Лекции 4 Обзор международных стандартов информационной безопасности. Информационные войны и информационное противоборство

План лекции:

1. Роль стандартов информационной безопасности. Критерии безопасности компьютерных систем министерства обороны США (Оранжевая книга), TCSEC.
2. Европейские критерии безопасности информационных технологий (ITSEC). Федеральные критерии безопасности информационных технологий США.
3. Единые критерии безопасности информационных технологий. Группа международных стандартов 270000.
4. Определение и основные виды информационных войн.
5. Информационно-техническая война.
6. Информационно-психологическая война.

1 Роль стандартов информационной безопасности. Критерии безопасности компьютерных систем министерства обороны США (Оранжевая книга), TCSEC

Роль стандартов информационной безопасности

С развитием информационных технологий появилась необходимость стандартизации требований в области защиты информации. Главная задача стандартов информационной безопасности — создать основу для взаимодействия между производителями, потребителями и специалистам по сертификации. Каждая из этих групп имеет свои интересы и свои взгляды на проблему информационной безопасности.

Производители нуждаются в стандартах как средстве сравнения возможностей своих продуктов, и в применении процедуры сертификации как механизме оценки их свойств, а также в стандартизации определенного набора требований безопасности, который мог бы ограничить фантазию заказчика конкретного продукта и заставить его выбирать требования из этого набора.

Потребители заинтересованы в методике, позволяющей обоснованно выбрать продукт, отвечающий их нуждам и решающий их проблемы, для чего им необходима шкала оценки безопасности и инструмент, с помощью которого они могли бы формулировать свои требования производителям.

Специалисты по сертификации рассматривают стандарты как инструмент, позволяющий им оценить уровень безопасности, обеспечиваемый системой, и предоставить потребителям возможность сделать обоснованный выбор. Специалисты по сертификации заинтересованы в четких и простых критериях, так как они должны дать обоснованный ответ пользователям — удовлетворяет продукт их нужды, или нет. В конечном счете именно они принимают на себя ответственность за безопасность продукта, получившего квалификацию уровня безопасности и прошедшего сертификацию.

Таким образом, перед стандартами информационной безопасности стоит непростая задача создать эффективный механизм взаимодействия всех сторон.

Критерии безопасности компьютерных систем министерства обороны США (Оранжевая книга), TCSEC

«Критерии безопасности компьютерных систем» (Trusted Computer System Evaluation Criteria), получившие неформальное название Оранжевая книга, были разработаны Министерством обороны США в 1983 году с целью определения требований безопасности, предъявляемых к аппаратному, программному и специальному обеспечению компьютерных систем, и выработки соответствующей методологии и технологии анализа степени поддержки политики безопасности в компьютерных системах военного назначения.

В данном документе были впервые нормативно определены такие понятия, как «политика безопасности», «ядро безопасности» (TCB) и т. д.

Предложенные в этом документе концепции защиты и набор функциональных требований послужили основой для формирования всех появившихся впоследствии стандартов безопасности.

Классификация требований и критериев Оранжевой книги

В Оранжевой книге предложены три категории требований безопасности — политика безопасности, аудит и корректность, в рамках которых сформулированы шесть базовых требований безопасности. Первые четыре требования направлены непосредственно на обеспечение

безопасности информации, а два последних — на качество самих средств защиты. Рассмотрим эти требования подробнее.

1. *Политика безопасности.*

· Политика безопасности Система должна поддерживать точно определённую политику безопасности. Возможность осуществления субъектами доступа к объектам должна определяться на основе их идентификации и набора правил управления доступом. Там, где необходимо, должна использоваться политика нормативного управления доступом, позволяющая эффективно реализовать разграничение доступа к категорированной информации (информации, отмеченной грифом секретности: «секретно», «сов. секретно» и т. д.).

· Метки С объектами должны быть ассоциированы метки безопасности, используемые в качестве атрибутов контроля доступа.

Для реализации нормативного управления доступом система должна обеспечивать возможность присваивать каждому объекту метку или набор атрибутов, определяющих степень конфиденциальности (гриф секретности) объекта и/или режимы доступа к этому объекту.

2. *Аудит*.

· Идентификация и аутентификация. Все субъекты должны иметь уникальные идентификаторы. Контроль доступа должен осуществляться на основании результатов идентификации субъекта и объекта доступа, подтверждения подлинности их идентификаторов (аутентификации) и правил разграничения доступа. Данные, используемые для идентификации и аутентификации, должны быть защищены от несанкционированного доступа, модификации и уничтожения и ассоциированы со всеми активными компонентами компьютерной системы, функционирование которых критично с точки зрения безопасности.

· Регистрация и учет

Для определения степени ответственности пользователей за действия в системе все происходящие в ней события, имеющие значение с точки зрения безопасности, должны отслеживаться и регистрироваться в защищенном протоколе. Система регистрации должна осуществлять анализ общего потока событий и выделять из него только те события, которые оказывают влияние на безопасность для сокращения объема протокола и повышения эффективность его анализа. Протокол событий должен быть надежно защищен от несанкционированного доступа, модификации и уничтожения.

3. *Корректность*.

· Контроль корректности функционирования средств защиты

Средства защиты должны содержать независимые аппаратные и/или программные компоненты, обеспечивающие работоспособность функций защиты. Это означает, что все средства защиты, обеспечивающие политику безопасности, управление атрибутами и метками безопасности, идентификацию и аутентификацию, регистрацию и учёт, должны находиться под контролем средств, проверяющих корректность их функционирования. Основной принцип контроля корректности состоит в том, что средства контроля должны быть полностью независимы от средств защиты.

· Непрерывность защиты

Все средства защиты (в т. ч. и реализующие данное требование) должны быть защищены от несанкционированного вмешательства и/или отключения, причем эта защита должна быть постоянной и непрерывной в любом режиме функционирования системы защиты и компьютерной системы в целом. Данное требование распространяется на весь жизненный цикл компьютерной системы. Кроме того, его выполнение является одним из ключевых аспектов формального доказательства безопасности системы.

Приведенные базовые требования к безопасности служат основой для критериев, образующих единую шкалу оценки безопасности компьютерных систем, определяющую семь классов безопасности.

Классы безопасности компьютерных систем

Оранжевая книга предусматривает четыре группы критериев, которые соответствуют различной степени защищенности: от минимальной (группа D) до формально доказанной (группа A). Каждая группа включает один или несколько классов.

Группы D и A содержат по одному классу (классы D и A соответственно), группа C — классы C1, C2, а группа B — Bl, B2, B3, характеризующиеся различными наборами требований безопасности. Уровень безопасности возрастает при движении от группы D к группе A, а внутри группы — с возрастанием номера класса.

Группа **D**. Минимальная защита.

Класс **D**. Минимальная защита. К этому классу относятся все системы, не удовлетворяющие требованиям других классов.

Группа **C**. Дискреционная защита.

Группа характеризуется произвольным управлением доступом и регистрацией действий субъектов.

Класс **C1.** Дискреционная защита. Системы этого класса удовлетворяют требованиям обеспечения разделения пользователей и информации и включают средства контроля и управления доступом, позволяющие задавать ограничения для индивидуальных пользователей, что дает им возможность защищать свою приватную информацию от других пользователей. Класс C1 рассчитан на многопользовательские системы, в которых осуществляется совместная обработка данных одного уровня секретности.

Класс **C2.** Управление доступом. Системы этого класса осуществляют более избирательное управление доступом, чем системы класса C1, с помощью применения средств индивидуального контроля за действиями пользователей, регистрацией, учетом событий и выделением ресурсов.

Группа **B**. Мандатная защита.

Основные требования этой группы — нормативное управление доступом с использованием меток безопасности, поддержка модели и политики безопасности, а также наличие спецификаций на функции ТСВ. Для систем этой группы монитор взаимодействий должен контролировать все события в системе.

