Вводная лекция. Теоретические основы защиты информации

Лекция

Ревизия: 0.1

Последняя модификация: Vlad Kovtun

Дата последней модификации: 07.12.2010 0:03:00

История изменений

01.09.2009 – Версия 0.1. Первичный документ. Ковтун В.Ю.

Содержание

История изменений 2
Содержание 3
Лекция 1. Основы теории защиты информации 4
- Вопросы 4
- Предисловие 4
  - Разведка 4
  - Каналы распространения информации 5
  - Каналы несанкционированного получения информации 7
- Защита информации 8
  - Основные понятия и определения 9
  - Введение в криптографию 12
  - Примечание 15
- Криптоанализ 15

Литература 17

Лекция 1. Основы теории защиты информации

Вопросы

1. Предисловие.
2. Основные положения.
3. Понятия криптографической системы.

Предисловие

Разведка

Задача защиты информации (ЗИ) решается, как правило, при наличии внешнего, иногда весьма мощного воздействия, заключающегося в разведывательной деятельности конкурента или противника (далее — противника). Поэтому для эффективного решения задачи ЗИ необходимо хорошо представлять смысл разведывательной деятельности (далее — разведки), ее характеристики, методы, виды и т.п.

Смысл разведки заключается в следующем.

- **Добывании** информации (политической, экономической, военной) для принятия стратегических, оперативных или тактических решений в соответствующих областях деятельности.
- **Получении** преимущества над противником на основе использования в своих целях его научно-технических, технологических и других достижений.

Для добывания информации разведка противника может использовать:

- легальные,
- полулегальные,
- нелегальные методы.

Разведке присущи следующие характеристики:

- разведка носит **номинальный характер** по отношению к повышению достоверности добытой информации;
- разведка **действует эшелонировано**, что позволяет проводить детальную разведку;
- разведка носит **координированный характер**;
- разведка носит **глобальный характер**;
- разведка направлена, прежде всего, на **особо важные объекты** (например, военные).

С точки зрения разведки, информация не является простой совокупностью равнозначных сведений. Можно сказать, что всю информацию по ее важности и, как правило, по степени защищенности, можно разделить на:

- секретную,
- конфиденциальную,
- открытую.

Экономическая разведка — это широкое понятие, объединяющее в себе промышленную и коммерческую разведку.

Промышленная разведка — это несанкционированное получение научно-технической и технологической информации, например, о документации, схемах каких-либо устройств, изобретениях, процессах производства продукции и т.п.

Коммерческая разведка — это несанкционированное получение информации, представляющей собой коммерческую тайну компании.

Итак, поскольку разведка занимается добыванием информации, необходимо рассмотреть формы представления интересующей ее информации, поскольку эти формы оказывают существенное влияние на методы добывания информации, и, следовательно, на методы и средства ее защиты.

Виды представления информации:

- Рукописная информация;
- Машинописная информация;
- Электронная информация;

- Устная информация.

Каналы распространения информации

На рис. 1, рассмотрим каналы распространения информации.

Рис. 1. Классификация каналов распространения информации

К **формальным** каналам распространения информации относятся:

- деловые встречи и совещания;
- обмен официальными деловыми научными документами с помощью средств передачи информации.

Неформальными каналами распространения информации являются: личное общение, выставки, семинары, конференции, съезды, средства массовой информации.

Каналами распространения информации могут также быть:

- распространение в стране и за рубежом официальных изданий о зарегистрированных в нашей стране изобретениях;
- рассылка по подписке вестников Академии Наук и отдельных ее институтов;
- обмен научно-технической литературой (книги, журналы), осуществляемый библиотеками и другими организациями по межбиблиотечному обмену, как внутри страны, так и с зарубежными организациями;
- обмен отчетами по НИОКР с научными учреждениями в соответствии с соглашениями о сотрудничестве или о совместном выполнении исследований и разработок;
- вывоз за границу книг и журналов научно-технического и экономического характера нашими гражданами, выезжающими в служебные командировки
- публикации специалистами и учеными научных и технических материалов в зарубежных изданиях, в том числе в World Wide Web;
- личная переписка специалистов и ученых по интересующей их тематике с зарубежными коллегами, особенно по электронной почте;
- рассылка научно-технических бюллетеней в электронные группы новостей, обсуждение интересующих тем в дискуссионных группах, форумах Internet и т.п.

Постараемся классифицировать способы НСД к источникам, рис. 2.

Рис. 2. Основные способы НСД

Рассмотрев основные методы, характеристики, виды и способы разведки, можно сделать вывод о том, что эффективной может быть лишь комплексная ЗИ, сочетающая следующие меры:

- законодательные (использование законодательные актов);
- морально-этические (сознательное соблюдение правил поведения, способствующих поддержанию здоровой моральной атмосферы в коллективе);
- физические (создание препятствий для доступа к охраняемой информации);
- административные (организация соответствующего режима секретности, пропускного и внутреннего режима);
- технические (применение электронных и других устройств защиты информации);
- криптографические;
- программные.

