И.Ю. Юрин

ТЕОРЕТИЧЕСКИЕ И ПРАКТИЧЕСКИЕ ОСНОВЫ ЗАЩИТЫ ИНФОРМАЦИИ

Учебное пособие

Саратов – 2012

Содержание

Часть I. ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ЗАЩИТЫ ИНФОРМАЦИИ

СПИСОК ИСПОЛЬЗУЕМЫХ СОКРАЩЕНИЙ

ЗИ - защита информации

ИБ - информационная безопасность

ИТ - информационные технологии

НСД - несанкционированный доступ

ПО - программное обеспечение

ПС – парольная система

РФ - Российская Федерация

СЗИ - средства защиты информации

СМИ - средства массовой информации

Тема 1. *ОСНОВНЫЕ КОНЦЕПТУАЛЬНЫЕ ПОЛОЖЕНИЯ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ.*

Информация - сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления.

Анализ состояния дел в сфере ЗИ показывает, что уже сложилась концепция и структура защиты, основу которой составляют:

- весьма развитый арсенал технических СЗИ, производимых на промышленной основе;
- значительное число фирм, специализирующихся на решении вопросов ЗИ;
- четко очерченная система взглядов на эту проблему;
- наличие значительного практического опыта.

Тем не менее, злоумышленные действия над информацией не только не уменьшаются, но и имеют достаточно устойчивую тенденцию к росту. Опыт показывает, что для борьбы с этой тенденцией необходима стройная и целенаправленная организация процесса защиты информационных ресурсов.

Следует помнить, что

1) обеспечение безопасности информации не может быть одноразовым актом. Это непрерывный процесс, заключающийся в обосновании и реализации наиболее рациональных методов, способов и путей совершенствования и развития системы защиты, непрерывном контроле ее состояния, выявлении ее узких и слабых мест и противоправных действий;

2) безопасность информации может быть обеспечена лишь при комплексном использовании всего арсенала имеющихся средств защиты во всех структурных элементах производственной системы и на всех этапах технологического цикла обработки информации. Наибольший эффект достигается тогда, когда все используемые средства, методы и меры объединяются в единый целостный механизм - систему ЗИ. При этом функционирование системы должно контролироваться, обновляться и дополняться в зависимости от изменения внешних и внутренних условий;

3) никакая система ЗИ не может обеспечить требуемого уровня безопасности информации без надлежащей подготовки пользователей и соблюдения ими всех установленных правил, направленных на ее защиту.

Система ЗИ - это организованная совокупность специальных органов, средств, методов и мероприятий, обеспечивающих ЗИ от внутренних и внешних угроз.

С позиций системного подхода к ЗИ предъявляются определенные требования. Защита информации должна быть:

1) непрерывной;

2) плановой;

3) целенаправленной;

4) конкретной (защите подлежат конкретные данные, объективно подлежащие охране, утрата которых может причинить организации определенный ущерб);

5) активной (защищать информацию необходимо с достаточной степенью настойчивости);

6) надежной (методы и формы защиты должны надежно перекрывать возможные пути неправомерного доступа к охраняемым секретам, независимо от формы их представления, языка выражения и вида физического носителя, на котором они закреплены);

7) универсальной (в зависимости от вида канала утечки или способа НСД его необходимо перекрывать, где бы он ни проявился, разумными и достаточными средствами, независимо от характера, формы и вида информации);

8) комплексной (недопустимо применять лишь отдельные формы или технические средства).

Для обеспечения выполнения столь многогранных требований безопасности система ЗИ должна удовлетворять определенным условиям:

1) охватывать весь технологический комплекс информационной деятельности;

2) быть разнообразной по используемым средствам, многоуровневой с иерархической последовательностью доступа;

3) быть открытой для изменения и дополнения мер обеспечения безопасности информации;

4) быть нестандартной, разнообразной (при выборе средств защиты нельзя рассчитывать на неосведомленность злоумышленников относительно ее возможностей);

5) быть простой для технического обслуживания и удобной для эксплуатации пользователями;

6) обладать целостностью (ни одна ее часть не может быть изъята без ущерба для всей системы).

К системе защиты информации предъявляются определенные требования:

1) четкость определения полномочий и прав пользователей на доступ к определенным видам информации;

2) предоставление пользователю минимальных полномочий, необходимых ему для выполнения порученной работы;

3) сведение к минимуму числа общих для нескольких пользователей средств защиты;

4) учет случаев и попыток НСД к конфиденциальной информации;

5) обеспечение оценки степени конфиденциальной информации;

6) обеспечение контроля целостности средств защиты и немедленное реагирование на их выход из строя.

