ОГЛАВЛЕНИЕ

ВСТУПЛЕНИЕ

На сегодняшний день написано уже множество книг и статей, посвященных этичному хакингу и тестированию на проникновение. В сети Интернет найдутся тысячи видеороликов, в которых демонстрируются обход различных защит. Существует даже курс обучения этичному хакингу (Certified Ethical Hacker, CEH). Но при этом в абсолютном большинстве случаев в качестве используемых инструментов для реализации атак выступают различные программные средства. Возьмем, к примеру, тот же курс CEH: в нем для демонстрации большинства атак используются приложения, входящие в состав загружаемого дистрибутива Kali Linux. А для реализации оставшихся используется хакерский софт для Windows. Таким образом, большинство специалистов по Информационной безопасности (пентестеров, аудиторов, этичных хакеров), даже пройдя специальное обучение и являясь, по сути, квалифицированными профессионалами, может не знать о том, что угрозу могут представлять не только различные хакерские утилиты, но и специальные устройства, собрать которые не слишком сложно. По сути, не зная о существовании таких угроз, мы не можем от них защититься.

Обычно под шпионскими устройствами понимают разнообразное оборудование, предназначенное для подслушивания и подсматривания: закладки-жучки, скрытые камеры, направленные микрофоны и т. д.

Кроме того, в состав шпионского оборудования также входят средства обнаружения побочных электромагнитных излучений и наводок (ПЭМИН), также позволяющие перехватывать конфиденциальную информацию.

Однако существует также класс устройств, предназначенных для осуществления несанкционированного проникновения и копирования информации непосредственно из компьютеров и каналов связи, с использованием лишь штатного функционала данных систем. В чем отличие данных устройств от закладок и средств перехвата ПЭМИН? Закладки размещаются вне атакуемого узла и не используют его функционала. Так, жучок-закладка просто подслушивает разговоры. Скрытая камера может быть использована для хищения паролей и съема информации с экрана, однако в общем случае она не взаимодействует с компьютером. Аппаратный клавиатурный шпион (кейлоггер) – устройство, подключающееся между клавиатурой и системным блоком компьютера и записывающее все нажатые клавиши, тоже не использует функционал компьютера. Оно лишь выступает «посредником» при подключении периферийного устройства к компьютеру. Соответственно, для обнаружения и противодействия таким шпионским устройствам есть специальные средства: детекторы жучков, подавители микрофонов, глушилки телефонов, элементы пассивной защиты и многое другое.

Однако для борьбы с устройствами, представленными в данной книге, эти средства будут малоэффективны. Причина проста: жучки и средства ПЭМИН используют особенности физической среды для перехвата информации, в то

время как устройства (будем называть их специальными), о которых речь пойдет далее в своей работе используют штатные функции компьютеров и средств передачи данных, такие как взаимодействие с компьютером по USB-порту или подключение по беспроводной сети Wi-Fi. Для средств обнаружения и предотвращения утечек по видовым и речевым каналам (так по-научному называются жучки и скрытые камеры), а также утечек ПЭМИН эти специальные устройства будут вполне легитимными клиентами сети и периферийными устройствами, как, к примеру, мобильный телефон или USB-модем.

Поэтому устройства, описываемые в этой книге, я предлагаю рассматривать, как новый вектор атак, назовем его Hardware Hacking.

Возможно некоторые читатели возразят, что здесь нет ничего нового, некоторые виды устройств существуют уже много лет. Например, в Интернете существует множество схем для сборки различных USB-ключей, предназначенных для обхода ограничений лицензий в различных дорогостоящих системах, типа 1С, CAD и других. Да, это все верно, однако для сборки этих устройств в прежние времена требовались достаточно глубокие знания как в области схемотехники, так и программирования. К примеру, для многих микроконтроллеров прошивку можно было написать только на ассемблере. Ну а кроме того, для работы с микроконтроллерами нужны аппаратные программаторы профессионального уровня, которые стоят немалых денег (до нескольких тысяч долларов). Таким образом, лет десять назад разработка устройств была уделом небольшой группы специалистов, обладающих необходимыми знаниями и оборудованием.

Но жизнь не стоит на месте, и в последние годы широкое распространение получили макетные платы и микрокомпьютеры, построенные на дешевых микроконтроллерах и процессорах, имеющие размер не более кредитной карты и обладающие при этом весьма обширным функционалом. Для работы с такими макетными платами не нужны дорогостоящие программаторы и низкоуровневые языки программирования. Для написания программы для микроконтроллера используются языки высокого уровня, а запись прошивки производится без помощи программатора, посредством USB-порта и программного программатора. А кроме того, все это программное обеспечение является свободно распространяемым.

Таким образом, современный Hardware Hacking стал более доступным как для специалистов по ИБ, так и для злоумышленников. В сети Интернет есть множество руководств по сборке различных околохакерских устройств, что позволяет злоумышленнику, обладающему минимальными знаниями в области программирования и суммой в пределах $100, собрать реально работающее устройство, позволяющее при правильном применении получить доступ к конфиденциальной информации.

Данная книга является логическим продолжением моей предыдущей книги «Информационная безопасность: защита и нападение», в которой рассматривались программные средства для реализации атак. Здесь же мы будем говорить об аппаратных средствах.

Думаю, что мне удалось заинтересовать читателя, и теперь я предлагаю приступить к рассмотрению основной темы книги, а именно разработке боевых устройств для проведения тестов на проникновение. В этой главе я расскажу о том, для кого эта книга, поясню структуру, по которой она построена, опишу, что нам потребуется для работы. Также я расскажу, чего не будет в этой книге, очертив таким образом границы обсуждаемых вопросов. Надеюсь, будет интересно. Приступим.

Приступая к работе

Поговорим о том, что нам потребуется знать и уметь и какие основные технические средства потребуются для того, чтобы приступить к сборке описываемых в книге устройств.

Для кого эта книга

Планируя структуру будущей книги, авторам неизбежно приходится отвечать на вопрос, для кого она предназначена. Так как в моей книге рассматривается стык нескольких направлений: микроэлектроники, программирования и информационной безопасности, то мне необходимо было четко понимать, какие требования предъявлять к будущему читателю. То есть для кого эта книга будет наиболее интересна.

В результате я пришел к выводу, что за основу необходимо брать требования информационной безопасности, так как описываемые устройства будут применяться для проведения тестов на проникновение. Таким образом, читателю желательно знать основы информационной безопасности, в частности что из себя представляет тест на проникновение, какие угрозы и нарушители бывают и как с этим бороться.

Что касается познаний в микроэлектронике, то они также желательны, однако, к примеру, умение паять нам почти не потребуется, так как все представленные устройства (по крайней мере, в виде опытных образцов) можно собрать без пайки.

Пожалуй, обязательным требованием я бы сделал навыки программирования на языках высокого уровня. В книге будут использоваться язык Arduino, C, Python, скрипты Bash. Я, конечно, постарался максимально подробно комментировать приведенные исходные коды. Однако для полного понимания и разработки собственных устройств читателю необходимо уметь строить алгоритмы. В рамки книги не входит обучение основам программирования.

Надеюсь, я не сильно напугал такими «запросами»? На самом деле все не так страшно. Для тех, кто не очень хорошо знаком с основами информационной безопасности, я подготовил главу, где описал, что такое тест на проникновение, модель нарушителя и угроз и что из себя представляют средства защиты.

Для тех, кто плохо знаком с микроэлектроникой, я подготовил главу и приложение, где описывается не только базовая настройка тех макетных плат и

микрокомпьютеров, которые нам потребуются, но и приводятся ссылки на те ресурсы, где можно скачать документацию и примеры работы, а также приобрести необходимые детали.