На основании многолетнего опыта к настоящему времени сформулирована система принципов создания СЗИ, среди которых можно выделить следующие:

- концептуальное единство;
- адекватность требованиям;
- гибкость (адаптируемость);
- функциональная самостоятельность;
- удобство использования;
- минимизация представляемых прав;
- полнота контроля;
- адекватность реагирования;
- экономическая целесообразность.

Также необходимо учитывать, что носителями информации, а, значит, и вероятными источниками ее утечки, являются следующие субъекты и объекты:

- персонал, имеющий допуск к информации;
- документы, содержащие ее (все типы носителей);
- технические средства и системы обработки информации, в том числе линии связи, по которым она передается.

Каналы несанкционированного получения информации

Чтобы справиться со стремительно нарастающим потоком информации, вызванным научно-техническим прогрессом, субъекты предпринимательской деятельности, учреждения и организации всех форм собственности вынуждены постоянно пополнять свой арсенал разнообразными техническими средствами и системами, предназначенными для приема, передачи, обработки и хранения информации. **Физические процессы, происходящие в таких устройствах при их функционировании, создают в окружающем пространстве побочные электромагнитные, акустические и другие излучения, которые в той или иной степени связаны с обработкой информации, схемой или конструкцией рассматриваемого технического средства передачи информации по паразитным связям напряжения, тока, заряда или магнитного поля.**

Под **паразитной связью** понимают связь по электрическим или магнитным цепям, появляющуюся независимо от желания конструктора. В зависимости от физической природы элементов паразитных электрических цепей, различают паразитную связь через общее полное сопротивление, емкостную или индуктивную паразитную связь.

Физические явления, лежащие в основе появления излучений, имеют различный характер, тем не менее, в общем виде утечка информации за счет побочных излучений может рассматриваться как непреднамеренная передача секретной информации по некоторой «побочной системе связи», состоящей из передатчика (источника излучений), среды, в которой эти излучения распространяются, и принимающей стороны. Причем, в отличие от традиционных систем связи, в которых передающая и принимающая стороны преследуют одну цель — передать информацию с наибольшей достоверностью, в рассматриваемом случае «передающая сторона» заинтересована в возможно большем ухудшении передачи информации, так как это способствует ее защите. Описанную «систему связи» принято называть **техническим каналом утечки информации**.

Основными **источниками** образования технических каналов утечки информации (рис. 4) являются:

- преобразователи физических величин;
- излучатели электромагнитных колебаний;
- паразитные связи и наводки на провода и элементы электронных устройств.

Источниками излучений в технических каналах являются разнообразные технические средства, в которых циркулирует информация с ограниченным доступом.

Такими средствами могут быть:

- сети электропитания и линии заземления;
- автоматические сети телефонной связи;
- системы телеграфной, телекодовой и факсимильной связи;
- средства громкоговорящей связи;
- средства звуко- и видеозаписи;
- системы звукоусиления речи;
- электронно-вычислительная техника;
- электронные средства оргтехники.

Технические каналы утечки информации принято делить на следующие типы:

- радиоканалы (электромагнитные излучения радиодиапазона);
- акустические каналы (распространение звуковых колебаний в любом звукопроводящем материале);
- электрические каналы (опасные напряжения и токи в различных токопроводящих коммуникациях);
- оптические каналы (электромагнитные излучения в инфракрасной, видимой и ультрафиолетовой части спектра);
- материально-вещественные каналы (бумага, фото, магнитные носители, отходы и т.д.).

