли из высококвалифицированных специалистов в различных областях деятельности. Первый «светский» «чёрный кабинет» (без криптоаналитической составляющей) был организован по приказу императора Священной Римской империи Максимилиана I в первом десятилетии XVI века, это была одна из первых в Европе служб перлюстрации почтовой корреспонденции, которую можно считать прародительницей всех европейских «черных кабинетов». Что касается Ватикана то подобные службы, работавшие на папский престол, в составе которых были и дешифровальщики, появились ещё ранее.

Во все времена дешифровальщики тесно сотрудничали со специалистами по перехвату и перлюстрации (тайное и безуликовое ознакомление с содержанием переписки), без перехвата нет дешифрования. До изобретения во второй половине XIX века электрических способов передачи информации (телеграф, телефон, радио) существовало два основных способа передачи сообщений – почта и специальные курьеры. Первый способ был дешевле и быстрее, но менее безопасным, «чёрные кабинеты» располагались, как правило, именно на почтамтах. Для защиты информации помимо шифрования использовались физические методы, конверты тщательно опечатывались сургучными и восковыми печатями, прошивались по контуру нитками, часто вместе с письмом в конверт вкладывался некий специальный знак (например волос) при вскрытии целостность этого знака нарушалась (тот же волос выпадал из конверта) и адресат мог понять что с письмом уже кто-то ознакомился. С курьерами было

ещё сложнее – их надо было подкупить, напоить, усыпить, а иногда даже убить, чтобы добыть секретную депешу.

Российские дипломаты имели некоторые сведения о возможностях «черных кабинетов» по перлюстрации дипломатической переписки и пускались на различные ухищрения, чтобы противодействовать этой деятельности. Так, например, посол России в Турции граф Н. П. Игнатьев (о нем упоминалось при описании примеров шифров, используемых во время русско-турецкой войны 1877–1878 гг .) знал о том, что посольская переписка перехватывается. Это было видно по внешним признакам получаемых пакетов. Кроме того, по внешним признакам письма, его объему, качеству пакета (конверта), почерку, запаху, можно было судить о важности корреспонденции. «Тонкий запах», высококачественный конверт, почерк посла вызывали настороженность специальных почтовых чиновников Турции. Поэтому посол прибегнул к следующему приему. Конверт был «простейшего» качества (очень дешевый), адресацию писал его лакей (якобы отправляя письмо своему знакомому или родственнику); само письмо несколько дней выдерживали рядом с открытой бочкой, в которой находилась соленая селедка. Запах от письма появлялся специфический, свойственный людям «низшего» сословия. Этот прием себя оправдал. Послания Игнатьева по внешним признакам не перехватывались.

В начале XIX в. в России была произведена реорганизация органов управления страной. Манифестом Александра I вместо коллегий учреждались министерства. В частности, было организовано МИД, руководителем которого был назначен граф А.Р. Воронцов. Канцелярия МИД содержала четыре основные экспедиции и три секретные. Первая секретная – цифирная (шифровальная), вторая – цифирная (дешифровальная), третья – газетная (служба перлюстрации). Позднее экспедиции стали называться отделениями.

«Черный кабинет» России, сосредоточенный в основном в МИД, совершенствовал методы, технику перехвата и перлюстрации сообщений

иностранных государств. На почтамтах были созданы профессиональные службы по перехвату и перлюстрации дипломатической переписки, разрабатывались методы быстрого копирования, перлюстрации без улик (подделка печатей и др.), оперативного ознакомления с содержанием сообщений и передачи их дешифровальным органам. За успехи в этой работе императоры щедро награждали подчиненных, так, например, один из чиновников «черного кабинета», который изобрел новый эффективный метод подделки печатей и аппарат для вскрытия конвертов паром, высочайшим указом был награжден орденом Святого Владимира 4-й степени «за полезные и применимые в деле открытия».

Обычно шифры классифицировались на общие и индивидуальные. Общие шифры предназначались для нескольких корреспондентов, как правило, расположенных в одном географическом регионе. Они обеспечивали им связь между собой и с «центром». Индивидуальный шифр предназначался исключительно для связи с центром. Идея такого разделения возникла еще при Екатерине II.

2.3.Организация защиты информации в XIX веке

Во второй половине XIX в. произошли революционные изменения средств передачи информации. Стали использовать телеграф, а с начала XXв. – радио.

Первая правительственная линия оптического телеграфа между Петербургом и Кронштадтом протяженностью 30 км бы-ла оборудована французским инженером Ж. Шато в 1833 г. Зимний дворец в 1835 г. получил прямую оптическую телеграфную связь с Царским Селом и Гатчиной. Тогда же международные события побудили русское правительство выделить средства для строительства линии оптического телеграфа от Петербурга до Варшавы. Линия протяженностью 1200 км, построенная в конце 1838 г., имела 149 промежуточных станций, через которые сигнал проходил за 15

мин. Правительственная шифрованная депеша, состоявшая из 45 сигналов, передавалась из Петербурга в Варшаву за 22 мин.

Оптический телеграф просуществовал в России около полувека примерно до середины 1850- х гг. Он сыграл значительную роль в развитии внутренних коммуникаций как средство оперативного управления исполнительными органами государства в мирное и военное время.

Однако более значительные перспективы давало использование электрического телеграфа. 21 октября 1832 г. в Петербурге состоялась публичная демонстрация электромагнитного телеграфного аппарата П. Л. Шиллинга фон Канштадта.

Увеличение количества линий связи приводило к необходимости разрабатывать новые шифры и коды, удобные для закрытия секретной информации, передаваемой с помощью телеграфа.

Следующий важнейший этап развития электрических средств связи начался с момента изобретения телефона. Его придумал американец А.Г. Белл в 1876 г. В России интерес к телефонной связи возник сразу после того, как стало известно об изобретении. Это было новое и эффективное средство управления. Первый телефонный разговор в России состоялся в ноябре 1879 г. между Петербургом и Малой Вишерой. В 1881 г. развернулось строительство телефонных станций в Петербурге.

К началу XX в. существовавшие электрические средства связи уже не в полной мере удовлетворяли потребности управления страной и вооруженными силами. Основная проблема заключалась в том, что для использования телеграфа и телефона необходимо протягивать кабель, по которому проходит сигнал. Впервые проблема передачи электрического сигнала без проводов была решена в России, где был создан беспроволочный телеграф – радио.

Таким образом, беспроволочный телеграф, несмотря на свою историческую молодость, еще до начала XX в. обратил на себя внимание

государственных и военных специалистов как наиболее перспективное средство связи с очень широкой предполагаемой областью применения.

Возможность быстрой передачи шифрованных сообщений на большие расстояния, а также возможность перехвата сообщений в пунктах передачи, приема и по пути следования депеш обусловливали рост криптографических отделов и отделений с привлечением на эту службу большого количества телеграфистов, радиотехников, лингвистов, математиков.

В конце XIX – начале XX вв. Россия активно использовала возможности подкупа иностранцев, имевших доступ к шифрам, кодам, шифрованной переписке. Особо важная корреспонденция иностранных дипломатов не отправлялась по почте, а обычно упаковывалась в специальные портфели с секретными замками и отправлялась к месту назначения с особыми курьерами. В результате она не попадала в «черный кабинет» и не могла быть перлюстрирована. В этих случаях приходилось прибегать к подкупу.

Подводя итог, отметим, что развитие криптографии и связи в России в XIX в. отвечало мировому уровню. Однако в организации шифровального дела имелись существенные недостатки, основными были длительные сроки действия ключей и использование ключей после их компрометации [33].

2.4.Организация защиты информации в XX веке

Уже в первые годы 20 века все крупные мировые державы начали подготовку к войне, напряжено наблюдая за тем, что делают потенциальные союзники и противники. В мирное время немногочисленные аппараты спецслужб «охотились» за мобилизационными планами, новинками военной техники и информацией о приготовление к будущей войне.

Как следствие этого, в военном ведомстве начались активные действия по созданию и совершенствованию системы по защите военной тайны. Работа велась по четырём направлениям:

1. Создание и совершенствование системы контрразведывательных органов. Их основной задачей являлось противодействие шпионажу противника в мирное и военное время.

2. Организация комплексной системы защиты информации, содержащей военную тайну.

3. Совершенствование системы фельдъегерской связи.

4. Организация военной цензуры.

2.4.1. Первая Мировая война.

Когда началась первая мировая война, то выяснилось, что армия и вместе с ней и государство, не способны обеспечить необходимый уровень защиты военной тайны. И как следствие этого, население не было готово активно помогать органам контрразведке.

И только 22 июня 1914 года газета “Русский инвалид” опубликовала обращение к гражданам Российской империи. Это было первая попытка выразить мнение властей об отношение к защите военной тайны в Российской империи. В нём власти призывали население хранить в тайне информацию о дислокации, перемещение и численности войск. Население призывали не верить различным слухам и сохранять спокойствие. Правительство обещало информировать о реальной обстановке на фронте.

К сожалению, время было упущено. Волна шпиономании, захлестнувшая Россию, как и другие европейские страны, не способствовало активизации мероприятий по защите военной тайны.

Самым опасным во время боевых действий считался перехват донесений и распоряжений противником. В качестве меры противодействия рекомендовалось посылать несколько экземпляров донесения для повышения вероятности доставки его адресату.

В отношение полевого телеграфа указывалось, что противник может только разрушить линии связи. О возможности съема информации с провода

или использование линий телеграфа противником в качестве средства оперативной связи ничего не говорилось.

В период первой мировой войны при Штабе верховного главнокомандующего, штабах фронтов и армий были сформированы специальные контрразведывательные отделения, которые развернули активную деятельность по выявлению и уничтожению вражеской агентуры.

В конце 1916 года во всех союзнических странах (Англия, Франция и Россия) были учреждены контрольные бюро, цель которых - обмен сведениями о лицах, заподозренных в военном шпионстве. Такое контрольное бюро в составе Особого Делопроизводства Отдела Генерал-Квартирмейстера в 1917 году называлось военно-регистрационным бюро.

До первой мировой войны, ни в одной стране мира, кроме Франции и Австро - Венгрии, не существовало военных дешифрованных органов. И созданное в ноябре 1911 года при Генштабе Австро-венгерской армии криптографическое бюро во главе с капитаном Андрашим Фиглем безуспешно пытались взломать русские дипломатические и военные криптосистемы.

Правда, ситуация резко изменилась в период первой мировой войны. Тогда дешифрованная служба Австро - Венгрии искусно вскрывало русские криптографические системы из за бесчисленных недоразумений связанных с военной мобилизацией в России.

Начальник армейского шифровального бюро полковник Андреев вплоть до последней минуты перед началом боевых действий воздерживался от рассылки копий новых шифров, предназначенных для использования в период войны. Эта мера привела к печальным последствиям.

К этому надо добавить, что материальное снабжение армий было налажено из рук вон плохо.

При таком беспорядке в начале войны неоднократно случалось, что радиостанции, прибывшие на фронт и принадлежавшие различным радиоподразделениям, не могли обменяться шифрованными сообщениями по

той простой причине, что отдельные радиороты снабжали свои радиостанции собственными шифрами.

Поскольку на один и тот же участок фронта могли попасть радиостанции разных рот, то в первые же дни войны выяснилось, что радиостанции, приданные одному и тому же армейскому корпусу или кавалерийской дивизии, говорят на разных шифроязыках.

А поскольку одна радиостанция не понимала другую, то при отсутствии надежной проволочно-телеграфной связи приходилось повторять шифрсообщение открытым текстом.

Но самый трагичный момент для русской армии наступил в августе 1914, когда в результате катастрофы у Мазурских озер из армии Раненкампфа сумело вырваться из окружения менее 2 тысяч человек.

Как писал Гофман, один из разработчиков этой операции в книги “Война упущенных возможностей”: “Русская радиостанция передала приказ в незашифрованном виде, и мы перехватили его. Это был первый из ряда других бесчисленных приказов, передававшихся у русских в первое время с невероятным легкомыслием ... Такое легкомыслие очень облегчало нам ведение войны на востоке, иногда лишь благодаря этому и вообще возможно было вести операции”. Сказано ясно. Перехват незашифрованных сообщений русских войск позволил немцам одержать победу в первой битве в мировой истории, на исход которой решающим образом повлияла несостоятельность в вопросах криптографии.

Хотя в начале войны Россия в начале войны испытывала большие трудности в обеспечение своих войск всем необходимым, в том числе и средствами связи, уже в первой половине сентября 1914 года ей удалось полностью снабдить их шифровальными средствами. 14 сентября 1914 года Ставка Верховного главнокомандующего отдала распоряжение о том, что все военные приказы подлежат зашифрованию.

Принятая шифросистема основывалась на многалфавитном шифре цифровой замены, в котором допускалась зашифрование несколько букв подряд по одному алфавиту.

Но уже 19 сентября молодой одаренный начальник русского отделения дешифрованной службы Австро - Венгрии капитан Герман Покорный вскрыл эту систему.

Дело в том, что такие шифросистемы не представляли непреодолимых преград для криптоаналитиков, поскольку в шифротексте зачастую сохранялась структура часто встречающихся в открытом тексте слов, таких как “атака”, “дивизия”, которые шифровали одной строкой таблицы.

К тому же поначалу русские связисты нередко вставляли открытый текст в шифрованный. Вскоре одновременное использование открытых и шифрованных текстов в сообщениях было запрещено, но было уже слишком поздно, и оно сыграло свою негативную роль.

И уже 25 сентября криптосистема была взломана окончательно.

О том, что криптосистема окончательно скомпрометирована русские догадались только 19 октября. До этого дня большинство приказов принимаемых германским командованием основывались на данных радиоперехвата. И это не случайно. Порой русские сами сообщали наиболее уязвимые места в своей обороне.

Чтение русских криптограмм позволило странам германского блока принимать время от времени такие меры, которые были единственно правильными тактическими решениями в данной ситуации. Российский Генеральный был озадачен прозорливостью противника.

Однажды немцы оставили занимаемые ими позиции за два дня до начало большого наступления русских войск. Одним из объяснений точного соответствия решений германского командование создавшиеся обстановке русские считали им аэрофотосъемки.

Но постепенно крепло убеждение, что противник читает русскую шифропереписку. Когда немецкое весеннее наступление второго года войны

достигло апогея, русские опять сменили шифр. Но эта смена доставила больше хлопот им самим. Почти все шифровки, переданные по радио в первые два дня после смены шифров, из - за допущенных ошибок, так и не были прочитаны адресатами.

В июне 1916 года вновь произошло изменение способа шифрования - русские ввели свой первый код. Возможно, это было сделано под влиянием Франции, которой из дешифрованных немецких криптограмм стало известно, что немцы читают русские шифрособщения, или под воздействием собственной службы радиоперехвата, которая начала функционировать в 1916 году.

Нарастающая дезорганизация русской армии оказывало отрицательное влияние и на службу связи. Пропорционально снижению дисциплины в войсках росла и болтливость радистов.

В начале 1917 года только в течение одного дня австрийская дешифровальная служба прочла более 300 русских шифротелеграмм, из чего следовало, что служба обеспечения связи России быстро развалилась.

Наличие слабых военных шифров, недостаточно продуманных инструкций к ним, большое количество нарушений шифродисциплины - все это в совокупности вело к тому, что русские шифры успешно раскрывались австрийскими и немецкими специалистами.

Правда проблемы с перехватом сообщений передавааемым по телеграфу возникли ещё в русско японскую войну. Если донесения в осажденный Порт-Артур шифровали, то по телеграфу информация передавалась в открытом виде.

И более того, уже в 1904 японские спецслужбы, впервые в истории радиотехнической разведки, реализовали на практики схему дистанционного съема акустической информации. Они использовали схему микрофон - кабель - приемник (наблюдатель).

Только в 1915 году в российской прессе прошло сообщение о том, что во время боевых действий в период русско-японской войны были случаи

перехвата телеграфных сообщений, которыми обменивалась Ставка главнокомандующего и войска.

2.4.2. Вторая мировая война.

К июню 1941, когда немецкие армии вторглись на территорию СССР, система защиты государственной тайны СССР была практически полностью сформирована. Она успешно выполняла целый ряд поставленных перед ней задач. От любых иностранных разведок надежно защищались все информационные ресурсы: мобилизационные, технические, военные, политические, идеологические и природные. Была организована бесперебойная поставка сведений о состоянии и положении военных, политических и экономических дел других государств. Производилась тотальная дезинформация противника о ситуации в СССР. Был установлен жесткий контроль над информацией, которая публиковалась в СМИ.

Уже 24-го июня, всего через 2 дня после начала Великой Отечественной войны, было создано «Совинформбюро», задачей которого было составление сводок для газет и радио о положение дел на фронте. Тогда же стала применяться практика «дезинформации населения», которая заключалась в замалчивании успехов противника на фронте и преувеличении результативности военных действий Рабоче-Крестьянской Красной Армии (РККА). Такой способ дезинформации способствовал сплочению населения СССР и уменьшал вероятность возникновения паники среди жителей прифронтовых районов.

Одна из важнейших ролей в информировании отводилась тогда проводному радио, по которому население и узнавало о достижениях армий на всех фронтах. В течение войны количество выпускаемых печатных изданий было сокращено практически в два раза, в печать выходило всего 18 газет. Был прекращен выпуск множества специализированных и отраслевых изданий, существенно сократился выпуск местной прессы. Тем не менее, все чаще стали появляться новые издания фронтовых газет всех уровней: бригадных, стрелковых и танковых.

Не стояло на месте и развитие технической защиты информации. Еще несколько лет назад повсеместно применялись ручные методы шифрования, которые занимали огромное количество времени и были недостаточно эффективны. Так, шифрование небольшого приказа занимало до 6 часов работы, примерно столько же требовалось на то, чтобы расшифровать полученное сообщение.

Однако, уже в 1937 году в Ленинграде на заводе «209», был образован комбинат техники особой секретности. Его основной задачей стало создание шифровальной техники для скрытого управления войсками. В этом же году на заводе были собраны первые опытные экземпляры шифровальной машины В-4, а в 1938 году началось серийное производство данных шифраторов. В 1939 году шифровальная машина была модернизирована, получила название М-100 и стала выпускаться параллельно с В-4. Основным недостатком этих машин был их огромный вес. Устройство весило 141 килограмм.

На смену М-100 пришла машина М-101, которая была в 6 раз меньше своей предшественницы и в несколько раз легче ее. Также были достигнуты успехи в разработке и выпуске компактных шифровальных машин.

В 1939 году была запущенна в серийное производство шифровальная машина К-37 «Кристалл», которая упаковывалась в ящик весом всего 19 килограмм. К началу войны на вооружение шифрорганов СССР было принято свыше 150 комплектов шифровальных устройств К-37. Это позволило значительно повысить скорость обработки шифрограмм, и к тому же улучшить криптостойкость.

В годы войны на машинную шифросвязь легли огромные нагрузки. Только шифровальной службой РККА (8-й отдел) за период войны было отработано 1,5 миллиона шифротелеграмм и кодограмм. Очень часто сотрудникам управления приходилось обрабатывать до 1500 шифрограмм в день, тогда как суточная норма составляла всего 400 шифрограмм. За все

время войны 8-е управление Генштаба разослало нижестоящим подразделениям и войскам почти 3,3 миллиона комплектов шифров.

2.4.3. Этапы развития системы защиты информации в настоящее время.

За истекшее после возникновения необходимости в обеспечении защиты информации время существенно изменилось как представление о ее сущности, так и методологические подходы к решению. Указанные изменения происходили постепенно и непрерывно, поэтому всякая периодизация этого процесса в значительной мере будет носить искусственный характер. Тем не менее, весь период активных работ по рассматриваемой проблеме в зависимости от подходов к ее решению довольно четко делится на три этапа.

Начальный этап защиты (60-е — начало 70-х гг.) характеризовался тем, что под защитой информации понималось предупреждение несанкционированного ее получения лицами, не имеющими на то полномочий. Для этого использовались формальные, функционирующие без участия человека средства. Наиболее распространенными в автоматизированных системах обработки данных (АСОД) в тот период были проверки по паролю прав на доступ к электронно-вычислительной технике (ЭВТ) и разграничение доступа к массивам данных. Эти механизмы обеспечивали определенный уровень защиты, однако проблему в целом не решали, поскольку для опытных злоумышленников не составляло большого труда найти пути их преодоления. Для объектов обработки конфиденциальной информации задачи по ее защите решались в основном с помощью установления так называемого режима секретности, определяющего строгий пропускной режим и жесткие правила ведения секретного документооборота.

Этап развития (70-е — начало 80-х гг.) отличается интенсивными поисками, разработкой и реализацией способов и средств защиты и определяется следующими характеристиками: постепенным осознанием необходимости комплексирования целей защиты. Первым итогом на этом пути стало совместное решение задач обеспечения целостности информации и предупреждения несанкционированного ее получения; расширением арсенала используемых средств защиты, причем как по их количеству, так и по их разнообразию. Повсеместное распространение получило комплексное применение технических, программных и организационных средств и методов, которое проявлялось в следующем:

1. Постепенное осознание необходимости комплексирования целей защиты. Первым итогом на этом пути стало совместное решение задач обеспечения целостности информации и предупреждения несанкционированного ее получения.

2. Расширение арсенала используемых средств защиты, причем как по их количеству, так и по их разнообразию. Повсеместное распространение получило комплексное применение технических, программных и организационных средств и методов. Широко стала практиковаться защита информации путем криптографического ее преобразования.

3. Все более целенаправленное объединение всех применяемых средств защиты в функциональные самостоятельные системы.