Что касается программирования, то если вы знаете C или Python, то освоение языка Arduino у вас не вызовет больших проблем. В книге приведены ссылки на учебные материалы по программированию Arduino.

Резюмируя вышеизложенное, отвечу на вопрос: «Для кого эта книга?» Книга будет полезна пентестерам, специалистам по информационной безопасности (особенно работающим непосредственно у заказчика), а также всем, кто интересуется микроэлектроникой и разработкой различных устройств.

Структура книги

Как уже было сказано в предыдущем разделе, за основу книги была взята информационная безопасность, в частности проведение теста на проникновение (пентеста). В соответствии с этим книга поделена на главы следующим образом: сначала мы рассматриваем основные аспекты информационной безопасности. Данная глава хотя и предназначена прежде всего для новичков, но тем, кто хорошо знаком с темой, я бы рекомендовал все-таки по ней пробежаться, так как там будут определены, ряд понятий, в дальнейшем используемых в книге.

В следующей главе мы подготовим макетные платы и микрокомпьютеры к разработке устройств. Здесь будут рассмотрены установка и настройка необходимого программного обеспечения (ПО), а также подготовительные действия на самих устройствах. В результате у нас будет готовая связка ПО плюс исходное целевое устройство.

Далее пойдет описание самих устройств. Сначала мы рассмотрим устройства, которые могут использоваться для реализации внешних угроз, затем внутренних. Новичкам в информационной безопасности (ИБ) такое структурирование может показаться странным, однако на самом деле оно логично вытекает из этапов проведения тестов на проникновение и позволит пентестеру правильно определить уязвимые места.

Ну и в завершение мы поговорим о том, как можно защититься от описанных устройств. Здесь мы также поговорим отдельно о внешних и отдельно о внутренних угрозах.

В приложениях я приведу полезную справочную информацию. В частности, будут приведены все модели используемых макетных плат (на момент написания книги), приведены ссылки на исходный код и дополнительную информация.

Какие детали нам потребуются

Нашим основным инструментом, который потребуется при изготовлении большинства устройств, является беспаечная монтажная плата. Применение

такой платы позволяет проверить, наладить и протестировать схему ещё до того, как устройство будет собрано на готовой печатной плате. Это позволяет избежать ошибок при конструировании, а также быстро внести изменения в разрабатываемую схему и тут же проверить результат. Самый важный плюс беспаечной монтажной платы – это отсутствие процесса пайки при макетировании схемы. Это обстоятельство значительно сокращает процесс макетирования и отладки устройств.

Ввиду того, что наши устройства могут содержать несколько деталей, я рекомендую плату, имеющую не менее 30 рядов отдельных контактов по вертикали (рис 1.1).

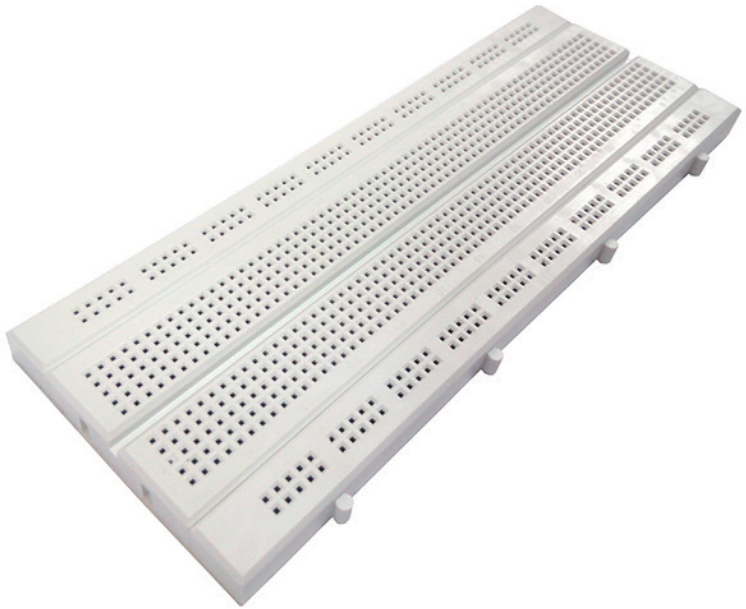

Рис. 1.1. Беспаечная макетная плата

Представленная на рисунке плата имеет горизонтальные ряды контактов, подключенных к общему проводнику. А вот по вертикали эти ряды контактов изолированы друг от друга. Таким образом, при сборке устройства мы размещаем детали, подключая их в разные ряды контактов. При этом левый и правый ряды ножек изолированы друг от друга.

Еще одним полезным средством является набор монтажных перемычек, предназначенных для соединения удаленных друг от друга контактов. Конечно, можно использовать обычные провода, например можно «разобрать» кусок сетевого кабеля с витой парой. Однако такие проводки могут плохо держаться в макетной плате, в результате чего может возникать «дребезг контактов». Поэтому я бы рекомендовал использовать наборы готовых перемычек (рис. 1.2).

Рис. 1.2. Набор перемычек

Большинство наших устройств будет мобильными, следовательно, им потребуется автономный источник питания. Хотя некоторые из устройств используют напряжение, отличное от 5 В, я предлагаю использовать Powerbank с USB-портом, с выходным напряжением 5 В. О том, как обеспечить другой уровень выходного напряжения, будет написано отдельно. Для устройств на базе Arduino вполне подойдет Powerbank, как на рис. 1.3.

Рис. 1.3. Маленький Powerbank

Его характеристики: выходное напряжение 5 В, выходная сила тока 0,7 А, емкость 2600 мА·ч.

Для микрокомпьютеров и в особенности для планшета такой силы тока не хватит, поэтому здесь можно воспользоваться либо аналогичным банком, с выходной силой тока более 1 А, либо приобрести аккумулятор, аналогичный вот такому Powerbank (Li-Ion, 3800 мА·ч) для Raspberry Pi. Здесь выходное напряжение 5 В, выходная сила тока 1,8 А, емкость 3800 мА·ч (рис. 1.4).

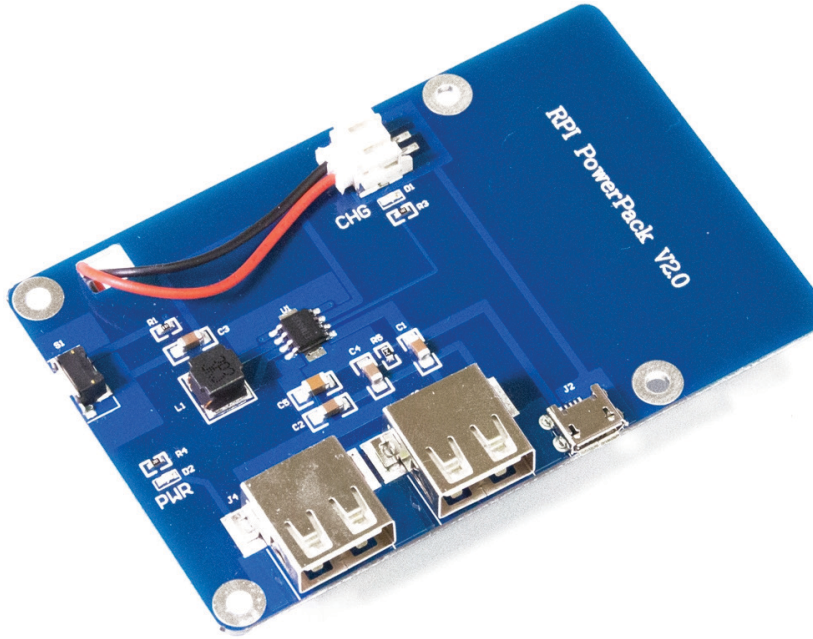

Рис. 1.4. Специальный Powerbank

Это основные наши инструменты. При сборке определенных устройств нам могут потребоваться также другие детали, однако о них будет сказано в описании соответствующего устройства.