Рис. 3. Классификация причин технических каналов утечки информации

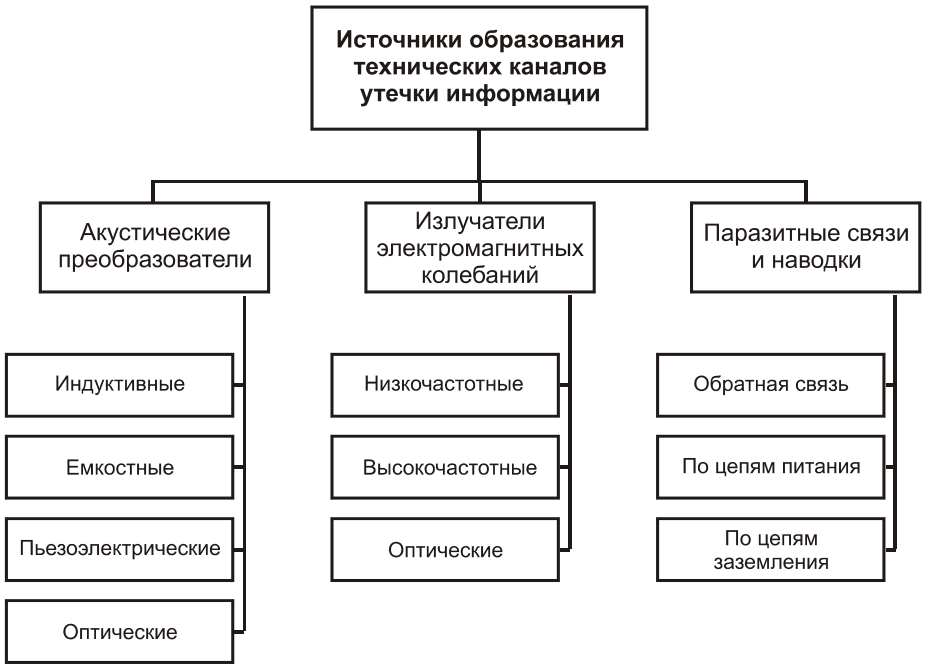

Рис. 4. Классификация источников технических каналов утечки информации

К основным информационным характеристикам канала относятся:

- местоположение начала и конца канала;
- форма передаваемой информации (дискретная, непрерывная) в звеньях канала;
- структура канала передачи (датчик, кодер, модулятор, линия, демодулятор, декодер, устройство фиксации и др.);
- вид канала (телефонный, телеграфный, телевизионный и др.);
- скорость передачи и объем передаваемой информации;
- способы преобразования информации в звеньях канала передачи (методы модуляции, кодирования и т.д.);
- пропускная способность канала;
- емкость канала.
- Кроме того, классификация каналов передачи возможна по следующим признакам:
- по виду сигналов и способу передачи;
- по исполнению: проводные, кабельные, световодные, радио и другое;
- по принципу действия: электромагнитные, оптические, акустические.

Защита информации

Автоматизированные системы обработки информации (АСОИ) — это человеко-машинные системы, обеспечивающие автоматизированный сбор и обработку

информации, необходимой для оптимизации управления в разных сферах деятельности.

Перечислим основные причины, которые позволяют говорить об актуальности и особой важности обеспечения безопасности функционирования АСОИ:

- резкое увеличение мощностей современных компьютеров, упрощение их эксплуатации;
- увеличение объемов информации, которые накапливаются, хранятся и обрабатываются в АСОИ;
- сосредоточение в единых БД информации различного назначения и принадлежности;
- расширение круга пользователей, которые имеют доступ к ресурсам АСОИ;
- стремительное развитие спектра программных средств, которые не удовлетворяют элементарным требованиям безопасности;
- расширение сетевых технологий, связь локальных сетей удаленных офисов через сеть Интернет. Развитие Интернет.

Хочется выделить факт разработка и принятия доктрины информационной войны ведущими мировыми державами (Российской Федерацией принята «Доктрина информационной безопасности» еще в 2000 году). Украина сильно отстает касательно обеспечения информационной безопасности на национальном уровне. На сегодняшний день, во втором чтении принят проект Закона Украины «О Концепции национальной информационной политики» №2526 от 13.12.2002 г**.** Однако следует выделить Указ Президента Украины № 377/2008 от 21.03.2008 г «О безотлагательных мероприятиях в обеспечении информационной безопасности Украины», в рамках которого предполагается разработка отечественной доктрины информационной безопасности. Появление данного указа свидетельствует о критичности разработки национальной доктрины информационной безопасности.

Познакомимся с основными понятиями и определениями.

Основные понятия и определения

Информация – публично оглашенные или опубликованные сведения о событиях и явлениях, происходящих в обществе, природной среде и т.д. (Закон Украины об информации).

Информация - совокупность данных, программ и сообщений, которые обрабатываются или хранятся в системе, независимо от физического или логического приложения.

Защита информации – совокупность организационно технических мероприятий, правовых и морально-этических норм, административных мероприятий, физических и программно-технических средств, направленных на противодействие угрозам АСОИ или сведение к минимуму возможности нанесения урона.

Безопасность АСОИ – защищенность от случайного или чрезмерного проникновения в нормальный процесс функционирования, а также от попыток кражи, изменения или нарушения ее компонентов.

Природа влияний на АСОИ может быть самою разной: стихийные бедствия, ошибки персонала, действия преступников.

Под доступом к информации подразумевается ознакомление с информацией, ее обработка, копирование, модификация, уничтожение.

Различают санкционированный и несанкционированный доступ.

Санкционированный доступ к информации – доступ, который не нарушает установленные правила разграничения доступа.

Правила разграничения доступа – служат для регламентации прав доступа субъектов доступа к объектам доступа.

Несанкционированный доступ – доступ к информации, который характеризуется нарушением установленных правил разграничения доступа. Наиболее распространенный тип компьютерных нарушений.

Конфиденциальность данных - статус, который присваивается данным и определяет требования к степени их защиты.

Субъект - активный компонент системы, который может стать причиной потока информации от объекта к субъекту или изменения состояния системы.

Объект - пассивный компонент системы, сохраняющий, принимающий либо передающий информацию. Доступ к объекту – доступ к информации, которая в нем хранится.

Целостность информации обеспечивается в том случае, если данные в системе, в семантическом смысле, не отличаются от данных в исходящих документах.