Система ЗИ как любая система должна иметь определенные виды собственного обеспечения, опираясь на которые она будет выполнять свою целевую функцию:

1) правовое (нормативные документы, положения, инструкции, руководства, требования которых являются обязательными в рамках сферы их действий);

2) организационное (реализация защиты информации осуществляется определенными структурными единицами - такими, как служба защиты документов; служба режима, допуска, охраны; служба защиты информации техническими средствами; информационно-аналитическая деятельность);

3) аппаратное (широкое использование технических средств для ЗИ и для обеспечения деятельности системы ЗИ);

4) информационное (сведения, данные, показатели, параметры, лежащие в основе решения задач, обеспечивающих функционирование системы);

5) программное (информационные, учетные, статистические и расчетные программы, обеспечивающие оценку наличия и опасности различных каналов утечки и путей НСД к источникам конфиденциальной информации);

6) математическое (использование математических методов для различных расчетов, связанных с оценкой опасности технических средств злоумышленников, зон и норм необходимой защиты);

7) лингвистическое (совокупность специальных языковых средств общения специалистов и пользователей в сфере ЗИ);

8) нормативно-методическое (нормы и регламенты деятельности органов, служб, средств, реализующих функции ЗИ, различного рода методики,

обеспечивающие деятельность пользователей при выполнении своей работы в условиях жестких требований ЗИ).

Удовлетворить современные требования по обеспечению безопасности предприятия и защиты его конфиденциальной информации может только *система безопасности* - организованная совокупность специальных органов, служб, средств, методов и мероприятий, обеспечивающих защиту жизненно важных интересов личности, предприятия и государства от внутренних и внешних угроз.

Тема 2. *КОНЦЕПТУАЛЬНАЯ МОДЕЛЬ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.*

ИБ - это состояние защищенности информации среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государств (Закон РФ "Об участии в международном информационном обмене").

Можно выделить угрозы безопасности информации, источники этих угроз, способы их реализации и цели, иные условия и действия, нарушающие безопасность. Так же следует рассматривать и меры ЗИ от неправомерных действий, приводящих к нанесению ущерба.

Можно предложить следующие компоненты модели ИБ:

1) объекты угроз;

2) угрозы;

3) источники угроз;

4) цели угроз со стороны злоумышленников;

5) источники информации;

6) способы НСД к конфиденциальной информации;

7) направления ЗИ;

8) способы ЗИ;

9) средства ЗИ.

Объектом угроз ИБ выступают сведения о составе, состоянии и деятельности объекта защиты (персонала, материальных и финансовых ценностей, информационных ресурсов).

Угроза – потенциально возможное событие, действие, процесс или явление, которое может привести к нанесению ущерба чьим-либо интересам.

Угроза информационной безопасности – возможность реализации воздействия на информацию, приводящего к искажению, уничтожению, копированию, блокированию доступа к информации, а также возможность воздействия на компоненты информационной системы, приводящего к утрате, уничтожению или сбою функционирования носителя информации, средства взаимодействия с носителем или средства его управления. Таким образом, угрозы информации выражаются в нарушении ее целостности, конфиденциальности, полноты и доступности.

Источниками конфиденциальной информации являются люди, документы, публикации, технические носители информации, технические средства обеспечения производственной и трудовой деятельности, продукция и отходы производства. Основными направлениями ЗИ являются правовая, организационная и инженерно-техническая ЗИ.

Средствами ЗИ являются физические средства, аппаратные средства, программные средства и криптографические методы. Последние могут быть реализованы как аппаратно, программно, так и смешанно (программно-аппаратными средствами).

В качестве способов защиты выступают всевозможные меры, пути и действия, обеспечивающие упреждение противоправных действий и противодействие НСД.

Тема 3. *УГРОЗЫ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ.*

Под угрозами конфиденциальной информации принято понимать потенциальные или реальные действия по отношению к информационным ресурсам, приводящие к неправомерному овладению охраняемыми сведениями и,

как следствие, моральному или материальному ущербу. Такими действиями являются:

- ознакомление с конфиденциальной информацией различными путями и способами без нарушения ее целостности;
- модификация информации в криминальных целях (частичное или значительное изменение состава и содержания сведений);
- разрушение (уничтожение) информации как акт вандализма с целью прямого нанесения материального ущерба.

Противоправные действия с информацией приводят к нарушению ее конфиденциальности, полноты, достоверности и доступности. Каждая угроза влечет за собой определенный ущерб - моральный или материальный, а защита и противодействие угрозе призвано снизить его величину.

Угрозы могут быть классифицированы по следующим типам:

1) по величине нанесенного ущерба:

а) предельный, после которого фирма может стать банкротом;

б) значительный, но не приводящий к банкротству;

в) незначительный, который фирма за какое-то время может компенсировать.

2) по природе воздействия:

а) естественные – вызванные воздействием на систему и ее компоненты объективных физических процессов или стихийных природных явлений, не зависящих от человека;

б) преднамеренные действия человека;

в) непреднамеренные действия человека: проявление ошибок проектирования программно-аппаратных средств; некомпетентное использование, настройка или неправомерное отключение средств защиты персоналом СБ; неправомерное включение оборудования или изменение режимов работы устройств и программ; удаление или искажение файлов, порча носителей информации, повреждение каналов связи; пересылка данных по ошибочному адресу; ввод ошибочных данных;

3) по непосредственному источнику угроз:

а) природная среда – стихии, магнитные бури, радиация;

б) человек – внедрение агентов в персонал; вербовка; угроза НС копирования данных пользователем ПК; разглашение, передача или утрата атрибутов разграничения доступа (ключи, пароли, карты, коды) и т.д.;

в) санкционированные программно-аппаратные средства – отказ в работе ОС и т.д.;