Немного о программном обеспечении

При работе с макетными платами Arduino, Teensy, ESP нашим основным программным средством будет среда Arduino IDE, содержащая в себе как интерфейс для написания кода, средства сборки прошивки и ее записи на макетную плату. Имеются сборки Arduino IDE как под Windows, так и под Linux и Mac. Последнюю версию данной среды можно скачать по адресу: https://www.arduino.cc/en/Main/Software.

С микрокомпьютерами также все достаточно просто. В качестве жесткого диска в них используется micro SD-карта и установка операционной системы сводится к записи ISO-образа на карту. Для записи ISO пользователи Windows могут использовать бесплатную утилиту Win32 Image Writer, которую можно скачать по адресу: https://launchpad.net/win32-image-writer.

Также для Windows, Linux и Mac можно использовать утилиту Etcher с сайта https://etcher.io/.

Вот основные программные инструменты, которые нам потребуются. Для некоторых устройств нам может потребоваться дополнительное ПО, которое будет рассмотрено отдельно.

Заключение

Мы определились с тем, какие знания нам потребуются, а также подготовили необходимые средства для начала работы. Теперь определимся с границами того, что мы собираемся делать.

Чего в книге не будет

В мире информационной безопасности многие средства могут использоваться как во благо, так и во вред. Договоримся о некоторых ограничениях.

Кодекс надо чтить

Прежде всего хотелось бы напомнить, что вся информация, приведенная в книге, носит исключительно ознакомительный характер. Автор не несет ответственности за результаты использования приведенных в книге сведений. Напомню, что основным предназначением приведенных устройств является использование их при проведении тестирования на проникновение.

Для лучшего понимания всей серьезности последствий бездумного использования «хакерских игрушек» я процитирую фрагменты некоторых статей Уголовного кодекса.

Статья 138. Незаконный оборот специальных технических средств, предназначенных для негласного получения информации

1. Незаконные производство, приобретение и (или) сбыт специальных технических средств, предназначенных для негласного получения информации, –

   наказываются штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо ограничением свободы на срок до четырех лет, либо принудительными работами на срок до четырех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового, либо лишением свободы на срок до четырех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.

   ...

3. Под специальными техническими средствами, предназначенными для негласного получения информации, понимаются аппаратура, техническое оборудование и (или) инструменты, разработанные, приспособленные или запрограммированные для негласного получения и регистрации акустической информации; прослушивания телефонных переговоров; перехвата и регистрации информации с технических каналов связи; контроля почтовых сообщений и отправлений; исследования предметов и документов; получения (изменения, уничтожения) информации с технических средств ее хранения, обработки и передачи.

Эта статья определяет все, что связано с жучками и иными средствами негласного сбора информации. Замечу, что пентест (аудит ИБ), при грамотном юридическом оформлении тест на проникновение не является негласным

сбором информации, так как перед его проведением заказчик теста уведомляется (и уведомляет ответственных сотрудников) о проведении пентеста.

Основными «клиентами» этой статьи являются незадачливые граждане, приобретающие в зарубежных интернет-магазинах средства негласного сбора информации. При получении таких заказов в отделениях почтовой связи их может ожидать неприятный сюрприз в виде общения с сотрудниками правоохранительных органов. Несмотря на то что во многих странах разрешена свободная продажа таких средств, в России все это требует дополнительных разрешений и лицензий как для тех, кто продает, так и для тех, кто покупает. Заказывая приобретение подобных средств через Интернет, вы рискуете попасть в поле зрения правоохранительных органов и получить очень серьезные проблемы.

Статья 272. Неправомерный доступ к компьютерной информации[1]

1. Неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации, –

   наказывается штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо исправительными работами на срок до одного года, либо ограничением свободы на срок до двух лет, либо принудительными работами на срок до двух лет, либо лишением свободы на тот же срок.

2. То же деяние, причинившее крупный ущерб или совершенное из корыстной заинтересованности, –

   наказывается штрафом в размере от ста тысяч до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до двух лет, либо исправительными работами на срок от одного года до двух лет, либо ограничением свободы на срок до четырех лет, либо принудительными работами на срок до четырех лет, либо лишением свободы на тот же срок.

3. Деяния, предусмотренные частями первой или второй настоящей статьи, совершенные группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, –

   наказываются штрафом в размере до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до трех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет, либо ограничением свободы на срок до четырех лет, либо принудительными работами на срок до пяти лет, либо лишением свободы на тот же срок.

4. Деяния, предусмотренные частями первой, второй или третьей настоящей статьи, если они повлекли тяжкие последствия или создали угрозу их наступления, –

   наказываются лишением свободы на срок до семи лет.

Как видно, здесь тяжесть наказания усиливается, если в действиях обвиняемого был умысел, если была группа лиц и ущерб был особо тяжким. Хотя

[1] Под компьютерной информацией понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи.

даже простое копирование конфиденциальной информации может повлечь за собой неприятные последствия.

Перед проведением теста на проникновение преследуемые цели должны быть зафиксированы в договоре между заказчиком и исполнителем. Например, целью может являться получение доступа к важным ресурсам сети (таким как домен Active Directory, бизнес-системы, СУБД). Более подробно о том, как грамотно составлять требования к тестированию на проникновение, мы поговорим в последующих главах. А сейчас нам важно понимать, что перед пентестом все его цели должны быть зафиксированы. В случае если никаких юридических договоренностей нет, попытка проникновения превращается в банальный взлом, подпадающий под действие этой статьи.

Статья 273. Создание, использование и распространение вредоносных компьютерных программ

1. Создание, распространение или использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации, –

   наказываются ограничением свободы на срок до четырех лет, либо принудительными работами на срок до четырех лет, либо лишением свободы на тот же срок со штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев.

2. Деяния, предусмотренные частью первой настоящей статьи, совершенные группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, а равно причинившие крупный ущерб или совершенные из корыстной заинтересованности, –

   наказываются ограничением свободы на срок до четырех лет, либо принудительными работами на срок до пяти лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового, либо лишением свободы на срок до пяти лет со штрафом в размере от ста тысяч до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от двух до трех лет или без такового и с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.

3. Деяния, предусмотренные частями первой или второй настоящей статьи, если они повлекли тяжкие последствия или создали угрозу их наступления, –

   наказываются лишением свободы на срок до семи лет.

Эта статья в меньшей степени относится к предмету данной книги, так как мы собираем устройства, а не разрабатываем программное обеспечение для компьютера. Однако некоторые из описываемых устройств вполне могут использоваться для распространения вредоносного кода, поэтому следует помнить о существовании данной статьи.

Статья 274. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей

1. Нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, а также правил доступа к информационно-телекоммуникационным сетям, повлекшее уничтожение, блокирование, модификацию либо копирование компьютерной информации, причинившее крупный ущерб, –

   наказывается штрафом в размере до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо исправительными работами на срок от шести месяцев до одного года, либо ограничением свободы на срок до двух лет, либо принудительными работами на срок до двух лет либо лишением свободы на тот же срок.

2. Деяние, предусмотренное частью первой настоящей статьи, если оно повлекло тяжкие последствия или создало угрозу их наступления, –

   наказывается принудительными работами на срок до пяти лет, либо лишением свободы на тот же срок.

Эта статья в нашем случае может определять ответственность за нарушение правил эксплуатации различных технических средств. Нарушения могут возникнуть в том числе вследствие некорректного использования хакерских инструментов при проведении теста на проникновение. Поэтому для пентестера необходимо четко понимать последствия всех его действий и не использовать инструменты, в результате работы которых могут возникнуть критичные сбои в работе целевых систем. По этой причине я в своей книге сознательно не привел некоторые схемы и исходные коды к устройствам, которые могут нанести вред обследуемым системам. Например, заглушить сигнал Wi-Fi.