Целостность компонента либо ресурса – способность компонента либо ресурса быть неизменным в семантичесеом смысле при функционировании системы в случайных условиях либо умышленных искажений либо проникновений.

Под угрозой безопасности АСОИ понимают возможные влияния на АСОИ, которые могут прямо либо косвенно нанести вред безопасности.

Уязвимость АСОИ – некоторая неудачная способность, которая делает возможным возникновение реализации угрозы.

Атака на компьютерную систему - действие, которое выполняется нарушителем, и состоит в поиске и использовании той или иной уязвимости системы. Атака - реализация угрозы.

Безопасная либо защищенная система - система с средствами защиты, которые успешно и эффективно противодействуют угрозам безопасности.

Комплекс средств защиты – совокупность программных и технических средств, которые создаются и поддерживаются, для обеспечения информационной безопасности АСОИ.

Политика безопасности – совокупность норм, правил, практических рекоммендаций, которые регламентируют работу средств защиты АСОИ от заданного множества угроз безопасности.

Согласно цели влияния, различают следующие угрозы АСОИ:

- угрозы нарушения конфиденциальности;
- угрозы нарушения целостности;
- угрозы нарушения работоспособности;

Направленные на разглашение конфиденциальной либо секретной информации. Информация становится известной лицам, которые не имеют к ней доступа.

Направленные на изменение и искажение информации, которое приводит к нарушению ее количества либо полному уничтожению. Может быть нарушена злоумышленником и через влияние среды. Актуальна для сетей передачи данных, компьютерных сетей и телекоммуникаций.

Указанные действия либо снижают работоспособность системы, либо блокируют доступ к ее ресурсам.

Современные АСУ являются сложной системой, состоящей из большого количества компонентов. Компоненты АСОИ выделяют в группы:

- аппаратные средства (ЭВМ и их составные части: процессоры, мониторы, терминалы и т.д.);
- программное обеспечение (купленные программы; исходные, объектные, загружаемые (статические и динамические) модули, операционные системы);
- данные, которые хранятся временно или постоянно;
- персонал (обслуживающий персонал и пользователи).

Опасные воздействия на АСОИ можно разделить на: случайные и преднамеренные.

Случайные угрозы:

- аварийные ситуации в результате стихийных бедствий;
- отказы и сбои аппаратуры;
- ошибки в программном обеспечении;
- ошибки в работе обслуживающего персонала и пользователей;
- помехи в линиях связи через влияние окружающей среды.

Преднамеренные угрозы связаны с целенаправленными действия злоумышленника.

Касательно АСОИ специального назначения, то выделяют следующие преднамеренные угрозы:

- НСД и ознакомление с конфиденциальной информацией;
- ознакомление служащих с информацией, к которой они обязаны иметь доступ;

- несанкционированное копирование программ и данных;
- кража магнитных, оптических носителей информации, содержащих конфиденциальную информацию;
- кража печатных документов;
- преднамеренное уничтожение информации;
- несанкционированная модификация финансовых документов;
- фальсификация документов, передаваемых по каналам связи;
- отказ от авторства сообщений (документов), передаваемых по каналам связи;
- отказ от факта получения сообщений (документов), передаваемых по каналам связи;
- навязывание ранее переданного сообщения;
- распространение вирусов, со всеми вытекающими последствиями;
- уничтожение архивной информации;
- кража оборудования.

Существуют следующие подходы к обеспечению защиты информации АСОИ:

- **«Фрагментарный»** - направленный на противодействие четко определенным угрозам. Достоинство – высокая степень противодействия конкретной угрозе.
- **Комплексный подход** – ориентированный на создание защищенной среды обработки конфиденциальной информации в АСОИ, который объединяет в единый комплекс разнородные мероприятия противодействия угрозам. Разрешает гарантировать определенный уровень безопасности АСОИ.

Под системой защиты АСОИ понимают единую совокупность правовых и морально-этических норм, административно–организационных мероприятий, физических и программно–технических средств, направленных на противодействие угрозам АСОИ с целью сведения к минимуму возможности нанесения вреда.

По способам реализации, все мероприятия по обеспечению безопасности АСОИ систем, делятся на:

- правовые;
- морально–этические;
- административные;
- физические;
- аппаратно-программные.

Правовые меры относятся все действующие в государстве законы, указы и нормативные акты, которые регламентируют правила обращения с информацией ограниченного использования (доступа) и ответственности об их нарушении.

Морально-этические меры. Различные нормы поведения, которые традиционно сложились либо складываются по мере распространения компьютеров в стране и мире.

Административные меры. Включают:

- разработку правил обработки информации в АСОИ;
- совокупность действий при проектировании и оборудовании вычислительных центров;
- совокупность действий при подборе и подготовке персонала;
- организация надежного пропускного режима;
- организация учета, хранения, использования, уничтожения документов, носителей конфиденциальной информации;
- распределение реквизитов разделения доступа;
- организация скрытого контроля за работой пользователей и персонала.