г) НС программно-аппаратные средства – нелегальное внедрение и использование неучтенных программ (не являющихся необходимыми для выполнения служебных обязанностей) с последующим необоснованным расходованием ресурсов (загрузка процессора, захват памяти ОЗУ и HDD); заражение вредоносными программами;

4) по положению источника угроз:

а) источник вне контролируемой территории – перехват побочных электромагнитных, акустических излучений устройств и линий связи, наводок на вспомогательные технические средства (телефонные линии, сети питания, отопления и т.п.); перехват передаваемой по линиям связи информации (выяснение протокола, правил схождения в сеть); дистанционная фото- и видео-съемка;

б) источник в пределах контролируемой территории – хищение производственных отходов (распечатки, записки, пароли); отключение или вывод из строя подсистем обеспечения функционирования системы; внедрение подслушивающих устройств;

в) источник имеет доступ к терминалам системы;

г) источник расположен в системе – некорректное использование ресурсов системы; вредоносное ПО;

5) по характеру нанесенного ущерба:

а) материальный;

б) моральный;

6) по степени зависимости от активности объекта (системы):

а) проявляются только в процессе работы системы;

б) проявляются только в процессе бездействия системы – хищение носителей информации;

в) проявляются независимо от активности системы – вскрытие шифров криптозащиты;

7) по характеру воздействия:

а) активные – вредоносное ПО; дезорганизация функционирования системы (помехи, забастовки, саботаж); умышленная модификация информации;

б) пассивные – ничего не меняют в структуре и содержимом системы;

8) по способу доступа к ресурсам системы:

а) использование прямого пути – незаконное получение паролей с последующей маскировкой под пользователя;

б) использование скрытого или нестандартного пути – обход СЗИ; использование недокументированных возможностей;

9) по месту расположения информации:

а) угрозы информации на внешних запоминающих устройствах;

б) угрозы информации в оперативной памяти (чтение остаточной информации, чтение в асинхронном режиме, доступ ПО к областям памяти ОС);

в) угрозы информации, передаваемой по линиям связи (подключение и работа «между строк», подмена пользователя, перехват и анализ информации);

г) угрозы информации, отображаемой на терминале или печатаемой;

10) по отношению к объекту:

а) внутренние;

б) внешние.

Источниками внешних угроз являются:

- недобросовестные конкуренты;
- преступные группировки и формирования;
- отдельные лица и организации административно-управленческого аппарата.

Источниками внутренних угроз могут быть:

- администрация предприятия;
- персонал;

- технические средства обеспечения производственной и трудовой деятельности.

Соотношение внешних и внутренних угроз можно охарактеризовать так:

- 82% угроз совершается собственными сотрудниками фирмы либо при их прямом или опосредованном участии;
- 17% угроз совершается извне (внешние угрозы);
- 1% угроз совершается случайными лицами.

Основные методы реализации угроз:

1) определение типа и параметров носителей информации;

2) получение информации о программно-аппаратной среде, типе, параметрах средств вычислительной техники, типе и версии ОС, составе ПО;

3) получение информации о функциях, выполняемых системой;

4) получение информации о применяемых системах защиты;

5) определение способа представления информации;

6) определение содержания данных на качественном уровне;

7) определение содержания данных на семантическом уровне;

8) использование специальных технических средств (СТС) для перехвата наводок;

9) уничтожение средств вычислительной техники и носителей информации;

10) копирование носителей информации;

11) хищение носителей информации;

12) НСД в обход или путем преодоления СЗИ с использованием спец. средств;

13) НС превышение пользователем своих полномочий;

14) НС копирование ПО;

15) перехват данных, передаваемых по линиям связи;

16) визуальное наблюдение;

17) раскрытие представления информации (дешифрование);

18) внесение НС изменений в программно-аппаратные компоненты системы и обрабатываемые данные;

19) установка и использование нештатного аппаратного и ПО;

20) заражение вредоносными программами;

21) искажение информации;

22) внедрение дезинформации;

23) проявление ошибок проектирования.

Тема 4. *ПАРОЛЬНЫЕ СИСТЕМЫ.*

Идентификатор (*логин*) – некоторая уникальная информация, позволяющая различать пользователей ПС.

Пароль – некоторая секретная информация, известная только пользователю и ПС, которая может быть запомнена пользователем и предъявлена ПС.

Ключ – аналог пароля, однако отличается от него тем, что не может быть легко запомнена пользователем (из-за большого объема или отсутствия смысловой нагрузки) или не может быть введена с клавиатуры (из-за содержащихся в ней служебных символов, которые отсутствуют на клавиатуре).

Учетная запись пользователя – совокупность его идентификатора и пароля.

Идентификация – присвоение пользователям идентификаторов и проверка предъявляемых идентификаторов по списку присвоенных.

Аутентификация – проверка принадлежности пользователю предъявленного им идентификатора.

Способы аутентификации:

1) по хранимой копии пароля;

2) по хранимому хэшу пароля;

3) по проверочному значению;

4) без передачи информации о пароле проверяющей стороне (доказательство с нулевым разглашением);

5) использованием пароля для получения криптоключа.