Ничего не прячем

Здесь я бы хотел обратить внимание читателя на такой немаловажный момент, как маскировку хакерских устройств. Помните, в предыдущем разделе, в статье 138.1, речь шла о скрытом получении информации. Одним из способов скрытого получения данных является маскировка одной вещи под другую. Например, скрытую камеру можно замаскировать под авторучку или брелок, жучок под пуговицу и так далее. Так вот, в контексте своей книги я не буду рассказывать о том, как лучше замаскировать или спрятать устройство в чем-то другом.

В книге будет приведено несколько фотографий готовых хакерских устройств, замаскированных под блоки питания, USB-концентраторы и флешки. Это сделано прежде всего для того, чтобы специалисты по информационной безопасности имели представление о том, как описываемые хакерские

устройства могут выглядеть в боевых условиях. Но рассказывать, как лучше скомпоновать детали и в каком легальном устройстве лучше прятаться, – эта информация останется за рамками данной книги.

Как я уже упомянул выше, нам не потребуется что-либо паять. Все устройства можно смонтировать на беспаечной плате. Для задач тестирования защищенности сети этого вполне достаточно.

Никакой «физики»

Физическая безопасность – это отдельная, большая и довольно интересная с точки зрения безопасности тема. По сравнению с миром информационной безопасности, здесь все не слишком хорошо. Можно собрать множество различных устройств для обхода тех средств защиты, которыми все мы пользуемся каждый день. Однако, учитывая то обстоятельство, что этими устройствами могут воспользоваться не только пентестеры, но и настоящие преступники, мы не будем касаться данной темы в этой книге.

Простота – залог успеха

Хватит околоуголовной тематики. Теперь о хорошем для многих читателей. Я постарался сделать материал, изложенный в книге, максимально простым, для того чтобы он был понятен для начинающих. Поэтому здесь не будет сложных устройств, состоящих из десятков деталей, хитро подключенных между собой.

Кроме того, я использовал только высокоуровневые языки программирования, сознательно отказавшись от ассемблера. Дело в том, что использование низкоуровневого языка в контексте описываемых хакерских устройств не дало бы нам особых преимуществ, зато существенно усложнило бы разработку прошивок.

Ассемблер нужен там, где требуются скорость и небольшой размер кода. Описываемые в книге микроконтроллеры имеют достаточно большой объем памяти, чтобы удовлетворять предъявляемым к устройствам требованиям. Что касается производительности, то для большинства устройств высокая скорость работы микроконтроллера нам не требуется.

Однако в случае, если читатель захочет модифицировать предлагаемые устройства самостоятельно и столкнется с нехваткой ресурсов, он всегда может выбрать более мощную модель макетной платы. В приложениях я привел все линейки моделей описываемых в книге макетных плат и микрокомпьютеров, продаваемые на момент издания книги.

Заключение

Целью этого раздела было определить некоторые ограничения для излагаемого в книге материала. Возможно, кого-то цитаты из Уголовного кодекса могут немного напугать, однако основной целью этих цитат было предостеречь читателя от разного рода необдуманных действий, способных привести

к весьма неприятным последствиям. Ведь банальный «хакинг из любопытства» при неудачном стечении обстоятельств может привести к нарушению приведенных статей и уголовному преследованию.

Напомню, что весь материал, приведенный в книге, носит чисто ознакомительный характер, и автор не несет ответственности за последствия применения приведенных в книге устройств. Так что продумывайте то, к каким последствиям может привести использование данных устройств, и соблюдайте закон.

Итоги главы

Итак, в этой вводной главе я постарался описать, для кого эта книга, какие знания и навыки необходимы читателю для лучшего понимания материала. Замечу, что в книге не приводится никакой особо сложной информации, требующей от читателя глубоких знаний в смежных областях. Конечно, те, кто хорошо разбирается в микроэлектронике, могут самостоятельно усовершенствовать некоторые из приведенных в книге устройств, например с целью автоматизации их работы. Серьезные эксперты в области тестирования на проникновение могут найти для описываемых устройств другие сценарии применения, возможно, более интересные, чем те, которые я привел в книге.

Требования к оборудованию и материалам не являются какими-то заоблачными с точки зрения расходов. Беспаечная монтажная плата и набор проводов в радиомагазине обойдутся максимум в одну тысячу рублей. Powerbank может обойтись несколько дороже, однако это уже зависит от характеристик аккумуляторов. Описанный мной Powerbank для Raspberry обошелся мне в московском интернет-магазине не многим более тысячи рублей. Забегая вперед, скажу, что, кроме микрокомпьютеров, все прочие макетные платы стоят в пределах $10. Лишь микрокомпьютер Raspberry Pi3 и Touchscreen к нему обойдутся существенно дороже.

С программным обеспечением все еще проще, так как все программные инструменты являются бесплатными и свободно распространяемыми.

Упоминание того, чего не будет в книге, позволяет скорректировать ожидания читателей от книги. Далее мы поговорим об основах информационной безопасности: о том, какие угрозы и нарушители бывают, и о том, как с ними бороться.

Глава 1.

ТЕОРИЯ И ПРАКТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Устройства, которые мы будем собирать в последующих главах, не являются самоцелью, в контексте моей книги это средства для проведения тестирования на проникновение. Поэтому, прежде чем приступить к их описанию, я хочу подробно рассмотреть, что из себя представляет информационная безопасность как в части нормативно-теоретической, так и в части практической.

1.1. Кратко о теории информационной безопасности (ИБ)

При построении системы информационной безопасности (СИБ) нам необходимо понимать, какие угрозы для нас наиболее опасны и какие нарушители могут их реализовать. Для этого строятся модель нарушителя и модель угроз – документы, по сути отражающие требования к создаваемой системе ИБ. На основании этих моделей затем составляется техническое задание (ТЗ) на систему ИБ. Далее по требованиям ТЗ система ИБ внедряется.

После ввода СИБ в промышленную эксплуатацию необходимо проверить, насколько правильно мы построили нашу систему ИБ, насколько корректно настроено наше оборудование, правильно составлены политики ИБ и насколько пользователи их соблюдают. Для этого периодически необходимо проводить тестирование на проникновение.

Что из себя представляет тест на проникновение, для которого мы будем собирать наши устройства? По сути, это согласованная с заказчиком попытка несанкционированного проникновения (взлома) его сети. По результатам этого теста составляется отчет, из которого мы понимаем, каких средств защиты нам не хватает, что настроено некорректно и чему необходимо обучить пользователей в плане ИБ.

Далее мы корректируем модели угроз и нарушителя и предпринимаем необходимые действия по модернизации СИБ. Через какое-то время (как правило, год) процесс повторяется. Снова пентест и корректировка по его результатам.

Таким образом, стоит запомнить, что обеспечение информационной безопасности – это непрерывный процесс. Нельзя один раз внедрить СИБ и забыть про нее. Технический прогресс не стоит на месте, постоянно появляются новые угрозы (в том числе и описываемые в книге устройства), поэтому система защиты должна быть постоянно в актуальном состоянии.

Для начала поговорим о том, какие угрозы вообще бывают.

1.1.1. Угрозы

Угрозы информационной безопасности достаточно разнообразны. На сайте bdu.fstec.ru на момент написания этих строк насчитывалось 207 различных угроз. Это и угрозы утечки пользовательских данных, и угрозы несанкционированной установки приложений на мобильные устройства, и угроза программного сброса пароля BIOS, и многие другие. Конечно, не все угрозы могут быть применимы к конкретной инфраструктуре, как по причинам технической реализуемости, так и из-за наличия средств защиты. Например, угрозы, связанные с мобильными устройствами, будут неактуальны, если на территории организации запрещено находиться с такими устройствами. А сетевые угрозы будут неактуальны для компьютеров, не подключенных к сети.