Класс **B1.** Защита с применением меток безопасности. Системы класса B1 должны соответствовать всем требованиям, предъявляемым к системам класса C2, и, кроме того, должны поддерживать определенную неформально модель безопасности, маркировку данных и нормативное управление доступом.

При экспорте из системы информация должна подвергаться маркировке. Обнаруженные в процессе тестирования недостатки должны быть устранены.

Класс **B2.** Структурированная защита. Для соответствия классу B2 ТСВ системы должна поддерживать формально определенную и четко документированную модель безопасности, предусматривающую произвольное и нормативное управление доступом, которое распространяется по сравнению с системами класса B1 на все субъекты. Кроме того, должен осуществляться контроль скрытых каналов утечки информации. В структуре ТСВ должны быть выделены элементы, критичные с точки зрения безопасности. Интерфейс ТСВ должен быть четко определен, а ее архитектура и реализация выполнены с учетом возможности проведения тестовых испытаний. По сравнению с классом B1 должны быть усилены средства аутентификации.

Управление безопасностью осуществляется администраторами системы. Должны быть предусмотрены средства управления конфигурацией.

Класс **B3.** Домены безопасности. Для соответствия этому классу ТСВ системы должна поддерживать монитор взаимодействий, который контролирует все типы доступа субъектов к объектам, который невозможно обойти. Кроме того, ТСВ должна быть структурирована с целью исключения из нее подсистем, не отвечающих за реализацию функций защиты, и достаточно компактна для эффективного тестирования и анализа. В ходе разработки и реализации ТСВ необходимо применение методов и средств, направленных на минимизацию ее сложности.

Средства аудита должны включать механизмы оповещения администратора при возникновении событий, имеющих значение для безопасности системы. Требуется наличие средств восстановления работоспособности системы.

Группа **A**. Верифицированная защита.

Данная группа характеризуется применением формальных методов верификации корректности работы механизмов управления доступом (произвольного и нормативного). Требуется дополнительная документация, демонстрирующая, что архитектура и реализация ТСВ отвечают требованиям безопасности.

Класс **A1.** Формальная верификация. Системы класса A1 функционально эквивалентны системам класса B3, и к ним не предъявляется никаких дополнительных функциональных требований. В отличие от систем класса B3 в ходе разработки должны применяться формальные методы верификации, что позволяет с высокой уверенностью получить корректную реализацию функций защиты. Процесс доказательства адекватности реализации начинается на ранней стадии разработки с построения формальной модели политики безопасности и спецификаций высокого

уровня. Для обеспечения методов верификации системы класса А1 должны содержать более мощные средства управления конфигурацией и защищенную процедуру дистрибуции.

Высший класс безопасности, требующий осуществления верификации средств защиты, построен на доказательстве соответствия программного обеспечения его спецификациям с помощью специальных методик, однако это доказательство (очень дорогостоящее, трудоемкое и практически неосуществимое для реальных операционных систем) не подтверждает адекватность реализации политики безопасности.

Согласно «Оранжевой книге» безопасная компьютерная система — это система, поддерживающая управление доступом к обрабатываемой в ней информации таким образом, что только соответствующие авторизованные пользователи или процессы, действующие от их имени, получают возможность читать, писать, создавать и удалять информацию.

Приведенные классы безопасности надолго определили основные концепции безопасности и ход развития средств защиты.

Устаревание ряда положений Оранжевой книги обусловлено прежде всего интенсивным развитием компьютерных технологий. Именно для того, чтобы исключить возникшую в связи с изменением аппаратной платформы некорректность некоторых положений Оранжевой книги, адаптировать их к современным условиям и сделать адекватными нуждам разработчиков и пользователей программного обеспечения, и была проделана огромная работа по развитию положений этого стандарта. В результате возник целый ряд сопутствующих Оранжевой книге документов, многие их которых стали ее неотъемлемой частью.

Круг специфических вопросов по обеспечению безопасности компьютерных сетей и систем управления базами данных нашел отражение в отдельных документах, изданных Национальным центром компьютерной безопасности США в виде дополнений к Оранжевой книге.

Итак, «Критерии безопасности компьютерных систем» Министерства обороны США представляют собой первую попытку создать единый стандарт безопасности, рассчитанный на разработчиков, потребителей и специалистов по сертификации компьютерных систем. В свое время этот документ явился настоящим прорывом в области безопасности информационных технологий и послужил отправной точкой для многочисленных исследований и разработок. Основной отличительной чертой этого документа является его ориентация на системы военного применения, причем в основном на операционные системы. Это предопределило доминирование требований, направленных на обеспечение секретности обрабатываемой информации и исключение возможностей ее разглашения. Большое внимание уделено меткам (грифам секретности) и правилам экспорта секретной информации.

Оранжевая книга послужила основой для разработчиков всех остальных стандартов информационной безопасности и до сих пор используется в США в качестве руководящего документа при сертификации компьютерных систем обработки информации.

2 Европейские критерии безопасности информационных технологий (ITSEC). Федеральные критерии безопасности информационных технологий США

Европейские критерии безопасности информационных технологий (ITSEC)

Обзор основывается на версии 1.2 этих критериев, опубликованной в июне 1991 года от имени четырех стран: Франции, Германии, Нидерландов и Великобритании.

Европейские критерии рассматривают следующие задачи средств информационной безопасности: · защита информации от несанкционированного доступа с целью обеспечение конфиденциальности; · обеспечение целостности информации посредством защиты от ее несанкционированной модификации или уничтожения;

· обеспечение работоспособности систем с помощью противодействия угрозам отказа в обслуживании.

В «Европейских критериях» проводится различие между системами и продуктами.

Система — это конкретная аппаратно-программная конфигурация, построенная с вполне определенными целями и функционирующая в известном окружении.

Продукт — это аппаратно-программный «пакет», который можно купить и по своему усмотрению встроить в ту или иную систему.

Таким образом, с точки зрения информационной безопасности основное отличие между системой и продуктом состоит в том, что система имеет конкретное окружение, которое можно

определить и изучить сколь угодно детально, а продукт должен быть рассчитан на использование в различных условиях.

Угрозы безопасности системы носят вполне конкретный и реальный характер. Относительно угроз продукту можно лишь строить предположения. Разработчик может специфицировать условия, пригодные для функционирования продукта; дело покупателя обеспечить выполнение этих условий.

Из практических соображений важно обеспечить единство критериев оценки продуктов и систем — облегчить и удешевить оценку системы, составленной из ранее сертифицированных продуктов. В этой связи для систем и продуктов вводится единый термин — *объект оценки.* В соответствующих местах делаются оговорки, какие требования относятся исключительно к системам, а какие — только к продуктам.

Для того чтобы удовлетворить требованиям конфиденциальности, целостности и работоспособности, необходимо реализовать соответствующий набор функций безопасности, таких как идентификация и аутентификация, управление доступом, восстановление после сбоев и т. д. Чтобы средства защиты можно было признать эффективными, требуется определенная степень уверенности в правильности их выбора и надежности функционирования. Для решения этой проблемы в «Европейских критериях» впервые вводится понятие адекватности (assurance) средств защиты.

Общая оценка уровня безопасности системы складывается из функциональной мощности средств защиты и уровня адекватности их реализации.

Большинство требований безопасности совпадает с аналогичными требованиями Оранжевой книги.

В «Европейских критериях» определено десять классов безопасности. Классы **F-C1, F-C2, F-B1, F-B2, F-B3** соответствуют классам безопасности Оранжевой книги с аналогичными обозначениями.

Класс **F-IN** предназначен для систем с высокими потребностями в обеспечении целостности, что типично для систем управления базами данных.