Угрозы безопасности ПС:

- подбор в интерактивном режиме;

- подсматривание;

- преднамеренная передача другому лицу;

- захват БД ПС;

- перехват переданной по сети информации о пароле (повторное использование информации, восстановление пароля, модификация передаваемой информации с целью ввести в заблуждение ПС, имитация действий ПС для введения в заблуждение пользователя);

- хранение информации о пароле в доступном месте;

- внедрение «закладок»;

- использование ошибок в ПО;

- выведение из строя ПС;

- обход ПС;

- социальная инженерия.

Тема 5. *ДЕЙСТВИЯ, ПРИВОДЯЩИЕ К НЕПРАВОМЕРНОМУ ОВЛАДЕНИЮ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИЕЙ.*

Отношение объекта (фирма, организация) и субъекта (конкурент, злоумышленник) в информационном процессе с противоположными интересами можно рассматривать с позиции активности в действиях, приводящих к овладению конфиденциальными сведениями. В этом случае возможны такие ситуации:

- владелец не принимает никаких мер к сохранению конфиденциальной информации, что позволяет злоумышленнику легко получить интересующие его сведения;
- владелец строго соблюдает меры ИБ, тогда злоумышленнику приходится прилагать значительные усилия к осуществлению доступа к охраняемым сведениям, используя для этого всю совокупность способов несанкционированного проникновения: легальное или нелегальное, заходовое или беззаходовое;

- промежуточная ситуация - это утечка информации по техническим каналам, при которой владелец еще не знает об этом (иначе он принял бы меры защиты), а злоумышленник без особых усилий может использовать это в своих интересах.

В общем, факт получения охраняемых сведений злоумышленниками или конкурентами называют утечкой. Одновременно с этим в значительной части законодательных актов, законов, кодексов, официальных материалов используются и такие понятия, как разглашение сведений и НСД к конфиденциальной информации.

Разглашение - это умышленные или неосторожные действия с конфиденциальными сведениями, приведшие к ознакомлению с ними лиц, не допущенных к ним. Разглашение выражается в сообщении, передаче, предоставлении, пересылке, опубликовании, утере и в других формах обмена и действий с деловой и научной информацией. Реализуется разглашение по формальным и неформальным каналам распространения информации. К формальным коммуникациям относятся деловые встречи, совещания, переговоры и тому подобные формы общения: обмен официальными деловыми и научными документами средствами передачи официальной информации (почта, телефон, телеграф и др.). Неформальные коммуникации включают личное общение (встречи, переписка и др.); выставки, семинары, конференции и другие массовые мероприятия, а также средства массовой информации (печать, газеты, интервью, радио, телевидение и др.). Иногда причиной разглашения конфиденциальной информации является недостаточное знание сотрудниками правил защиты коммерческих секретов и непонимание (или недопонимание) необходимости их тщательного соблюдения. Тут важно отметить, что субъектом в этом процессе выступает владелец охраняемых секретов.

Утечка - это бесконтрольный выход конфиденциальной информации за пределы организации или круга лиц, которым она была доверена. Утечка информации осуществляется по различным техническим каналам. Известно, что

информация вообще переносится или передается либо энергией, либо веществом. Можно утверждать, что по физической природе возможны следующие пути переноса информации: световые лучи, звуковые волны, электромагнитные волны, материалы и вещества. Соответственно этому каналы утечки информации классифицируются на визуально-оптические, акустические, электромагнитные и материально-вещественные. Под *каналом утечки* информации принято понимать физический путь от источника конфиденциальной информации к злоумышленнику, посредством которого последний может получить доступ к охраняемым сведениям. Для образования канала утечки информации необходимы определенные пространственные, энергетические и временные условия, а также наличие на стороне злоумышленника соответствующей аппаратуры приема, обработки и фиксации информации.

НСД - это противоправное преднамеренное овладение конфиденциальной информацией лицом, не имеющим права доступа к охраняемым сведениям. НСД к источникам конфиденциальной информации реализуется различными способами: от инициативного сотрудничества, выражающегося в активном стремлении "продать" секреты, до использования различных средств проникновения к коммерческим секретам. Для реализации этих действий злоумышленнику приходится часто проникать на объект или создавать вблизи него специальные посты контроля и наблюдения - стационарные или в подвижном варианте, оборудованные современными техническими средствами.

Условия, способствующие неправомерному овладению конфиденциальной информацией:

- разглашение (излишняя болтливость сотрудников) - 32%;
- подкуп и склонение к сотрудничеству со стороны конкурентов и преступных группировок - 24%;
- отсутствие на фирме надлежащего контроля и жестких условий обеспечения ИБ - 14%;
- обмен производственным опытом - 12%;

- бесконтрольное использование информационных систем - 10%;
- наличие предпосылок возникновения среди сотрудников конфликтных ситуаций 8%;

а также отсутствие высокой трудовой дисциплины, психологическая несовместимость, случайный подбор кадров, слабая работа кадров по сплочению коллектива.

Тема 6. *РАЗНОВИДНОСТИ АТАК НА ЗАЩИЩАЕМЫЕ РЕСУРСЫ.*

Выделим наиболее часто встречающиеся и поддающиеся классификации атаки на защищаемые ресурсы.