Например, только для решения режимных задач, имеющих право пользования конфиденциальной информацией, разрабатывались следующие *методы и средства идентификации лиц:*

- традиционные пароли, но по усложненным процедурам;
- голос человека, обладающий индивидуальными характеристиками;
- отпечатки пальцев;
- геометрия руки, причем доказано, что по длине четырех пальцев руки человека можно опознать его с высокой степенью надежности;
- рисунок сетчатки глаза;

– личная подпись человека, причем идентифицируемыми характеристиками служит графика написания букв, динамика подписи и давление пишущего инструмента;

– фотография человека.

Широко стала практиковаться защита информации путем криптографического ее преобразования; целенаправленным объединением всех применяемых средств защиты в функциональные самостоятельные системы.

Однако механическое нарастание количества средств защиты и принимаемых мер привело в конечном итоге к проблеме эффективности системы защиты информации, учитывающей соотношение затраченных на создание этой системы средств, к вероятным потерям защищаемой информации. Для проведения такой оценки необходимо применять основные положения теории оценки сложных систем. Кроме того, к концу второго периода математически было доказано, что обеспечить полную безопасность информации в системах ее обработки невозможно. Максимально приблизиться к этому уровню можно, лишь используя системный подход к решению проблемы. Другими словами, успешное решение проблемы комплексной защиты информации требует не только научно обоснованных концепций комплексной защиты, но и хорошего инструментария в виде методов и средств решения соответствующих задач. Разработка же такого инструментария, в свою очередь, может осуществляться только на основе достаточно развитых научно-методологических основ защиты информации.

Таким образом, характерной особенностью *третьего, современного этапа (середина 80-х гг. – настоящее время)* являются попытки аналитико-синтетической обработки данных всего имеющегося опыта теоретических исследований и практического решения задач защиты и формирования на этой основе научно-методологического базиса системы защиты информации. Основной задачей третьего этапа является перевод процесса защиты информации на строго научную основу, а также разработка целостной теории защиты информации. К настоящему времени уже разработаны основы теории

защиты информации. Формирование этих основ может быть принято за начало третьего этапа в развитии защиты информации.

Принципиально важным является то, что российские специалисты и ученые на данном этапе внесли существенный вклад в развитие основ теории защиты информации, чему способствовал бурный рост интереса к этой проблеме в высшей школе.

Контрольные вопросы

1. Каким образом передавались сообщения в Древней Руси, и как осуществлялась их защита?
2. С какой целью была учреждена ямская гоньба?
3. Кто из правителей лично проводил криптоанализ некоторых русских шифров для оценки их стойкости?
4. Кто входил в штат «чёрных кабинетов»?
5. Назовите основную причину, по которой в конце XIX – начале XX вв. Россия активно использовала возможности подкупа иностранцев, имевших доступ к шифрам, кодам, шифрованной переписке?
6. Назовите основные направления по созданию и совершенствованию системы по защите военной тайны в начале XX века.
7. Было ли у России преимущество в Первой мировой войне в отношении криптографии? Почему?
8. Когда и с какой целью было создано было создано «Совинформбюро»?
9. Назовите основные этапы развития защиты информации в послевоенное время.
10. Охарактеризуйте третий этап развития защиты информации.

ГЛАВА 3
ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКИЕ ПРОТИВОБОРСТВА И ИНФОРМАЦИОННЫЕ ВОЙНЫ

3.1. Информационно-психологическое воздействие

Информационное воздействие - это организованное целенаправленное применение специальных информационных средств и технологий для внесения деструктивных изменений в сознание личности, социальных групп или населения (коррекция поведения), в информационно-техническую инфраструктуру объекта воздействия и (или) физическое состояние человека. Информационное воздействие стоит делить на информационно-техническое и информационно-психологическое.

Информационно-техническое воздействие (ИТВ) - это влияние на информационно-техническую инфраструктуру объекта с целью обеспечения реализации необходимых изменений в ее функционировании (остановка работы, несанкционированный доступ к информации и ее искажение (искажение), программирование на определенные ошибки, снижение скорости обработки информации), а также влияние на физическое состояние человека. ИТВ представляет угрозу безопасности информационно-технической инфраструктуры и физическому состоянию человека.

Безопасность информационно-технической инфраструктуры это состояние защищенности, который обеспечивает ее эффективное использование и защиту от возможного ИТВ.

Безопасность информационно-технической инфраструктуры делится на безопасность:

- машинно-технических средств (автоматизированных систем и сетей);
- программного обеспечения;
- режима защиты от несанкционированной утечки информации.

Информационно-психологическое воздействие (ИПсВ) - это воздействие на сознание и подсознание личности и населения с целью внесения изменений в их поведение и мировоззрение. Базовыми методами ИПсВ является убеждение и внушение. Убеждение направлено к собственному критическому восприятию действительности объектом воздействия. Оно имеет определенные алгоритмы воздействия:

– логика убеждения должна быть доступной для интеллекта объекта воздействия;

– убеждение следует осуществлять, опираясь на факты, известные о объекта;

– убедительная информация должна содержать обобщающие предложения;

– убеждение должна содержать логически непротиворечивые конструкты;

– факты, доносятся до объекта воздействия, должны иметь соответствующую эмоциональную окраску. Внушение, напротив, направлено на субъекты, которые некритически воспринимают информацию. Его особенностями являются:

– целеустремленность и плановость применения;

– конкретность определения объекта внушения (селективное влияние на определенные группы населения с учетом их основных социально-психологических, национальных других особенностей);

– некритическое восприятие информации объектом внушения (внушение основано на эффекте восприятия информации как инструкции к действию без ее логического анализа);

– определенность, конкретность поведения, инициируется (объекта необходимо дать инструкцию относительно его конкретных реакций и поступков, которые соответствуют цели воздействия).

Внушение или суггестия - это процесс воздействия на психику человека, связанный со снижением сознательности и критичности при восприятии навеянного содержания, не требующий ни развернутого личного анализа, ни оценки побуждения к определенным действиям. Суть внушения состоит в воздействии на чувства человека, а через них - на ее волю и разум.

Внушение является основным способом манипулирования сознанием, прямым вторжением в психическую жизнь людей. При этом манипулятивное воздействие организуется так, чтобы мнение, представление, образ непосредственно входили в сферу сознания и закреплялись в ней как данные бесспорные и уже доказанные. Это становится возможным при подмене активного отношения психики к предмету коммуникации преднамеренно созданной пассивностью восприятия.

ИПсВ направляется на индивидуальное или общественное сознание информационно-психологическими или другими средствами, что приводит к трансформации психики, изменению взглядов, мнений, отношений, ценностных ориентаций, мотивов, стереотипов лица с целью повлиять на его деятельность и поведение. Конечной его целью выступает достижения определенной реакции, поведения (действия или бездействия) личности, соответствующей целям ИПсВ.

Процесс восприятия индивидом ИПсВ, направленного на эмоциональную сферу сознания, специфический. В общем, он больше свернут, чем, например, процесс восприятия пропагандистского воздействия: в нем функционируют только восприятия и запоминания, деятельность мышления выражена достаточно слабо. Информацию личность воспринимает или не воспринимает, воспринимает полностью или частично, но в формировании определенных выводов практически не участвует. Процесс ИПсВ на эмоциональную сферу сознания включая произвольное восприятие и запоминание и характеризуется очень пониженным уровнем осознания смысла воздействия. Осмысление полученной информации происходит позже, при более высокой познавательной активности индивида.

Мощность и эффективность манипулятивного воздействия зависит от наличия определенных преимуществ у манипулятора над адресатом. Ранее уже отмечалось скрытый от адресата характер манипулятивного воздействия, сразу создает преимущества манипулятору. Есть и другие преимущества, которые позволяют манипулятору использовать специфические приемы воздействия и усиливает его эффект.

Уровень эффективности ИПсВ зависит от таких условий:

– содержания материала: его сложности, конкретности, общественной важности и тому подобное. Например, при равных условиях чем проще информация, тем больше шансов, что действия, на которые она побуждает, могут выполняться автоматически, особенно когда не противоречат убеждениям объекта. То есть, чем более конкретный призыв к действию, тем выше степень автоматизма ответной реакции;

– психического состояния, характеризующегося наличием высокого уровня автоматизма соответствующей реакции. Страх, подавленность, апатия способствуют некритическому и подсознательном восприятию воздействия. Степень автоматизма в ответе лица связан с уровнем осознанности и критичности восприятия информации. Если влияние воспринимается подсознательно и некритично, то ответ аудитории может быть автоматическим;

– временного интервала между воздействиями и соответствующей реакции: с увеличением временного интервала автоматизм реакции уменьшается вследствие повышения критичности и умственной активности объекта (объясняется включением содержания полученной информации в систему знаний лица и осознанием его).

Источники угроз информационно-психологической безопасности человека в межличностной коммуникации при осуществлении на нее манипулятивного воздействия целесообразно структурировать на три основные группы.

Первая группа включает угрозы, связанные с возможностями манипулятора влиять на сам процесс межличностной коммуникации. То есть, согласно к своей цели менять его ход, организацию, процедуру, информационное содержание, используя для этого определенные приемы.

Вторая группа объединяет угрозы, связанные с возможностями использования манипулятором внешних для адресата факторов, и делится на следующие подгруппы:

– условия внешней социальной среды (например, возможность использования других лиц для оказания влияния; социальных связей, сложившихся с адресатом и его окружением и т.д.);

– личный потенциал манипулятора (скажем, такие его статусные преимущества, как ролевая позиция, должность, возраст, материальное положение, квалификация, образование, способности, знания, коммуникативные навыки, умения и т.д.);

– условия внешней физической среды (выбор места и времени проведения межличностной коммуникации, создания соответствующей обстановки и т.п.).

Третья группа включает угрозы, связанные с возможностями использования манипулятором внутренних, психологических, индивидуально-личностных качеств адресата (в частности его состояния).

Применяя соответствующие приемы воздействия на различные психические структуры личности адресата, манипулятор достигает своей цели. В отличие от межличностного, манипулирование на политическом уровне обезличенное и предполагает воздействие на широкие массы. Воля меньшинства (а то и отдельной личности) в завуалированной форме навязывается большинству. Манипулирование сознанием является системой ИПсВ с целью внедрения в сознание определенного мировоззрения, ценностных установок, представлений о морали, нравственности, нормативность тех или иных форм поведения.

Для манипулирования используются такие методы, как искажение, сокрытие и способ представления информации. Искажение информации варьирует от откровенной лжи до частичных деформаций (подтасовка фактов или смещение в семантическом поле понятия).

Сокрытие информации скорее проявляется как замалчивание/сокрытие определенных тем. Гораздо чаще используется метод частичного освещения или дифференцированного представления материала. Способ подачи информации нередко играет решающую роль в том, чтобы содержание, которое передается, было воспринято так, как необходимо его отправителю.

Например, большое количество информации в "сыром" или несистематизированном виде позволяет заполнить эфир потоками незначительных сведений, что еще больше усложняет и без того безнадежные поиски индивидом их сути. Так же информация, представленная небольшими порциями, не дает возможности эффективно воспользоваться ею. В обоих случаях заранее снимается вопрос нарекания в сокрытии тех или иных сведений.

Сокрытие манипулятивного воздействия.

В литературе не раскрыто рефлексного различия между сокрытием факта манипулятивного воздействия, с одной стороны, и намерений манипулятора - с другой. Однако следует понимать, что наиболее тщательно скрываются именно намерения.

Средства принуждения.

Здесь речь идет о силе властных политических структур или средств массовой информации, а также о степени принуждения к силовому давлению, его неотвратимость, способы скрытого или явного принуждения, предпосылки силового давления. В отношении межличностного влияния в рамках официальных социальных структур обсуждается проявление сильной или слабой позиции. Так, "истинная" позиция строгого начальника, практикует тотальный контроль или часто обращается к явному использованию своей силы (преимущество по должности), расценивается как

слабая. То же касается и подчиненных: открытая конфронтация подчиненного по отношению к своему начальнику скорее означает слабость первого. И наоборот, косвенное запугивание или неявное (неформальное) насилие со стороны подчиненного является признаком слабости позиции начальника; это означает, что последний сделал какую-то ошибку.

Логика манипуляторов очевидна и закономерна однозначно: чем шире аудитория, на которую необходимо оказать влияние, тем более универсальными должны быть цели. Специализированность и точная направленность массового воздействия возможны тогда, когда его организатору известны специфические качества нужных слоев населения или групп людей. Соответственно, чем уже предполагаемая аудитория, тем точнее должна быть подстройка под ее особенности. В случаях, когда такая подстройка по каким-либо причинам не проводится, снова появляются универсальные возбудители: гордость, стремление к удовлетворению, комфорта, желание иметь семейный уют, продвижение по службе, известность - вполне доступные большинства людей ценности. Если же при этом что-то не срабатывает, то это можно рассматривать как неизбежную плату за исходную экономию.

Более "продвинутые" технологии манипулирования предусматривают предварительную подготовку мнений или желаний, закрепление их в массовом сознании или представлениях конкретного человека для того, чтобы можно было к ним потом апеллировать (например, создание мифа о заботливом президенте или респектабельность компании, убеждение партнера в том, что ему хотят помочь или ему угрожает небезопасность).

Роботизация.

Особо следует выделить лейтмотив роботоподобности, который заключается в том, что люди - объекты манипулятивной обработки – превращаются в марионеток, управляемых властными силами с помощью "ниточек" - средств массовой информации. На социально-ролевом уровне обсуждается зависимость подчиненных от давления организации,

преобразования служащих на "прислужников". На межличностном уровне внимание обращается на наличие запрограммированных действий в ответ на те или иные воздействия со стороны партнеров в общении.

Кроме использования готовых к "употреблению" программ стереотипного поведения, усилия манипуляторов направленные на унификацию способов мышления, оценки и реагирования больших масс людей, что приводит к деиндивидуализации и деперсонификации лиц, превращение их в податливых объектов манипулирования.

Виды изменений в индивидуальном сознании, которые может повлечь ИПсВ:

1. изменения психики, психического здоровья человека. Поскольку в случае информационного воздействия сложно определить границы нормы и патологии, показателем изменений может быть потеря адекватности по отражению мира в сознании и индивидуальном отношении к миру. Можно говорить о деградации личности, если формы отражения действительности упрощаются, реакции грубеют и осуществляется переход от высших потребностей (в самоактуализации, социальном признании) до низших (физиологических, бытовых)

2. изменения в ценностях, жизненных позициях, ориентирах, мировоззрении личности. Такие изменения вызывают антисоциальные поступки и представляют опасность для всего общества, государства.

ИПсВ создают угрозу информационной безопасности личности, общества и государства. Информационная безопасность личности и общества является составной информационной безопасности государства: ее обеспечение занимает особое место в государственной политике. Эта особенность определяется спецификой угроз и их источников, особым характером принципов и задач государственной политики в этой сфере. Объектом информационно-психологической защиты (ИПсЗ) лица является состояние его духовного и физического комфорта. Объект защиты составляют и условия, факторы, которые обеспечивают развитие всех сфер

жизнедеятельности человека и общества, в частности культуры, науки, искусства, религиозных и межнациональных отношений.

К объектам относятся также языковую среду, социальные, идеологические, политические ориентиры, общественные и социальные связи, психофизические факторы, проявляющиеся в виде физических, химических и других воздействий природного, антропогенного и техногенного происхождения; генофонд народов, входящих в состав населения государства и тому подобное.

Наиболее важными объектами ИПсЗ в современных условиях является индивидуальное и массовое сознание. Для личности главными системообразующими качествами выступают целостность (тенденция к устойчивости) и развитие (тенденция к изменению). При разрушении или искажении этих качеств личность перестает существовать как социальный субъект. Это означает, что любое ИПсВ на лицо должно оцениваться с позиции сохранения или разрушения ее целостности. Для эффективной ИПсЗ необходимо знать признаки, которые позволяют выявить манипулятивность информационного воздействия через СМИ.

Эти признаки можно разделить на организационные (присуща системность и организованность) и содержательные.

К организационным относятся:

1.Массовое привлечение специалистов со знанием языка государства - субъекта действия (журналистов, писателей, редакторов, теле-, радиоведущих и т.д.) иностранными субъектами.

2.Сосредоточенность компании (организации, государства, других субъектов) на информационном обеспечении собственной деятельности, а не на решении проблем (снимают сюжет о безопасности производства и замечательных условиях труда вместо того, чтобы выделить средства на утилизацию нечистот и очистные сооружения).

3.Наличие в структуре организации информационно-аналитических служб (пресс-центр, информационная служба, собственные издания, интернет-страница).

4.Наём специалистов из сферы пиара, редакторов информационных служб, известных телеведущих (talking heads) и др.

5.Трансляция и ретрансляция теле- и радиопрограмм (прежде всего информационных) иностранного производства.

6.Привлечение журналистов издания или телеканала к участию в тренингах, которые проводят иностранные общественные организации (в процессе подготовки к выборам популярны тренинги по анализу источников информации; обработка результатов социологических исследований; сбор информации о конкретных политиках; психологических аспектов формирования общественного мнения; специфики освещения экономической, социальной и политической тематики; технологий журналистских расследований и т.п.).

7.Получение финансовой помощи (в обмен на заказную направленность материалов).

8.Формирование собственного "agenda" - Перечень информационных сообщений будут освещены в СМИ, основных новостей, порядка их представления. Наглядной формой реализации этого организационного мероприятия является подготовка и распространение так называемых "темников" (государственных рекомендаций СМИ, которые содержат подробные инструкции относительно того, каким образом необходимо освещать в новостях политические события, чтобы власть была представлена в благоприятном свете).

9.Информационная изоляция или введение цензуры на информацию, которая попадает к субъекту.

10.Удержание до поры до времени (межгосударственные официальные переговоры, зарубежные визиты, выборы), нераспространение компрометирующей информации, которая стала известна СМИ.

11.Время выхода материалов – публикация материалов в то время, когда у ответчика нет возможности для ответа или когда этот ответ не будет услышан.

12.Информация с манипулятивными признаками синхронно появляется сразу в нескольких источниках (организовать это может только единый координационный центр). Известны случаи, когда материал с ссылкой на первоисточник выходил раньше, чем его обнародовал первоисточник.

13.Акцентирование внимания источником на событиях, которые являются заведомо конфликтными в государстве. Этот признак фиксируется путем сравнения количества повторов конфликтных тем в разных источниках информации (осуществляется по заранее определенным перечням конфликтных тем). Организация пресс-конференций с целью формирования собственного перечня информационных сообщений, освещаемых в СМИ.

14.Информация появляется в заранее определенных рубриках с негативным контекстом: "неудачник года", "разочарование года", "ссора года" ...

15.Обнародование информации через интернет, который содержит "специализированные" общедоступные сайты для "слива" компромата (например, reporter.com.ua, compromat.ru, informacia.ru, Regnum.ru, vlasti.net и т.д.).

16.Источником информации выступает лицо (организация), деятельность которой связана с иностранными спецслужбами.

17.Осветителем информации являются так называемые "шоумены от политики": скандально известные личности (Н. Шуфрич, В.Жириновский).

К содержательным признакам осуществления манипулятивного информационного воздействия относятся:

18.Растерянность, неопределенность, многовариантность и ужасно общий контекст информации. Любое лицо психологически стремится к стабильности, определенности, конкретных целей и безопасности. Путевой

камень с тремя вариантами выбора дороги ставил в тупик даже эпических богатырей.

19.Количество повторов ключевых слов, которые определяют суть сообщения и могут привязывать к тексту негативные штампы: фашизм, нацизм, коррупция, предательство, боль, террор и т. д.

20.Присутствие сенсации искусственного происхождения (взрывы, катастрофы, преступления и т.п., а не стихийные бедствия или явления природы).

21.Анонимность, использование псевдонимов авторами информации: " по сообщению нашего информированного источника "; "В кулуарах власти ходят слухи", "источник, пожелавший остаться неизвестным" ...

22.Ссылки на другой СМИ, а не на первоисточник информации: Как сообщает информагентство "Риа-нововсти": "…Сейчас все то же самое, только берут больше. Только ставка за риск увеличилась …", - сказал Президент о коррупции.

23.Использование мнения авторитетов: "как доказано учеными", "не соответствует мировым стандартам", "эксперты ФБР", "В то время как еще Аристотель (Маркс, Пушкин) отмечал" и другие. Ссылка на авторитеты используется, когда надо без рационального доказательства подтвердить свою позицию.

24.Использование готовых утверждений без аргументации (доказательства): "Россия лишена выходов в мировое информационное пространство", "у нас всегда так ...", "Россия отстает от развитых стран в развитии информационных технологий на несколько десятилетий",

25.Использование общеупотребительных штампов: "демократические страны", "мировой терроризм", "права человека", "клановo-олигархическая система", "антисемит", "бюрократ" и другие.

26.Оперирование так называемыми "идеальными понятиями": свобода, демократия, справедливость, порядочность, честность, истина, любовь, Родина, Бог, вера, святость, счастье. Джордж Буш в своей ежегодной речи в

Конгрессе в 2004 году 52 раза употребил слово "свобода" в разных сочетаниях, демаскируя истинный смысл послания, авторское прочтение которого ассоциируется с понятиями "преимущество" (primacy), "война", "агрессия", "новый мировой порядок ".

27.Несоответствие общего контекста информационного сообщения задекларированному названию.

28.Наличие неоднозначного факта, эффект которого пытаются смягчить, на общем положительном фоне (набожный, рассудительный, мудрый священник, имеющий уважение прихожан, помогает им, возрождает и оберегает помещения церкви от корыстолюбивых олигархов и ... благословляет однополые браки). Или же наоборот: представление положительного факта, лица на общем негативном фоне.