Физические меры. Различные механические, электрические и электро-механические устройства и сооружения, которые предназанчены для создания физических преград (препятствий).

Аппаратно-программные средства. Различные электронные устройства и специальные программы, которые реализуют самостоятельно, либо совместно с другими средствами защиты:

- идентификацию;
- аутентификацию;
- разделение доступа к ресурсам АСОИ;
- контроль целостности данных;
- обеспечение конфиденциальности;
- регистрация и анализ действий (событий), которые происходят в АСОИ;

- резервирование ресурсов и компонентов АСОИ.

Большинство из перечисленных способов защиты, реализуется криптографическими методами защиты информации.

Безопасность информации – защищенность данных, программ, сообщений, протоколов, средств, от нарушения конфиденциальности, целостности, доступности и наблюдаемости информации.

Обеспечение безопасности информации – совокупность мероприятий, направленных на обеспечение конфиденциальности, целостности, доступности и наблюдаемости информации. Основным средством защиты информации есть применение криптографического преобразования.

Криптографическое преобразование информации (КПИ) – преобразование информации с целью обеспечения целостности, подтверждения подлинности, авторства, защиты от несанкционированного доступа, шифрования информации, которое осуществляется с использованием ключей.

Криптографическая защита информации (КЗИ) – защита информации, которая осуществляется с использованием криптографического преобразования.

Криптографическая система – совокупность средств КЗИ, необходимой ключевой, руководящей и др. документации.

Средства КЗИ – есть аппаратный, программный либо программно-аппаратный способ преобразования информации, который предназначен для КЗИ.

Ключевые данные – совокупность случайных или псевдослучайных значений изменяемых параметров КПИ, с помощью которых достигается цель КЗИ (обеспечивается стойкость).

Услуги криптографической системы – конфиденциальность, целостность, доступность и наблюдаемость информации и ресурсов в информационных системах и технологиях, которые обеспечиваются за счет применения КЗИ.

Конфиденциальность – свойство защищенности информации от несанкционированного доступа и попыток раскрытия ее содержания неавторизованными лицами и (или) процессами.

Целостность – свойство информации, заключающееся в том, что она не может быть изменена случайно или преднамеренно неавторизованными субъектами или объектами.

Доступность – свойство ресурса, информации, объекта, услуги, системы, которое заключается в том, что объект или субъект, наделенный полномочиями, может использовать ресурс с заданным качеством, в том числе за счет использования методов КЗИ.

Наблюдаемость – свойство ресурса, системы, которое позволяет регистрировать все действия объектов и субъектов однозначно устанавливать имена объектов/субъектов, причастных к определенным действиям, а также реагировать на все действия с целью минимизации потерь.

Криптографический анализ – анализ криптографической системы, ее входных и выходных параметров, включая часть ключа с целью определения значимой информации, включая ключи, которые могут быть использованы для нарушения: конфиденциальности, целостности, доступности, наблюдаемости.

Информационная война – противоборство непримиримых сторон в информационной среде, осуществляемой с целью нанесения максимальных убытков другой стороне и минимизации своих убытков в разных сферах.

Информационная безопасность – защищенность от воздействий, естественного или искусственного характера в различных сферах.

Информационное оружие – совокупность организационных и организационно-технических влияний на информационную систему или информационную технологию, осуществляемых с целью разведки, обмена и т.д.

Введение в криптографию

Наиболее общей наукой о тайне является **криптология**. Криптология как наука изучает закономерности обеспечения конфиденциальности, целостности и т.д. критичной информации в условиях интенсивного противодействия (криптоанализа).

Криптология делится на: криптографию и криптоанализ.

Криптография - изучает методы, алгоритмы и средства осуществления криптографической защиты информации.

Криптоанализ – изучает методы, алгоритмы и средства вскрытия криптографической системы при неизвестной части ключа.

Криптографическое преобразование информации – осуществляется с использованием симметричных, несимметричных криптосистем. Криптографическая система называется **симметричной**, если ключ прямого преобразования совпадает и с ключом обратного преобразования $K_{Forw.Tran} = K_{Back.Tran}$ (условие 1) или вычисляется один из другого не выше чем с полиномиальной сложностью (не более 1 сек).

Криптосистема (алгоритм) является **несимметричной** (ассиметричной, с открытым ключом), если ключ прямого преобразования не совпадает с ключом обратного преобразования $K_{Forw.Tran} \neq K_{Back.Tran}$ (условие 2), и один может быть вычислен из другого не ниже чем с экспоненциальной сложностью.

В Европе проводился конкурс на базовые криптопримитивы NESSIE –2000-2003, в нем определено 10 видов криптопреобразований (www.cryptonessie.org).

Симметричные – блочные (блоковые) симметричные шифр, лоточный шифр, аутентификация (процедура установления подлинности источника, приемника сообщений).