1. *«Отказ от обслуживания» (Denial of Service - DoS)*

Отказ от обслуживания - нарушение корректной работы программного или аппаратного обеспечения, путем создания огромного количества фальшивых запросов на доступ к некоторым ресурсам или путем создания неочевидных препятствий корректной работе. Отказ от обслуживания может быть сетевым и локальным. Сетевая атака осуществляется посылкой большого количества пакетов с фальшивыми обратными адресами.

Разновидностью DoS является DDoS - Distributed DoS (Распространенная атака «Отказ от обслуживания»), когда запросы идут не от одного, а от нескольких компьютеров сети. DDoS-атаки могут быть вызваны действием вирусов или троянских коней, поэтому владельцы атакующих компьютеров не обязательно знают о том, что с их компьютера осуществляется атака. DDoS-атака гораздо эффективнее DoS: из-за большого количества участвующих компьютеров желаемый эффект достигается раньше, администратору атакуемого компьютера труднее отфильтровать адреса атакующих от адресов простых пользователей. Все что может сделать администратор, чтобы предотвратить переполнение дисковой памяти и уберечь информацию сервера от потерь - это отключить компьютер от сети, что будет означать успех атаки.

2. *Срыв стека (Переполнение буфера).*

Используется в эксплоитах (Exploit) и вирусах для выполнения кода (подпрограммы), который не должен выполняться на этом компьютере, для дистанционного запуска программ, для выполнения кода с привилегиями (полномочиями, уровнем доступа) гораздо выше, чем привилегии текущего пользователя. Именно этим способом размножаются IIS, SQL, RPC и LSA интернет-черви (CodeRed, Hellkern, Sasser). Для того, чтобы реализовать срыв стека, нужно знать несколько подробностей об атакуемой системе или программе:

a) версия;
b) наличие определенной ошибки, которая позволит произвести срыв стека;
c) наличие открытого (контролируемого программой) порта;
d) адрес в памяти, по которому необходимо разместить код.

Эта информация может быть получена путем анализа (дизассемблирования) ПО (т.е. атакующий должен иметь доступ к точно такому же ПО, как и установленное на атакуемой системе).

3. *Внедрение на компьютер деструктивных программ.*

Деструктивные программы можно разделить на несколько видов:

a) вирусы - программы, размножающиеся путем создания и распространения своей возможно измененной копии. Они занимают дисковое пространство, оперативную память, могут мешать корректной работе программ и содержать в себе деструктивные компоненты;
b) деструктивные троянцы - программы, созданные для уничтожения или модификации тех или иных данных при запуске или в другой момент времени;
c) троянцы, ворующие информацию (PSW - Password Stealer Ware) - программы, отсылающие злоумышленнику (т.е. их автору или пользователю) конфиденциальную информацию с пораженного компьютера;
d) Backdoor (бакдор, от англ. «back door» - «задняя дверь», «черный ход») - программы, предоставляющие удаленному пользователю возможности по управлению пораженным компьютером (доступ ко всем ресурсам);

е) KeyLogger (кейлоггер, от англ. «key logger» - «сохраняющий клавиши», «клавиатурный шпион») - программы, сохраняющие все нажатые пользователем клавиши в специальный файл, возможно с последующей отправкой злоумышленнику (см. PSW-троянцы). Некоторые кейлоггеры позволяют ограничить окна, нажатия клавиш в которых нужно сохранять. В первую очередь интересны клавиши, нажимаемые в окнах с определенным заголовком и в окнах, где вводимые символы заменяются звездочками.

Для обнаружения деструктивных программ и предотвращения их появления необходимо использовать антивирусы и файерволы. Некоторые деструктивные программы обходят это, закрывая и/или удаляя их.

4. *Перехват передаваемой по сети информации (Sniffing).*

Sniffer (сниффер, от англ. sniff - «нюхать») - программа для перехвата идущей по локальной сети информации. Некоторые снифферы умеют автоматически разбирать формат перехваченных пакетов и извлекать из них пароли, скачиваемые файлы и другую интересную информацию.

Для защиты от снифферов необходимо свести к минимуму количество транзитных узлов, через которые может передаваться важная информация, а еще лучше - полностью контролировать доступ к ним и передающей среде.

5. *Спуфинг (Spoofing).*

Spoofer (спуфер) - программа, позволяющая воровать логины и пароли пользователей, путем имитации приглашения входа в систему или регистрации для работы с программой. Все вводимые пароли сохраняются или отсылаются взломщику, после чего спуфер имитирует ошибку ввода пароля и/или запускает настоящую программу входа в систему (иногда даже автоматически передает ей введенную информацию). Спуфер может быть запущен даже пользователем с минимальными правами в системе. Для защиты от спуферов не стоит доверять приглашениям входа в систему или программу, если они инициализированы не вами - нужно перезагрузить компьютер или самостоятельно запустить программу.

6. *Сканирование портов.*

Сканирование портов - сетевая атака, целью которой является поиск открытых портов работающих в сети компьютеров, определение типа и версии ОС и ПО, контролирующего открытый порт, используемых на этих компьютерах. В зависимости от обнаруженных открытых портов и версий ПО, далее последует попытка подобрать пароль, вызвать отказ от обслуживания или срыв стека.