29.Освещение материала в виде диалога. Читатель (зритель, слушатель) выступает пассивным потребителем готовых идей, в то время как в процессе обсуждения потребитель информации подводится к нужному выводу.

30. Количество прилагательных по объему текста. Прилагательные придают тексту эмоциональной окрашенности, тогда как новости должны точно отражать факты, а не давать им эмоциональную оценку. Любое выступление, документ, решение можно охарактеризовать таким образом, что их текст будет иметь характер темного, страшного, агрессивного, а эти характеристики вызывают негативные эмоции. Вам нужно отрицательное отношение к нововведениям? -Напечатайте их черными буквами на красном фоне.

31.Использование метафор (поэтически, образно выражена мысль), гипербол (преувеличений), сравнений. Это, опять же, свидетельствует о субъективизме, эмоциональности (а не объективности) оценок.

32.Использование глаголов для обозначения умственной действия и его временных границ ("сосредоточиться", "представлять", "начинать", "заканчивать", "продолжать", "кажется" и т.д.).

33.Постановка вопросов, которые постепенно подводят читателя (зрителя, слушателя) к требуемой мысли: "Сколько средств бюджета США необходимо выделить на иракскую кампанию?" Вместо "Является ли иракская кампания легитимной? Поддерживают граждане эту кампанию?».

34.Использование псевдонаучных терминов (вроде "корреляция детерминированных дефиниций") приводит к потере внимания или даже отпугивания львиной доли аудитории.

35.Использование неологизмов (вновь слов).

36.Использование синонимов с нужным контекстом. Вместо "война" - "принуждение к миру", "миротворческая операция", "умиротворение"; вместо "блокада" - "эмбарго"; вместо "акции неповиновения", "бунт" - "проявления протестов" и другие. И наоборот.

37.Несоответствие содержания (текст, звук) и видеоряда: сообщения о деятельности радикальной политической группировке показывают на фоне картинки о столкновении в Северной Ирландии или террористической атаки 11сентября 2001г. Терроризм - это всегда плохо, значит, событие, о котором идет речь, - отрицательное.

38.Использование технического приема съемки снизу, известного как перспектива "Жабы", или показ объекта сверху (перспектива "птичьего полета"). Этот ракурс вызывает антипатию к объекту, создает впечатление слабости, позорности.

Положительная установка создается с помощью фронтальной съемки на уровне глаз, так как психологами доказано, что это вызывает симпатию к объекту, впечатление покоя, непринужденности.

39.Прямые указания в СМИ на желаемое для внешнего субъекта поведение.

40. Использование только части фактов из общего объема в нужном контексте.

Необходимо понимать, наличие только одного из признаков еще не предусматривает высокую вероятность того, что мы имеем дело с

манипулятивным информационным влиянием как составной спецоперации. Оценке подлежит соответствие информации сразу ряда признаков. Объективность и беспристрастность оценок на основе перечисленных критериев может обеспечить или коллектив специалистов-аналитиков, или применения математической теории вероятности.

Для оценки содержания текстовых сообщений широко используется контент-анализ (от англ. Content- содержание) - формализованный метод изучения текстовой и графической информации, который заключается в переводе изучаемой, в количественные показатели и ее статистической обработки [34].

3.2. Специальные информационные операции и акции информационного воздействия

Специальные информационные операции (далее - СИО) - это спланированные действия, направленные на врага, дружескую или нейтральную аудиторию путем воздействия на его сознание и поведение посредством использования определенным образом организованной информации и информационных технологий для достижения определенной цели.

Они помещают в себя психологические действия со стратегическими целями, психологические консолидирующие действия и психологические действия с непосредственной поддержки боевых действий. Они подразделяются на следующие виды:

– Операции, направленные против субъектов, принимающих решения.

– Операции, направленные на компрометацию, причинение вреда оппонентам.

– Операции, направленные на политическую (экономическую) дестабилизацию.

Следует иметь в виду, что СИО происходит на макро- и микроуровне. То есть, СИО макроуровня - это любая агитационно-пропагандистская и разведывательно-организационная деятельность, которая ориентирована на конкретные социальные группы людей и осуществляемая в основном через средства массовой информации и по каналам коммуникаций. СИО микроуровня, со своей стороны, олицетворяет любую агитационно-пропагандистскую и разведывательно-организационную деятельность идеологического характера, прицельно персонализированную и осуществляемую преимущественно через межличностное общение. Для этого часто используется деятельность, направленная на распространение слухов или возбуждения другими методами запланированного негативного поведения населения государства-объекта информационной войны.

Если же мы затрагиваем понятия СИО в контексте мероприятий политической разведки, то следует отметить, что с ее помощью должны решаться определенные политические проблемы, достигаться стратегические цели общества определенного государства или иного субъекта разведывательной деятельности. Для объекта, на который направлено СИО, должны наступить или образоваться угрозы или опасности возникновения негативных последствий. Итак, такое влияние на объект по своей сути является также отрицательным. Влияние, как таковой, применяется как к отдельной личности или группы лиц, так и на все общество в целом или определенный его социальный слой. Отсюда, в контексте информационной войны, СИО должно быть деятельностью, которая проводится, как правило, специальными органами иностранных государств или транснациональных структур (в последние годы даже частных лиц с мировым уровнем авторитета, капитала, потребностей и интересов), которые уполномочены субъектом информационной войны осуществлять подобную деятельность. То есть - это специальные службы, прежде всего разведывательные, которые применяются для достижения общей политической цели путем реализации оперативных задач.

Итак, СИО _- это проведение спецслужбами, прежде всего, иностранных государств тайных операций и акций негативного или даже деструктивного идеологического, идейно-политического и социального воздействия на личность, группу лиц или общество в целом с целью их переориентации на другие ценности и идеалы, подтолкнуть к совершению противоправных действий в направлении подрыва и ослабления государственного и общественно-политического строя для решения задач осуществления выгодного влияния.

Следует отметить, что СИО проводится путем распространения информации определенного рода (правдивой или ложной) различными способами. Это использование коммуникативных технологий по влиянию на массовое сознание с долговременными или кратковременными целями. Надо подчеркнуть, что СИО создает угрозу не столько своим существованием как явление вообще, а тем, что она "включает" и запускает в действие вещественно-энергетические процессы, а также контролирует их. Суть как раз и состоит в том, что она может возбуждать и направлять такие процессы, масштабы которых во много раз больше самой операции.

Именно этот вид информационной борьбы, как правило, направлен на переориентацию отдельных лиц, их групп или общества в целом на другие ценности и идеалы для ослабления политического и социально-политического устройства. В случае, когда меры непосредственного информационного подрыва является инструментом политической разведки, их цель также носит политический характер. Итак, СИО предполагает указано причинение вреда жизненно важным интересам в политической, экономической, научно-технической, социальной или любой другой общественной сферах жизни государства-противника и на этой основе осуществления выгодного влияния для получения преимуществ в той или иной области.

Рассмотрим теперь в каких конкретных формах осуществляется деструктивное влияние в процессе информационного противоборства и приемы и методы при этом используются.

Можно выделить следующие основные методы специальных информационных операций соответствующими структурами для осуществления скрытого выгодного влияния на иностранные государства с целью создания благоприятной политической, идеологической, социальной, экономической обстановки при реализации собственной правящей элитой внешнеполитического курса:

- дезинформации;
- пропаганда;
- диверсификация общественного сознания;
- психологическое давление;
- распространения слухов.

Рассмотрим более подробно каждую из форм, ее сущность, основные черты и виды.

Дезинформации - форма СИО, которая специализируется на обмане или введении объекта направлений в заблуждение относительно подлинности намерений для побуждения его к запрограммированных субъектом СИО действий.

Исторический опыт свидетельствует, что существуют различные методы проведения мероприятий по дезинформации, каждый из которых обычно имеет собственные положительные и отрицательные черты. Конкретный выбор того или иного метода напрямую зависит от оперативной обстановки, которая складывается на конкретном участке деятельности спецслужбы, стоящих перед ней поставлены и тому подобное. Чаще всего в мировой практике применяются следующие методы:

1. тенденциозное изложение фактов - вид дезинформации, который заключается в предвзятом освещении тех или иных фактов или другой информации о событиях с помощью специально подобранных правдивых

данных в определенные промежутки времени. Как правило, с помощью этого метода объекта направлений приходится дозировано, к постоянно растущему напряжения, и поддерживается в таком состоянии специально сформированная информация и поддерживается такой напряженное состояние объекта путем постоянного "подбрасывания" новых порций строго ограниченных и дозированных данных в среду информационного дефицита;

2. дезинформации от "обратной" - происходит путем предоставления правдивых сведений в искаженном виде или в такой ситуации, когда они воспринимаются объектом устремлений как лживые. В результате применения подобных мер возникает ситуация, когда объект фактически знает правдивую информацию о намерениях или конкретные действия противоположной стороны, но воспринимает ее адекватно, не готов противостоять негативному влиянию;

3. терминологическое "минировании" - заключается в искажении первичной правильной сути принципиально важных, базовых терминов и толкований общих мировоззренческого и оперативно-прикладного характера.

В обобщенном виде акции дезинформации могут проводиться путем создания видимости успехов разведки иностранных партнеров, использование средств массовой информации, включая собственные информационные агентства, теле-, радиокомпании, печатные издания и отдельных "карманных" журналистов, или же создание видимости случайной утечки закрытой информации.

Пропаганда - распространение различных политических, философских, научных, художественных, других художественных идей с целью их внедрения в массовое сознание общества и активизации, тем самым, использование этих идей в массовом практической деятельности населения. Одновременно, к пропаганде относятся сообщения, которые распространяются для осуществления выгодного влияния на общественное мнение, провоцирование запрограммированных эмоций и изменения

отношения или поведение определенной группы людей в направлении, прямо или косвенно выгодном организаторам.

По своей сути пропаганда делится на "белую", "серую" и "черную". Так, "белая" пропаганда представляет откровенно лояльную по объекту направлений позицию, которая проводится через любые СМИ по официальным каналам без утайки ее направленности и источники. "Серая" - нелояльная до адресата пропаганды, проводится через СМИ по официальным каналам, но с сокрытием ее источники и достоверной направленности. "Черная" - проводится по официальным каналам через оперативные возможности спецслужб от имени несуществующих или специально созданных под соответствующими легендами подпольных оппозиционных организаций.

Методы проведения пропаганды:

– пропаганда образа жизни (социологическая) - натуральный показ достижений, преимуществ, перспектив и т. д. конкретного государства;

– использование средств массовой информации и печатных научных и художественных изданий;

– Резонансная" - корректировка уже существующих мнений, а не формулировки и создание новых.

Психологическое давление - воздействие на психику человека путем запугивания, угроз с целью побуждения его к определенной запланированной модели поведения.

Методы психологического давления:

– доведение до объекта сведений о реальных или мнимые угрозы и опасности;

– прогнозы о репрессиях, преследований, убийств и т.д.;

– шантаж;

– осуществления взрывов, поджогов, массовых отравлений, захват заложников, других террористических или диверсионных акций.

Диверсификация общественного сознания - распыление внимания правящей элиты государства для решения различных искусственно акцентированных проблем и отвлечения тем самым ее внимания от решения насущных первоочередных задач общественно-политического и экономического развития, которые необходимы для нормального функционирования общества и государства.

Методы диверсификации общественного сознания:

– дестабилизация обстановки в государстве или отдельных ее регионах;

– активизация кампании против политического курса правящей элиты государства и отдельных ее лидеров в различных международных учреждениях;

– инициирование антидемпинговых кампаний и другого рода скандальных судебных процессов, применения международных санкций по другим причинам.

Распространение слухов - деятельность по распространению различной информации (как правило, ложной) среди широких слоев населения, в основном, по неофициальным каналам с целью дезорганизации общества и государства или же их отдельных учреждений или организаций.

Одно из толкований определяет, что слухи - это циркулирующая форма коммуникации, с помощью которой люди, которые находятся в неоднозначной ситуации, объединяются, образуя понятную им интерпретацию этой ситуации, совместно используя при этом собственные интеллектуальные возможности.

Слухи по своей характеристике является самораспространяемыми. Их природа базируется на такого рода информации, которую трудно удержать. Лицо обязательно должен рассказать об услышанном кому-то другому. Достаточно создать соответствующую слух и запустить ее в обращение в нужном месте в нужное время. "Человеческий шум" сделает остальных. Положительный фактор использования данной формы СИО заключается еще

и в том, что практически не существует эффективных средств противодействия слухам. На официальном уровне остановить их невозможно: официальные меры противодействия вызывают прямо противоположный эффект. Фактически это означает для людей, которых непосредственно интересуют эти слухи, подтверждения их правдивости. Чем больше попыток их опровергнуть, тем больше становится уверенность и обоснованность достоверности слухов. Единственно возможный вариант преодоления эффективности слухов - полное их игнорирование. Как правило, через некоторые время напряжение спадает, излишняя активность в обсуждении уже неактуальных новостей угасает, интерес к затронутой в слухах проблемы исчезает. Появление новых проблем полностью нейтрализует возможные опасные последствия для дезорганизации общества и государства.

Перечисленные выше формы и методы, условия их применения на определенном промежутке времени и территории, задачи, которые должны быть достигнуты при их применении, - обусловливают использование соответствующих сил и средств, способных проводить необходимые специфические меры непосредственного подрыва или предоставления скрытого выгодного влияния. В каждом отдельном случае они могут быть разными. Целесообразно подчеркнуть, что все тайные подготовительные действия и акции такого рода используются в политической разведке для создания необходимых условий проведения государственной политики по той или иной страны, международной структуры или внутренних оппозиционных кругов. А значит, если разведка поднята до такого высокого уровня, то в таком случае могут быть привлечены в качестве прикрытия ("подкрышевые структуры") практически все государственные ресурсы, включая неразведовательные государственные органы и учреждения, неправительственные организации (благотворительные и благотворительные организации, фонды поддержки демократических ценностей , организации

культурологической направленности и т.д.), подконтрольные субъекту разведывательной деятельности.

В разное время к осуществлению операций информационной борьбы привлекались различные силы с разной степенью организации и отношение к государственно-правительственных структур. В частности упоминалось, что специальные подразделения информационной (психологической) борьбы в структуре государственных органов появились только во время первой мировой войны в государствах-участниках последней. Дальнейшее опыт организации информационной борьбы показал, что силы, которые привлекаются к созданию необходимых благоприятных условий реализации политических и военных мер в рамках государственной внешней политики, могут относиться как к специально созданных подразделений специальных учреждений и организаций, так и к таким, которые не имеют в своих основных функциональных обязанностях задач взрывного характера.

Примером первой категории могут служить специальные подразделения войны, например, армии США (группы и отдельные батальоны психологической борьбы). На вооружении указанных подразделений сил специальных операций находятся передвижные теле- и радиоцентры, типографии, оборудование для проведения устных агитационных программ на личный состав и население иностранного государства, соответствующие технические средства: так называемые "агитационные" снаряды, бомбы, воздушные шары и т.д., с помощью которых забрасываются на территорию противника и распыляются спецпропагандические печатные материалы (листовки, газеты, брошюры и т.д.).

Наличие подобных средств позволяет указанным подразделениям за короткий промежуток времени наладить целенаправленную работу по осуществлению выгодного идеологического и психологического воздействия на противника на определенных театрах военных действий в ходе проведения различных специальных или непосредственно военных операций

вооруженными силами США. Наглядными примерами оперативной деятельности подразделений специального назначения США могут служить события в годы "холодной войны" вокруг СССР (1945-1991 гг.), ГДР (1953-1954 гг.) Венгрии (в 1956 г..), Чехословакии (1968г.), Польши (1968, 1980-1982 гг.), Румынии (1985-1990 гг.) которые разворачивались по сценарию руководства Соединенных Штатов в направлении свержения коммунистических режимов.

Целесообразно отметить, что в последнее время наблюдается постоянно растущая активность неправительственных структур, также задействованные в осуществлении выгодного психологического воздействия с целью создания благоприятных политико-идеологических условий в государстве-объекте воздействия.

К указанных организаций и учреждений относятся разного рода миссионерские религиозные структуры, навязывают чужие для нашего народа культы, верования и вероучения, нередко даже противоправным путем с использованием методик и технологий нейропсихического программирования, гипноза, с применением наркотических и психотропных веществ, которые подавляют волю человека.

Активно действуют также организации и лица, участвующие в гуманитарных программах сотрудничества между государствами: культурные и образовательные центры, ассоциации, фонды и др. Под видом просветительских акций они занимаются идеологической обработкой, агитацией и пропагандой собственного образа жизни как единственно верного, распространяют слухи о невозможности положительных сдвигов в государстве без существенных изменений социально-политического строя и т. Как правило, координацией подобной деятельности указанных организаций и учреждений занимаются культурно-гуманитарные, научно-технические отделы при посольствах и консульствах иностранных государств и других дипломатических представительствах международных организаций.

С целью организации противодействия СИО, необходимо знать факторы, способствующие возникновению рисков, угроз и опасностей в идеологически-информационной области государства, выяснить их сущность, уметь оценивать и определять реальность и уровень негативного воздействия на общество и государство.

К главным факторам, которые влияют на состояние морально-идеологической стабильности и безопасности в государстве, относятся:

– отсутствие целостной системы информационно-аналитического обеспечения органов государственной власти и управления;

– разрушения интеллектуального потенциала, неготовность существующей системы образования к поддержанию процессов опережающего развития государства;

– медлительность процесса осознания прослойкой бывшей советской партийно-хозяйственной номенклатуры, научной и творческой интеллигенции, ростков новой буржуазии своего места в обществе и формирование собственно элиты, что приводит к невозможности сформировать правящими кругами понятной и привлекательной для общества национальной идеи;

– низкий общий уровень развития информационной инфраструктуры, что не исключает возможность экспансии иностранных компаний на рынке информационных услуг; разрушения национального информационного пространства и возникновения возможности его использования в антигосударственных интересах;

– недостаточный профессиональный, интеллектуальный и творческий уровень отечественных производителей информационного продукта и услуг, их неконкурентоспособность на мировом информационном рынке;

– информационная экспансия со стороны ведущих иностранных государств; разработка и использование ими, международными или отечественными преступными организациями различных современных способов непосредственного подрыва, в частности СИО;

– малоконтролируемая деятельность отдельных политических сил, СМИ и лиц, которая направлена на разрушение нравственных ценностей, сознания, подрыв морального и физического здоровья нации; использование средств массовой информации с позиций, противоположных интересам граждан, политических и общественных организаций, государства; манипулирование информацией (дезинформация, искажение фактографических данных, замалчивание истинных сведений и т.п.);

– потеря доверия к власти со стороны значительной части населения вследствие распространения компромата, применение грязных политических технологий, особенно во время избирательных кампаний;

– навязывание путем информационно-психологического воздействия на сознание и подсознание, применением различных информационных ресурсов и социотехнических систем лицам, обществу желательных для иностранцев решений определенных вопросов в жизненно важных сферах общественной и государственной жизни;

– конкурентная борьба за обладание СМИ, процесс их монополизации и концентрация в их пределах информационной и политической власти [35].

3.3. Информационные войны

На концептуальном уровне можно сказать, что государства стремятся приобрести информации, обеспечивающую выполнение их целей, воспользоваться ей и защитить ее. Эти использование и защита могут осуществляться в экономической, политической и военной сферах. Знание об информации, которой владеет противник, является средством, позволяющим усилить нашу мощь и понизить мощь врага или противостоять ей, а также защитить наши ценности, включая нашу информацию.

Информационное оружие воздействует на информацию, которой владеет враг и его информационные функции. При этом наши информационные функции защищаются, что позволяет уменьшить его волю

или возможности вести борьбу. Поэтому дадим определение **информационной войне** (ИВ) - это любое действие по использованию, разрушению, искажению вражеской информации и ее функций; защите нашей информации против подобных действий; и использованию наших собственных военных информационных функций.

Это определение является основой для следующих утверждений.

Информационная война - это комплексное совместное применение сил и средств информационной и вооруженной борьбы.

Информационная война - это коммуникативная технология по воздействию на информацию и информационные системы противника с целью достижения информационного превосходства в интересах национальной стратегии, при одновременной защите собственной информации и своих информационных систем.

Информационная война - только средство, а не конечная цель, аналогично тому как бомбардировка - средство, а не цель. Информационную войну можно использовать как средство для проведения стратегической атаки или противодействия.

Первым использовал термин "информационная война" американский эксперт Томас Рона в отчете, подготовленным им в 1976 году для компании Boeing, и названный "Системы оружия и информационная война". Т. Рона указал, что информационная инфраструктура становится ключевым компонентом американской экономики. В то же самое время, она становится и уязвимой целью, как в военное, так и в мирное время. Этот отчет и можно считать первым упоминанием термина «информационная война».

Публикация отчета Т. Рона послужила началом активной кампании в средствах массовой информации. Сама постановка проблемы весьма заинтересовала американских военных, которым свойственно заниматься «секретными материалами». Военно-воздушные силы США начали активно обсуждать этот предмет уже с 1980 года.

С военной точки зрения термин «информационная война» в наше время был употреблен в середине 80-х годов XX в. в связи с новыми задачами Вооруженных сил США после окончания «холодной» войны. Это явилось результатом работы группы американских военных теоретиков в составе Г.Е. Экклз, Г.Г. Саммерз и др. В дальнейшем термин начал активно употребляться после проведения операции «Буря в пустыне» в 1991 г. в Ираке, где новые информационные технологии впервые были использованы как средство ведения боевых действий. Официально же этот термин впервые введен в директиве министра обороны США DODD 3600 от 21 декабря 1992 года.