Несимметричные – функции хеширования (вычисление криптографических контрольных сумм) однонаправленная хеш-функция (сжатия из большого пространства в малое), ключевая хеш-функция (однонаправленная хеш-функция с использованием ключа).

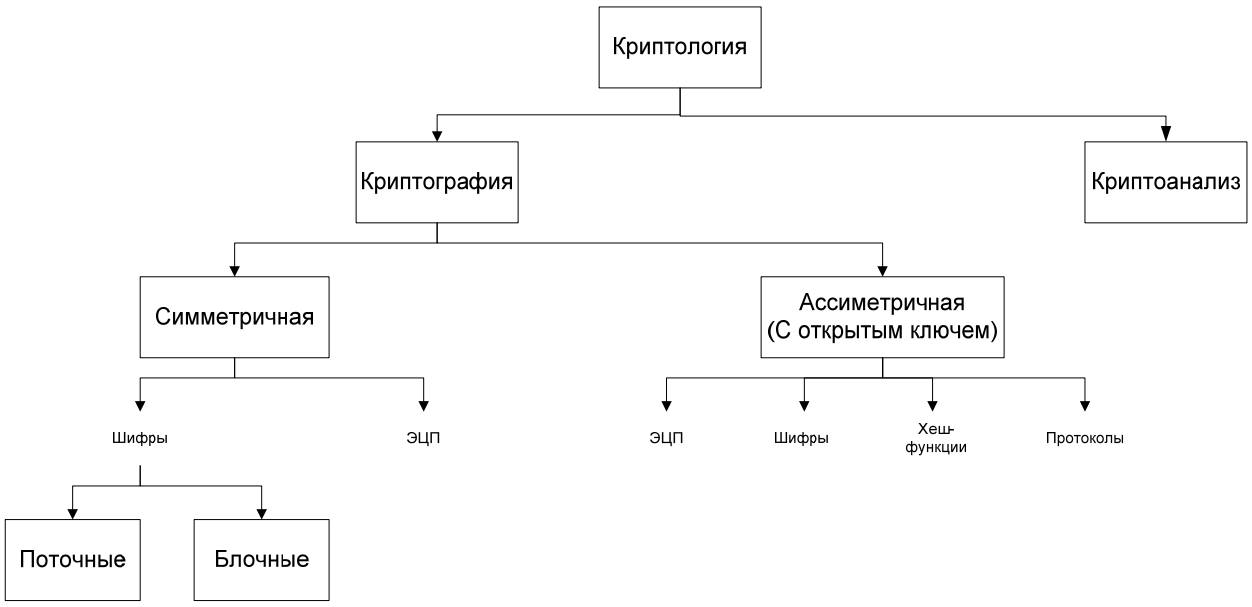

Рис. 5. Направления в современной криптографии

Направленное шифрование - выполняется условие (2).

Идентификация (аутентификация) – выполняется условие (1), (2).

Криптопротокол - решение распределенной задачи, многоэтапное.

В соответствии с принятой в защищенных системах моделью в информационном отношении участвуют 4 стороны: источник и получатель информации, злоумышленник (криптоаналитик), арбитр, рис. 6.

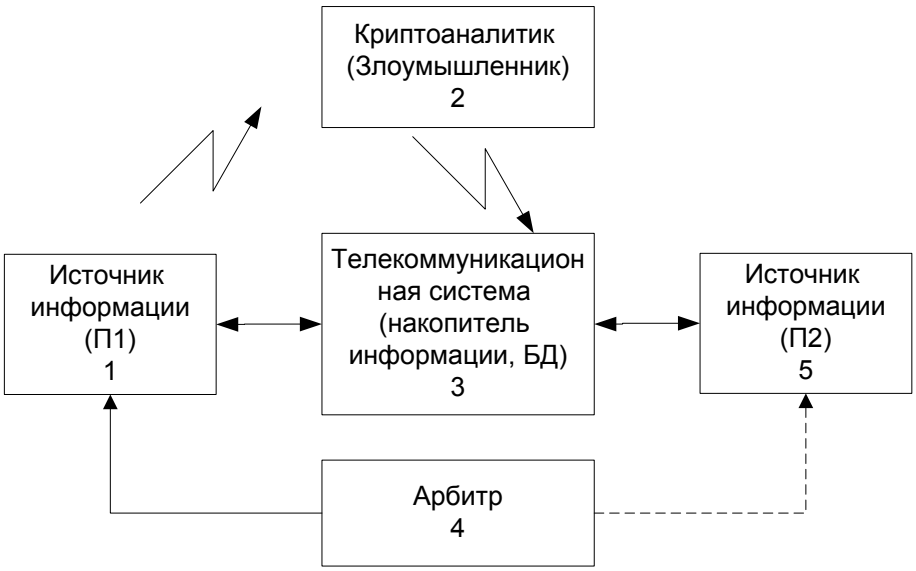

Рис. 6. Модель защищенной системы

В такой системе пользователи П1, П2 осуществляют информационные отношения и передается информация по не защищенной телекоммуникационной системе, или хранится в открытых базах данных, доступных носителях. В связи с этим злоумышленник имеет возможность осуществлять различного рода угрозы с целью нанесения ущерба П1, П2. Злоумышленник бывает:

- Санкционированный пользователь системы (нарушитель).
- Криптоаналитик (КРА), внешний объект – субъект.