Его описание основано на концепции «ролей», соответствующих видам деятельности пользователей, и предоставлении доступа к определённым объектам только посредством доверенных процессов. Должны различаться следующие виды доступа: чтение, запись, добавление, удаление, создание, переименование и выполнение объектов.

Класс **F-AV** характеризуется повышенными требованиями к обеспечению работоспособности. Это существенно, например для систем управления технологическими процессами.

В требованиях этого класса указывается, что система должна восстанавливаться после отказа отдельного аппаратного компонента таким образом, чтобы все критически важные функции постоянно оставались доступными. В таком же режиме должна происходить и замена компонентов системы. Независимо от уровня загрузки должно гарантироваться определенное время реакции системы на внешние события.

Класс **F-DI** ориентирован на распределенные системы обработки информации.

Перед началом обмена и при получении данных стороны должны иметь возможность провести идентификацию участников взаимодействия и проверить ее подлинность. Должны использоваться средства контроля и исправления ошибок. В частности, при пересылке данных должны обнаруживаться все случайные или намеренные искажения адресной и пользовательской информации. Знание алгоритма обнаружения искажений не должно позволять злоумышленнику производить нелегальную модификацию передаваемых данных. Необходимо обнаруживать попытки повторной передачи ранее переданных сообщений.

Класс **F-DC** уделяет особое внимание требованиями к конфиденциальности передаваемой информации.

Информация по каналам связи должна передаваться в зашифрованном виде. Ключи шифрования защищают от несанкционированного доступа.

Класс **F-DX** предъявляет повышенные требования и к целостности и к конфиденциальности информации.

Его можно рассматривать как объединение классов F-DI и F-DC с дополнительными возможностями шифрования и защиты от анализа трафика. Следует ограничить доступ к ранее переданной информации, которая в принципе может способствовать проведению криптоанализа.

Критерии адекватности Адекватность включает в себя два аспекта: эффективность, отражающую соответствие средств безопасности решаемым задачам, и корректность, характеризующую процесс их разработки и функционирования.

Эффективность — соответствие между задачами, поставленными перед средствами безопасности, и реализованным набором функций защиты — их функциональной полнотой и согласованностью, простотой использования, а также возможными последствиями использования злоумышленниками слабых мест защиты.

Корректность — правильность и надежность реализации функций безопасности.

Европейские критерии уделяют адекватности средств защиты значительно больше внимания, чем функциональным требованиям. Как уже говорилось, адекватность складывается из двух компонентов — эффективности и корректности работы средств защиты.

Европейские критерии определяют семь уровней адекватности — от Е0 до Е6. При проверке адекватности анализируется весь жизненный цикл системы — от начальной фазы проектирования до эксплуатации и сопровождения. Уровни адекватности от Е1 до Е6 выстроены по нарастанию требований тщательности контроля. Так, на уровне Е1 анализируется лишь общая архитектура системы, а адекватность средств защиты подтверждается функциональным тестированием. На уровне Е3 к анализу привлекаются исходные тексты программ и схемы аппаратного обеспечения.

На уровне Е6 требуется формальное описание функций безопасности, общей архитектуры, а также политики безопасности.

В Европейских критериях определены три уровня безопасности — базовый, средний и высокий. Степень безопасности системы определяется самым слабым из критически важных механизмов защиты.

Безопасность считается базовой, если средства защиты способны противостоять отдельным случайным атакам.

Безопасность считается средней, если средства защиты способны противостоять злоумышленникам, обладающим ограниченными ресурсами и возможностями.

Наконец, безопасность можно считать высокой, если есть уверенность, что средства защиты могут быть преодолены только злоумышленником с высокой квалификацией, набор возможностей и ресурсов которого выходит за рамки возможного.

Итак, Европейские критерии безопасности информационных технологий, появившиеся вслед за Оранжевой книгой, оказали существенное влияние на стандарты безопасности и методику сертификации.

Главное достижение этого документа — введение понятия адекватности средств защиты и определение отдельной шкалы для критериев адекватности. Как уже упоминалось, Европейские критерии придают адекватность средств защиты даже большее значение, чем их функциональности. Этот подход и пользуется во многих появившихся позднее стандартах информационной безопасности.

Федеральные критерии безопасности информационных технологий США

Федеральные критерии безопасности информационных технологий (Federal Criteria for Information Technology Security) разрабатывались как одна из составляющих Американского федерального стандарта по обработке информации (Federal Information Processing Standard), призванного заменить Оранжевую книгу. Разработчиками стандарта выступили Национальный институт стандартов и технологий США (Nationa Institute of Standards and Technology) и Агентство национальной безопасности США (National Security Agency). Данный обзор основан на версии 1.0 этого документа, опубликованной в декабре 1992 года.

Этот документ разработан на основе результатов многочисленных исследований в области обеспечения безопасности информационных технологий 1980-х — начала 1990-х гг., а также на основе анализа опыта использования Оранжевой книги.

Федеральные критерии безопасности информационных технологий (далее, просто Федеральные критерии) охватывают практически полный спектр проблем, связанных с защитой и обеспечением безопасности, т. к. включают все аспекты обеспечения конфиденциальности, целостности и работоспособности.

Основными объектами применения требований безопасности Федеральных критериев являются · продукты информационных технологий (Information Technology Products); · системы обработки информации (Information Technology Systems).

Под *продуктом информационных технологий* (далее просто ИТ-продукт) понимается совокупность аппаратных и/или программных средств, которая представляет собой поставляемое конечному потребителю готовое к использованию средство обработки информации.

Как правило, ИТ-продукт эксплуатируется не автономно, а интегрируется в систему обработки информации, представляющую собой совокупность ИТ-продуктов, объединенных в функционально полный комплекс, предназначенный для решения прикладных задач. В ряде случаев система обработки информации может состоять только из одного ИТ-продукта, обеспечивающего решение всех стоящих перед системой задач и удовлетворяющего требованиям безопасности. С точки зрения безопасности принципиальное различие между ИТ- продуктом и системой обработки информации определяется средой их эксплуатации. Продукт информационных технологий обычно разрабатывается в расчете на то, что он будет использован во многих системах обработки информации, и, следовательно, разработчик должен ориентироваться только на самые общие предположения о среде эксплуатации своего продукта, включающие условия применения и общие угрозы. Напротив, система обработки информации разрабатывается для решения прикладных задач в расчете на требования конечных потребителей, что позволяет в полной мере учитывать специфику воздействий со стороны конкретной среды эксплуатации.

Федеральные критерии содержат положения, относящиеся к отдельным продуктам информационных технологий. Вопросы построения систем обработки информации из набора

ИТ-продуктов не являются предметом рассмотрения этого документа.

Положения Федеральных критериев касаются собственных средств обеспечения безопасности ИТ-продуктов, т. е. механизмов защиты, встроенных непосредственно в эти продукты в виде соответствующих программных, аппаратных или специальных средств. Для повышения их эффективности могут дополнительно применяться внешние системы защиты и средства обеспечения безопасности, к которым относятся как технические средства, так и организационные меры, правовые и юридические нормы. В конечном счете, безопасность ИТ-продукта определяется совокупностью собственных средств обеспечения безопасности и внешних средств.

Ключевым понятием концепции информационной безопасности Федеральных критериев является понятие *Профиль защиты* (Protection Profile). Профиль защиты — это нормативный документ, который регламентирует все аспекты безопасности ИТ-продукта в виде требований к его проектированию, технологии разработки и квалификационному анализу. Как правило, один Профиль защиты описывает несколько близких по структуре и назначению ИТ-продуктов. Основное внимание в Профиле защиты уделяется требованиям к составу средств защиты и качеству и реализации, а также их адекватности предполагаемым угрозам безопасности.