Часть II. СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

Тема 7. *ПРОГРАММНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ.*

Программные средства защиты информации включают программы для:

- защиты от вредоносных программ (антивирусы);
- идентификации технических средств (терминалов, устройств группового управления вводом-выводом, ЭВМ, носителей информации), задач, пользователей;
- определения прав технических средств (дни и время работы, разрешенные к использованию задачи) и пользователей;
- контроля работы (доступа) технических средств и пользователей;
- регистрации работы технических средств и пользователей при обработке информации ограниченного использования;
- шифрования и сокрытия информации (криптографические и стеганографические);
- удаления остаточной (рабочей) информации типа временных файлов (в том числе – невосстановимого);
- восстановления удаленной информации;
- сигнализации при несанкционированных действиях (например, сетевые экраны для защиты от сетевых атак);
- проставления грифа секретности на выдаваемых документах;
- тестового контроля системы защиты и др.

Преимущества программных средств — универсальность, гибкость, надежность, простота установки, способность к модификации и развитию. Недостатки — ограниченная функциональность, использование части ресурсов компьютера, высокая чувствительность к случайным или преднамеренным изменениям, возможная зависимость от аппаратных средств компьютеров.

Пример программы для идентификации пользователей - Electronic Signature Lock - анализирует манеру пользователя работать на клавиатуре (в том числе – непрерывно).

Тема 8. *ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ.*

1. **Средства защищенного хранения информации** – шифрующиеся записные книжки на смарт-картах и флэш-картах.

2. **Технические средства защиты авторских прав** (ТСЗАП или DRM) - затрудняют создание копий защищаемых произведений (распространяемых в электронной форме) либо позволяют отследить создание таких копий. Хотя ТСЗАП призваны воспрепятствовать лишь *неправомерному* копированию произведений, зачастую они препятствуют *любому* копированию, в том числе, добросовестному (fair use), которое разрешено законодательством. Такое излишнее ограничение возможностей пользователя вызывает критику ТСЗАП со стороны правозащитников. Обычно ТСЗАП сопровождают защищаемые произведения (файлы, диски, программы-оболочки для просмотра), реже — встраиваются в средства воспроизведения (например, mp3-плееры). На нынешнем этапе развития ТСЗАП сами по себе не в состоянии эффективно ограничить неправомерное использование произведений. разрешить воспроизведение (просмотр) и в то же время запретить копирование представляет теоретически неразрешимую задачу (Воспроизведение сводится к операциям чтение + запись на устройство вывода, копирование сводится к операциям чтение + запись на устройство хранения; таким образом, если возможно чтение, то возможно и копирование.) Эффективная техническая защита от копирования при разрешённом воспроизведении может быть достигнута, только когда всё устройство (компьютер, проигрыватель) целиком под контролем правообладателя.

3. **Биометрические системы контроля и управления доступом** (СКУД). Помимо проверки отпечатков пальцев существует возможность проверки формы кисти. Применяются для идентификации пользователей и контроля рабочего

времени. Достоинства биометрических систем заключаются в том, что нельзя передать ключевую информацию другому пользователю.

Недостатки систем:

- нельзя автоматизировать проходные с большим потоком людей;
- не все отпечатки поддаются автоматическому распознаванию (т.н. «плохие отпечатки»).

Алгоритмы работы дактилоскопического ПО:

Разработка комбинированного алгоритма классический/корреляционный. Термин классический означает, что находятся особые точки в строении папиллярного узора. Такие алгоритмы имеют очень высокую скорость сравнения, но не могут работать с нечеткими папиллярными узорами. Корреляционные алгоритмы используют прямое совмещение узоров и поэтому работают даже с нечеткими рисунками, но значительно медленнее. Поскольку 90% пальцев имеют качественные рисунки папиллярного узора, то комбинированный алгоритм должен сочетать в себе все положительные стороны обоих алгоритмов.

Некоторые биометрические системы требуют двоекратного приложения пальца к считывающему полю, для того, чтобы исключить возможность прикладывания скопированного отпечатка пальца (отпечатки должны быть похожими, но не совпадать в точности). Так же как нельзя дважды одинаково расписаться, нельзя дважды прислонить палец идентичным образом (меняется сила нажатия, которая считывается сенсором, площадь соприкосновения, область соприкосновения, угол и т.д.).

4. **Системы аппаратного шифрования передаваемой по сети информации**.

Сетевые адаптеры AncNet для сетей Ethernet/Fast Ethernet производят шифрование информации на аппаратном уровне и обеспечивают совместимость со всеми типами активного сетевого оборудования и сетевыми адаптерами зарубежных производителей.

Сетевые протоколы и требуемые интерфейсы реализованы в виде однокристальных схемотехнических модулей разработки АНКАД. Специально разработаны также драйверы сетевой платы, которые поддерживают работу под управлением ОС Windows и DOS. Наличие на плате аттестованного ФАПСИ датчика случайных чисел и уникального программного драйвера позволяют использовать эти платы при построении криптографических систем защиты информации.