Таким образом, модель угроз содержит в себе описание возможных угроз для данной отрасли, в которой напротив каждой угрозы указывается, актуальна она или нет.

Как мы уже договорились в предыдущей главе, мы не рассматриваем угрозы, связанные с доступом к защищаемой информации при помощи побочных электромагнитных излучений и наводок (ПЭМИН). Однако стоит отметить, что обычно данные угрозы признаются неактуальными в связи с высокой трудоемкостью и экономической нецелесообразностью их реализации предполагаемыми типами нарушителей.

По этим же причинам обычно признают неактуальными следующие угрозы:

- угрозы утечки информации по техническим каналам;
- угрозы утечки акустической (речевой) информации;
- угрозы утечки видовой информации.

Это и есть те самые жучки, которые мы договорились не рассматривать, а также всевозможные формы подслушивания и подсматривания.

Далее поговорим о типах угроз, которые могут быть актуальны для большинства организаций.

Начнем с угроз наличия недекларированных возможностей в системном и прикладном программном обеспечении, используемом в корпоративной инфраструктуре. По сути, это ошибки в коде, допущенные при разработке ПО.

Далее идет целая серия угроз, связанных с непосредственным доступом:

- угрозы, реализуемые в ходе загрузки операционной системы и направленные на перехват паролей или идентификаторов, модификацию базовой системы ввода/вывода (BIOS), перехват управления загрузкой;
- угрозы, реализуемые после загрузки операционной системы и направленные на выполнение несанкционированного доступа с применением стандартных функций (уничтожение, копирование, перемещение, форматирование носителей информации и т. п.) операционной системы или какой-либо прикладной программы (например, системы управле-

ния базами данных), с применением специально созданных для выполнения НСД программ (программ просмотра и модификации реестра, поиска текстов в текстовых файлах и т. п.);

- угрозы, связанные с физическим доступом к основным техническим средствам и системам (ОТСС) информационных систем. Если по-простому, то это угрозы, связанные как с хищением, так и с несанкционированным копированием, изменением или удалением информации. Например, если в серверную имеют доступ посторонние, то кто угодно может забрать диск из сервера или выдернуть питание из сервера. Если по каким-либо причинам консоль на сервере не заблокирована, то он вполне может получить доступ к данным;
- угрозы внедрения вредоносных программ. Это всевозможные вирусы, черви, трояны. Наверное, это наиболее известная угроза.

На этом с локальными угрозами мы закончим и перейдем к рассмотрению угрозы удаленного доступа. Угрозы удаленного доступа бывают локальные, то есть реализуемые по локальной сети, и реализуемые из сетей общего доступа. Начнем с угроз из локальной сети.

- Угрозы анализа сетевого трафика с перехватом информации, передаваемой по сети. Это прослушивание трафика с помощью специализированных средств – снифферов.
- Угрозы сканирования, направленные на выявление сетевых адресов, типа операционных систем, открытых портов и служб, открытых соединений и другие.
- Угрозы навязывания ложного маршрута путем несанкционированного изменения маршрутно-адресных данных. Про эти угрозы иногда забывают, считая их неактуальными, однако такое мнение в корне ошибочно. Навязывание ложного маршрута можно осуществить различными способами: как посредством изменения сетевых настроек на отдельном узле, так и посредством модификации настроек сетевого оборудования. Первый вариант можно реализовать довольно легко, и далее в книге мы соберем несколько устройств, реализующих данные атаки. Второй вариант достаточно подробно рассматривался в моей книге «Информационная безопасность: защита и нападение».

Есть также еще и третий вариант навязывания ложного маршрута – это перенаправление трафика через устройство, полностью контролируемое нарушителем. Это может быть как поддельная точка доступа к беспроводной сети, к которой будут подключаться пользователи, так и скомпрометированное устройство сети, на которое злоумышленник настроил функционал по перехвату трафика. Под «полным контролем» имелось в виду наличие административных прав или иных прав, достаточных для включения смешанного режима на сетевой карте и установки необходимого ПО.

Угрозы типа «отказ в обслуживании», известные также как DoS (Denial of Service). Это вывод из строя узлов сети посредством передачи большого объема тра-

фика, превышающих допустимый объем для данного оборудования. Существуют также DoS-атаки, для реализации которых не нужно большого объема трафика. Вместо этого уязвимому узлу передаются специально подготовленные пакеты, обработка которых приводит к сбоям в работе узла. Как правило, DoS-атаки не приводят к выходу из строя аппаратной части. Последствия DoS второго вида обычно лечатся перезагрузкой зависшего сервиса или всей машины.

Угрозы удаленного запуска приложений – это когда злоумышленник может запустить то или иное приложение на удаленной машине. Например, запустить сервер Telnet для последующего подключения.

Угрозы внедрения по сети вредоносных программ аналогичны описанной ранее локальной угрозе. Однако здесь имеются в виду прежде всего черви, так как именно они самостоятельно распространяются по сети.

Теперь рассмотрим угрозы удаленного доступа, реализуемые из Интернета. Здесь также будут актуальны угрозы для локальной сети, с некоторыми дополнениями. Так, угрозы типа «отказ в обслуживании» могут быть дополнены DDoS (Dynamic DoS), это атаки, в которых участвует большое количество узлов, контролируемых злоумышленником.

Кроме приведенных выше технических угроз, существуют также угрозы, реализуемые при обслуживании технических и программных средств ИС и средств защиты, угрозы природного характера (стихийные бедствия и природные явления), угрозы техногенного характера, угрозы социально-политического характера, сопровождаемые нападением на объекты, в которых размещаются ресурсы ИС. Все эти угрозы также могут быть актуальны или нет, однако они не имеют прямого отношения к информационной безопасности, поэтому далее не рассматриваются.

Каждая угроза описывается совокупностью соответствующих составляющих: способа реализации угрозы, объекта воздействия, результата реализации угрозы и уязвимости программного или аппаратного обеспечения, а также нарушителя (источника).

1.1.2. Нарушители

Нарушителем в контексте информационной безопасности являются лица, способные реализовать те или иные угрозы. При этом нарушители разделяются на две группы. С точки зрения наличия возможности постоянного или разового доступа в контролируемую зону предприятия, в которой размещены технические средства ИС, все нарушители могут быть отнесены к следующим двум категориям:

- **категория I:** внешние нарушители – лица, не имеющие права пребывания на контролируемой территории предприятия, в пределах которого размещаются технические средства ИС;
- **категория II:** внутренние нарушители – лица, имеющие право пребывания на контролируемой территории предприятия, в пределах которой размещаются технические средства ИС.

Рассмотрим эти два вида нарушителей более подробно.

Внешние нарушители

Итак, под внешним нарушителем безопасности защищаемой информации рассматривается нарушитель, не имеющий непосредственного доступа к техническим средствам и ресурсам системы, находящимся в пределах контролируемой зоны. Также к внешним нарушителям могут относиться нарушители категории II, реализующие угрозы из-за пределов контролируемой зоны. То есть если сотрудник компании по тем или иным причинам пытается реализовать атаку, находясь за пределами контролируемой зоны, то для нас он все равно будет внешним.

В общем виде в роли внешних нарушителей могут выступать лица, описанные в табл. 1.1.