Федеральные критерии представляют процесс разработки систем обработки информации, начинающийся с формулирования требований потребителями и заканчивающийся введением в эксплуатацию, в виде следующих основных этапов:

1. Разработка и анализ Профиля защиты. Требования, изложенные в Профиле защиты, определяют функциональные возможности ИТ-продуктов по обеспечению безопасности и условия эксплуатации, при соблюдении которых гарантируется соответствие предъявляемым требованиям. Кроме требований безопасности, Профиль защиты содержит требования по соблюдению технологической дисциплины в процессе разработки, тестирования и квалификационного анализа ИТ-продукта.

Профиль безопасности анализируется на полноту, непротиворечивость и техническую корректность.

2. Разработка и квалификационный анализ ИТ-продуктов.

Разработанные ИТ-продукты подвергаются независимому анализу, целью которого является определение степени соответствия характеристик продукта сформулированным в Профиле защиты требованиям и спецификациям.

3. Компоновка и сертификация системы обработки информации в целом. Успешно прошедшие квалификацию уровня безопасности ИТ-продукты интегрируются в систему обработки информации. Полученная в результате система должна удовлетворять заявленным в Профиле защиты требованиям при соблюдении указанных в нем условий эксплуатации.

Федеральные критерии регламентируют только первый этап этой схемы — разработку и анализ Профиля защиты, процесс создания ИТ-продуктов и компоновка систем обработки информации остаются вне рамок этого стандарта.

Профиль защиты 1) Описание.

Информация для его идентификации в специальной картотеке (характеристика проблемы обеспечения безопасности). 2) Обоснование.

Описание среды эксплуатации, предполагаемых угроз и методов использования ИТ-продукта; перечень задач по обеспечению безопасности, решаемых с помощью данного профиля.

3) Функциональные требования к ИТ-продукту.

Определение условий, в которых обеспечивается безопасность в виде перечня парируемых угроз.

4) Требования к технологии разработки ИТ-продукта.

Требования к самому процессу разработки, к условиям, в которых она проводится, к используемым технологическим средствам, к документированию процесса.

5)Требования к процессу сертификации Порядок сертификации в виде типовой методики тестирования и анализа

Этапы разработки профиля защиты.

1) Анализ среды применения ИТ-продукта с точки зрения безопасности.

2) Выбор профиля-прототипа.

3) Синтез требований.

Выбор наиболее существенных функций защиты, их ранжирование по степени важности с точки зрения обеспечения качества защиты.

После разработки профиль защиты проверяется для подтверждения полноты, корректности, непротиворечивости и реализуемости.

Классы функциональных требований к ИТ-продукту.

1) Политика безопасности.

2) Мониторинг взаимодействий.

3) Логическая защита ТСв.

· требования корректности внешних субъектов относительно субъектов ТСВ;

· требования к интерфейсам взаимодействия.

4) Физическая защита ТСв.

5) Самоконтроль ТСв.

6) Инициализация и восстановление ТСв.

7) Ограничение привилегий при работе с ТСв.

8) Простота использования ТСв.

Классификация функциональных требований.

1. Широта сферы применения.

Пользователи системы, субъекты и объекты доступа; функции ТСВ и интерфейс взаимодействия; аппаратные, программные и специальные компоненты; параметры конфигурации.

2. Степень детализации.

Определяется множеством атрибутов сущностей, к которым применяются данные требования.

3. Функциональный состав средств защиты.

Определяется множеством функций, включённых в ТСВ для реализации группы требований. 4. Обеспечиваемый уровень безопасности.

Определяется условиями, в которых компоненты системы способны противостоять заданному множеству угроз.

Итак, Федеральные критерии безопасности информационных технологий — первый стандарт информационной безопасности, в котором определяются три независимые группы требований: функциональные требования к средствам защиты, требования к технологии разработки и к процессу квалификационного анализа. Авторами этого стандарта впервые предложена концепция Профиля защиты — документа, содержащего описание всех требований безопасности как к самому ИТ-продукту, так и к процессу его проектирования, разработки, тестирования и квалификационного анализа.

Функциональные требования безопасности хорошо структурированы и описывают все аспекты функционирования ТСв. Требования к технологии разработки, впервые появившиеся в этом документе, побуждают производителей использовать современные технологии программирования как основу для подтверждения безопасности своего продукта.

Требования к процессу квалификационного анализа носят общий характер и не содержат конкретных методик тестирования и исследования безопасности ИТ-продуктов.

Разработчики Федеральных критериев отказались от используемого в Оранжевой книге подхода к оценки уровня безопасности ИТ-продукта на основании обобщенной универсальной шкалы классов безопасности. Вместо этого предлагается независимое ранжирование требований каждой группы, т. е. вместо единой шкалы используется множество частных шкалкритериев, характеризующих обеспечиваемый уровень безопасности. Данный подход позволяет разработчикам и пользователям ИТ-продукта выбрать наиболее приемлемое решение и точно определить

необходимый и достаточный набор требований для каждого конкретного ИТ-продукта и среды его эксплуатации.

Стандарт рассматривает устранение недостатков существующих средств безопасности как одну из задач защиты наряду с противодействием угрозам безопасности и реализацией модели безопасности.

Данный стандарт ознаменовал появление нового поколе- ния руководящих документов в области информационной безопасности, а его основные положения послужили базой для разработки Канадских критериев безопасности компьютерных систем и Единых критериев безопасности информационных технологий.

3 Единые критерии безопасности информационных технологий. Группа международных стандартов 270000

Единые критерии безопасности информационных технологий

Единые критерии безопасности информационных технологий (Common Criteria for Information Technology Security Evaluation, далее — Единые критерии) являются результатом совместных усилий авторов Европейских критериев безопасности информационных технологий, Федеральных критериев безопасности информационных технологий и Канадских критериев безопасности компьютерных систем, направленных на объединение основных положений этих документов и создание Единого международного стандарта безопасности информационных технологий. Работа над этим самым масштабным в истории стандарте информационной безопасности проектом началась в июне 1993 года с целью преодоления концептуальных и технических различий между указанными документами, их согласования и создания единого международного стандарта. Версия 2.1 этого стандарта утверждена Международной организацией по стандартизации (ISO) в 1999 г. в качестве Международного стандарта информационной безопасности ISO/IEC 15408. В Российской федерации стандарт действует под номером ГОСТ Р ИСО/МЭК 15408.

Единые критерии сохраняют совместимость с существующими стандартами и развивают их путем введения новых концепций, соответствующих современному уровню развития информационных технологий и интеграции национальных информационных систем в единое мировое информационное пространство.

Этот документ разработан на основе достижений многочисленных исследований в области безопасности информационных технологий 1990-х гг. и на результатах анализа опыта применения положенных в его основу стандартов. Единые критерии оперируют уже знакомым по Федеральным критериям понятием *продукт информационных технологий*, или ИТ-продукт, и используют предложенную в них концепцию Профиля защиты.

Единые критерии разрабатывались в расчете на то, чтобы удовлетворить запросы трех групп специалистов, в равной степени являющихся пользователями этого документа: производителей и потребителей продуктов информационных технологий, а также экспертов по квалификации уровня их безопасности.

Заинтересованные стороны могут задать функциональные возможности безопасности продукта с использованием стандартных профилей защиты и самостоятельно выбрать оценочный уровень уверенности в безопасности из совокупности семи возрастающих оценочных уровней уверенности в безопасности от 1 до 7.

Потребители рассматривают квалификацию уровня безопасности ИТ-продукта как метод определения соответствия ИТ- продукта их запросам. Обычно эти запросы составляются на основании результатов проведенного анализа рисков и выбранной политики безопасности. Единые критерии играют существенную роль в процессе формирования запросов потребителей, так как содержат механизмы, позволяющие сформулировать эти запросы в виде стандартизованных требований. Это позволяет потребителям принять обоснованное решение о возможности использования тех или иных продуктов. Наконец, Единые критерии предоставляют потребителям механизм Профилей защиты, с помощью которого они могут выразить специфичные для них требования, не заботясь о механизмах их реализации.