5. Средства криптографической защиты информации

Возможности серии «КРИПТОН»:

- аппаратная реализация алгоритма криптографического преобразования гарантирует целостность алгоритма;

- шифрование производится и ключи шифрования хранятся в самой плате, а не в оперативной памяти компьютера;

- аппаратный датчик случайных чисел создает действительно случайные числа для формирования надежных ключей шифрования и электронной цифровой подписи;

- загрузка ключей шифрования в устройство КРИПТОН со смарт-карт и идентификаторов Touch Memory (i-Button) производится напрямую, минуя ОЗУ и системную шину компьютера, что исключает возможность перехвата ключей;

- на базе устройств КРИПТОН можно создавать системы защиты информации от несанкционированного доступа и разграничения доступа к компьютеру;

- применение специализированного шифрпроцессора для выполнения криптографических преобразований разгружает центральный процессор компьютера; возможна также установка на одном компьютере нескольких устройств КРИПТОН, что еще более повысит скорость шифрования (для устройств с шиной PCI);

- использование парафазных шин в архитектуре шифрпроцессора исключает угрозу снятия ключевой информации по возникающим в ходе криптографических

преобразований колебаниям электромагнитного излучения в цепях "земля - питание" микросхемы.

Программное обеспечение устройств КРИПТОН позволяет:

- шифровать компьютерную информацию (файлы, группы файлов и разделы дисков), обеспечивая их конфиденциальность;

- осуществлять электронную цифровую подпись файлов, проверяя их целостность и авторство;

- создавать прозрачно шифруемые логические диски, максимально облегчая и упрощая работу пользователя с конфиденциальной информацией;

- формировать криптографически защищенные виртуальные сети, шифровать IP-трафик и обеспечивать защищенный доступ к ресурсам сети мобильных и удаленных пользователей;

- создавать системы защиты информации от несанкционированного доступа и разграничения доступа к компьютеру;

- работать на компьютерах под управлением ОС MS DOS, Windows, UNIX.

Защита данных при работе с жестким диском (“Криптон IDE”) реализована на базе платы шифратора жёсткого диска и обеспечивает «прозрачное» шифрование информации, передаваемой между контроллером на системной плате компьютера и жестким магнитным диском. Шифрование реализуется аппаратно. Недостаток – работа только с IDE-устройствами.

Возможности изделия «ШИПКА» (Шифрование, Идентификация, Подпись, Коды Аутентификации) - содержит микропроцессор с встроенным программным обеспечением, аппаратный датчик случайных чисел, подключается через имеющийся интерфейс (USB) и может выполнять операции:

- шифрование по ГОСТ 28147-89;

- хеширование по ГОСТ Р 34.11-94;

- формирование и проверка электронной цифровой подписи по ГОСТ Р 34.10-94;

- выработка и проверка защитных кодов аутентификации.

В последней модификации изделия имеется защищенный электронный диск объемом 16 Мбайт, 32, 64 или 128 Мбайт для записи пользовательской информации.

6. **Виртуальные частные сети.**

Возможности комплекса «Континент»:

- криптографическая защита данных;
- межсетевое экранирование;
- обеспечение удаленного доступа;
- интеграции с системами обнаружения атак;
- простая масштабируемость решений;
- авторизованное обучение работе с комплексом;
- оповещение администратора (в реальном режиме времени) о событиях, требующих оперативного вмешательства;
- абсолютная прозрачность для всех приложений.

7. **Электронные замки**

Возможности электронного замка «Соболь»:

- регистрация пользователей, выдача логинов и паролей;
- идентификация и аутентификация при входе в систему;
- регистрация событий;
- контроль целостности файлов;
- контроль целостности секторов;
- гибкая настройка (число неудачных попыток входа, ограничение времени использования пароля, время для входа в систему);
- защита от несанкционированной загрузки системы с CD, ZIP, Flash, дискет и т.п. (администратор может разрешить это отдельным пользователям), реализуется блокированием доступа к этим устройствам в момент загрузки компьютера;
- использование внешних и внутренних (беспроводных) считывателей;
- создание резервных копий идентификаторов;

- совместная работа с «SecretNet» (для генерации ключей шифрования и электронно-цифровой подписи) и «Континент» (для идентификации и аутентификации администратора криптографического шлюза и генерации ключей шифрования).

Ограничения:

- нельзя шифровать каталог самой программы;
- ограничения на использование boot manager при включении контроля целостности.

Контроль целостности по умолчанию включается:

- для системных файлов из корня диска с ОС;
- секторы MBR, Boot Record, Partition Table;
- sys, drv, vxd из каталога Windows/System.

После установки:

- рекомендуется провести проверку целостности платы (тестирование правильности работы ГСЧ);
- первичная регистрация администратора (прошивка информации в ключ - может уничтожить данные на нем).

Перед загрузкой ОС:

- выдается информация о проверенных на целость объектах;
- администратор имеет возможность просмотра и редактирования списка пользователей, просмотра статистики по пользователям.

В журнале событий различные события выделяются цветом:

- красные – ошибки;
- желтые – события от администратора;
- белые – события от пользователей.

Возможности «Secret Net» 5.0:

- идентификация и аутентификация пользователей;
- защита от загрузки с внешних носителей;
- полномочное управление доступом;

- разграничение доступа к устройствам;

- замкнутая программная среда;

- контроль целостности;

- шифрование файлов;

- гарантированное уничтожение данных;

- контроль аппаратной конфигурации компьютера (что отсутствует в «Соболе», поэтому есть смысл использовать их в связке);

- контроль печати конфиденциальной информации;

- регистрация событий.