Спустя несколько лет, в феврале 1996 года, Министерство обороны США ввело в действие «Доктрину борьбы с системами контроля и управления». Публикация определяет борьбу с системами контроля и управления как «объединенное использование приемов и методов безопасности, военного обмана, психологических операций, радиоэлектронной борьбы и физического разрушения объектов системы управления, поддержанных разведкой, для недопущения сбора информации, оказания влияния или уничтожения способностей противника по контролю и управлению над полем боя, при одновременной защите своих сил и сил союзников, а также препятствование противнику делать тоже самое».

Наиболее важным является то, что эта публикация определила понятие войны с системами контроля и управления. И это было впервые, когда Министерство обороны США определило возможности и доктрину ИВ.

В конце 1996 г. Роберт Банкер, эксперт Пентагона, на одном из симпозиумов представил доклад, посвященный новой военной доктрине вооруженных сил США XXI столетия (концепции "Force XXI"). В ее основу было положено разделение всего театра военных действий на две составляющих - традиционное пространство и киберпространство, причем последнее имеет даже более важное значение. Р. Банкер предложил доктрину "кибермaневра", которая должна явиться естественным дополнением

традиционных военных концепций, преследующих цель нейтрализации или подавления вооруженных сил противника.

Таким образом, в число сфер ведения боевых действий, помимо земли, моря, воздуха и космоса теперь включается и инфосфера. Как подчеркивают военные эксперты, основными объектами поражения в новых войнах будут информационная инфраструктура и психика противника (появился даже термин "human network").

В октябре 1998 года, Министерство обороны США вводит в действие «Объединенную доктрину информационных операций». Первоначально эта публикация называлась «Объединенная доктрина информационной войны». Позже она была переименована в «Объединенную доктрину информационных операций». Причина изменения состояла в том, чтобы разъяснить отношения понятий информационных операций и информационной войны. Они были определены, следующим образом:

– информационная операция: действия, предпринимаемые с целью затруднить сбор, обработку передачу и хранение информации информационными системами противника при защите собственной информации и информационных систем;

– информационная война: комплексное воздействие (совокупность информационных операций) на систему государственного и военного управления противостоящей стороны, на ее военно-политическое руководство, которое уже в мирное время приводило бы к принятию благоприятных для стороны-инициатора информационного воздействия решений, а в ходе конфликта полностью парализовало бы функционирование инфраструктуры управления противника.

Сейчас существует довольно много разных определений ИВ и с технико-технологической точки зрения. В коридорах Пентагона ходит, например, такое шутливое определение «Информационная война - это компьютерная безопасность плюс деньги».

А если серьезно, то военные подходят к ИВ так, как это было сформулировано еще в Меморандуме N30 (1993 г) заместителей Министра Обороны и Комитета начальников штабов Вооруженных Сил США.

Под информационной войной здесь понимаются действия, предпринимаемые для достижения информационного превосходства в поддержке национальной военной стратегии посредством воздействия на информацию и информационные системы противника при одновременном обеспечении безопасности и защиты собственной информации и информационных систем.

В гуманитарном смысле «информационная война» понимается как те или иные активные методы трансформации информационного пространства. В информационных войнах этого типа речь идет об определенной системе (концепции) навязывания модели мира, которая призвана обеспечить желаемые типы поведения, об атаках на структуры порождения информации, процессы рассуждений.

Основными формами ведения технической ИВ являются радиоэлектронная борьба, война с использованием средств электронной разведки и наведения, нанесения удаленных точечных ударов с воздуха, психотропная война, борьба с хакерами, кибернетическая война.

Прежде чем всерьез анализировать различные определения информационной войны с технической точки зрения отметим присущее ей важное свойство: ведение информационной войны никогда не бывает случайным или обособленным, а подразумевает согласованную деятельность по использованию информации как оружия для ведения боевых действий - будь то на реальном поле боя, либо в экономической, политической, социальной сферах.

Поэтому в качестве основного и наиболее общего определения ИВ используется следующее:

Информационная война - это всеобъемлющая целостная стратегия, обусловленная все возрастающей значимостью и ценностью информации в вопросах командования, управления и политики.

Поле действия информационных войн при таком определении оказывается достаточно широким и охватывает следующие области:

1) инфраструктуру систем жизнеобеспечения государства - телекоммуникации, транспортные сети, электростанции, банковские системы и т.д.;

2) промышленный шпионаж - хищение патентованной информации, искажение или уничтожение особо важных данных, услуг; сбор информации разведывательного характера о конкурентах и т.п.;

3) взлом и использование личных паролей VIP-персон, идентификационных номеров, банковских счетов, данных конфиденциального плана, производство дезинформации;

4) электронное вмешательство в процессы командования и управления военными объектами и системами, "штабная война", вывод из строя сетей военных коммуникаций;

5) всемирная компьютерная сеть Интернет, в которой, по некоторым оценкам, действуют 150.000 военных компьютеров, и 95% военных линий связи проходят по открытым телефонным линиям.

Какой бы смысл в понятие "информационная война" ни вкладывался, оно родилось в среде военных и обозначает, прежде всего, жесткую, решительную и опасную деятельность, сопоставимую с реальными боевыми действиями. Военные эксперты, сформулировавшие доктрину информационной войны, отчетливо представляют себе отдельные ее грани: это штабная война, электронная война, психотронная война, информационно-психологическая война, кибернетическая война и т.

Итак, информационная война - это такая форма конфликта, в которой происходят прямые атаки на информационные системы для воздействия на знания или предположения противника.

Информационная война может проводиться как часть большего и более полного набора военных действий.

Таким образом, под угрозой информационной войны понимается намерение определенных сил воспользоваться поразительными возможностями, скрытыми в компьютерах, на необозримом кибер-пространстве, чтобы вести «бесконтактную» войну, в которой количество жертв (в прямом значении слова) сведено до минимума. Гражданская информационная война может быть развязана террористами, наркотическими картелями, подпольными торговцами оружием массового поражения.

Военные всегда пытались воздействовать на информацию, требующуюся врагу для эффективного управления своими силами. Обычно это делалось с помощью маневров и отвлекающих действий. Так как эти стратегии воздействовали на информацию, получаемую врагом, косвенно путем восприятия, они атаковали информацию врага косвенно. То есть, для того чтобы хитрость была эффективной, враг должен был сделать три вещи:

1. наблюдать обманные действия
2. посчитать обман правдой
3. действовать после обмана в соответствии с целями обманывающего.

Тем не менее, современные средства выполнения информационных функций сделали информацию уязвимой к прямому доступу и манипуляции с ней. Современные технологии позволяют противнику изменить или создать информацию без предварительного получения фактов и их интерпретации. Вот краткий список характеристик современных информационных систем, приводящим к появлению подобной уязвимости: концентрированное хранение информации, скорость доступа, повсеместная передача информации, и большие возможности информационных систем выполнять свои функции автономно. Механизмы защиты могут уменьшить, но не до нуля эту уязвимость.

3.3.1. Составные части информационной войны

К составным частям информационной войны относятся:

1) психологические операции - использование информации для воздействия на аргументацию солдат врага.

2) электронная война - не позволяет врагу получить точную информацию

3) дезинформация - предоставляет врагу ложную информацию о наших силах и намерениях

4) физическое разрушение - может быть частью информационной войны, если имеет целью воздействие на элементы информационных систем.

5) меры безопасности - стремятся избежать того, чтобы враг узнал о наших возможностях и намерениях.

6) прямые информационные атаки - прямое искажение информации без видимого изменения сущности, в которой она находится.

Как ранее говорилось, существует два способа повлиять на информационные функции врага - косвенно или напрямую. Проиллюстрируем разницу между ними на примере.

Пусть нашей целью является заставить врага думать, что авиаполк находится там, где он совсем не находится, и действовать на основании этой информации таким образом, чтобы это было выгодно нам.

Косвенная информационная атака: используя инженерные средства, мы можем построить макеты самолетов и ложные аэродромные сооружения, и противник будет наблюдать ложный аэродром и считать его настоящим. Только тогда эта информация станет той, которую должен иметь противник по нашему мнению.

Прямая информационная атака: если мы создаем информацию о ложном авиаполке в хранилище информации у противника, то результат будет точно такой же. Но средства, задействованные для получения этого результата, будут разительно отличаться.

Другим примером прямой информационной атаки может быть изменение информации во вражеской базе данных об имеющихся коммуникациях в ходе боевых действий (внесение ложной информации о том, что мосты разрушены) для изоляции отдельных вражеских частей. Этого же можно добиться бомбардировкой мостов. И в том, и в другом случае вражеские аналитики, принимая решение на основе имеющейся у них информации, примут одно и то же решение - производить переброску войск через другие коммуникации.

Оборонительной стороной информационной войны являются меры безопасности, имеющие своей целью защитить информацию - не позволить противнику провести успешную информационную атаку на наши информационные функции. Современные меры защиты, такие как операционная безопасность и коммуникационная безопасность - типичные средства по предотвращению и обнаружению косвенных действий врага, направленных на наши военные информационные функции. Напротив, такие меры защиты, как компьютерная безопасность включают в себя действия по предотвращению, обнаружению прямых информационных действий врага и организации контрдействий.

3.3.2. Цели информационной войны

Существуют три цели информационной войны:

– контролировать информационное пространство, чтобы мы могли использовать его, защищая при этом наши военные информационные функции от вражеских действий (контринформация).

– использовать контроль за информацией для ведения информационных атак на врага

– повысить общую эффективность вооруженных сил с помощью повсеместного использования военных информационных функций.

Следует отличать информационную войну от компьютерной преступности. Любое компьютерное преступление представляет собой факт нарушения того или иного закона. Оно может быть случайным, а может быть специально спланированным; может быть обособленным, а может быть составной частью обширного плана атаки. Напротив, ведение информационной войны никогда не бывает случайным или обособленным (и может даже не являться нарушением закона), а подразумевает согласованную деятельность по использованию информации как оружия для ведения боевых действий - будь то на реальном поле брани, либо в экономической, политической или социальной сферах. Театр информационных боевых действий простирается от секретного кабинета до домашнего персонального компьютера и ведется на различных фронтах.

Электронное поле боя представлено постоянно растущим арсеналом электронных вооружений, преимущественно засекреченных. Говоря военным языком, они предназначены для боевых действий в области командования и управления войсками, или «штабной войны». Последние конфликты уже продемонстрировали всю мощь и поражающую силу информационных боевых действий - война в Персидском заливе и вторжение на Гаити. Во время войны в Персидском заливе силы союзников на информационном фронте провели комплекс операций в диапазоне от старомодной тактики разбрасывания пропагандистских листовок до вывода из строя сети военных коммуникаций Ирака с помощью компьютерного вируса.

Атаки инфраструктуры наносят удары по жизненно важным элементам, таким как телекоммуникации или транспортные системы. Подобные действия могут быть предприняты геополитическими или экономическими противниками или террористическими группами. Примером служит вывод из строя междугородной телефонной станции компании AT&T в 1990 году. В наши дни любой банк, любая электростанция, любая транспортная сеть и любая телевизионная студия представляют собой потенциальную мишень для воздействия из киберпространства.

Промышленный шпионаж и другие виды разведки грозят великим множеством тайных операций, осуществляемых корпорациями или государствами в отношении других корпораций или государств; например, сбор информации разведывательного характера о конкурентах, хищение патентованной информации и даже акты саботажа в форме искажения или уничтожения данных. Иллюстрацией этой угрозы служит документально доказанная деятельность французских и японских агентов на протяжении восьмидесятых годов.

Сбор разведывательной информации также выходит на новые рубежи. Лаборатория Линкольна в Массачусетском технологическом институте разрабатывает аппарат для воздушной разведки размером с пачку сигарет. Другая лаборатория работает над химическими веществами, которые можно ввести в провизию неприятельских войск, чтобы позволить датчикам отслеживать их перемещение по дыханию или выделению пота. Помимо этого уже имеются спутниковые системы слежения, имеющие разрешающую способность в несколько сантиметров.

Конфиденциальность все более уязвима по мере появления возможности доступа к постоянно растущим объемам информации в постоянно растущем числе абонентских пунктов. Важные персоны, таким образом могут стать объектом шантажа или злобной клеветы, и никто не гарантирован от подложного использования личных идентификационных номеров.

Как бы то ни было, термин "информационная война" обязан своим происхождением военным и обозначает жестокую и опасную деятельность, связанную с реальными, кровопролитными и разрушительными боевыми действиями. Военные эксперты, сформулировавшие доктрину информационной войны, отчетливо представляют себе отдельные ее грани: это штабная война, электронная война, психологические операции и так далее.

Информационная война представляет собой всеобъемлющую, целостную стратегию, призванную отдать должное значимости и ценности информации в вопросах командования, управления и выполнения приказов вооруженными силами и реализации национальной политики. Информационная война нацелена на все возможности и факторы уязвимости, неизбежно возникающие при возрастающей зависимости от информации, а также на использование информации во всевозможных конфликтах. Объектом внимания становятся информационные системы (включая соответствующие линии передач, обрабатывающие центры и человеческие факторы этих систем), а также информационные технологии, используемые в системах вооружений. Информационная война имеет наступательные и оборонительные составляющие.

Многие ведущие стратеги полагают, что противостояние армий, погибающих на полях генеральных сражений, очень скоро займет свое место на свалке истории рядом со шпорами и арбалетами. Высшая форма победы теперь состоит в том, чтобы выигрывать без крови. В то же время довольно трудно представить боевые действия как игру на видеоприставке без страха и боли.

Таким образом, под угрозой информационной войны понимается намерение определенных сил воспользоваться поразительными возможностями, скрытыми в компьютерах, на необозримом киберпространстве, чтобы вести "бесконтактную" войну, в которой количество жертв (в прямом значении слова) сведено до минимума. "Мы приближаемся к такой ступени развития, когда уже никто не является солдатом, но все являются участниками боевых действий, - сказал один из руководителей Пентагона. - Задача теперь состоит не в уничтожении живой силы, но в подрыве целей, взглядов и мировоззрения населения, в разрушении социума".

Гражданская информационная война может быть развязана террористами, наркотическими картелями, подпольными торговцами

оружием массового поражения. Крупномасштабное информационное противостояние между общественными группами или государствами имеет целью изменить расстановку сил в обществе.

Поскольку такая война связана с вопросами информации и коммуникаций, то если смотреть в корень, это есть война за знания - за то, кому известны ответы на вопросы: что, когда, где и почему и насколько надежными считает отдельно взятое общество или армия свои знания о себе и своих противниках.

Исследователи выделили характерную особенность человеческого восприятия, заключающуюся в том, что человек лучше усваивает ту информацию, которая похожа на уже существующие у него представления.

Основные средства ИВ ориентированы на этот феномен. Любые манипуляции и пропагандистские компании основаны на «эффекте резонанса», когда «имплантируемая» информация, направленная на изменение поведения общности, маскируется под знания и стереотипы, уже существующие в конкретной социальной общности на которую направлена пропагандистская компания.

Целью манипуляции является асинхронизации представлений группы-адресата с помощью «эффекта резонанса» и перевод ее на другие модели поведения, ориентированные на совершенно иную систему ценностей.

«Эффект резонанса» достигается, когда тому или иному факту, проблеме или психологической установке придается искусственно преувеличенное значение, которое по мере продвижения в культурное ядро, диссонирует и разрушает существующую в обществе систему ценностей. Диссонанс достигается при раздувании одной из уже существующих моральных норм, которые в определённых рамках сами по себе помогают обществу.

Крупномасштабное информационное противостояние между общественными группами или государствами имеет целью изменить расстановку сил в обществе.

Как указывают американские военные эксперты, ИВ состоит из действий, предпринимаемых с целью достижения информационного превосходства в обеспечении национальной военной стратегии путем воздействия на информацию и информационные системы противника с одновременным укреплением и защитой собственной информации и информационных систем и инфраструктуры.

Информационное превосходство определяется как способность собирать, обрабатывать и распределять непрерывный поток информации о ситуации, препятствуя противнику делать то же самое. Оно может быть также определено и как способность назначить и поддерживать такой темп проведения операции, который превосходит любой возможный темп противника, позволяя доминировать во все время ее проведения, оставаясь непредсказуемым, и действовать, опережая противника в его ответных акциях.

Информационное превосходство позволяет иметь реальное представление о боевой обстановке и дает интерактивную и высокоточную картину действий противника и своих войск в реальном масштабе времени. Информационное превосходство является инструментом, позволяющим командованию в решающих операциях применять широко рассредоточенные построения разнородных сил, обеспечивать защиту войск и ввод в сражение группировок, состав которых в максимальной степени соответствует задачам, а также осуществлять гибкое и целенаправленное материально-техническое обеспечение.

Информационное противоборство осуществляется путем проведения мероприятий направленных против систем управления и принятия решений (Command & Control Warfare, C2W), а также против компьютерных и информационных сетей и систем (Computer Network Attack, CNA).

Деструктивное воздействие на системы управления и принятия решений достигается путем проведения психологических операций (Psychological Operations, PSYOP), направленных против персонала и лиц,

принимающих решения и оказывающих влияние на их моральную устойчивость, эмоции и мотивы принятия решений; выполнения мероприятий по оперативной и стратегической маскировке (OPSEC), дезинформации и физическому разрушению объектов инфраструктуры.

Вообще, по словам некоторых экспертов, попытки в полной мере осознать все грани понятия информационной войны напоминают усилия слепых, пытающихся понять природу слона: тот, кто ощупывает его ногу, называет его деревом; тот, кто ощупывает хвост, называет его канатом и так далее. Можно ли так получить более верное представление? Возможно, слона-то и нет, а есть только деревья и канаты. Одни готовы подвести под это понятие слишком много, другие трактуют какой-то один аспект информационной войны как понятие в целом [4].

Однако проблема поиска надлежащего определения этому явлению весьма серьезная и требует детальнейшей и серьезной проработки.

3.3.3. Последствия информационной войны.

Взрыв нескольких гранат нельзя назвать войной, кто бы их не бросал. Взрыв нескольких водородных бомб - это уже и начатая и завершенная война.

Информационную пропаганду 50-ых, 60-ых годов, которой занимались СССР и США, можно сравнить именно с несколькими гранатами. Поэтому никто не называет прошлое противостояние информационной войной, в лучшем случае оно заслуживает термина "холодная война".

День сегодняшний, с его телекоммуникационными вычислительными системами, психотехнологиями кардинально изменил окружающее пространство. Отдельные информационные ручейки превратились в сплошной поток. Если ранее было возможно "запрудить" конкретные информационные каналы, то сегодня все окружающее пространство информационно коллапсировалось. Время на информационное взаимодействие между самыми отдаленными точками приблизилось к нулю.

В результате проблема защиты информации, которая ранее была как никогда актуальна, перевернулась подобно монете, что вызвало к жизни ее противоположность - защиту от информации.

Почему надо защищать информационную систему от информации? Потому что любая поступающая на вход системы информация неизбежно изменяет систему. Целенаправленное же, умышленное информационное воздействие может привести систему к необратимым изменениям и к самоуничтожению.

Поэтому информационная война - это не что иное, как явные и скрытые целенаправленные информационные воздействия систем друг на друга с целью получения определенного выигрыша в материальной сфере.

Исходя из приведенного определения информационной войны, применение информационного оружия означает подачу на вход информационной самообучающейся системы такой последовательности входных данных, которая активизирует в системе определенные алгоритмы, а в случае их отсутствия - алгоритмы генерации алгоритмов.

Создание универсального защитного алгоритма, позволяющего выявить системе-жертве факт начала информационной войны, является алгоритмически неразрешимой проблемой. К таким же неразрешимым проблемам относится выявление факта завершения информационной войны. Однако, несмотря на неразрешимость проблем начала и окончания информационной войны, факт поражения в ней характеризуется рядом признаков, присущих поражению в обычной войне. К ним относятся:

1) включение части структуры пораженной системы в структуру системы победителя (эмиграция из побежденной страны и в первую очередь вывоз наиболее ценного человеческого материала, наукоемкого производства, полезных ископаемых);

2) полное разрушение той части структуры, которая отвечает за безопасность системы от внешних угроз (разрушение армии побежденной страны);

3) полное разрушение той части структуры, которая ответственна за восстановление элементов и структур подсистемы безопасности /разрушение производства, в первую очередь, наукоемкого производства, а также научных центров и всей системы образования; прекращение и запрещение разработок и производств наиболее перспективных видов вооружения);

4) разрушение и уничтожение той части структуры, которая не может быть использована победителем в собственных целях;

5) сокращение функциональных возможностей побежденной системы за счет сокращения ее информационной емкости (в случае страны: отделение части территории, уничтожение части населения).

Обобщив перечисленные признаки, можно ввести понятие "степень поражения информационным оружием", оценив ее через информационную емкость той части структуры пораженной системы, которая либо погибла, либо работает на цели, чуждые для собственной системы.

Информационное оружие даст максимальный эффект только тогда, когда оно применяется по наиболее уязвимым от него частям ИСС. Наибольшей информационной уязвимостью обладают те подсистемы, которые наиболее чувствительны к входной информации - это системы принятия решения, управления. На основании сказанного можно ввести понятие информационной мишени. Информационная мишень - множество элементов информационной системы, принадлежащих или способных принадлежать сфере управления, и имеющих потенциальные ресурсы для перепрограммирования на достижение целей, чуждых данной системе.