Нарушитель – физическое или юридическое лицо, которое преднамеренно (непреднамеренно) осуществляет в системе неправомерные действия, т.е. с нарушением установленного порядка. Все воздействия на систему нарушителя или КРА называются угрозы.

Угроза – потенциально существующая опасность воздействия на систему с целью нанесения ущерба системе, обусловленное процессом и обработкой информации.

Угрозы бывают активные и пассивные.

Пассивная – угроза, в результате реализации которой не изменяется информационное состояние системы, но ущерб наносится.

Активная – изменение информационного состояния системы.

Основные угрозы, которые может реализовать криптоаналитик:

1. Компрометация защищенной информации и ключей, в смысле получения содержательной части – расшифрования, получение ключей в явном виде.
2. Передачи через телекоммуникационную систему ложных криптограмм с целью обмана П2.
3. Модификация истинной информации.
4. Нарушение работоспособности системы за счет передачи ложных команд и сигналов.
5. Угрозы, связанные с нарушением наблюдаемости информационных отношений пользователей.
6. Несанкционированный доступ к информации.

Для защиты от 1-6 угроз с целью обеспечения конфиденциальности (К), целостности (Ц), пользователи П1 и П2 должны осуществлять криптографическое преобразование (КП).

Как правило, с целью обеспечения Ц, пользователем вначале формируется цифровая подпись (ЦП) информации M_i, формируемой источником 1.

$$DS = \mathbf{F}_i^+\left(M_i, K_j, P_r\right), \tag{1}$$

где DS – функция КП. K_j – ключ, P_r – дополнительные параметры, M_i – сообщение, $\mathbf{F}_i$ - функция преобразования.

В результате реализации (1), к сообщению M_i добавляется ЦП, вычисляемая по (1).

$$M_i \mapsto DS ,$$

Отображение пространства сообщений M_i' множества криптограмм C_i, процедура $\mathbf{F}_i^+$ прямого преобразования.

$$M_i \mapsto C_i ,\ C_i = \mathbf{F}_i^+\left(M_i', K_j^{en}, P_r\right), \tag{2}$$

где K_j^{en} - ключ зашифровывания.

Криптограмма C_i хранится и передается открыто. Получатель П2 или П1 (если это носитель информации) при необходимости доступа к ней M_i^*. П осуществляет ее расшифровывание.

$$M_i^* = \mathbf{F}_i^-\left(C_i^*, K_j^{dec}, P_r\right), \tag{3}$$

где K_j^{dec} - ключ расшифровывания.

Если в C_i^* нет ошибок, и используются согласованно ключи и параметры, то M_i^* совпадает с M_i', т.е. с исходным сообщением.

$$M_i^* = M_i' . \tag{4}$$

Для проверки целостности и подлинности информации получатель П2, используя ключ проверки ЦП, проверив ЦП, вычисляет обратную подпись.

$$BDS = \mathbf{F}_i^-\left(M_i^*, K_j', P_r\right). \tag{5}$$

Примечание

П1, П2 должны согласованно использовать ключи, в системе должен быть источник ключей, должны быть система управления ключей к данным.

Преобразования 1-5 осуществляются таким образом, чтобы арбитр на их основе мог провести эксперимент и вынести решение.

Криптоанализ

Существуют четыре типа криптоаналитических атак. Они формулируются в соответствии с предположением, что криптоаналитику известен алгоритм и шифртекст сообщения.

Криптоаналитическая атака при наличии только известного шифртекста. Работа криптоаналитика состоит в том, чтобы раскрыть исходные тексты большинства

сообщений, более того вычислить ключ, для того, что бы расшифровать все сообщения зашифрованные этим ключом.

Криптоаналитическая атака при наличии известного открытого текста. Работа криптоаналитика состоит в поиске ключа, либо алгоритму расшифровывания.

Криптоаналитическая атака при возможности подбора открытого текста. Более мощный криптоанализ.

Криптоаналитическая атака с адаптивным выбором открытого текста. Эта атака предоставляет криптоаналитику еще больше возможностей.

Кроме того, можно выделить **атаку полного перебора** и **атаку с использованием избранного шифртексту.**

Шеннон в своих трактатах отвечал на очень важные вопросы:

1. Можно ли создать систему защиты информации со стойкостью, которая требуется, абсолютно стойкую, если криптоаналитик имеет неограниченные ресурсы энергии (энергия Солнца).

2. Можно ли создать систему защиты, если криптоаналитик имеет ограниченные ресурсы времени и производительности.

Шеннон показал, что можно создать такие системы защиты:

1.Теоретиески недешифруемые.

2. Вычислительно стойкие.