Производители должны использовать Единые критерии в ходе проектирования и разработки ИТ-продуктов, а также для подготовки к квалификационному анализу и сертификации.

Этот документ дает возможность производителям на основании анализа запросов потребителей определить набор требований, которым должен удовлетворять разрабатываемый ими продукт.

Производители используют предлагаемую Едиными критериями технологию для обоснования своих претензий на то, что поставляемый ими ИТ-продукт успешно противостоит угрозам безопасности, на основании того, что он удовлетворяет выдвинутым функциональным требованиям и их реализация осуществлена с достаточным уровнем адекватности. Для осуществления этой технологии Единые критерии предлагают производителям специальный механизм, названный Проект защиты, дополняющий Профиль защиты и позволяющий соединить описания требований, на которые ориентировался разработчик, спецификации механизмов реализации этих требований.

Кроме того, производители могут использовать Единые критерии для определения границ своей ответственности, а также условий, которые необходимо выполнить для успешного прохождения квалификационного анализа и сертификации созданного ими продукта.

Эксперты по квалификации используют этот документ в качестве основных критериев определения соответствия средств защиты ИТ-продукта требованиям, предъявляемым к нему по требителями, и угрозам, действующим в среде его эксплуатации.

Единые критерии описывают только общую схему проведения квалификационного анализа и сертификации, но не регламентируют процедуру их осуществления. Вопросам методологии квалификационного анализа и сертификации посвящен отдельный документ — «Общая методология оценки безопасности информационных технологий».

Таким образом, Единые критерии обеспечивают нормативную поддержку процесса выбора ИТ-продукта, к которому предъявляются требования функционирования в условиях действия определенных угроз, служат руководящим материалом для разработчиков таких систем, а также регламентируют технологию их создания и процедуру оценки обеспечиваемого уровня безопасности.

Единые критерии рассматривают информационную безопасность как совокупность конфиденциальности и целостности информации, обрабатываемой ИТ-продуктом, а также доступности ресурсов ВС, ставят перед средствами защиты задачу противодействия угрозам, актуальным для среды эксплуатации этого продукта и реализации политики безопасности, принятой в этой среде эксплуатации.

Единые критерии регламентируют все стадии разработки, квалификационного анализа и эксплуатации ИТ-продуктов, используя схему из Федеральных критериев. Единые критерии предлагают достаточно сложный процесс разработки и квалификационного анализа ИТ-продуктов, требующий от потребителей и производителей составления и оформления весьма объемных и подробных нормативных документов.

Задачи защиты — базовое понятие Единых критериев, выражающее потребность потребителей ИТ-продукта в противостоянии заданному множеству угроз безопасности или в необходимости реализации политики безопасности.

Профиль защиты — специальный нормативный документ, представляющий собой совокупность Задач защиты, функциональных требований, требований адекватности и их обоснования. Служит руководством для разработчика ИТ-продукта при создании Проекта защиты.

Проект защиты — специальный нормативный документ, представляющий собой совокупность Задач защиты, функциональных требований, требований адекватности, общих спецификаций средств защиты и их обоснования.

Каталог функциональных классов:

· аудит,
· связь (подтверждение приёма/передачи информации),
· криптографическая поддержка,
· защита данных пользователя (конфиденциальность, целостность, доступность),
· идентификация и аутентификация,
· управление безопасностью,
· приватность (конфиденциальность работы в системе),
· надёжность средств защиты,
· контроль за использованием ресурсов,
· контроль доступа к объекту оценки,
· доверенный маршрут/канал (прямое взаимодействие).

Требования уверенности в безопасности (адекватности)

· управление проектом,
· дистрибуция,
· разработка,

· документация,
· процесс разработки,
· тестирование,
· анализ защиты.

«Единые критерии» содержат совокупность предопределённых оценочных уровней уверенности в безопасности, составленных из компонентов семейств требований уверенности в безопасности. Эти уровни предназначены: · для достижения совместимости с исходными критериями;

· для обеспечения потребителя пакетами компонентов общего назначения.

Для достижения конкретных целей уровень может быть усилен дополнительными компонентами.

ОУБ1 — функциональное тестирование (соответствует американскому TCSEC — D, европейскому ITSEC — E1).

ОУБ2 — структурное тестирование (C1, E2).

ОУБ3 — методическое тестирование и проверка (C2, E3).

ОУБ4 — методическое проектирование, тестирование и просмотр (B1, E4).

ОУБ5 — полуформальное проектирование и тестирование (B2, E5).

ОУБ6 — полуформальная верификация проекта и тестирование (B3, E6).

ОУБ7 –формальная верификация проекта и тестирование (A1, E7).

Эквивалентность указана в целом, точного соответствия не существует, т. к. различаются подходы.

Согласно Единым критериям, безопасность информационных технологий может быть достигнута посредством применения предложенной технологии разработки, сертификации и эксплуатации ИТ-продуктов.

Единые критерии определяют множество типовых требований, которые в совокупности с механизмом Профилей защиты позволяют потребителям создавать частные наборы требований, отвечающие их нуждам. Разработчики могут использовать Профиль защиты как основу для создания спецификаций своих продуктов. Профиль защиты и спецификации средств защиты составляют Проект защиты, который и представляет ИТ- продукт в ходе квалификационного анализа.

Квалификационный анализ может осуществляться как параллельно с разработкой ИТ-продукта, так и после ее завершения. Для проведения квалификационного анализа разработчик продукта должен представить следующие материалы:

· профиль защиты, описывающий назначение ИТ-продукта и характеризующий среду его эксплуатации, а также устанавливающий Задачи защиты и требования, которым должен отвечать продукт;

· проект защиты, включающий спецификации средств защиты, также обоснование соответствия ИТ-продукта задачам защиты из Профиля защиты и указанным в нем требованиям Единых критериев;

· различные обоснования и подтверждения свойств и возможностей ИТ-продукта, полученные разработчиком;

· сам ИТ-продукт; · дополнительные сведения, полученные путем проведения различных независимых экспертиз.

Процесс квалификационного анализа включает три стадии:

1. Анализ Профиля защиты на предмет его полноты, непротиворечивости, реализуемости и возможности использования в качестве набора требований для анализируемого продукта.

2. Анализ Проекта защиты на предмет его соответствия требованиям Профиля защиты, а также полноты, непротиворечивости, реализуемости и возможности использования в качестве эталона при анализе ИТ-продукта.

3. Анализ ИТ-продукта на предмет соответствия Проекту защиты. Результатом квалификационного анализа является заключение о том, что проанализированный ИТ-продукт соответствует представленному Проекту защиты. Заключение состоит из нескольких отчетов, отличающихся уровнем детализации и содержащих мнение экспертов по квалификации об ИТ-продукте на основании критериев квалификации Единых критериев.

Применение квалификационного анализа и сертификации приводит к повышению качества работы производителей в процессе проектирования и разработки ИТ-продуктов. В продуктах, прошедших квалификацию уровня безопасности, вероятность появления ошибок и изъянов защиты

и уязвимостей существенно меньше, чем в обычных продуктах. Все это позволяет говорить о том, что применение Единых критериев оказывают положительное и конструктивное влияние на процесс формирование требований, разработку ИТ-продукта, сам продукт и его эксплуатацию.

Таким образом, Единые критерии безопасности информационных технологий представляют собой результат обобщения всех достижений последних лет в области информационной безопасности. Впервые документ такого уровня содержит разделы, адресованные потребителям, производителям и экспертам по квалификации ИТ-продуктов.

Разработчики Единых критериев продолжили работу над Федеральными критериями, направленными на отказ от единой шкалы безопасности, усилив гибкость предложенных в них решений путем введения частично упорядоченных шкал, благодаря чему потребители и производители получили дополнительные возможности по выбору требований и их адаптации к своим прикладным задачам.