Исходя из определения информационной мишени, намечаются основные направления работ, как по обеспечению се безопасности, так и по повышению ее уязвимости. Например, для того, чтобы повысить уязвимость противника, следует максимально расширить его информационную мишень, т.е. подтолкнуть его на включение в мишень как можно больше равноправных элементов, причем желательно открыть доступ в сферу

управления таким элементам, которые легко поддаются перепрограммированию и внешнему управлению.

Заставить противника изменить свое поведения можно с помощью явных и скрытых, внешних и внутренних информационных угроз.

Причины внешних угроз в случае целенаправленного информационного воздействия (в случае информационной войны) скрыты в борьбе конкурирующих информационных систем за общие ресурсы обеспечивающие системе допустимый режим существования.

Причины внутренних угроз - в появлении внутри система множества элементов, подструктур, для которых привычный режим функционирования стал в силу ряда обстоятельств недопустимым.

Скрытая угроза - это неосознаваемые системой в режиме реального времени входные данные, угрожающие ее безопасности.

Связи с общественностью играют важную роль в жизни общества. Изначально созданные для информирования общественности о ключевых событиях в жизни страны и властных структур, они постепенно стали выполнять еще одну не менее важную функцию - воздействие на сознание своей аудитории с целью формирования определенного отношения к сообщаемым фактам, явлениям действительности. Это воздействие осуществлялось при помощи методов пропаганды и агитации, разрабатываемых на протяжении не одной тысячи лет.

В скором времени связи с общественностью заняли важное место в жизни государств, а с развитием техники и технологии стали активно использоваться и на международном уровне с целью приобретения каких-либо преимуществ контролируемым им государством. В наши дни особое внимание следует уделить роли связей с общественностью в международных конфликтах, в том числе и геополитического характера, поскольку в последние годы наряду с классическими видами оружия все чаще применяется информационно-пропагандистское, в основе которого - работа с различными средствами массовой информации.

Таким образом, на основе ранее сказанного, можно сформулировать следующие утверждения:

1. Наступление информационной эры привело к тому, что информационное воздействие, существовавшее испокон веков во взаимоотношениях между людьми, в наши дни все более очевидно приобретает характер военных действий.

2. В настоящее время накоплен значительный опыт научных исследований в области информационного противоборства и информационно-психологических войн. Какой бы смысл в понятие "информационная война" ни вкладывался, оно родилось в среде военных и обозначает, прежде всего, жесткую, решительную и опасную деятельность, сопоставимую с реальными боевыми действиями. Военные эксперты, сформулировавшие доктрину ИВ, отчетливо представляют себе отдельные ее грани и виды. Гражданское же население пока не готово в силу причин социального и психологического характера в полной мере ощутить всю опасность неконтролируемого применения НКТ в информационной войне.

3. Информация действительно стала реальным оружием. Пример с февральской атакой китайцев, затронувшей корневые серверы Интернет, стала чем-то большим, чем забавы нескольких хакеров. Этот инцидент мог стать "первым залпом" в глобальной информационной войне.

Информационная война идет уже в третьем поколении. Сергей Гриняев, доктор технических наук даёт следующую классификацию:

1-е поколение информационной войны - это РЭБ (радиоэлектронная борьба). Проводная, частотная, сотовая связь, подслушки, глушилки, блокировки, помехи и т.д.;

2-е поколение информационной войны - это РЭБ плюс партизанская и контрпартизанская пропаганда. Так было в Чечне в 90-х. У сепаратистов-боевиков были свои пропагандистские сайты в Интернете, они распространяли газеты и боевые листки, организовывали интервью для сочувствующих им западных журналистов. Контрпропаганда велась

доступными федеральному центру средствами как на территории конфликта и смежных территориях, так и на более широкую общественность.

3-е поколение информационной войны - это глобальная информационная война, специалисты называют её так же "войной на эффектах". Информационная войны вокруг событий в Южной Осетии - именно война третьего поколения.

Формирование вокруг России "санитарного пояса" из стран-соседей происходит политическими средствами - проведением цветных революций, формированием органов власти и парламентского большинства из проамериканских сил, и экономическими средствами - скупкой национальных бирж, наращиванием американского капитала в ключевых государственных отраслях и компаниях. Но в эпоху информационного общества ключевое значение приобрели СМИ, Интернет-каналы и контроль над информпотоками. Из представленного материала очевидно, что Россия в этом отношении значительно отстает от США. Для формирования нового многополярного мирового порядка России необходимо предпринимать решительные действия для прорыва в информационной сфере [36].

3.4. Информационная безопасность государства

Совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности Российской Федерации определяется в «Доктрине информационной безопасности Российской Федерации» (утверждена Президентом Российской Федерации В.Путиным 9 сентября 2000 г., № Пр-1895).

Под **информационной безопасностью Российской Федерации** понимается состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства.

Интересы личности в информационной сфере заключаются в реализации конституционных прав человека и гражданина на доступ к информации, на использование информации в интересах осуществления не запрещенной законом деятельности, физического, духовного и интеллектуального развития, а также в защите информации, обеспечивающей личную безопасность.

Интересы общества в информационной сфере заключаются в обеспечении интересов личности в этой сфере, упрочении демократии, создании правового социального государства, достижении и поддержании общественного согласия, в духовном обновлении России.

Интересы государства в информационной сфере заключаются в создании условий для гармоничного развития российской информационной инфраструктуры, для реализации конституционных прав и свобод человека и гражданина в области получения информации и пользования ею в целях обеспечения незыблемости конституционного строя, суверенитета и территориальной целостности России, политической, экономической и социальной стабильности, в безусловном обеспечении законности и правопорядка, развитии равноправного и взаимовыгодного международного сотрудничества.

3.4.1.Виды угроз информационной безопасности Российской Федерации.

По своей общей направленности угрозы информационной безопасности Российской Федерации подразделяются на следующие виды:

– угрозы конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности, индивидуальному, групповому и общественному сознанию, духовному возрождению России;

– угрозы информационному обеспечению государственной политики Российской Федерации;

– угрозы развитию отечественной индустрии информации, включая индустрию средств информатизации, телекоммуникации и связи, обеспечению потребностей внутреннего рынка в ее продукции и выходу этой продукции на мировой рынок, а также обеспечению накопления, сохранности и эффективного использования отечественных информационных ресурсов;

– угрозы безопасности информационных и телекоммуникационных средств и систем, как уже развернутых, так и создаваемых на территории России.

В сфере внутренней политики.

Наиболее важными объектами обеспечения информационной безопасности Российской Федерации в сфере внутренней политики являются:

– конституционные права и свободы человека и гражданина;

– конституционный строй, национальное согласие, стабильность государственной власти, суверенитет и территориальная целостность Российской Федерации;

– открытые информационные ресурсы федеральных органов исполнительной власти и средств массовой информации.

Наибольшую опасность в сфере внутренней политики представляют следующие угрозы информационной безопасности Российской Федерации:

– нарушение конституционных прав и свобод граждан, реализуемых в информационной сфере;

– недостаточное правовое регулирование отношений в области прав различных политических сил на использование средств массовой информации для пропаганды своих идей;

– распространение дезинформации о политике Российской Федерации, деятельности федеральных органов государственной власти, событиях, происходящих в стране и за рубежом;

– деятельность общественных объединений, направленная на насильственное изменение основ конституционного строя и нарушение целостности Российской Федерации, разжигание социальной, расовой, национальной и религиозной вражды, на распространение этих идей в средствах массовой информации.

Основными мероприятиями в области обеспечения информационной безопасности Российской Федерации в сфере внутренней политики являются:

– создание системы противодействия монополизации отечественными и зарубежными структурами составляющих информационной инфраструктуры, включая рынок информационных услуг и средства массовой информации;

– активизация контрпропагандистской деятельности, направленной на предотвращение негативных последствий распространения дезинформации о внутренней политике России.

В сфере внешней политики.

К наиболее важным объектам обеспечения информационной безопасности Российской Федерации в сфере внешней политики относятся:

– информационные ресурсы федеральных органов исполнительной власти, реализующих внешнюю политику Российской Федерации, российских представительств и организаций за рубежом, представительств Российской Федерации при международных организациях;

– информационные ресурсы представительств федеральных органов исполнительной власти, реализующих внешнюю политику Российской Федерации, на территориях субъектов Российской Федерации;

– информационные ресурсы российских предприятий, учреждений и организаций, подведомственных федеральным органам исполнительной власти, реализующим внешнюю политику Российской Федерации;

– блокирование деятельности российских средств массовой информации по разъяснению зарубежной аудитории целей и основных

направлений государственной политики Российской Федерации, ее мнения по социально значимым событиям российской и международной жизни.

Из внешних угроз информационной безопасности Российской Федерации в сфере внешней политики наибольшую опасность представляют:

– информационное воздействие иностранных политических, экономических, военных и информационных структур на разработку и реализацию стратегии внешней политики Российской Федерации;

– распространение за рубежом дезинформации о внешней политике Российской Федерации;

– нарушение прав российских граждан и юридических лиц в информационной сфере за рубежом;

– попытки несанкционированного доступа к информации и воздействия на информационные ресурсы, информационную инфраструктуру федеральных органов исполнительной власти, реализующих внешнюю политику Российской Федерации, российских представительств и организаций за рубежом, представительств Российской Федерации при международных организациях.

Система обеспечения информационной безопасности Российской Федерации является частью системы обеспечения национальной безопасности страны.

Система обеспечения информационной безопасности Российской Федерации строится на основе разграничения полномочий органов законодательной, исполнительной и судебной власти в данной сфере, а также предметов ведения федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации.

3.4.2. Основными элементами организационной основы системы обеспечения информационной безопасности Российской Федерации являются:

– Президент Российской Федерации,

– Совет Федерации Федерального Собрания Российской Федерации,

– Государственная Дума Федерального Собрания Российской Федерации,

– Правительство Российской Федерации,

– Совет Безопасности Российской Федерации,

– федеральные органы исполнительной власти, межведомственные и государственные комиссии, создаваемые Президентом Российской Федерации и Правительством Российской Федерации,

– органы исполнительной власти субъектов Российской Федерации,

– органы местного самоуправления,

– органы судебной власти,

– общественные объединения,

– граждане, принимающие в соответствии с законодательством Российской Федерации участие в решении задач обеспечения информационной безопасности Российской Федерации [37].

Контрольные вопросы

1. Что такое информационное воздействие? Какие виды информационного воздействия существуют?

2. Перечислите пять признаков воздействия посредством СМИ, которые, на Ваш взгляд, встречаются чаще остальных? Приведите примеры.

3. Дайте определение понятию «специальные информационные операции». На какие виды они подразделяются?

4. Дайте определение понятию «информационная война». Кто впервые его использовал и при каких обстоятельствах?

5. Перечислите составные части информационной войны.

6. Каковы цели информационной войны?

7. В чем состоит отличие информационной войны от компьютерной атаки?

8. Дайте определение понятию «информационная безопасность государства».

9. Какой нормативный документ представляет собой совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности Российской Федерации?

10. Назовите основные элементы организационной основы системы Обеспечения информационной безопасность РФ.

ГЛАВА 4
СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ В ВЕДУЩИХ СТРАНАХ

4.1. Структура систем защиты информации, применяемых в общемировой практике обеспечения информационной безопасности

Широкое использование в процессе информатизации мирового общества современных методов и средств обработки информации, в том числе вычислительной техники создало не только объективные предпосылки повышения эффективности всех видов деятельности личности, общества и государства, но и ряд проблем защиты информации, обеспечивающей требуемое ее качество. Сложность решения этой проблемы обусловлена необходимостью создания целостной системы комплексной защиты информации, базирующейся на стройной организации и регулярном управлении.

Современное понятие защиты информации находится в центре внимания исследователей в различных странах уже несколько десятков лет и ассоциируется, как правило, с проблемами создания систем защиты информации на различных уровнях её использования. Несмотря на то, что существует еще большое количество неразрешенных и спорных вопросов в теории информационной безопасности, в настоящее время сложилась типовая структура системы защиты информации, используемая большинством развитых стран мира.

Структурно-типовая система защиты информации (рис.7) представляет собой совокупность отдельных взаимосвязанных элементов, реализующих следующие её виды:

Рис.7. Структурно-типовая система защиты информации

Правовая защита информации – защита информации, базирующаяся на применении статей конституции и законов государства, положений гражданского и уголовного кодексов и других нормативно-правовых документов в области информатики, информационных отношений и защиты информации. Правовая защита информации регламентирует права и обязанности субъектов информационных отношений, правовой статус органов, технических средств и способов защиты информации и является основой для морально – этических норм в области защиты информации.

Организационная защита информации – это комплекс направлений и методов управленческого, ограничительного и технологического характера, определяющих основы и содержание системы защиты, побуждающих персонал соблюдать правила защиты конфиденциальной информации. Организационные меры связаны с установлением режима конфиденциальности в организации.

Техническая или инженерно- техническая защита, основывающаяся на использовании технических устройств, узлов, блоков, элементов, систем, как в виде отдельных средств, так и встроенных в процессе единого технологического цикла создания средств обработки информации, сооружений и т.д.;

Программно- аппаратная защита, предполагающая использование программного обеспечения информационных систем, комплексов и систем, а также аппаратных устройств, встроенных в состав технических средств и систем обработки информации .

В качестве отдельного вида наиболее эффективных средств защиты информации выделяются математические или криптографические методы, которые могут быть реализованы в виде технических устройств, программ и программно-аппаратных средств.

Рассмотренные виды в основном обеспечивают надежную защиту информации в различных системах ее обработки и различных условиях их функционирования. Однако опыт практического обеспечения безопасности информации в России и за рубежом показывает, что для надежной защиты, в условиях обязательного участия человека, массовости решения задач защиты необходимо использовать психологические и морально-этические виды, а в ряде случаев и страховые.

Под *психологическими видами* защиты понимаются допускаемые нормами права и морали методы и средства изучения психофизиологических особенностей и возможностей людей, а также психологического воздействия на людей с целью оценки соответствия их требованиям для допуска к обработке защищаемой информации.

Под *морально - этическими видами* защиты понимаются нормы и правила, которые не имеют юридической силы, но их нарушение ведет к потере авторитета, возникновению дополнительных трудностей и другим негативным последствиям для человека и организации.

Страховая защита информации – защита информации, предусматривающая возмещение убытков от её уничтожения или модификации путем получения страховых выплат.

Очевидно, что в ряде стран при построении систем защиты в типовую модель вносят изменения. Так, во Франции элементы правовой и организационной защиты информации рассматривают в едином ракурсе, а в программно-аппаратной защите наоборот выделяют отдельно программные и аппаратные методы и средства защиты информации. Морально-этические и психологические элементы защиты информации практически во всех странах до настоящего времени рассматривались лишь в теории [38].

4.2.Организация системы защиты информации в США

В США национальная безопасность имеет широкое толкование и включает в себя защиту образа жизни, населения и территории страны.

Проблемы информационной безопасности рассматриваются американской администрацией как один из ключевых элементов национальной безопасности. Национальная политика США в области защиты информации формируется Агентством национальной безопасности (АНБ). При этом наиболее важные стратегические вопросы, определяющие национальную политику в данной сфере, как правило, решаются на уровне Совета национальной безопасности, а решения оформляются в виде директив Президента США.

В период с 1967 года по настоящее время в США принят целый ряд федеральных законов, создавших правовую основу для формирования и проведения единой государственной политики в области информатизации и защиты информации с учетом интересов национальной безопасности страны.

Правительство США при реализации своей политики в области защиты информации исходит из того, что перехват иностранными государствами конфиденциальной государственной и частной информации, а также

больших объемов открытой информации, передаваемых по правительственным и коммерческим сетям телекоммуникаций, после их обработки, сопоставления и объединения разрозненных сведений приведет к раскрытию государственных секретов. Поэтому, начиная с середины 80-х годов, защита линий связи и автоматизированных систем становится важной задачей компетентных государственных органов США.

В законодательстве США имеется специальный нормативный акт, посвященный коммерческой тайне, что в международной практике является скорее исключением, чем правилом. Отметим, что основная масса нормативного материала о коммерческой тайне (используется термин “trade secret” - “торговый секрет”) приходится на уровень отдельных штатов. Федеральный Единообразный закон о торговых секретах 1979 года (The Uniform Trade Secrets Act) одобрен не всеми штатами, однако законодательство штатов находится под влиянием Федерального закона и в целом соответствует ему. Закон гласит, что коммерческой тайной является информация, которая имеет самостоятельную экономическую стоимость вследствие того, что не является общеизвестной или доступной лицам, которые могут ее использовать в коммерческих целях, а также является объектом разумных усилий по защите.

Помимо Единообразного закона, торговые секреты затрагивает еще целый ряд нормативных актов.

Практика защиты коммерческой тайны в США предусматривает заключение соглашения о сохранении коммерческой тайны, подписываемого в ходе оформления на работу, а также проведение специальной разъяснительной работы, которая также регламентирована соответствующими документами. Поступающему на работу может быть предложено написать заявление, касающееся посторонней частной информации, которую он получил по месту предыдущей работы. Практически речь идет о своего рода предупредительной работе, которая проводится в конкретной фирме и направлена на сохранение ее высокой

репутации в деловом мире. Нанимающийся на работу сообщает, как правило, что он обязан сохранять в тайне секреты, полученные им по прежнему месту работы и срок сохранения такой информации в тайне, а также информирует нового работодателя о том, что эту информацию он не вправе раскрывать и использовать по новому месту работы. Практика защиты коммерческой тайны в США предусматривает написание заявления увольняющегося служащего, где он фактически ставит фирму в известность относительно взятых им на себя обязательств о сохранении коммерческой тайны. В заявлении служащий сообщает, что обязательства по сохранению коммерческой тайны им выполнены и что в процессе своей работы он не участвовал в какой-либо деятельности, составляющей конкуренцию или противоречащей его обязательствам как служащего. Руководитель организации, откуда уволился работник, может поставить в известность нового работодателя в отношении информированности о коммерческой тайне организации принятого на службу работника. Кроме того, обычно руководитель организации письменно напоминает уволившемуся служащему об обязательствах по сохранению коммерческой тайны, что были подписаны им при приеме на работу.

Ежегодно США расходуют на информационные технологии только из федерального бюджета порядка 38 млрд. $, из которых около 20 млрд. $ (более 50%) составляют расходы военного ведомства. И это без учета десятков млрд. $, затрачиваемых на бортовые системы управления спутников, ракет, самолетов, танков и кораблей. Сегодня Пентагон это не только один из крупнейших владельцев, арендаторов и пользователей информационных и телекоммуникационных ресурсов, ведущих заказчиков программного обеспечения, компьютерного оборудования и средств цифровой связи, но и, по сути дела, законодатель государственной политики и промышленных стандартов в области информационной безопасности. Только в 2000 г. на защиту национальных информационных ресурсов в США было выделено 1,5 млрд. $, в то время как Пентагон истратил на защиту

военных информационных систем 1,1 млрд. $.

4.3. Организация системы защиты информации в ведущих странах Западной Европы

Европейские специалисты в области информационных систем, безопасности и стратегического планирования активно обсуждают проблемы, возникающие перед странами Европейского союза в условиях возможности применения информационного оружия.

Эксперты особо выделяют такую особенность использования информационного оружия, как скрытность. Его применение в мирное время при отсутствии силового противостояния считается одной из главных угроз, поскольку позволяет незаметно для «противника» не только взять под контроль его информационные ресурсы, но и произвольно манипулировать связанными с ними сферами государства, особенно экономической сферой. Учитывая растущую зависимость управленческих решений на высшем уровне от обеспечивающего их информационного потока, возможность полной дезорганизации экономики и финансов, по мнению ряда западных ученых, делает информационное оружие одним из наиболее эффективных и, вероятно, наиболее распространенных уже к концу нынешнего века.

В настоящее время реализуются на практике планы организационного и технического обеспечения национальной информационной безопасности, создаются подразделения, предназначенные для отражения «информационной агрессии». Правительства берут на себя роль координатора межведомственных усилий в этой сфере. Разработка методов и средств обеспечения информационной безопасности ведется на Западе по следующим основным направлениям: выявление угрозы нападения, нейтрализация нападения, защита и восстановление собственных систем.

Кроме изучения технических аспектов информационной безопасности, на Западе активизировалась работа по оценке влияния информации на

личность и общество. При этом делается упор на определение методов и средств оказания «информационного противодействия», каналов воздействия на человека, влияния той или иной информации на боеспособность ВС, исследование взаимоотношений СМИ и общественного мнения.

Эксперты ведущих западных стран пришли к выводу, что в связи с возрастанием значимости информационного фактора для принятия решений на правительственном, военном и промышленном уровнях необходима диверсификация источников получения данных, а также механизмов их обработки и способов доведения до потребителей. Подчеркивается важность наличия национальных информационных агентств с независимой сетью корреспондентов, что позволит выявлять дезинформацию, способную оказывать влияние на принятие государственных решений. Выдвигаются идеи создания баз данных по источникам информации (научные учреждения, СМИ, частные лица) для получения достоверных и оперативных сведений в кризисных ситуациях.

Сейчас на Западе организуются закрытые межведомственные информационные инфраструктуры, призванные обеспечить защищенную связь. Такие системы строятся на выделенных каналах связи и не имеют выхода на глобальные сети, поскольку, как утверждается, именно от гражданских коммуникаций исходит основная угроза безопасности.

До последнего времени значение уязвимости единой объединенной инфраструктуры Европейского союза недооценивалось. Основными причинами явились преобладающее внимание к общеевропейским интеграционным процессам и общее ослабление силового противостояния на континенте.