Возможности «Спектр 2000»:

- идентификация и аутентификация пользователей в доверенной среде и с применением электронных устройств RuToken;

- проверкой целостности ОС Windows из доверенной среды и последующая ее загрузка под контролем ядра «Спектр 2000»;

- дискреционный и мандатный принцип контроля доступа к устройствам (жестким дискам, дискетам, компакт-дискам), а так же к файлам и папкам;

- управление печатью и блокировка консоли компьютера;

- автоматическая маркировка и учёт отпечатанных материалов;

- защита от загрузки в обход системы;

- прозрачное кодирование диапазонов секторов жестких дисков, дискет и компакт-дисков целиком, виртуальных дисков целиком;

- интерактивная очистка освобождаемых областей дисковой памяти при удалении файлов;

- регистрация событий, связанных с управлением доступом и средствами защиты в системных журналах ОС;

- контроль целостности как системы защиты, так и основных компонент ОС;

- централизованное единообразное управление модулями системы защиты.

Возможности «Фильтра USB-устройств»:

- разделение доступа пользователей к USB-устройствам;

- контроль несанкционированного подключения USB-устройств к компьютеру;

- гибкая настройка списков USB-устройств и прав доступа пользователей к ним.

Программа выпускается в двух вариантах:

1) Фильтр USB-устройств (по серийным номерам устройств). Контроль доступа осуществляется на основе уникальных идентификаторов устройств: для доступа к конкретному устройству необходимо его предварительно зарегистрировать в системе.

2) Фильтр USB устройств (по категориям устройств). Контроль доступа осуществляется на основе категорий устройств: можно предоставить пользователю доступ только к определённым типам устройств, например, к принтерам и сканерам, в то время как другим типам устройств (например, USB-flash) будет запрещён.

8. **Аппаратные антивирусы**

Пример – программно-аппаратный комплекс «Шериф», производства «Диалог Наука».

9. **Аппаратная защита от записи на носитель информации** (например, на IDE). Используется для защиты от изменения обрабатываемой информации, например при производстве компьютерных экспертиз.

Тема 9. *АППАРАТНЫЕ СРЕДСТВА КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ.*

Аппаратные средства криптографической защиты информации (АСКЗИ) отличаются простотой и оперативностью их внедрения. Для этого достаточно у абонентов на передающей и приемной сторонах иметь аппаратуру АСКЗИ и комплект ключевых документов, чтобы гарантировать конфиденциальность циркулирующей в АСУ информации.

Современные АСКЗИ строятся на модульном принципе, что дает возможность комплектовать структуру АСКЗИ по выбору заказчика.

Состоят из:

- входные устройства, предназначенные для ввода информации;

- устройства преобразования информации, предназначенные для передачи информации от входных устройств на устройства вывода в зашифрованном, расшифрованном или открытом виде;

- устройства вывода, предназначенные для вывода информации на соответствующие носители.

Подсистема вывода является оконечным устройством АСКЗИ, то есть находится на высшей ступени иерархии и включает в себя устройства отображения, печати и перфорации. Следовательно, на этом уровне в качестве целевой установки будет выступать быстрота обработки входящих криптограмм. Тогда в качестве обобщенного критерия целесообразно выбрать время обработки потока криптограмм за один цикл функционирования современных АСКЗИ, не превышающего заданного интервала времени и обусловленного необходимостью принятия управленческих решений.

Подсистема обработки информации находится на втором уровне иерархии и включает в себя тракты печати и перфорации, шифратор и систему управления и распределения потоком информации.

Основные направления работ по рассматриваемому аспекту защиты можно сформулировать таким образом:

- выбор рациональных систем шифрования для надежного закрытия информации;

- обоснование путей реализации систем шифрования в автоматизированных системах;

- разработка правил использования криптографических методов защиты в процессе функционирования автоматизированных систем;

- оценка эффективности криптографической защиты.

К шифрам, предназначенным для закрытия информации в ЭВМ и автоматизированных системах, предъявляется ряд требований, в том числе:

- достаточная стойкость (надежность закрытия);
- простота шифрования и расшифрования;
- нечувствительность к небольшим ошибкам шифрования;
- возможность внутримашинной обработки зашифрованной информации;
- незначительная избыточность информации за счет шифрования.

КОНТРОЛЬНЫЕ ВОПРОСЫ
К КУРСУ «ТЕОРЕТИЧЕСКИЕ И ПРАКТИЧЕСКИЕ ОСНОВЫ ЗАЩИТЫ ИНФОРМАЦИИ»

1. Каковы общие требования к защите информации?
2. Из каких компонент состоит модель информационной безопасности?
3. Каковы способы классификации угроз информации?
4. Каковы основные методы реализации угроз информации?
5. Каковые основные угрозы парольным системам?
6. В чем различие между разглашением, утечкой, и несанкционированным доступом к информации?
7. Каковы основные виды атак на защищаемые ресурсы?
8. Какие виды вредоносных программ используются для воздействия на защищаемую информацию?
9. Какие виды программых средств используются для защиты информации?
10. Какие виды программно-аппаратных средств используются для защиты информации?
11. Каковы возможности электронных замков?
12. Каковы возможности средств криптографической защиты информации?