Особое внимание этот стандарт уделяет адекватности реализации функциональных требований, которая обеспечивается как независимым тестированием и анализом ИТ-продукта, так и применением соответствующих технологий на всех этапах его проектирования и реализации.

Таким образом, требования Единых критериев охватывают практически все аспекты безопасности ИТ-продуктов и технологии их создания, а также содержат все исходные материалы, необходимые потребителям и разработчикам для формирования Профилей и Проектов защиты.

Кроме того, требования Единых критериев являются практически всеобъемлющей энциклопедией информационной безопасности, поэтому их можно использовать в качестве справочника по безопасности информационных технологий.

Данный стандарт ознаменовал собой новый уровень стандартизации информационных технологий, подняв его на межгосударственный уровень. За этим проглядывается реальная перспектива создания единого безопасного информационного пространства, в котором сертификация безопасности систем обработки информации будет осуществляться на глобальном уровне, что предоставит возможности для интеграции национальных информационных систем.

Группа международных стандартов 270000

Основное назначение международных стандартов — это создание на межгосударственном уровне единой основы для разработки новых и совершенствования действующих систем качества. Сотрудничество в области стандартизации направлено на приведение в соответствие национальной системы стандартизации с международной. Международные стандарты не имеют статуса обязательных для всех стран-участниц. Любая страна мира вправе применять или не применять их. Решение вопроса о применении международного стандарта связано в основном со степенью участия страны в международном разделении труда.

Международные стандарты принимаются Международной организацией по стандартизации — ИСО (International Organization for Standardization, ISO).

ИСО учреждена в 1946 г. представителями двадцати пяти индустриально развитых стран и обладает полномочиями по координации на международном уровне разработки различных промышленных стандартов и осуществляет процедуру принятия их в качестве международных стандартов.

Сфера деятельности ИСО касается стандартизации во всех областях, кроме электротехники и электроники, относящихся к компетенции Международной электротехнической комиссии (МЭК, IEC). Некоторые виды работ выполняются этими организациями совместно. В этом случае в наименовании стандарта появляется аббревиатура ИСО/МЭК.

В системе международных стандартов в 2008 г. выделена отдельная группа, связанная с информационной безопасностью, имеющая наименование ISO/IEC 27000. Эти стандарты опубликованы совместно Международной организацией по стандартизации (ISO) и Международной электротехнической комиссией (IEC).

Серия содержит лучшие практики и рекомендации в области информационной безопасности для создания, развития и поддержания Системы менеджмента информационной без опасности.

В настоящее время серия содержит более 30 стандартов, большинство из которых действуют на территории Российской Федерации с аналогичным номером ГОСТ. В первую десятку группы входят: ГОСТ Р ИСО/МЭК 27000–2012— «СМИБ. Общий обзор и терминология».

ГОСТ Р ИСО/МЭК 27001–2006— «СМИБ. Требования» ГОСТ Р ИСО/МЭК 27002–2012— «СМИБ. Свод норм и правил менеджмента информационной безопасности».

ГОСТ Р ИСО/МЭК 27003–2012—»СМИБ. Руководство по реализации системы менеджмента информационной безопасности».

ГОСТ Р ИСО/МЭК 27004–2011— «СМИБ. Измерения».

ГОСТ Р ИСО/МЭК 27005–2010 — «СМИБ. Менеджмент риска информационной безопасности».

ГОСТ Р ИСО/МЭК 27006–2008— «СМИБ. Требования к органам, осуществляющим аудит и сертификацию систем менеджмента информационной безопасности».

ГОСТ Р ИСО/МЭК 27007–2014 — «СМИБ. Руководства по аудиту систем менеджмента информационной безопасности».

Итак, главная задача стандартов информационной безопасности — согласовать позиции и цели производителей, потребителей и аналитиков-классификаторов в процессе создания и эксплуатации продуктов информационных технологий.

Первые версии стандартов создавались в основном исходя из нужд обороны и были нацелены на обеспечение секретности информации. С развитием средств вычислительной техники и телекоммуникаций возникла потребность создания новых стандартов, отражающих особенности современного уровня информационных технологий. Применяемые международные стандарты не содержат сквозных шкал и перечней требований безопасности, они ориентированы на применение профилей защиты, представляющих собой перечень функциональных требований для систем определённого назначения.

4 Определение и основные виды информационных войн

Информационная война — открытые или скрытые целенаправленные информационные воздействия систем друг на друга с целью получения определенного выигрыша в материальной, военной, политической или идеологической сферах.

Впервые термин «информационная война» появился в США в середине 70-х гг. XX в., его появление было обусловлено скачком в развитии компьютерных технологий и средств связи. Информационное оружие не менее опасно, чем оружие традиционное. Информационная борьба может быть как самостоятельным видом противоборства (без вооруженного конфликта), так и дополнением традиционных военных действий.

В зависимости от масштабов информационные войны делятся:

· на персональные,

· корпоративные,

· глобальные.

Персональные информационные войны чаще всего связаны с нарушением личной информационной неприкосновенности. Корпоративные информационные войны возникают вследствие соперничества между корпорациями и нацелены на получение информации о деятельности конкурента или его ликвидацию. Во время глобальной информационной войны наносится ущерб информационным ресурсам противника при одновременной защите своих на уровне государства. При глобальной информационной войне можно выделить три основных направления ведения войны:

· воздействие на индивидуальное, групповое и массовое сознание с использованием СМИ;

· воздействие на системы принятия решений в политической, экономической, военной, научно-технической, социальной сферах;

· воздействие на информационные системы с целью управления, блокирования, съема обрабатываемой информации.

Рассмотрим отличия традиционной и информационной межгосударственных войн. Если схематично представить государство в виде пирамиды, на вершине которой находится аппарат государственной власти, основание составляют ресурсы (материальные, человеческие, энергетические), а между ними расположен социум (общество), то отличие информационной и традиционной войны можно проиллюстрировать рис. 4.1, 4.2.

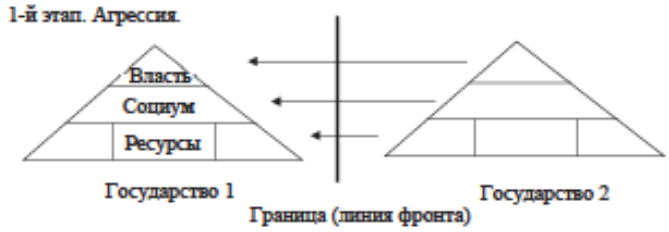

Рис. 4.1. Схема ведения традиционной войны

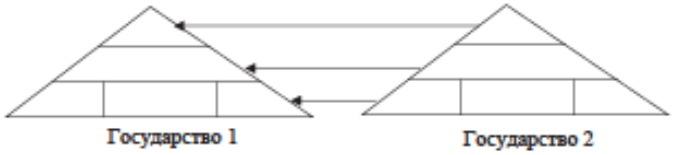

Рис. 4.2. Схема ведения информационной войны

Считается, что цель войны — получение ресурсов. При ведении традиционной войны разрушается надстройка побежденного государства, гибнет часть ресурсов; определенный ущерб наносится и государству-победителю. Последствия традиционной войны в современном мире могут быть неприемлемы для победителя (например, в случае ядерного конфликта). При информационной войне нет явной границы противоборства (фронта), однако в результате успешной информационной войны под контроль победителя попадают все уровни, включая власть, ресурсы, территорию.

По направленности воздействий информационная борьба подразделяется на два основных вида [10]:

· информационно-техническую,

· информационно-психологическую.

Они отличаются объектами защиты и воздействия.

Основные объекты воздействия информационно-психологической войны: · психика человека, · система принятия политических решений,

· система общественного сознания,

· система формирования общественного мнения.