Однако за политической интеграцией последовало фактическое объединение в сфере информационных ресурсов, приводящее к формированию единого информационного пространства, что в свою очередь привело к зависимости отдельных государств от информационных потоков, охватывающих общество. Таким образом, воздействие на эти потоки с целью

порчи, искажения находящейся в них информации, а также вывода из строя информационных инфраструктур перерастает в Европе из национальной проблемы в международную. В качестве примера можно привести ряд реализуемых проектов сбора и анализа информации о разных сферах в масштабах объединенной Европы. Зарубежные аналитики отмечают, что стремление ликвидировать границы во всех областях приводит к снижению внимания к вопросам защиты информационных ресурсов от предумышленного воздействия со стороны с целью манипулирования информацией или нарушения работоспособности. Также отмечаются трудности, возникающие при попытках идентификации такого воздействия, которое может быть как случайным, так и направленным вмешательством различных террористических организаций и спецслужб иностранных государств. Американские эксперты заостряют внимание на том, что в реальной коммерческой практике выгоднее не утаивать, а активно распространять и внедрять свои технологии.

Ряд аналитиков, указывая на значительные расходы США по обеспечению своей информационной безопасности, отмечают устойчивое стремление создать впечатление открытости информационных сетей общего пользования и отсутствия контроля над ними. Лидерство в сфере передовых разработок позволяет Соединенным Штатам устанавливать стандарты в области систем связи и обработки данных и таким образом формировать зависимость иностранных государств от американских программных и аппаратных средств. Тем самым подавляются стимулы к организации другими государствами аналогичных конкурентоспособных разработок. Поэтому попытки США превратить свои национальные стандарты защиты информации в международные вызывают неоднозначную реакцию. По мнению европейских специалистов, это создает американским фирмам-производителям средств защиты информации благоприятные условия для захвата европейского рынка, потенциально расширяет возможности контроля

за защищаемой информацией и дает преимущества американским разведывательным службам.

Соединенным Штатам, провозгласившим в качестве одной из стратегических инициатив образование «информационной супермагистрали», приходится призывать своих западноевропейских партнеров сделать их рынки телекоммуникаций открытыми для конкуренции извне. Политика, проводимая ведущими промышленно развитыми европейскими государствами, до последнего времени всячески препятствовала проникновению иностранных связных компаний на собственный рынок, осознавая «чувствительность» этого сектора экономики к проблеме обеспечения национальной безопасности. Однако при подготовке к подписанию глобального телекоммуникационного пакта (февраль 1997 г.) в рамках Всемирной торговой организации (ВТО) Франция, Бельгия, Испания и Португалия согласились отменить все еще существующие внутренние ограничения на допуск иностранного капитала в область национальных телекоммуникаций в обмен на встречные уступки США в вопросе о прокладке подводных кабелей связи.

С учетом изложенного приобретает популярность идея создания системы коллективного контроля и обеспечения информационной безопасности. К трудностям в ее реализации эксперты относят:

- неоднородность развития инфраструктур в разных странах;
- различие подходов и законодательств;
- трудности в технической реализации;
- отсутствие единых стандартов.

Европейским союзом было принято решение по скорейшему созданию единой трансевропейской сети информационной связи, вследствие чего утверждена программа INFO2000, реализуется ряд проектов по внедрению новых информационных технологий в административный сектор - IDA, EPHOS, APPLICAZIONI TELEMATICHE и другие.

На рассмотрение Комиссии европейских сообществ представлена программа по преодолению языковых различий в единых информационных системах. В ближайший период планируется ряд мероприятий по решению вопросов безопасного обмена информацией в сетях и внедрению единого стандарта для объединения локальных сетей различных стран и регионов.

Изменения, происходящие в европейской информационной инфраструктуре, потребовали серьезных поправок законодательных и регулирующих актов. В этой связи 11 марта 1996 г. Европейским союзом принята совместная Директива о юридической защите баз данных. Рост информационного рынка означает возможность обращения к национальным базам данных пользователей других стран, что требует приведения в соответствие внутригосударственных актов и принятия общего законодательства о защите авторских прав. Новая директива обеспечит согласование национальных и общеевропейских правил по защите авторских прав для баз данных (БД), представленных в электронной и неэлектронной формах, без ущерба для авторских работ, входящих в эти БД.

В этой связи 21 марта 1996 г. в Брюсселе прошел совет на уровне министров, ответственных за развитие телекоммуникаций в европейских странах, на котором были достигнуты политические согласия по новой директиве о взаимодействии в этой области. Директива затронула проблему организации универсальных услуг и взаимосвязи на основе применения принципов открытой сети (Open network provision - ONP). Совет также принял решение по основным направлениям развития трансевропейских телекоммуникационных сетей, установил процедуру отбора проектов.

В Брюсселе обсуждались поправки к юридическим актам ONP Frame Work и Leased Lines Directives. Рассматривались предложения Комиссии европейских сообществ по координации подходов стран к введению единых требований к персональной спутниковой связи (S-PCS) с целью избегания проблем несовместимости и отсутствия законодательных актов, особенно в

тех случаях, когда услуги спутниковой связи будут предоставляться всем странам на территории Европы.

Большинство стран, не обладающих мощными информационными ресурсами, склоняются к созданию международной договорно-правовой базы обеспечения безопасности в глобальном масштабе и налаживанию взаимодействия в указанной сфере. Европейцы уже приступили к изучению вопроса о принятии нормативных документов по информационной безопасности в рамках ЮНЕСКО. По их мнению, это позволит придать контролю за глобальными сетями многополюсный характер, уменьшив тем самым влияние США в данной сфере.

Некоторые европейские государства рассчитывают на более тесное взаимодействие в рамках НАТО и Евросоюза при выявлении рисков внедрения новых технологий, разработке критериев, методов и испытательных средств для оценки защищенности национальных коммуникационных систем, выдаче разрешений на внедрение информационных систем в важные объекты и осуществлении специальных мер безопасности в правительственных и военных структурах.

Основываясь на оценках специалистов в области стратегических исследований, необходимо обратить внимание, во-первых, на особую угрозу использования информационного оружия с целью взятия под контроль информационной инфраструктуры государства, а во-вторых, в связи с опасностью упомянутой угрозы, актуальность приобретает разработка международных соглашений по информационной безопасности и кодекса поведения в международном информационном пространстве.

4.3.1. Организация защиты информации в Великобритании.

Правительство Великобритании начало заниматься проблемами защиты информации раньше остальных европейских государств. Закон «О государственных документах», в части ограничений на работы с секретными документами. Закон «О государственной тайне» – ответственность за

разглашение тайны, неразглашение коммерческой тайны фиксируется в договорных обязательствах. Основной недостаток – отсутствие закона «О свободе информации». Для обеспечения безопасности остальной информации используются уголовный кодекс и некоторые другие правовые акты. О защите коммерческой тайны каждая организация должна заботиться самостоятельно, используя специальные договоры, которые заключаются с сотрудниками перед предоставлением им доступа к данным.

В Соединённом Королевстве Великобритании и Северной Ирландии (далее Великобритания) государственную систему обеспечения информационной безопасности строят, исходя из понимания информационной войны как действий, оказывающих влияние на информационные системы противника, при одновременной защите собственных систем. Структура государственной системы ИБ изображена на рис.8.

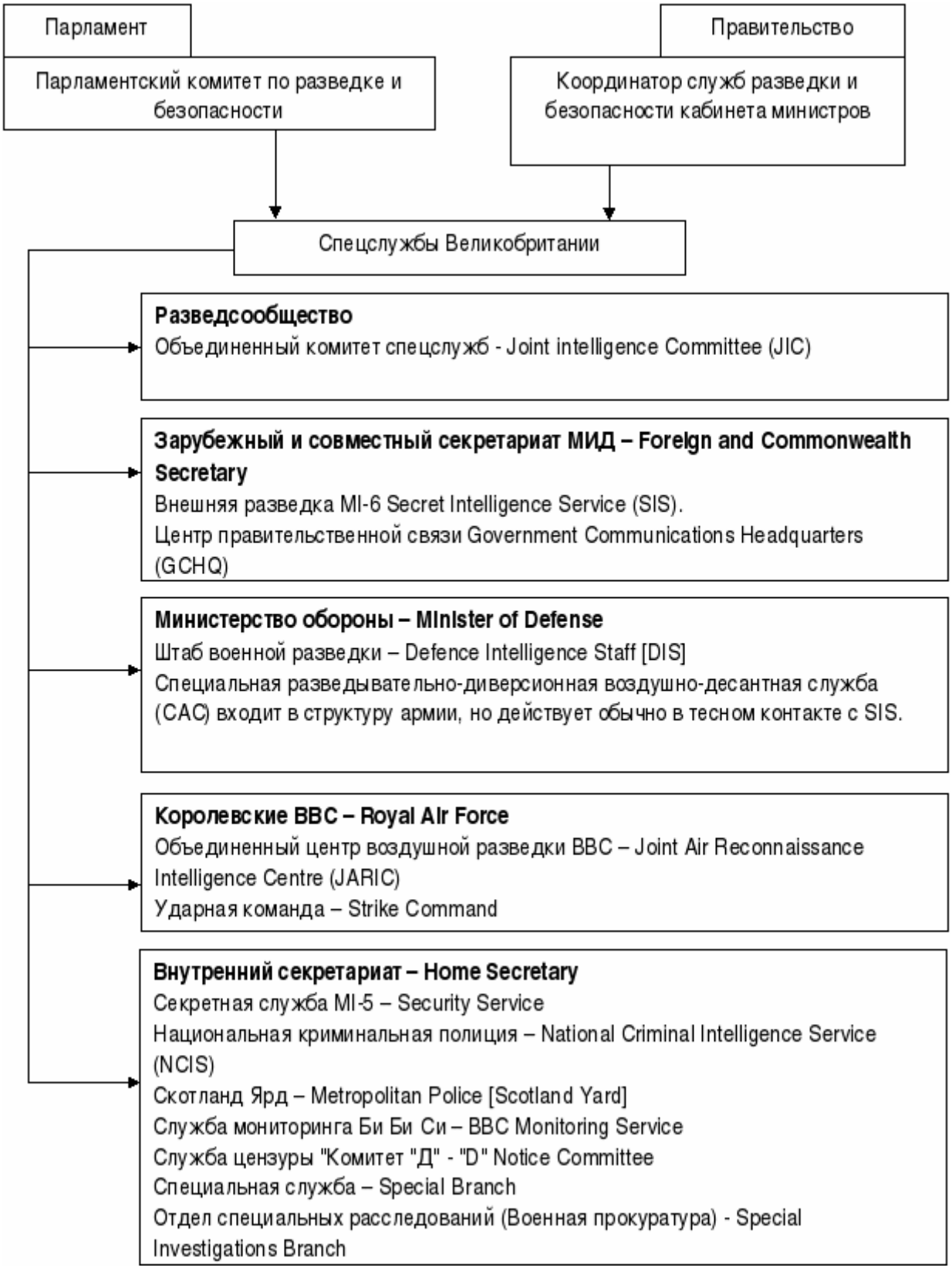

Рис. 8. Структура государственной системы ИБ Великобритании

В Великобритании существует самая жесткая система органов защиты информации, так как она создавалась в рамках государства и ради его целей.

Обеспечение безопасности персональных и коммерческих данных оказалось второстепенной задачей. Все крупные компании имеют собственные службы безопасности. Средний бизнес зачастую пользуется услугами частных фирм, реализующих и поддерживающих корпоративные системы защиты информации. Эти службы часто объединяют усилия и сотрудничают друг с другом и с государственными структурами.

Проблемой организации системы защиты информации в Великобритании является консервативность. Разработанная когда-то система остается неизменной уже достаточно давно. Между тем в области информационных технологий все меняется очень быстро, так что периодически возникает необходимость в определенной коррекции органов защиты данных (Давлетханов, 2004).

4.3.2. Организация защиты информации в Германии.

Германия - одна из самых продвинутых в области информационной безопасности стран Западной Европы. Она обладает развитой структурой органов, заботящихся о защите различных видов тайн. Первоначальной задачей этих структур была защита от промышленного шпионажа и охрана государственных секретов. Впервые организации, занимающиеся этими вопросами, начали создаваться в 19 веке. Однако и сегодня во всех компаниях, в которых работают хотя бы десять человек, один из сотрудников назначается уполномоченным по защите информации. В его обязанности входит противостояние всем преступлениям в компьютерной сфере, а также тесное сотрудничество с соответствующими отделами правоохранительных органов.

До 1970 года в Германии (то есть в ФРГ) никто не занимался вопросами защиты персональных данных. Однако с тех пор все изменилось. Сегодня каждый гражданин Германии имеет право на защиту личной информации.

Немецкое представление об информационной войне объединяет наступательную и оборонительную составляющие в единое целое для

достижения национальных интересов. При определении угроз и возможных ответных действий, иностранные государства рассматриваются отдельно от негосударственных объединений (политические партии, международные организации и средства массовой информации), преступных сообществ (организованные преступные группы, хакеры и т.д.), и индивидуумов (включая религиозных фанатиков и др.).

Управление средствами массовой информации является особенностью немецкого представления об информационной войне. Кроме того, специалисты Федеративной Республики Германии (далее Германия) отдельно вводят понятие экономической информационной войны.

Немецкие эксперты в связи с обострением интереса к проблеме ИВ считают в ближайшие годы вероятным возрастание уязвимости экономической и политической инфраструктуры индустриально развитых стран в результате нарушения нормального функционирования информационных систем под действием информационного оружия. Данное обстоятельство специалисты объясняют наблюдаемой тенденцией к переходу ведущих государств на новый тип организации общества - «информационное общество».

Предполагается, что в результате развития информационных технологий произойдет глобализация не только мирового рынка товаров, но и производственных услуг. Предприятия вынуждены будут перейти от специализации на виде продукции к специализации на конкретном технологическом процессе. Это приведет к резкому увеличению кооперационных связей и соответственно уязвимости сведений, составляющих коммерческую тайну при нарушении работы внешних коммуникационных цепей.

В «информационном обществе» будет наблюдаться дальнейшая монополизация рынков, в том числе и информационно-коммуникационных услуг.

Сосредоточение в рамках транснациональных компаний, различных компонентов информационных систем приведет к угрозе потери суверенитетов государств и сделает уязвимой всю инфраструктуру принятия политических решений и управления. Так, монопольные позиции фирм США в системах глобальной космической связи (проект Iridium), глобальной навигационной системы (GPS) в рамках сети Интернет уже сейчас рассматриваются некоторыми экспертами страны как угроза национальному суверенитету Германии.

Различные вопросы обеспечения безопасности информационного обслуживания в таких областях, как промышленное производство, банковское дело, научные исследования, медицина, по оценкам немецких специалистов в области информационной безопасности, имеют важное значение и являются неотъемлемым условием сохранения лидирующих позиций Германии.

Координирующим правительственным органом, ответственным за обеспечение безопасности информационных потоков, является образованная в 1991 году Федеральная служба безопасности в сфере информационной техники (BSI). Общая концепция деятельности BSI в настоящее время предусматривает выполнение в тесном взаимодействии с НАТО и ЕС следующих функций:

– оценка риска внедрения информационных технологий;

– разработка критериев, методов и испытательных средств для оценки степени защищенности национальных коммуникационных систем;

– проверка степени защищенности информационных систем и выдача соответствующих сертификатов;

– выдача разрешений на внедрение информационных систем в важные государственные объекты;

– осуществление специальных мер безопасности информационного обмена в государственных органах, полиции и т. д.;

– консультация представителей промышленности.

Для контроля защиты личной информации была создана специальная структура из уполномоченных по защите персональной тайны. Ее главная особенность - независимость от любых государственных органов. В задачи уполномоченных входит проверка жалоб граждан о незаконном использовании их личных данных. Причем большая часть претензий предъявляется государственным структурам, в том числе и правоохранительным органам. Таким образом, независимость уполномоченных органов - это гарантия свободы граждан и надежная защита от произвола со стороны государства.

4.3.3. Организация защиты информации во Франции.

Правительство Французской Республики (далее Франция) рассматривает концепцию информационной войны, как совокупность двух главных элементов: военного и экономического. Военная концепция видит место информационным действиям в контексте конфликтов малой интенсивности или в миротворческих операциях, т.е. предполагает несколько ограниченный характер. В этом контексте союзники не рассматриваются противниками.

Напротив, экономический элемент включает более широкий диапазон потенциального применения информационных операций. Французское представление конфликта в экономической сфере имеет более глубокое понимание в отличие от большинства других европейских стран. В этом случае французы не видят себя связанными рамками НАТО, ООН или согласием США. Их подход к экономическому конфликту учитывает тот факт, чтобы быть и союзником и противником одновременно.

Франция активно формирует структуры по контролю ее граждан в киберпространстве. По аналогии с американской системой «Эшелон» французы создали собственную версию этой системы, которая направлена на перехват фактически всех частных глобальных коммуникаций.

Французское военное руководство проявляет растущую озабоченность по поводу отставания национальных исследований в области ИВ от

лидирующих в этой сфере США. В специальной записке, посвященной указанной проблеме, начальник штаба ВС Франции, констатируя появление новой разновидности войны - информационной и пристальное внимание к ней со стороны США и ряда других стран, призвал ускорить и расширить соответствующие национальные научно-исследовательские и опытно-конструкторские работы (НИОКР).

Французские специалисты в области информационных технологий развернули обсуждение роли и значения ИВ в современных условиях. По их мнению, ход войны в Персидском заливе показал, что информационное оружие выходит на первое место среди применяемых в современной войне видов вооружений. Это явилось причиной ускорения ряда европейских программ в области средств коммуникаций. В то же время меры европейских государств по увеличению собственного потенциала информационного оружия, по мнению аналитиков французского Центра исследований стратегических технологий (Centre de recherche et d'etudes sur les strategic tecnologiques), наталкиваются на серьезное противодействие США. Стремясь затормозить собственные разработки европейцев, США даже идут на продажу по демпинговым ценам космических систем слежения и контроля линий связи, предоставляют доступ к накопленным базам данных.

Эксперты Института международных отношений и стратегических исследований (Institut de relations intemationales et strategiques) полагают, что сегодня союзники США по НАТО находятся в серьезной военной зависимости от них, поскольку в своих системах вооружений широко используют американское программное обеспечение (в частности, указывают на систему позиционирования французских ракет).

Анализируя новые аспекты американской военной доктрины, направленные на достижение победы бескровными методами при минимуме потерь, французские специалисты обращают внимание на то, что главным средством является не контроль над территорией, а полное господство в «инфосфере», представляющей собой совокупность информационных систем

и сетей связи на планете. При этом война приобретает виртуальный и невидимый характер, что позволяет добиться решающего преимущества, не разворачивая боевых действий.

Указывая на эту особенность устремлений США, ряд не связанных с Министерством обороны Франции экспертов из Центра исследований в области социальных наук критикуют существующие программы военных инвестиций. По их мнению, французские военные находятся под впечатлением успехов США в области применения высокоточного оружия и систем радиоэлектронной борьбы (РЭБ) и упускают значительно большую составляющую ИВ - средства контроля за информацией.

Французские вооруженные силы, в отличие от американских, не располагают высокими технологиями, позволяющими осуществлять открытое или неявное руководство операциями. Следовательно, они могут оказывать на поле боя лишь второстепенное значение, быть придатком американских высоких технологий и нести непосредственные потери.

В настоящее время во Франции создается информационно-аналитическая система поддержки принятия решений высшего руководства страны в любых кризисных ситуациях. Основная цель разрабатываемой системы - обеспечение высших органов государственного управления необходимой информацией, моделирование реальной обстановки в развитии, подготовка прогнозов и рекомендаций.

По мнению руководителей Центра исследований стратегии и технологии, Франция должна изменить свою политику в области информационных разработок и финансирования военного производства, отдав приоритет информационным системам, в том числе разведывательным спутникам, телекоммуникационным сетям, средствам управления, и при этом активно использовать средства гражданской информатики. Кроме того, учитывая темпы развития электроники и информатики, представленных во всех системах вооружений, необходимо увеличить срок службы материальной части, осуществляя регулярную модернизацию за счет

электронно-информационных компонентов. А также необходимо значительно увеличить долю расходов на системы, позволяющие осуществлять моделирование как на всех этапах создания систем вооружений, так и на этапе их боевого применения, что обеспечит высокий уровень технологических исследований.

Франция уделяет особое внимание вопросу защиты своих информационных ресурсов от несанкционированного проникновения и манипулирования.

Разработкой стратегических направлений политики по обеспечению национальной безопасности занимается объединение CLUSIF (Club de la securite informatique francaise), являющееся по своему статусу открытой ассоциацией юридических и физических лиц, работающих в области информатики. CLUSIF пользуется полной поддержкой государства и имеет тесный контакт со спецслужбами.

Французские эксперты полагают, что наилучшую защиту информации в сетях обеспечивают только методы шифрации. В связи с этим ведется активное внедрение криптографического программного обеспечения и оборудования в наиболее важные системы. Работы по созданию соответствующих устройств осуществляются фирмами Thomson, Sagem, Matra.

Анализ оценок французских экспертов показывает, что угроза ИВ воспринимается как реальная, однако защитные действия по предотвращению или снижению вероятности угрозы наталкиваются на инерционность системы военных расходов и недостаточное осознание всех возможностей информационного оружия, которые далеко выходят за рамки традиционных средств защиты информации.