3. Ограниченной стойкости.

4. Доказуемо стойкие (Ель-Гамала, RSA, ECC и т.д.).

Теорема. Необходимым и достаточным условием теоретической недешифруемости является:

$$\mathbf{P}(C_j / M_i) = \mathbf{P}(C_j),$$

Т.е. вероятность возникновения криптограммы не зависит от сформированного отправителем сообщения. Произвольное сообщение обязано равновероятно отображаться повинно в произвольную криптограмму.

Введем обозначения:

Отправитель информации формирует на выходе сообщение M_i, а также известна априорная статистика $\mathbf{P}(M_i)$ - вероятность появления сообщения, для $i = \overline{1, n_m}$, где n_m - количество сообщений.

Предполагается, что известен алфавит источника ключей m_k, вероятность появления ключей $\mathbf{P}(K_i)$, для $i = \overline{1, n_k}$, где n_k - количество ключей.

На выходе шифратора-аутентификатора формируются криптограммы C_j, предполагается известной априорная информация статистика $\mathbf{P}(C_j / M_i)$ для всех i и j, $j = \overline{1, n_c}$, где n_c - количество криптограмм.

Криптограммы передаются по КС либо записываются на носители информации. Когда происходит прием криптограммы, производят обратное преобразование. Криптоаналитик с вероятностью близкой к 1 перехватывает все криптограммы и пробует сначала определить:

$\mathbf{P}(M_i / C_j)$ либо $\mathbf{P}(K_i / C_j)$,

Другими словами:

1. Что в C_j-криптограмме содержится M_i-сообщение.

2. C_j-криптограмме получена при использовании K_i-ключа.

Доказательство

$$\mathbf{P}(M_i/C_j)=\frac{\mathbf{P}(M_i)\mathbf{P}(C_j/M_i)}{\mathbf{P}(C_j)}=\frac{\mathbf{P}(M_i)\mathbf{P}(K_{ij})}{\mathbf{P}(C_j)},$$

$$\mathbf{P}(C_j)=\sum_{i=1}^{N}\mathbf{P}(M_i)\mathbf{P}(C_j/M_i),$$

$$\mathbf{P}(M_i/C_j)=\mathbf{P}(M_i).$$

Т.е. система теоретически недешифруемая. Криптоаналитик в результате перехвата ничего не узнал.

$\frac{\mathbf{P}(M_i/C_j)}{\mathbf{P}(M_i)}=\frac{\mathbf{P}(C_j/M_i)}{\mathbf{P}(C_j)}=1$, т.е. $\mathbf{P}(C_j/M_i)=\mathbf{P}(C_j)$

Шеннон ввел понятие **энтропии** – среднего количества информации, которая содержится в одном сообщении, знаке и т.д.

$$\mathbf{H}(M_i)=\sum_{i=1}^{N}\mathbf{P}(M_i)\log_2\mathbf{P}(M_i)$$

Энтропия ключа определяется:

$$\mathbf{H}(K_i)=\sum_{i=1}^{N}\mathbf{P}(K_i)\log_2\mathbf{P}(K_i)$$

До перехвата криптоаналитик находился в априорной неопределенности $\mathbf{H}(M)$, после перехвата большого количества криптограмм, криптоаналитик находится в неопределенности $\mathbf{H}(M/C)$.

Количество информации, которую получил криптоаналитик, относительно источника сообщений:

$\mathbf{H}(M)-\mathbf{H}(M/C)=\Delta\mathbf{I}(M/C)$ либо $\mathbf{H}(K)-\mathbf{H}(K/C)=\Delta\mathbf{I}(K/C)$

Граничные случаи

1. $\Delta\mathbf{I}(M,C)=0$, т.е. $\mathbf{H}(M)=\mathbf{H}(M/C)$ - энтропия не изменилась, ничего о системе не узнал.
2. $\mathbf{H}(M/C)$, т.е. $\mathbf{H}(M)=\Delta\mathbf{I}(M/C)$ - о системе стало известно все (система раскрыта).
3. $0<\mathbf{H}(M/C)\le\mathbf{H}(M)$ - в реальных ситуациях. Чем меньше $\mathbf{H}(M)$, тем меньше вероятность успеха раскрытия системы.

Расстояние единственности – количество символов, которые необходимо перехватить криптоаналитику, что бы иметь единственное решение.

Для теоретически недешифруемой системы длина ключа должна быть не менее длины сообщения.

Литература

1. Криптографическая защита информации в АСУ СН. Курс лекций. В.И. Долгов. ХВУ. 1998.

2. Криптографическая защита информации в информационных системах. Курс лекций. И.Д. Горбенко. ХНУРЭ. 2002.

3. Теория информации. Курс лекций. В.И. Долгов. ХВУ. 1998.

4. Закон Украины «О информации». Доступно: http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=2657-12

5. Теория информации. Доступно: http://www.msclub.ce.cctpu.edu.ru/bibl/TI/t1.htm