Таблица 1.1. Внешние нарушители

Индекс категории	Категория нарушителя	Описание категории нарушителя
$К_{внеш}1$	Физические и юридические лица, не имеющие санкционированного доступа к ИС	• Физические лица – злоумышленники; • организации (в том числе конкурирующие или террористические); • криминальные группировки

В рамках рассматриваемых действия нарушителей предполагается, что внешний нарушитель может использовать как технические каналы утечки информации для осуществления несанкционированного доступа (далее – НСД) к защищаемой информации, так и пытаться воздействовать на защищаемую информацию путем использования вредоносного программного обеспечения, а также во время передачи защищаемой информации по каналам связи, выходящим за пределы КЗ.

Внутренние нарушители

Под внутренним нарушителем безопасности защищаемой информации рассматривается нарушитель, имеющий непосредственный доступ к каналам связи, техническим средствам и ресурсам системы, находящимся в пределах контролируемой зоны.

Внутренними нарушителями могут быть только лица категории II.

В роли внутренних нарушителей могут выступать лица, описанные в табл. 1.2.

Таблица 1.2. Внутренние нарушители

Индекс категории	Категория нарушителя	Описание категории нарушителя
$К_{вн}1$	Пользователи ИС	Работники Заказчика, являющиеся пользователями ИС

Индекс категории	Категория нарушителя	Описание категории нарушителя
$К_{вн}2$	Администраторы ИС	Работники следующих отделов предприятия Заказчика: • отдел системного, программного и технического обеспечения; • отдел обработки информации и электронного обмена данными
$К_{вн}3$	Работники сторонних организаций, осуществляющие доработку и сопровождение части прикладного программного обеспечения ИС	Работники сторонних организаций, осуществляющие доработку и сопровождение информационных систем
$К_{вн}4$	Работники сторонних организаций, обеспечивающие поставку, сопровождение и ремонт технических средств ИС	Работники сторонних организаций, обеспечивающие поставку, сопровождение и ремонт технических средств ИС
$К_{вн}5$	Обслуживающий персонал	Уборщицы, работники инженерно-технических служб и другие лица, выполняющие обслуживание помещений контролируемой зоны

Приведенная выше таблица отражает общую классификацию нарушителей информационной безопасности, однако в своей книге я предлагаю несколько упростить виды внутренних нарушителей, сведя все к одному виду: лицу, имеющему физический доступ на контролируемую территорию. Все, что требуется от нашего внутреннего нарушителя, – это пронести на контролируемую территорию хакерское устройство. При этом от него не требуется наличия каких-либо прав в атакуемой сети, требования к квалификации определяются лишь необходимостью наличия навыков работы с данным устройством. Таким образом, внутренним нарушителем в контексте моей книги может являться уборщица, не обладающая никакими знаниями о компьютерных системах, или курьер, прошедший на контролируемую территорию.

Мы определились с тем, кто и что может сделать. Теперь необходимо поговорить о такой важной для бизнеса теме, как риски информационной безопасности.

1.1.3. Риски

Вообще, использование информационных систем и технологий связано с определенной совокупностью рисков. При этом оценка рисков необходима для контроля эффективности деятельности в области информационной безопасности, принятия целесообразных защитных мер и построения эффективных экономически обоснованных систем защиты.

Причинами рисков являются угрозы для организации, поэтому важно выявление потенциальных или реально существующих рисков нарушения конфиденциальности, целостности и доступности информации.

Риски, как и всю информационную безопасность, нужно контролировать постоянно, периодически проводя их переоценку. При этом чем лучше будет задокументирована первая оценка, тем легче будет проводить переоценки впоследствии.

Для оценки рисков необходимо выделить все актуальные угрозы и оценить степень их влияния на бизнес-приложения. Здесь правда, только безопасникам справиться сложно, так как мы не можем правильно оценить, к примеру, стоимость часа простоя базы закупок или логистической системы. Эти цифры могут предоставить только владельцы данных систем. К примеру, час простоя логистической системы обходится компании в 1 млн руб, а час простоя базы закупок – в 3 млн. Исходя из полученных значений, мы должны приоритизировать риски, например риск простоя логистики является средним, а риск простоя закупок – высоким.

Далее необходимо выстроить процесс управления рисками. По отношению к выявленным рискам возможны следующие действия:

- ликвидация риска (например, за счет устранения уязвимости);
- уменьшение риска (например, за счет использования дополнительных защитных средств или действий);
- принятие риска (и выработка плана действия в соответствующих условиях).

Управление рисками можно подразделить на следующие этапы:

- инвентаризация анализируемых объектов;
- выбор методики оценки рисков;
- идентификация активов;
- анализ угроз и их последствий;
- определение уязвимостей в защите;
- оценка рисков;
- выбор защитных мер;
- реализация и проверка выбранных мер;
- оценка остаточного риска.

Для определения основных рисков можно следовать следующей цепочке: **нарушитель → угроза → последствия**.

Под последствиями мы понимаем возможные последствия реализации угрозы и связанный с ними ущерб. При этом ущерб может быть как материальным и выражаться в конкретной денежной сумме, так и репутационным, когда вред наносится репутации компании. Посчитать убытки от ущерба репутации не всегда просто, так как он может состоять из множества факторов. Однако про репутационные риски также необходимо помнить при анализе возможных рисков.

1.1.4. Модель нарушителя

Итак, мы разобрались с тем, какие нарушители бывают, какие угрозы бывают и к каким последствиям могут привести их действия.

Теперь нам необходимо применить описанное в предыдущих разделах. Например, у нас имеется конкретная организация со своим штатным расписанием и регламентированными обязанностями сотрудников и субподрядчиков. Тогда мы можем сопоставить, кто из них может что сделать в плане реализации угроз. Документ, описывающий подобные действия называется, моделью нарушителя.

Вспомним наши таблицы с внешними и внутренними нарушителями (см. табл. 1.1 и 1.2).

С внешними нарушителями все довольно просто. Как мы уже договорились, это все те, кто находится за периметром контролируемой территории. Мы им абсолютно не доверяем, поэтому это одна категория $К_{внеш}1$.

С внутренними нарушителями все несколько сложнее. В нашем примере их пять категорий. Рассмотрим, что могут сделать каждые из них, более подробно.

Пользователи информационных систем ($К_{вн}1$):

- могут иметь доступ к фрагментам информации, содержащей защищаемую информацию и распространяющейся по внутренним каналам связи;
- могут располагать фрагментами информации о топологии информационных систем (коммуникационной части подсети) и об используемых коммуникационных протоколах и их сервисах;
- знают, по меньшей мере, одно легальное имя доступа;
- могут обладать всеми необходимыми атрибутами доступа, обеспечивающими доступ к некоторому объему защищаемой информации;
- располагают конфиденциальными данными, к которым имеют доступ.

Работники сторонних организаций, осуществляющие доработку и сопровождение части прикладного программного обеспечения информационных систем ($К_{вн}3$). Данные лица:

- знают, по меньшей мере, одно легальное имя доступа;
- обладают всеми необходимыми атрибутами доступа, обеспечивающими полный доступ к полному объему защищаемой информации;
- обладают всеми необходимыми атрибутами доступа для заведения учетных записей пользователей информационных систем;
- располагают конфиденциальными данными, к которым имеют доступ;
- обладают информацией об алгоритмах и программах обработки информации в информационных системах;
- обладают возможностями внесения ошибок, недекларированных возможностей, программных закладок, вредоносных программ в программное обеспечение информационных систем на стадии ее доработки и сопровождения;

- могут располагать любыми фрагментами информации о топологии информационных систем и технических средствах обработки и защиты информации, обрабатываемой в информационных системах.

Работники сторонних организаций, обеспечивающие поставку, сопровождение и ремонт технических средств информационных систем ($К_{вн}4$). Данные лица:

- обладают возможностями внесения закладок в технические средства на стадии их внедрения и сопровождения;
- могут располагать любыми фрагментами информации о топологии и технических средствах обработки и защиты информации в информационных системах.