Во Франции и Германии существует наиболее совершенная защита персональных данных и система служб безопасности на предприятиях

4.4. Организация системы защиты информации в КНР

Информационная безопасность для Китая — это прежде всего безопасность его инноваций, и в этом важная особенность подхода страны к вопросам информационной и кибербезопасности. Китайская модель инновационного развития основывается на четком следовании национальным интересам, непрерывном расширении научной и технической базы страны, активном привлечении инвестиций в разработку научно-исследовательской и опытно-конструкторской работы (НИОКР), постоянном совершенствовании законодательства в сфере защиты интеллектуальной собственности. В программе признается, что в производстве высокотехнологичных продуктов в области информационно-коммуникационных технологий (ИКТ) Китай все еще зависим от западных технологий, которые при помощи встроенных шпионских программ могут нанести вред всей китайской информационной инфраструктуре, инновационным разработкам и создать угрозу национальной безопасности страны. Снижение зависимости от западных ИКТ рассматривается как одно из важных средств обеспечения кибербезопасности КНР.

В Китае отсутствует единая стратегия развития киберпространства и обеспечения безопасности информационных систем, но это вовсе не означает, что отсутствует концептуальное обоснование значимости проблемы. Основным документом, в котором подчеркивается значимая роль ИКТ в жизни китайского общества, является Всеобъемлющая концепция национальной безопасности Китая. В концепции отмечено, что информация в современном мире не только открывает много возможностей, но и создает угрозы политической, экономической, военной безопасности КНР. Большое внимание в документе уделено интернету как наиболее значимому, но наименее управляемому сегменту глобального информационного пространства

«Интернет — это орудие работы, а не средство времяпрепровождения», — этот лозунг, широко распространенный в стране, четко отражает отношение властей к новым средствам массовой коммуникации. Овладение китайцами приемами работы в сети, а также получение информации, полезной для нации, по мнению властей, способны создать новые рабочие места, повысить жизненный уровень населения, ускорить развитие отсталых регионов, сформировать новую прогрессивную китайскую нацию, а значит, сделать Китай самодостаточной державой и помочь ей занять лидирующие позиции в мире во всех сферах жизнедеятельности.

Китайские законы и нормативные акты, регулирующие развитие интернета, отличаются особой жесткостью. В 1994 г. Госсовет КНР издал Правила регулирования, обеспечивающие безопасность компьютерных и информационных систем, которые дали Министерству государственной безопасности права и полномочия на управление Сетью. В соответствии с правилами правительство имеет право нейтрализовать практически любой неугодный ресурс. К примеру, ответственность предусмотрена за публикацию «материалов, вредящих репутации государства», но интернет-пользователь не имеет никаких способов определения, вреден ли материал или нет (в сводах законов данное понятие никак не расшифровывается).В соответствии с национальным законодательством, в Китае существует двухступенчатый доступ к интернету. На первом уровне пользователи могут выйти в мировую сеть лишь через магистральные узлы [backbone networks]. Существует ограниченное количество подобных ключевых узлов, которые находятся в ведении центральных министерств или групп, имеющих мощную политическую поддержку власти. На китайский интернет-трафик была наложена сложная система файрволов [system of firewalls], которая ограничивает доступ к проблемным, по мнению государства, внешним ресурсам. В стране успешно реализуется проект Золотой щит(неофициальное название — Великий китайский файрвол, игра слов по ассоциации с Великой китайской стеной), в рамках которого создана сложная система фильтрации

содержимого интернета в КНР. В рамках проекта функционирует система серверов на интернет-канале между провайдерами и международными сетями передачи информации, которая фильтрует информацию. Файрволы применяются китайскими провайдерами для защиты от вирусов и хакеров, а также для блокирования доступа к определенным сайтам.

В 2005 г. были введены усиленные меры по регламентированию деятельности граждан в интернете. Так, было запрещено анонимное общение, введена обязательная регистрация сайтов, проведена серия облав на владельцев нелегальных интернет-кафе. С 2006 г. в Китае начало свою работу специальное полицейское ведомство для контроля за интернетом.

Интернет-полицейские призваны следить за содержанием сайтов, онлайн-форумов и социальных сетей. На многих, прежде всего крупных китайских сайтах, чтобы завести свой блог или оставить сообщение на форуме, нужно пройти обязательную регистрацию, при которой необходимо указать свои настоящие личные данные, включая имя, адрес и идентификационный номер. Все эти данные через компьютерный банк данных проверяют на подлинность, и только после этого регистрация считается пройденной.

К корпоративным пользователям всемирной сети предъявляются более жесткие правила пользования интернетом. Любая компания, желающая подключится к интернету, в течение нескольких месяцев проходит тщательную проверку. Определенные послабления со стороны цензоров имеют лишь крупные компании, которым в силу их коммерческой деятельности необходим доступ к более широкому контенту. Действия всех корпоративных клиентов фиксируются, нарушители наказываются. На предприятиях ведется журнал, где аргументируется посещение каждого сомнительного сайта. Распространена практика использования публичной электронной почты, когда группе сотрудников компании присваивается один и тот же адрес, а переадресация корреспонденции производится через системного оператора или дежурного администратора локальной сети.

Создать собственный интернет-сайт юридическому лицу также непросто. Каждый онлайн-ресурс должен получить лицензию, выданную Министерством промышленности и информатизации. Для этого компании необходимо иметь солидный уставный капитал. С 2008 г., согласно новым правилам, подавать заявки на получение лицензий на радиовещание или потоковую трансляцию (видео) онлайн могут только компании, принадлежащие властям или контролируемые государством. В 2009 г. вступил в силу закон о том, что для регистрации доменных имен в зоне необходимо подавать письменное заявление, в котором помимо всех личных данных надо и номер лицензии предприятия на коммерческую деятельность.

Методы контроля, существующие в Китае, вовсе не означают, что интернет в стране отстает от западных тенденций развития глобальной сети. Китайская система управления интернетом весьма гибкая и предусматривает различные послабления для определенных категорий пользователей: ученых, работников СМИ, бизнесменов, в том числе иностранных инвесторов. Китайский рынок интернет-услуг — один из самых быстрорастущих, что особо привлекает внимание инвесторов.

Поощряются научные и прикладные исследования зарубежных компаний в КНР, внедряется система так называемых информационных портов — зон свободного таможенного и налогового регулирования, ориентированных на развитие инновационных технологий, электронной коммерции и информатики.

Активное привлечение западных технологий и иностранных инвестиций вовсе не означает, что они свободно ведут свою деятельность в стране и неподконтрольны власти. Госсовет КНР рассматривает интернет как важный объект государственной инфраструктуры, который должен находиться в рамках суверенного управления Китая. Посягательства на китайский сегмент интернета со стороны внешних сил рассматриваются как угроза национальной безопасности. Иностранные граждане и компании, находящиеся в КНР, при пользовании глобальной сетью должны следовать

нормам законодательства и требованиям властей. Любое иностранное юридическое лицо, перед тем как войти на китайский рынок, принимает правила игры китайского правительства и вынуждено действовать в соответствии с ними [39].

4.5. Организация системы защиты информации в ведущих мировых компаниях

4.5.1. Практика компании Microsoft в области информационной безопасности.

Компания Microsoft обладает сложной корпоративной инфраструктурой, которая состоит из 5 тысяч серверов Windows Server 2003 (из них 800 серверов приложений). В штате компании работает более 55 тысяч сотрудников. Сотрудники очень хорошо подготовлены технически, и 95% из них обладают администраторскими полномочиями на своих компьютерах. Более 300 тысяч компьютеров компании, на которых используется более 1600 приложений, расположены в 400 представительствах по всему миру.

В сеть компании ежедневно поступает приблизительно 8 миллионов почтовых сообщений извне, и приблизительно 6,5 миллионов почтовых сообщений циркулирует ежедневно в сети самой компании, доступ к которой имеют 30 тысяч партнеров.

Уникальная инфраструктура по разработке продуктов, тестированию и поддержке, исходный код продуктов требуют особой защиты. Ежемесячно осуществляется свыше 100 тысяч попыток вторжения в сеть компании. Впочтовую систему ежемесячно поступает свыше 125 тысяч почтовых сообщений, зараженных вирусами (примерно 800 новых вирусов в день) и 2,4 миллиона почтовых сообщений со спамом ежедневно.

Обязанность по обеспечению информационной безопасности в Microsoft возложена на две группы: Corporate Security Group и Operations and Technology Group.

Компания Microsoft разработала стратегию безопасности, состоящую из четырех основных компонентов:

– миссии корпоративной безопасности;

– принципов операционной безопасности:

– модели принятия решений, основанной на анализе рисков;

– тактической приоритезации деятельности по уменьшению рисков.

Фундаментом для дизайна, разработки и работы защищенных систем являются принципы безопасности, разделенные на несколько категорий (таблица 1).

Таблица 1

Классификация принципов ИБ

Категория	Принцип безопасности
Организационная Направлена на получение поддержки со стороны руководства по управлению рисками и на ознакомление с вопросами безопасности	Управление рисками в соответствии с задачами бизнеса Определение ролей и обязанностей Инвестиции в дизайн защищенности Обеспечение безопасности операций
Пользователи и данные Включает аутентификацию, защиту данных пользователей, авторизацию	Управление принципом наименьших привилегий Классификация данных и их использование Внедрение защиты данных и идентичности пользователя Защита информации Гарантия целостности данных Мониторинг гарантии идентичности Доступность
Разработка приложений и систем Выделена для дизайна и разработки защищенных систем	Встраивание безопасности в жизненный цикл Дизайн «многоуровневой защиты» Уменьшение поверхности атаки Сохранение простоты использования
Операции и сопровождение Объединение людей, процессов и технологий для построения, поддержки и использования защищенных систем	План по поддержке систем Внедрение защищенных конфигураций Мониторинг и журналирование Практика реагирования на инциденты Проверка процедур восстановления в случае аварии

Для обеспечения информационной безопасности Corporate Security Group использует управление информационными рисками, под которым здесь понимается процесс определения, оценки и уменьшения рисков на

постоянной основе. Управление рисками безопасности позволяет найти разумный баланс между стоимостью средств/мер защиты и требованиями бизнеса.

Модель управления рисками Corporate Security Group представляет собой комбинацию различных подходов, таких как количественный анализ рисков, анализ возврата инвестиций в безопасность, качественный анализ рисков, а также подходы лучших практик. Для реализации этого подхода Corporate Security Group разработала структуру, которая основана на традиционной модели управления информационными рисками.

Инвестирование в процесс управления риском с цельной структурой и определенными ролями и обязанностями готовит организацию к определению приоритетов, планированию уменьшения угрозы и переход к следующей угрозе или уязвимости. Для наилучшего управления рисками Corporate Security Group следует традиционному подходу по управлению рисками, состоящему из четырех этапов:

– *оценки информационных рисков* (выполнение методологии оценки рисков для определения величины риска);

– *политики безопасности* (разработка политики безопасности по уменьшению, уклонению и предупреждению рисков);

– *внедрения средств защиты* (объединение сотрудников, процессов и технологий для уменьшения рисков, основанных на анализе соотношения цена/качество);

– *аудита безопасности и измерения текущей защищенности* (мониторинг, аудит безопасности и измерение защищенности информационных систем компании).

Как видно из рис. 9, разработка политики безопасности является одним из этапов по управлению информационными рисками.

Рис. 9. Этапы управления рисками

Методология, используемая при разработке политики, базируется на Стандарте ISO 17799:2002 (BS 7799).

Рекомендуемая Microsoft политика безопасности включает в себя:

– определение целей безопасности;

– важность обеспечения безопасности;

– определение требуемого уровня безопасности;

– стандарты безопасности, включая стратегии их мониторинга и аудита;

– роли и ответственность по обеспечению безопасности;

– цели и задачи офицера по безопасности;

– определение процессов по защите индивидуальных компонентов архитектуры;

– определение требуемого обучения вопросам безопасности.

Примерами декларируемых целей безопасности являются:

– достижение максимально возможного уровня качества, надежности и конфиденциальности информации;

– сохранение репутации компании;

– недопущение повреждения или утери информации, процессов, собственности компании и обеспечение, таким образом, непрерывности работы компании;

– сохранение ценности информации, интеллектуальной собственности и технологических ресурсов.

Для разработки целей безопасности создается комитет по информационной безопасности, состоящий из сотрудников с опытом работы в области безопасности, технических сотрудников и представителей других подразделений под руководством офицера по безопасности.

Комитет решает следующие задачи:

– разработку и управление жизненным циклом политики безопасности;

– создание процессов, обеспечивающих достижение целей безопасности;

– создание процессов и планов по реализации стандартов, описанных в политике;

– помощь и организации программ ознакомления с вопросами безопасности;

– консультирование персонала по вопросам безопасности;

– определение бюджета и требуемых ресурсов по обеспечению безопасности.

4.5.2. Практика компании Cisco Systems в разработке сетевой политики безопасности.

По мнению специалистов по информационной безопасности компании Cisco, отсутствие сетевой политики безопасности может привести к серьезным инцидентам. Ее разработку рекомендуется начинать с оценки рисков сети и создания рабочей группы по реагированию на инциденты.

В компании Cisco рекомендуют создавать политики использования, которые описывают роли и обязанности сотрудников компании для надлежащей защиты корпоративной конфиденциальной информации. Начать можно с разработки главной политики безопасности, в которой четко нужно прописать общие цели и задачи организации режима информационной безопасности компании.

Следующий шаг - создание политики допустимого использования для партнеров, чтобы проинформировать их о доступной им информации. При этом следует четко изложить любые действия, которые будут восприниматься как враждебные, а также описать возможные способы реагирования при обнаружении таких действий.

В заключение необходимо создать политику допустимого использования для администраторов, где будут описаны процедуры администрирования учетных записей сотрудников, внедрения политики и проверки привилегий. Также, если в компании существуют определенные политики использования паролей или категорирования информации, они должны быть здесь упомянуты. Далее необходимо проверить названные политики на непротиворечивость и полноту, а также убедиться в том, что сформулированные требования к администраторам нашли свое отображение в планах по обучению.

Проведение анализа рисков информационной безопасности.

Назначение анализа рисков состоит в том, чтобы категорировать информационные активы компании, определить наиболее значимые угрозы и уязвимости активов и обоснованно выбрать соответствующие контрмеры безопасности. Подразумевается, что это позволит найти и поддерживать приемлемый баланс между безопасностью и требуемым уровнем доступа к сети. Различают следующие уровни информационных рисков:

1. *Низкий уровень риска.* Скомпрометированные информационные системы и данные (доступные для изучения неавторизованными лицами,

поврежденные или утерянные) не приведут к серьезному ущербу, финансовым проблемам или к проблемам с правоохранительными органами.

2. *Средний уровень риска.* Скомпрометированные информационные системы и данные приведут к умеренному ущербу или к небольшим проблемам с правоохранительными органами, или к умеренным финансовым проблемам, а также к получению дальнейшего доступа к другим системам. Затронутые системы и информация требуют умеренных усилий по восстановлению.

3. *Высокий уровень риска*. Скомпрометированные информационные системы и данные приведут к значительному ущербу или к серьезным проблемам с правоохранительными органами, или к финансовым проблемам, нанесению ущерба здоровью и безопасности сотрудников. Затронутые системы и информация требуют существенных усилий по восстановлению.

Рекомендуется определить уровень риска для каждого из перечисленных устройств: сетевых устройств, устройств мониторинга сети, серверов аутентификации, почтовых серверов, файловых серверов, серверов сетевых приложений (DNS и DHCP), сервера баз данных (Oracle, MS SQL Server), персональных компьютеров и других устройств.

При этом считается, что сетевое оборудование, такое как коммутаторы, маршрутизаторы, DNS- и DHCP-серверы в случае компрометации могут быть использованы для дальнейшего проникновения в сеть и поэтому должны относиться к группе среднего или высокого уровней рисков. Возможное повреждение этих устройств может привести к прекращению работы всей сети. Такие инциденты могут нанести серьезный ущерб компании.

После определения уровней риска необходимо определить роли пользователей этих систем. Рекомендуется выделять пять наиболее общих типов пользователей.

1. *Администраторы.* Внутренние пользователи, отвечающие за сетевые ресурсы.

2. *Привилегированные пользователи.* Внутренние пользователи с необходимостью высокого уровня доступа.

3. *Рядовые пользователи.* Внутренние пользователи с обычным уровнем доступа.

4. *Партнеры.* Внешние пользователи с необходимостью доступа к некоторым ресурсам.

5. *Другие.* Внешние пользователи или клиенты.

Определение уровней рисков и типов доступа, требуемых для каждой сети, позволяет сформировать некоторую матрицу безопасности (таблица 2). Эта матрица безопасности является стартовой точкой для дальнейших шагов по обеспечению безопасности, например таких, как создание соответствующей стратегии по ограничению доступа к сетевым ресурсам.

Таблица 2

Матрица безопасности Cisco

Система	Описание	Уровень риска	Типы пользователей
ATM-коммутаторы	Основные сетевые устройства	Высокий	Администраторы для конфигурирования (только персонал поддержки]; все другие для использования в качестве транспорта
Сетевые маршрутизаторы	Сетевые устройства распределения	Высокий	Администраторы для конфигурирования (только персонал поддержки); все другие для использования в качестве транспорта
Коммутаторы доступа	Сетевые устройства доступа	Средний	Администраторы для конфигурирования (только персонал поддержки); все другие для использования в качестве транспорта
ISDN или dial up сервера	Сетевые устройства доступа	Средний	Администраторы для конфигурирования (только персонал поддержки); партнеры и привилегированные пользователи для специального доступа
Межсетевые экраны	Сетевые устройства доступа	Высокий	Администраторы для конфигурирования (только персонал поддержки]; все другие для использования а качестве транспорта
Серверы DNS и DHCP	Сетевые приложения	Средний	Администраторы для конфигурирования; пользователи для повседневного использования
Внешние	Сетевое	Низкий	Администраторы для

почтовые серверы	приложение		конфигурирования; все другие как транспорт для передачи почты между Интернетом и внутренним почтовым сервером
Внутренний почтовый сервер	Сетевое приложение	Средний	Администраторы для конфигурирования; все другие для повседневного использования
Сервер базы данных Oracle	Сетевое приложение	Средний или высокий	Администраторы для конфигурирования; привилегированные пользователи для обновления информации; сотрудники компании для доступа к информации; все остальные имеют частичный доступ к информации

Определение состава и структуры группы сетевой безопасности.

Специалистами по защите информации компании Cisco Systems рекомендуется создать группу сетевой безопасности под руководством менеджера по безопасности с представителями из каждой значимой бизнес-единицы компании (минимум - из представителей бизнес-единиц развития, исполнения и производства и/или продаж). Члены группы должны хорошо знать политику безопасности и технические аспекты защищаемых систем и сетей. Часто это требует дополнительного обучения сотрудников названной группы. Группа безопасности должна принимать участие в разработке политики безопасности, организации режима информационной безопасности, а также своевременно реагировать на инциденты в области информационной безопасности компании.

Процесс сопровождения политик безопасности заключается в контроле и при необходимости пересмотре политик безопасности компании. Как минимум, необходим ежегодный пересмотр политики безопасности и проведение анализа рисков.

На практике группа сетевой безопасности должна проводить анализ рисков, подтверждать запросы на проведение изменений в системе безопасности, проводить мониторинг оповещений о появлении новых уязвимостей с использованием списков рассылок вендоров и независимых аналитических центров, например CERT или SANS, и поддерживать

соответствие требованиям политики безопасности с помощью определенных технических и организационных мер.

Так как нарушения безопасности часто обнаруживаются во время проведения мониторинга сети, члены группы сетевой безопасности должны участвовать в расследовании инцидентов и предупреждению подобных нарушений в дальнейшем. Каждый член группы безопасности должен обладать хорошими знаниями в области прикладного, системного и сетевого программного и аппаратного обеспечения систем безопасности. При этом рекомендуется определить индивидуальные роли и обязанности каждого члена группы сетевой безопасности.

Предупреждение нарушений политики безопасности компании.

Под предупреждением нарушений компания Cisco понимает подтверждение изменений в системах безопасности и мониторинг безопасности сети.

Изменения в системах безопасности могут быть определены как изменения в сетевом оборудовании, которые могут иметь потенциальное воздействие на состояние безопасности сети. Политика безопасности компании должна определять специфические требования конфигурации безопасности, описанные не техническими терминами. Другими словами, вместо формулировки «Не разрешены внешние ftp-соединения во внутреннюю сеть» лучше воспользоваться определением «Внешние соединения не должны быть способны получать файлы из внутренней сети». При этом желательно стремиться к определению уникальных требований компании. Использование стандартных шаблонов обеспечения безопасности и настроек по умолчанию в подходе компании Cisco настоятельно не рекомендуется.

Группа сетевой безопасности просматривает описанные общедоступным языком требования и определяет соответствие технического дизайна и настроек элементов сети этим требованиям. Если выявляются несоответствия, группа безопасности вносит необходимые изменения в

сетевую конфигурацию для выполнения требований политики безопасности, при этом группой сетевой безопасности могут контролироваться не все изменения. Важно просмотреть те из них, которые наиболее значимы и существенны для сети компании в плане безопасности, например:

– любые изменения в конфигурации межсетевых экранов;

– любые изменения в списках контроля доступа;

– любые изменения в конфигурации SNMP;

– любые изменения или обновления программного обеспечения, версии которого отличаются от разрешенного списка версий программного обеспечения.

Компания Cisco рекомендует следовать следующим правилам:

– регулярно изменять пароли на сетевых устройствах;

– ограничить доступ к сетевым устройствам согласно утвержденному списку сотрудников;

– гарантировать, что текущая версия программного обеспечения сетевого и серверного оборудования соответствует требованиям безопасности.