Основные объекты воздействия информационно-технической войны:

· радиоэлектронная борьба,

· линии связи и телекоммуникации.

Выделяется четыре сферы ведения информационной войны:

1. Политическая.

К этой сфере относятся:

· борьба за ноосферу. Объекты этой битвы — государственные идеи, духовные и национальные ценности, системы вероисповеданий, т. е. духовная сфера жизнедеятельности людей;

· интеллектуальная борьба элит (инновации, рефлексивное управление). Исследования показывают, что воздействие на информационный ресурс государства может стать одним из источников угроз для национальной безопасности.

Наиболее сложная форма воздействия — рефлексивное управление процессом принятия решения в государственных структурах посредством формирования выгодной для воздействующего информации или дезинформации.

· информационное противоборство в ходе избирательных процессов.

2. Финансово-экономическая.

В настоящее время мировая финансовая система стала главной ареной информационно-психологического противоборства между ведущими государствами мира. Одним из теоретиков и практиков информационно-психологического противоборства в финансовой сфере является Д. Сорос. Первой информационно-психологической битвой в финансовой сфере между ведущими странами мира можно считать мировые финансовые кризисы 1997–1998 гг. В будущем информационные войны будут в основном вестись именно в финансовой, а не в военной сфере. В условиях создания единого общемирового информационного пространства развернется геостратегическое противоборство между ведущими мировыми державами за доминирование в информационной среде мировой финансовой системы.

Для того чтобы стать экономически процветающей державой, Россия должна научиться защищать свои национальные интересы в мировой информационной среде и противодействовать информационной экспансии других стран в мировой финансовой системе.

3. Дипломатическая.

4. Военная.

Отдельно можно выделить противоборство в Интернете.

Информационная революция способствовала появлению новых форм и способов ведения информационно-психологического противоборства в мировом информационном пространстве. Во многом это связано с созданием сети Интернет, данную тенденцию необходимо учитывать при разработке теории информационно-психологического обеспечения национальной безопасности России.

5 Информационно-техническая война

В информационно-технической борьбе главными объектами нападения и защиты являются системы управления и связи, телекоммуникационные системы, различные радиоэлектронные средства. Понятие «информационное оружие», получившее широкое распространение после завершения военной операции против Ирака в 1991 г., сформировалось как раз в результате появления средств ведения информационно-технической борьбы. Решающий вклад в поражение Ирака внесло комплексное применение средств разведки, управления, связи, навигации и радиоэлектронной борьбы, совокупность которых и была определена как информационное оружие театра военных действий. Опыт локальных войн конца XX в. свидетельствует о том, что обязательным атрибутом победы в современном бою является завоевание превосходства в информационной сфере. В военное время ведение информационной войны предполагается на стратегическом, оперативном и тактическом уровнях. Но информационное оружие необходимо задействовать еще до начала боевых действий, а в полной мере применять уже в ходе сражений. Еще в мирное время объектами и целями этой борьбы являются информационные ресурсы государства, в которые включается прежде всего информация, существующая на материальных носителях или в любой другой форме. Особое значение информационных ресурсов обусловлено тем ключевым положением, которое они в силу особой роли информации как системообразующего фактора занимают по отношению к любым другим ресурсам государства — экономическим, научно-техническим и собственно военным.

В первую очередь информационное оружие направлено против вооруженных сил, предприятий оборонного комплекса, структур безопасности. При атаках удары наносят по телекоммуникациям или транспортным системам. Универсальность, скрытность, многовариантность форм программно-аппаратной реализации, радикальность воздействия, достаточный выбор места и времени применения, экономичность делают информационное оружие чрезвычайно опасным. Оно позволяет вести наступательные действия анонимно, без объявления войны. Классификация Мартина Либицки рассматривает методы ведения этих действий в рамках следующих форм:

· командно-управленческой,

· разведывательной,

· электронной,

· экономической,

· кибер-войны,

· хакерской войны.

1. Командно-управленческая информационная война.

Разрушить структуру управления войсками противника можно, направив удар на лидера армии или штаб командования — «голову» или сеть коммуникаций, соединяющих командование с основной массой войск, — «шею». Удар по «голове» — это испытанный прием всех военных операций с древности. Во время войны в Заливе успешность военных действий американцев во многом была обеспечена предварительным разрушением структуры командования и управления войсками противника. Им удалось добиться, таким образом, дезориентации иракских войск и неэффективности их военных действий. Штабы командования противника легко распознать по большому количеству коммуникаций, которые их окружают, постоянному движению больших потоков информации. Современные информационные технологии дают возможность использовать этот метод по-новому. Теперь коммуникации противника можно разрушить не только при помощи бомб, или физической атаки, а через компьютерную систему, например перекрыв подачу электричества, глуша радиоволны, внедрив вирусы в компьютерную сеть. Удар по «шее», разрыв связи между командованием и основной армией позволит отделить «голову» от «туловища», тем самым противник потеряет дееспособность. Для того чтобы использовать этот способ, нужно точно знать, каким образом происходит коммуникация противника, насколько важно командованию врага постоянно поддерживать связь с армией. Каждому действию в информационной войне должна предшествовать тщательная исследовательская и разведывательная работа, чтобы оно принесло необходимый результат. Например, во время войны во Вьетнаме разрушение связи между армией и командованием не имело ожидаемого эффекта, поскольку стратеги в США не учли особенности вьетнамских традиций в ведении войны. Оказалось, что во Вьетнаме, в отличие от США, отдельные подразделения армии обладают большой независимостью и они способны самостоятельно планировать военные действия, организовывать сопротивление без верховного командования в течение длительного времени. Таким образом, удары по «голове» и «шее» не дали никаких положительных результатов. Кроме того, уничтожение лидера или командования может привести к такому неприятному эффекту, как распространение неконтролируемой партизанской войны.

2. Разведывательная война.

Традиционно командование армии получает от разведки информацию о месторасположении противника, его качественных и количественных характеристиках. Это необходимо, чтобы планировать дальнейшую военную деятельность. Современная разведка благодаря развитию информационных технологий может обеспечивать командование достаточным количеством информации о противнике. Основная работа разведчика сегодня состоит в адекватном анализе полученной информации, способствующем принятию эффективных действий. Оборонительная составляющая этого типа войны включает работу по «обману» источников развединформации, когда они не уничтожаются, но нарушаются так, чтобы передавать неверную информацию.

3. Радиоэлектронная война.

Это особый вид информационной борьбы, призванный нарушать или затруднять функционирование электронных средств противника путем излучения, отражения электромагнитных сигналов, акустических и инфракрасных сигналов. Эта борьба осуществляется наземными, корабельными и авиационными системами постановки помех. Сюда входят способы по глушению радиосигналов противника, радиоперехваты, нарушение правильной работы радаров посредством введения ошибок в компьютерную сеть. К средствам ведения радиоэлектронной войны относятся электромагнитные бомбы и электромагнитные пушки. Мощный электромагнитный импульс (до десятков гигаватт), излучаемый этими устройствами, выводит из строя все электронное оборудование.

4. Хакерская война (компьютерные войны).

Целью нападения может быть полное разрушение компьютерной системы, ее временный выход из строя, программирование на выдачу ошибочной информации, кража информации или услуг. Нападение на военные информационные системы может осуществляться как во время конфликта, так и в мирное время. Атакующее информационное оружие этого типа широко распространено и многообразно. По мнению С. П. Расторгуева, информационным оружием следует называть средства уничтожения, хищения, искажения информационных массивов, средства дезорганизации работы технических устройств, компьютерных систем.

Вредоносные программы способны разрушать программное обеспечение компьютерных систем. Они могут размножаться, внедряться в программы, передаваться по линиям связи, сетям передачи данных, выводить из строя системы управления.