Обслуживающий персонал ($К_{вн}5$). Данные лица могут изменять конфигурацию технических средств, вносить в нее программно-аппаратные закладки и обеспечивать съем информации, используя непосредственное подключение к техническим средствам информационных систем.

Внимательный читатель наверняка обратил внимание на то, что в своем перечислении я пропустил $К_{вн}2$ – наших администраторов информационных систем. Сделано это не случайно, о них мы поговорим особо.

Лица, подпадающие под категорию $К_{вн}2$, выполняют задачи по администрированию программно-аппаратных средств информационных систем, администрированию доступа к информационным ресурсам, а также обеспечению информационной безопасности информационных систем. Данные лица потенциально могут реализовать угрозы ИБ, используя свои возможности по доступу к защищаемой информации, обрабатываемой в информационных системах, а также к техническим и программным средствам, включая средства защиты, используемые в информационных системах.

Данные лица хорошо знакомы с устройством информационных систем, а также с применяемыми принципами и концепциями безопасности. Предполагается, что они могут использовать стандартное оборудование либо для идентификации уязвимостей, либо для реализации угроз ИБ. Данное оборудование может быть как частью штатных средств, так и относиться к легко получаемому (например, программное обеспечение, полученное из общедоступных внешних источников).

К данным лицам ввиду их исключительной роли в ИС должен применяться комплекс особых организационно-режимных мер по подбору, принятию на работу, назначению на должность, повышению лояльности и контролю выполнения функциональных обязанностей. Кроме того, проводятся регулярное обучение и проверка знаний персонала в области ИБ.

Лица, попадающие под категорию $К_{вн}2$, являются специалистами высокой квалификации, вероятность совершения ими непреднамеренных (случайных) ошибочных действий при выполнении работ по техническому обслуживанию и сопровождению эксплуатации ИС, представляющих собой угрозу конфиденциальности и достоверности информации при ее хранении, обработке и передаче по каналам связи, крайне мала.

Таким образом, предполагается, что в число лиц категории $К_{вн}2$ будут включаться только доверенные лица, поэтому указанные лица исключаются из числа вероятных нарушителей.

Как видите, администраторы в большинстве случаев не могут являться нарушителями. Конечно, многие могут сейчас возразить, приведя в пример массу случаев, когда именно обиженные системные администраторы становились виновниками различных инцидентов, связанных как с хищением конфиденциальной информации, так и с выводом из строя вверенных им систем. Однако, в случае если мы признаем сисадминов вероятными нарушителями, нам необходимо будет защищаться и от них. А как можно эффективно защищаться от того, кто по определению должен иметь доступ ко всем настройкам и элементам управления информационных систем? Техническими средствами это реализовать крайне сложно и дорого, поэтому обычно задачу отбора и контроля работы администраторов решают организационными мерами.

Справедливости ради стоит отметить, что защищаться от администраторов тоже можно, например с помощью ролевой модели доступа, когда отдельные роли даются разным пользователям, и для выполнения какой-либо административной задачи в систему должно войти и подтвердить выполнение сразу несколько пользователей. Смысл сводится к тому, чтобы у одного пользователя не было всех прав в системе. Однако подобные механизмы используются, как правило, только в системах, работающих с гостайной, ввиду сложности их эксплуатации.

Еще один вариант – это мониторинг действий администраторов в критических системах. Такой мониторинг реализуется с помощью специальных приложений, речь о которых пойдет немного позже, когда мы будем говорить о практических аспектах ИБ. А пока вернемся к нашим нарушителям и угрозам.

1.1.5. Модель угроз

Мы рассмотрели возможных нарушителей информационной безопасности в нашей системе. Теперь поговорим об угрозах и возможностях их реализации.

Каждая угроза имеет определенную вероятность, то есть частоту реализации. Под вероятностью реализации угрозы понимается определяемый экспертным путем показатель, характеризующий, насколько вероятным является реализация конкретной угрозы безопасности защищаемой информации для данной ИС в складывающихся условиях.

Вероятность реализации (коэффициент Y_2) определяется по 4 вербальным градациям этого показателя (см. табл. 1.3):

Таблица 1.3. Вероятность реализации

Градация	Описание	Вероятность (Y_2)
Маловероятно	Отсутствуют объективные предпосылки для осуществления угрозы	$Y_2 = 0$
Низкая вероятность	Объективные предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют ее реализацию	$Y_2 = 2$
Средняя вероятность	Объективные предпосылки для реализации угрозы существуют, но принятые меры обеспечения безопасности защищаемой информации недостаточны	$Y_2 = 5$
Высокая вероятность	Объективные предпосылки для реализации угрозы существуют, и меры по обеспечению безопасности защищаемой информации не приняты	$Y_2 = 10$

Возможность реализации угрозы (коэффициент реализуемости угрозы Y) определяется на основе двух показателей: исходной защищенности ИС (Y_1) и вероятности реализации угрозы (Y_2).

Коэффициент реализуемости угрозы рассчитывается по формуле:

$$Y = (Y_1 + Y_2)/20.$$

По значению коэффициента реализуемости угрозы Y формируется вербальная интерпретация *возможности реализации угрозы* следующим образом:

- если $0 \leqslant Y \leqslant 0{,}3$, то возможность реализации угрозы признается **Низкой**;
- если $0{,}3 < Y \leqslant 0{,}6$, то возможность реализации угрозы признается **Средней**;
- если $0{,}6 < Y \leqslant 0{,}8$, то возможность реализации угрозы признается **Высокой**;
- если $Y > 0{,}8$, то возможность реализации угрозы признается **Очень высокой**.

Опасность угрозы для рассматриваемой ИС также определяется экспертным путем на основе вербальных показателей, которые могут принимать следующие значения:

- **низкая опасность**, если реализация угрозы может привести к незначительным негативным последствиям для обладателя информации;
- **средняя опасность**, если реализация угрозы может привести к негативным последствиям для обладателя информации;
- **высокая опасность**, если реализация угрозы может привести к значительным негативным последствиям для обладателя информации.

Отнесение угроз к разряду актуальных производится по правилам, приведенным в табл. 1.4.

Таблица 1.4. Актуальность угроз

Возможность реализации угрозы	Показатель опасности угрозы		
	Низкий	**Средний**	**Высокий**
Низкая	неактуальная	неактуальная	актуальная
Средняя	неактуальная	актуальная	актуальная
Высокая	актуальная	актуальная	актуальная
Очень высокая	актуальная	актуальная	актуальная

Далее мы будем предполагать, что нарушитель имеет все необходимые средства для реализации угроз по доступным ему каналам.

Внешний нарушитель (лица категории I, а также лица категории II при нахождении за пределами КЗ) может использовать следующие средства доступа к защищаемой информации:

- доступные в свободной продаже аппаратные средства и программное обеспечение;
- специально разработанные технические средства и программное обеспечение;
- специальные технические средства перехвата визуальной и аудиоинформации.

Внутренний нарушитель для доступа к защищаемой информации может использовать доступные ему штатные средства ИС и/или своего автоматизированного рабочего места (далее – АРМ).

К вероятным объектам реализации угроз защищаемой информации (объектам защиты) могут быть отнесены следующие объекты обработки защищаемой информации:

- записи электронных таблиц баз данных информационных систем;
- файлы данных, обрабатываемые на серверах информационных систем;
- серверное прикладное программное обеспечение информационных систем;
- информация, содержащаяся в экранных формах прикладного интерфейса АРМ пользователей информационных систем;
- файлы данных, обрабатываемые на АРМ информационных систем;
- распечатанные файлы с защищаемой информацией;
- сетевые пакеты передачи данных;
- технологическая и служебная информация, в том числе конфигурационные данные (файлы настроек) средств вычислительной техники.