В добавление к этим правилам необходимо включить представителя группы сетевой безопасности в постоянно действующую комиссию компании по утверждению изменений для отслеживания всех изменений, происходящих в сети компании. Представитель группы безопасности может запретить реализацию любого изменения, связанного с безопасностью, до тех пор, пока это изменение не будет разрешено руководителем группы сетевой безопасности.

Мониторинг сетевой безопасности фокусируется на обнаружении изменений в сети, позволяющих определить нарушение безопасности. Отправной точкой мониторинга безопасности является определение понятия нарушения безопасности. Анализ угроз и информационных рисков позволяет сделать выводы о требуемом уровне полноты мониторинга безопасности сети компании. В дальнейшем при проведении процесса утверждения изменений

безопасности каждый раз проверяется значимость выявленных угроз сети. Оценивание этих угроз определяет объекты и частоту мониторинга.

Так, в матрице анализа рисков межсетевой экран определен как устройство с высоким уровнем риска. Это означает, что мониторинг межсетевого экрана выполняется постоянно в режиме реального времени. Из раздела подтверждения изменений безопасности следует, что необходимо отслеживать все изменения в настройках конфигурации межсетевого экрана, то есть SNMP-агент должен отслеживать такие события, как отвергнутые попытки регистрации, необычный трафик, изменения на межсетевом экране, предоставление доступа к межсетевому экрану и установление соединений через межсетевой экран.

Следуя этому примеру, можно создать политику мониторинга для каждого компонента сети, определенного при проведении анализа рисков. Рекомендуется проводить мониторинг компонентов сети с низким уровнем риска еженедельно, со средним уровнем риска ежедневно, с высоким уровнем риска раз в час. При этом, если требуется более быстрое время реагирования, необходимо уменьшить названные промежутки времени.

Важно также определить в политике безопасности порядок уведомления членов группы сетевой безопасности о нарушениях. Как правило, средства мониторинга безопасности сети будут первыми автономно обнаруживать нарушения. Должна быть предусмотрена возможность отправки по любым доступным каналам связи уведомлений в центр реагирования на инциденты в области безопасности для оперативного оповещения членов группы сетевой безопасности.

Реагирование на нарушения политики безопасности.

Под реагированием на нарушения безопасности здесь понимается определение нарушений безопасности, порядка восстановления и пересмотра правил безопасности.

При обнаружении нарушения безопасности важно своевременно отреагировать и оперативно восстановить нормальное функционирование

сервисов сети. Главное правило - своевременное оповещение группы сетевой безопасности после обнаружения нарушения. Если оно не выполняется, реагирование будет замедлено, а, следовательно, последствия вторжения окажутся более тяжелыми, поэтому необходимо разработать соответствующую процедуру реагирования и оповещения действенную 24 часа в день, 7 дней в неделю.

Далее необходимо четко определить уровень привилегий по внесению изменений, а также порядок внесения изменений. Здесь возможны следующие корректирующие действия:

– реализация изменений для предупреждения дальнейшего распространения нарушения;

– изолирование поврежденных систем;

– взаимодействие с провайдером для отслеживания источника атаки;

– использование записывающих устройств для сбора доказательств;

– отключение поврежденных систем или источников атаки;

– обращение в правоохранительные органы или федеральные агентства;

– выключение поврежденных систем;

– восстановление систем в соответствии со списком приоритетности;

– уведомление руководства и юристов компании.

Необходимо детализировать любые изменения в политике безопасности, которые могут быть произведены без необходимости получения разрешения от руководства.

Отметим, что существует две основных причины сбора и хранения информации об атаках: для определения последствий реализации атаки и для расследования и преследования злоумышленников. Тип информации и способ ее сбора зависит от этих целей.

Для определения последствий нарушения безопасности рекомендуется проделать следующие шаги:

– зафиксировать инцидент с помощью записи сетевою трафика, снятия копий файлов журналов, активных учетных записей и сетевых подключений;

– ограничить дальнейшие нарушения путем отключения учетных записей, отсоединения сетевого оборудования от локальной сети и от Интернета;

– провести резервное копирование скомпрометированных систем для проведения детального анализа повреждений и метода атаки;

– попытаться найти другие подтверждения компрометации (часто при компрометации системы оказываются затронутыми другие системы и учетные записи);

– хранить и просматривать файлы журналов устройств безопасности и сетевого мониторинга, так как они часто являются ключом к определению метода атаки.

В случае необходимости проведения юридических действий, следует уведомить руководство компании и привлечь обслуживающих компанию юристов для сбора соответствующих доказательств. Если нарушение было внутренним, потребуется привлечь сотрудников отдела кадров.

Восстановление работоспособности сервисов сети компании является конечной целью процедуры реагирования на нарушения в области безопасности. Здесь необходимо определить порядок восстановления доступности сервисов, например с помощью процедур резервного копирования. При этом надо учитывать, что каждая система имеет для этого собственные механизмы, поэтому политика безопасности, являясь общей для всех элементов сети, при необходимости должна позволять детализировать условия восстановления конкретного элемента. Если требуется получить разрешение на восстановление, необходимо описать порядок получения разрешения в политике безопасности.

Пересмотр политики безопасности является заключительным этапом ее жизненного цикла. Здесь важно обратить внимание на следующие аспекты. Политика безопасности должна быть «жизнеспособным» документом,

адаптированным к изменяющимся условиям. Сравнение существующей политики безопасности с лучшими практиками в этой области и последующий пересмотр политики должны поддерживать в состоянии защищенность активов сети. Необходимо регулярно обращаться на сайты различных независимых аналитических центров, например CERT или SANS, за полезными советами и рекомендациями по обеспечению безопасности и учитывать их в поддерживаемой политике безопасности компании.

Также рекомендуется проводить аудит безопасности сети силами консалтинговых компаний, обладающих опытом таких работ. Для сетей с высокими требованиями к доступности информационных ресурсов рекомендуется проведение, как минимум, ежегодного независимого аудита безопасности. Кроме того, достаточно эффективны и внутренние тренировки, направленные на отработку действий в чрезвычайных ситуациях.

4.5.3. Практика компании IBM в области защиты информации.

В компании IBM считается что, разработка корпоративных руководящих документов в области безопасности должна начинаться с создания политики информационной безопасности компании. При этом рекомендуется использовать международный стандарт ISO 17799:2005 и рассматривать политику безопасности компании как составную часть процесса управления информационными рисками (рис. 10). Считается, что разработка политики безопасности относится к стратегическим задачам TOP-менеджмента компании, который способен адекватно оценить стоимость информационных активов компании и принять обоснованные решения по защите информации с учетом целей и задач бизнеса.

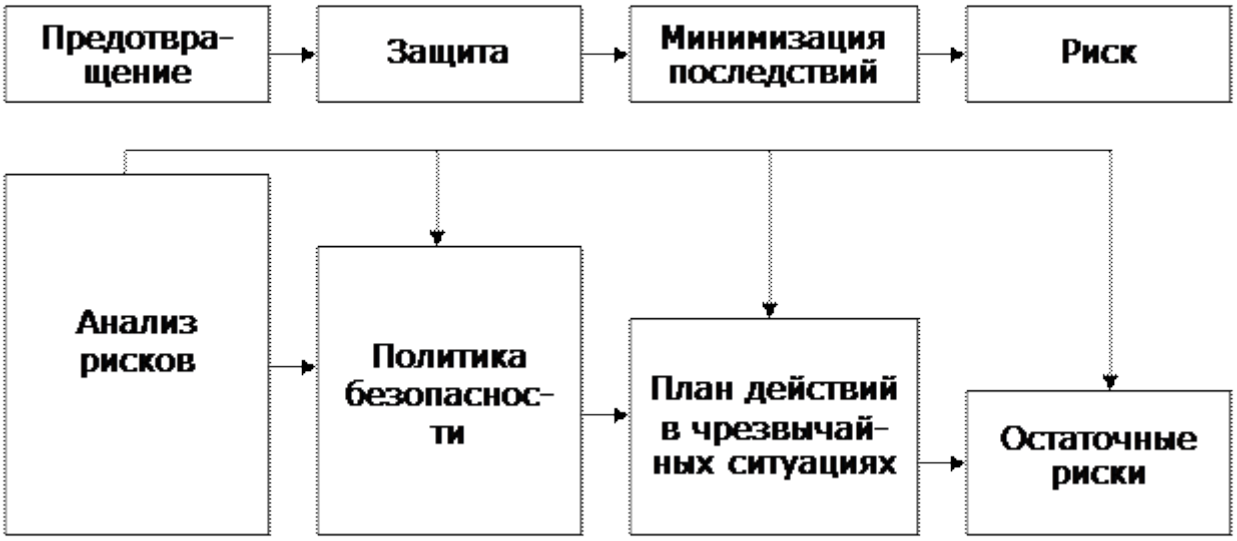

Рис. 10. Процесс разработки политики безопасности компании

Компания IBM выделяет следующие основные этапы разработки политики безопасности:

1. Определение информационных рисков компании, способных нанести максимальный ущерб для разработки в дальнейшем процедур и мер по предупреждению их возникновения,

2. Разработка политики безопасности, которая описывает меры защиты информационных актинов, адекватных целям и задачам бизнеса.

3. Выработка планов действий в чрезвычайных ситуациях и в случаях, когда выбранные меры защиты не смогли предотвратить инциденты в области безопасности.

4. Оценка остаточных информационных рисков и принятие решения о дополнительных инвестициях в средства и меры безопасности. Решение принимает руководство на основе анализа остаточных рисков.

Структура документов безопасности

По мнению специалистов IBM, политика безопасности компании должна содержать явный ответ на вопрос: «Что требуется защитить?». Только после этого можно приступать к созданию эффективной политики информационной безопасности. При этом политика безопасности является первым стратегическим документом, который необходимо создать, и содержит минимум технических деталей, являясь настолько статичным

(неизменяемым) актом, насколько это возможно. Предполагается, что политика безопасности компании будет содержать:

1. определение информационной безопасности с описанием позиции и намерений руководства компании по ее обеспечению;

2. описание требований по безопасности, которые включают:

– соответствие требованиям законодательства и контрактных обязательств;

– обучение вопросам информационной безопасности;

– предупреждение и обнаружение вирусных атак;

– планирование непрерывности бизнеса;

– определение ролей и обязанностей по различным аспектам общей программы информационной безопасности;

– описание требований и процесса отчетности по инцидентам, связанным с информационной безопасностью;

– описание процесса поддержки политики безопасности.

Специалисты по информационной безопасности компании IBM выделяют следующие основные этапы разработки политики безопасности компании:

– анализ бизнес-стратегии компании и связанные с этим требования по информационной безопасности;

– анализ ИТ-стратегии, текущие проблемы информационной безопасности и требования по информационной безопасности, которые появятся в будущем;

– создание политики безопасности, взаимно увязанной с бизнес - и ИТ-стратегиями.

Рекомендуемая структура руководящих документов по обеспечению информационной безопасности компании представлена на рис. 11.

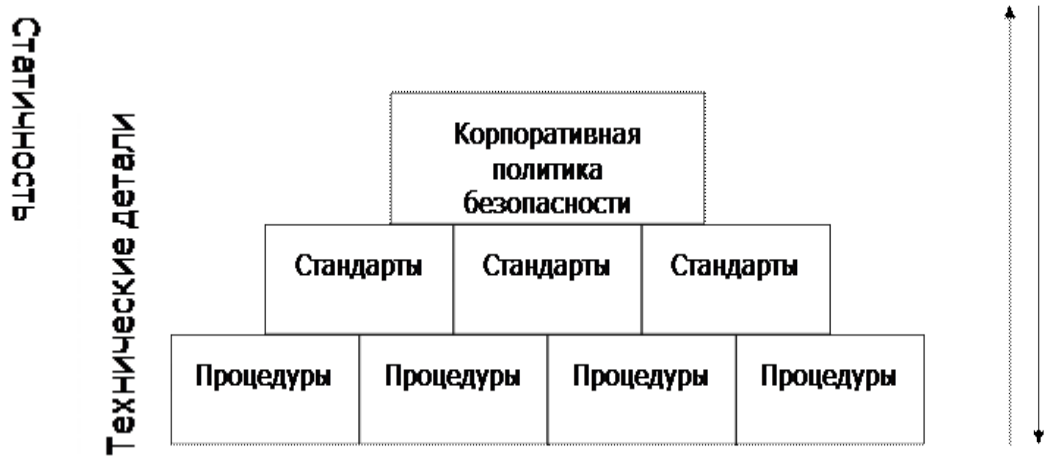

Рис. 11. Структура руководящих документов безопасности

После корпоративной политики создаётся серия стандартов, под которыми в компании IBM понимают документы, описывающие порядок применения корпоративной политики безопасности в терминах аутентификации, авторизации, идентификации, контроля доступа и т. д. Стандарты могут быть часто изменяющимися документами, так как на них оказывают влияние текущие угрозы и уязвимости информационных технологий.

В представлении IBM, политики и стандарты безопасности служат для:

– создания правил и норм безопасности уровня компании;

– анализа информационных рисков и способов их уменьшения;

– формализации способов защиты, которые должны быть реализованы;

– определения ожиданий со стороны компании и сотрудников;

– четкого определения процедур безопасности, которым нужно следовать;

– обеспечения юридической поддержки в случае возникновения проблем в области безопасности [40].

Контрольные вопросы:

1. Перечислите элементы общей структуры системы защиты информации.

2. Почему начиная с середины 80-х годов, защита линий связи и автоматизированных систем становится важной задачей компетентных государственных органов США?

3. Что является проблемой организации системы защиты информации в Великобритании? Почему?

4. Как власти Германии рассматривают угрозы информационной войны национальным интересам государства?

5. В чем суть французской концепции информационной войны?

6. В чем состоит особенность организации системы защиты информации Китая?

7. Охарактеризуйте подход компании IBM к построению корпоративных политик безопасности.

8. В чем заключаются особенности оценки информационных рисков компанией CISCO?

9. Что представляет собой «матрица безопасности» CISCO?

10. Назовите этапы реагирования на события безопасности в компании CISCO.

11. Охарактеризуйте основные принципы обеспечения информационной безопасности в компании Microsoft

12. На чем базируются политики безопасности компании Microsoft?

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Основные понятия и определения - http://ypn.ru/102/introduction-to-information-protection-and-information-security/ (дата обращения 27.09.15 14:55)

2. Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 31.12.2014) "Об информации, информационных технологиях и о защите информации" (с изм. и доп., вступ. в силу с 01.09.2015) – «Российская Газета» - Федеральный выпуск № 4131.

3. Закон РФ от 21.07.1993 N 5485-1 (ред. от 08.03.2015) «О государственной тайне» – «Российская Газета», 1993, 21 сентября

4. Федеральный закон РФ «О персональных данных», N 152-ФЗ от 27.07.2006– «Российская Газета» - Федеральный выпуск № 4131.

5. Федеральный закон от 29.07.2004 N 98-ФЗ (ред. от 12.03.2014) «О коммерческой тайне» – «Российская Газета» - Федеральный выпуск № 3543.

6. Федеральный закон «О банках и банковской деятельности» от 02.12.1990 N 395-1– «Российская Газета» - 1996, 10 февраля.

7. Федеральный закон от 08.07.1999 N 144-ФЗ «О реструктуризации кредитных организаций» - «Российская Газета» - Федеральный выпуск № 3543

8. Указ Президента Российской Федерации от 13.07.2015 N 357 «Об утверждении перечня сведений конфиденциального характера» – «Российская Газета», 2015, 15 июля.

9. Гражданский кодекс РФ (ГК РФ) от 30.11.1994 N 51-ФЗ– «Российская Газета», 2008, 24 марта.

10. Федеральный закон от 31.07.1995 N 119-ФЗ (ред. от 27.05.2003) «Об основах государственной службы Российской Федерации» – «Российская Газета» - 1995, 31 июля.

11. Постановление Правительства Российской Федерации от 3 ноября 1994 г. N 1233 "Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти" (Собрание законодательства Российской Федерации, 2005, N 30, ст. 3165) – «Российская Газета», 2012, 31 июля.

12. Федеральный закон от 30 декабря 2004 года N 218-ФЗ "О кредитных историях" (Собрание законодательства Российской Федерации, 2005, N 1, ст. 44) – «Российская Газета», - Федеральный выпуск №3831.

13. Налоговый кодекс РФ (НК РФ) от 31.07.1998 N 146-ФЗ (действующая редакция от 08.06.2015) – «Российская Газета», 2015, 12 января.

14. Семейный кодекс РФ (СК РФ) от 29.12.1995 N 223-ФЗ – «Российская Газета» - 2007, 22 октября.

15. Федеральный закон Российской Федерации от 2 июля 1992 г. N 3185-«О психиатрической помощи и гарантиях прав граждан при ее оказании», 1992, 25 августа.

16. Федеральный закон от 17.07.1999 N 176-ФЗ (ред. от 06.12.2011) «О почтовой связи»– «Российская Газета» - Федеральный выпуск № 3375.

17. Федеральный закон от 18.06.2003 № 126-ФЗ (ред. от 24 июля 2015 года, с изм. от 13 июля 2015 года) «О связи». - «Российская Газета» - Федеральный выпуск № 3249.

18. Конституция РФ, принята народным голосованием 12.12.1993 г. – «Российская Газета» - Федеральный выпуск № 4831.

19. Федеральный закон от 30.12.2008 N 307-ФЗ (ред. от 01.12.2014) «Об аудиторской деятельности» (с изм. и доп., вступ. в силу с 01.08.2015) – «Российская Газета» - Федеральный выпуск № 4824.

20. Уголовно-процессуальный кодекс Российской Федерации" от 18.12.2001 N 174-ФЗ (ред. от 13.07.2015) (с изм. и доп., вступ. в силу с 15.09.2015) – «Российская Газета» - Спецвыпуск №2861.

21. Гражданский процессуальный кодекс Российской Федерации от 14 ноября 2002 г. N 138-ФЗ– «Российская Газета» - Федеральный выпуск № 3088.

22. Арбитражный процессуальный кодекс РФ (АПК РФ) от 24.07.2002 N 95-ФЗ – «Российская Газета» - Федеральный выпуск № 3534.

23. Федеральный закон от 31.05.2002 N 63-ФЗ (ред. от 13.07.2015) «Об адвокатской деятельности и адвокатуре в Российской Федерации»– «Российская Газета» - Федеральный выпуск №2968.

24. Федеральный закон от 26.09.1997 N 125-ФЗ (ред. от 13.07.2015) «О свободе совести и о религиозных объединениях» - «Российская Газета»- Федеральный выпуск № 5965.

25. Федеральный закон от 18.05.2005 N 51-ФЗ (ред. от 02.04.2014, с изм. от 16.12.2014) «О выборах депутатов Государственной Думы Федерального Собрания Российской Федерации» -«Российская Газета» Федеральный выпуск № 3777.

26. Федеральный закон от 10.01.2003 N 19-ФЗ (ред. от 24.11.2014) «О выборах Президента Российской Федерации» - «Российская Газета» - Федеральный выпуск № 4533.

27. Федеральный закон от 12.06.2002 N 67-ФЗ (ред. от 06.04.2015) «Об основных гарантиях избирательных прав и права на участие в референдуме граждан Российской Федерации» - «Российская Газета»- Федеральный выпуск № 2974.

28. Уголовный кодекс РФ (УК РФ) от 13.06.1996 N 63-ФЗ– «Российская Газета» 2010, 8 июня.

29. Закон РФ «О средствах массовой информации» (о СМИ) от 27.12.1991 N 2124-1 - «Российская Газета»- 2007, 28 ноября.

30. Федеральный закон от 06.02.1997 N 27-ФЗ (ред. от 02.07.2013) «О внутренних войсках Министерства внутренних дел Российской Федерации» - «Российская Газета»- Федеральный выпуск № 2974.

31. Статистика утечки информации - http://www.infowatch.ru/report2014

32. История развития систем защиты информации - http://fullref.ru/job_603b438a4c2cf799517fc7c88ad88997.html (дата обращения 27.09.15 11:14)

33. Бабаш А.В., Баранова Е.К., Ларин Д.А. информационная безопасность. История защиты информации в России: Учебно-практическое пособие. – М: Изд. центр ЕАОИ, 2012. – 736 с.

34. Информационно-психологическое противоборство (эволюция и современность): Монография./ Я.М. Жарков, В.М. Петрик, М.М. Присяжнюк и др. – К.: ПАТ «Випол», 2013. – 248 с.

35. Специальные информационные операции - http://psyfactor.org/infops.htm (дата обращения 28.09.15 12:22)

36. Почепцов Г.Г. Психологические войны. – М., К., 2000.

37. Доктрина информационной безопасности Российской Федерации (утверждена Президентом Российской Федерации В. Путиным 9 сентября 2000 г., № Пр-1895) – «Российская Газета» 2000, 28 сентября.

38. Системы защиты информации в ведущих зарубежных страна: учебное пособие для вузов/В. И. Аверченков, М. Ю. Рытов, Г. В. Кондрашин, М. В. Рудановский. – 3-е изд , стереотип. – М.: Флинта, 2011. – 224 с.

39. Системы защиты инфорамации в ведущих странах http://pandia.ru/text/78/544/54505-7.php (дата обращения 28.09.15 13:05)

40. Системы защиты информации в ведущих компаниях - http://studopedia.ru/6_14223_glava-.html (дата обращения 28.09.15 13:43)