Кроме того, сюда относятся различные средства подавления информационного обмена в телекоммуникационных сетях, фальсификация информации в каналах государственного и военного

управления, различного рода ошибки, сознательно вводимые лазутчиком в программное обеспечение объекта.

5. Экономическая война.

Выделяется две ее разновидности. Первая — это информационная блокада, когда страна-агрессор перекрывает потоки информации из внешнего мира, необходимые для процветания государства. Вторая разновидность — формационный империализм — преобладание информационных продуктов одной страны, экспансия своих ценностей и культуры в различных проявлениях. Наиболее ярким примером являются процессы «американизации» современного мира.

6. Кибер-война.

Этот тип информационной войны пока не существует, но предполагается, что к нему должно привести дальнейшее развитие информационных технологий.

Среди вариантов кибер-войн сейчас наиболее понятны для осмысления семантические атаки и симуляционные войны. Отличие семантических атак от обычного хакерства в том, что система не выводится из строя, не разрушается, она продолжает нормально функционировать, но настраивается таким образом, чтобы выдавать пользователю неверные ответы, неправильно решает поставленные задачи. Симуляционные войны ведутся только в виртуальном пространстве, причем победивший в них признается победителем и в реальном мире.

6 Информационно-психологическая война

В информационно-психологической борьбе главными объектами нападения и защиты являются психика личного состава вооруженных силовых структур, населения противостоящих сторон, системы формирования общественного мнения и принятия решений. Такая борьба ведется методами и средствами информационно-психологического воздействия, ориентированного на войска и население по обе стороны «фронта».

Под *информационно-психологическими воздействиями* понимаются информационные воздействия на психику, в первую очередь на сознание человека и сообществ людей, проявляющиеся в изменении восприятия ими реальной действительности, коррекции своего поведения и принятия решений, а также, в некоторых случаях — в изменении физиологического состояния организма человека. Так, информационно-психологические воздействия в политической сфере понимаются как использование дипломатических, военно-демонстрационных, экономических, политических, информационных приемов для прямого или косвенного воздействия на мнение, настроения, чувства и, в итоге, на поведение другой стороны с целью подавить волю, заставить действовать под диктовку.

Информационно-психологические методы и средства психотехнологий подразделяются на открытые и скрытые, положительные и негативные, и деструктивные, преследующие явные и скрытые цели. Открытые психотехнологии реализуются с помощью честных «чистых» и обманных «грязных» методов и приемов. Информационно-психологические воздействия скрытого типа направлены на прямую манипуляцию сознанием человека через его подсознание путем применения скрытых психотехнологий, когда объект воздействия не осознает самого факта воздействия. Указанные скрытые воздействия включают психотропные (техногенные) средства, а также суггестивные (внушение, массовый гипноз) и психотропные (фармакологические) воздействия. Психофизические воздействия имеют скрытую насильственную направленность на психику и подсознание человека с целью безусловной модификации сознания, поведения и здоровья в нужном для воздействующей стороны направлении. Стремление скрыто воздействовать через подсознание человека осуществляется современными психотехнологиями, в том числе с применением сверхслабых энергоинформационных взаимодействий. В данный момент многие аналитики обращают внимание на нарастающее со стремительной скоростью совершенствование старых и на появление новых информационных психотехнологий, составляющих реальное оружие и опасность для интеллекта отдельной личности и народа в целом, его армии, силовых структур, руководящих органов власти.

До последнего времени главным объектом воздействия утверждалось сознание человека. Считалось непреложной истиной, что осязаемые эффекты могут быть восприняты нашим сознанием тогда и только тогда, когда они критически осмыслены нашим сознанием, пройдут через фильтр нашей оперативной памяти, а лишь потом отложатся в хранилище памяти — в нашем подсознании, прямой доступ к которому категорически закрыт. Подсознание рассматривается скорее как нечто мифическое, эфемерное как нечто спящее, неактивное, не способное влиять на «здравые» мысли и поступки личности. Новейшие исследования убедительно доказали, что наша оперативная

память, формирующая наш здравый смысл, — это всего лишь малая часть от нашей суммарной памяти, которой обладает человек. Главный ее резерв и хранилище — наше подсознание. В подсознании содержится от 70 до 99 процентов объема нашей памяти (всех знаний). Отсюда огромный интерес к раскрытию резервных возможностей человека путем прямого воздействия на его подсознание. Попытка «раскопать» глубинные залежи нашего мозга направлена на активное задействование подсознания в оперативный процесс мышления, когда реализуются феноменальные возможности человека по запоминанию информации, по фантастической скорости счета, по раскрытию его парапсихических способностей. С другой стороны, за этим стоит желание научиться прямо воздействовать на подсознание людей, программировать их на определенные мысли и поступки. Подобные действия влекут за собой не только фундаментальные сдвиги в подсознании и психике людей, но и изменение их мировоззренческих позиций.

Стремление воздействовать на человека напрямую через его подсознание выражено в разработке самых различных методов, при использовании которых объект воздействия не осознает ни цель, ни даже сам факт воздействия. Их коренное отличие от информационных воздействий открытого типа заключается в том, что они скрытно, то есть без ведома объекта воздействия, лишают его права самостоятельного выбора логически обоснованных решений, свободы выбора своего поведения, исполнения желаний, выражения эмоций и даже психофизиологического состояния организма (настроения, здоровья). Это достигается либо предварительным введением объекта воздействия в измененное состояние сознания, либо внедрением манипулирующей информации на фоне отвлекающих сообщений прямо в подсознание, минуя этап критического восприятия ее сознанием человека. В востребованное время эта информация по условному сигналу (паролю) с уровня подсознания всплывает в сознании и воспринимается человеком как его собственные мысли и убеждения. В соответствии с заложенной программой человек — объект воздействия — организует свое поведение, принимая решения. В предельном варианте этот человек в результате информационно-психологического воздействия скрытого типа превращается в зомби, который безотказно выполняет волю своего повелителя. Человек, подвергшийся «программированию», внешне ведет себя так же, как обычный человек, и не подозревает о том, что он «запрограммирован». Он среагирует только на ключевую команду, переданную ему в нужное время. После выполнения задания человек-зомби даже не осознает, что он сделал по этой команде, — программой ему «приказали» забыть этот факт. В подсознание такого человека можно заложить и несколько спецпрограмм.

Использование психотропных средств возможно и в военных целях, что позволяет говорить о психотропном оружии, которое может применяться как отдельно, так и в сочетании с другими средствами воздействия.

Итак, по мере повышения роли информации и информационных технологий в жизнедеятельности человека противоборство между государствами, политическими партиями, транснациональными корпорациями и международными террористическими организациями стало приобретать новые формы. В настоящее время ученые из разных стран в основном проанализировали систему закономерностей информационной борьбы. Они связывают воедино явления и процессы, протекающие в различных сферах: экономической, политической, духовной, военной. Закономерности информационной борьбы выступают как отношения не только между материальными факторами, но и между активно действующими в ней духовными силами.

Если до конца 40-х гг. XX в. информационная борьба между государствами в основном велась в период боевых действий и подчинялась военной стратегии, то сегодня она ведется практически постоянно и повсеместно. Необходимо пристальное внимание политиков и международной общественности, чтобы своевременно увидеть и по возможности предотвратить угрозу перехода от информационной борьбы к более агрессивным и разрушительным формам.

Возрастает необходимость создать условия для заключения многосторонних международных соглашений о запрещении применения средств технологического воздействия на национальные информационные ресурсы, определить принципы контроля использования информационных систем и сформировать основные приоритеты в проводимой международными организациями политике интеграции национальных сегментов информационных систем в единую мировую информационную инфраструктуру. Традиционно для разрешения задач внешней политики используются экономические, дипломатические, идеологические, культурные и другие «невоенные» средства. Сегодня к этому перечню средств можно добавить информационные технологии.