Целью реализации угроз является нарушение определенных для объекта реализации угроз характеристик безопасности.

Возможными каналами реализации угроз, которые может использовать нарушитель для доступа к защищаемой информации в ИС, являются:

- каналы непосредственного доступа к объекту (визуально оптический, акустический, физический);
- электронные носители информации, в том числе носители с резервными копиями, съемные, сданные в ремонт и вышедшие из употребления;
- штатные программно-аппаратные средства ИС;
- незащищенные каналы связи.

Результат всех приведенных выше выкладок сводится к следующей таблице, которая, по сути, и отражает модель угроз (см. табл. 1.5).

Таблица 1.5. Фрагмент таблицы с актуальными угрозами

№	Способ реализации	Уязвимости	Результат реализации угрозы	Объект воздействия	Объект защиты	Нарушитель (источник угрозы)	Вероятность реализации угрозы
1	**Угрозы внедрения вредоносных программ**						
	Подключение к техническим средствам стороннего оборудования (компьютеров, КПК, смартфонов, телефонов, фотоаппаратов, видеокамер, флеш-дисков и иных устройств)	• Отсутствие либо нарушение регламентов использования средств вычислительной техники; • отсутствие в должностных обязанностях работников ответственности за нарушение ИБ; • отсутствие контроля использования отчуждаемых носителей и портов ввода/вывода; • отключение средств антивирусной защиты пользователями; • избыточные права пользователей в операционной системе на СВТ ИС; • отсутствие мероприятий по работе с персоналом, допущенным к обработке защищаемой информации; • отсутствие регламента резервного копирования; • человеческий фактор	• Нарушение конфиденциальности; • нарушение целостности	АРМ пользователей информационных систем	• Защищаемая информация, доступная через экранные формы прикладного интерфейса АРМ пользователя ИС; • файлы, содержащие защищаемую информацию; • технологическая и служебная информация, в том числе конфигурационные данные (файлы настроек) СВТ и СЗИ ИС		Маловероятно

№	Способ реализации	Уязвимости	Результат реализации угрозы	Объект воздействия	Объект защиты	Нарушитель (источник угрозы)	Вероятность реализации угрозы
2	**Угрозы удаленного доступа, реализуемые в ЛВС информационных систем**						
	Использование программ-анализаторов пакетов (снифферов) для перехвата защищаемой информации	• Отсутствие либо нарушение регламентов использования СВТ; • отсутствие в должностных обязанностях работников и договоре со сторонними организациями, осуществляющими сопровождение прикладного программного обеспечения ИС, положений, определяющих ответственность за нарушение ИБ; • передача защищаемой информации по сетям в открытом (или слабо защищенном) виде; • избыточные права пользователей в операционной системе на СВТ ИС; • плоская (неиерархическая) модель (структура) сети; • отсутствие средств обнаружения сетевых интерфейсов, находящихся в promiscuous mode	Нарушение конфиденциальности	Каналы связи локальной сети	Сетевые пакеты передачи данных		Маловероятно

№	Способ реализации	Уязвимости	Результат реализации угрозы	Объект воздействия	Объект защиты	Нарушитель (источник угрозы)	Вероятность реализации угрозы
3	**Угрозы выявления атрибутов доступа, передаваемых по сети**						
	Использование программ-анализаторов пакетов (снифферов) для перехвата идентификаторов и паролей удаленного доступа. Взлом перехваченных в сети защищенных паролей (хэш) при помощи специализированного программного обеспечения	• Отсутствие либо нарушение регламентов использования СВТ; • отсутствие в должностных обязанностях работников и договоре со сторонними организациями, осуществляющими сопровождение прикладного программного обеспечения ИС, положений, определяющих ответственность за нарушение ИБ; • передача идентификационной информации по сетям в открытом (или слабо защищенном) виде; • избыточные права пользователей в операционной системе на СВТ ИС; • отсутствие или недостатки парольной политики в ИС; • нарушения или недостатки физической защиты сетевого активного оборудования и каналов связи; • плоская (неиерархическая) модель (структура) сети; • отсутствие средств обнаружения сетевых интерфейсов, находящихся в promiscuous mode; • отсутствие регламента резервного копирования	• Нарушение конфиденциальности; • нарушение целостности; • нарушение доступности	Каналы связи локальной сети	Сетевые пакеты передачи данных		Маловероятно
	…	…	…	…	…		…

Здесь приводится лишь фрагмент данной таблицы, отражающий несколько наиболее типичных и актуальных для большинства организаций угроз. Таблица, отражающая все угрозы, заняла бы несколько десятков страниц.

1.1.6. Заключение

На этом тяжелую и сложную тему теоретических основ ИБ я закончу. Но нам важно понять, что же мы получили в результате всех этих выкладок. Благодаря составлению моделей нарушителя и угроз мы знаем, какие у нас в сети возможны нарушители и какие угрозы, каким образом они могут реализоваться. На практике при составлении моделей угроз используется анализ эксплуатационной документации на информационные системы, а также опрос обслуживающих их сотрудников.

Зная, кто и как может попытаться атаковать нашу сеть, мы можем начать построение системы обеспечения информационной безопасности.

1.2. Практика

1.2.1. Строим систему информационной безопасности

Имея список актуальных угроз, можно составить список требований к системе информационной безопасности, которые будут закрывать актуальные угрозы. Сразу хочу заметить, что не все актуальные угрозы можно закрыть техническими средствами. Например, угрозы разглашения пользователями своих учетных данных посредством приклеивания паролей на монитор нейтрализовать с помощью технических средств не удастся. Для этого необходимо подготовить соответствующие регламенты, в которых будет прописан запрет на выполнение подобных действий. С данным регламентом под роспись должны ознакомиться все сотрудники организации.

Итак, для примера я приведу несколько наиболее распространенных актуальных угроз, от которых мы будем защищаться:

- сетевые угрозы из сети Интернет;
- отказ в обслуживании;
- перехват трафика;
- вредоносный код;
- утечки конфиденциальной информации.

Для нейтрализации сетевых угроз необходимы межсетевые экраны для защиты периметра и системы обнаружения вторжений. Правильно настроенный межсетевой экран в связке с системой обнаружения вторжений может помочь при борьбе с примитивными DDoS-атаками. Для защиты от перехвата трафика при передаче через Интернет помогут средства криптографической защиты. Для защиты от вредоносного кода помогут антивирусные решения. Утечки конфиденциальной информации присутствуют во многих организациях, поэтому эти угрозы также широко распространены.

Такой набор актуальных угроз и соответственно средств защиты не является исчерпывающим. Для некоторых организаций актуальны могут быть также другие угрозы. Однако указанные выше угрозы являются наиболее распространенными. Далее мы рассмотрим, что из себя представляет каждое из приведенных средств защиты.

1.2.2. Защищаем периметр

Построение нашей системы информационной безопасности мы начнем с основополагающего элемента – защиты на периметре, обеспечиваемой межсетевыми экранами. Основная задача межсетевого экрана, – это защита вашей сети или компьютера от угроз, исходящих из Интернета, а также сегментация, то есть разделение, сети. Межсетевой экран осуществляет контроль доступа на основании IP-адресов или диапазонов адресов и портов отправителя и получателя, на основании правил доступа. Правила определяют, каким адресам и по каким портам и протоколам разрешено подключение, а по каким запрещено.

Межсетевые экраны существуют уже не одно десятилетие, и при этом решения данного класса постоянно развиваются. Изначально это был сетевой фильтр, который ставился между доверенной внутренней сетью и Интернетом и блокировал подозрительные сетевые пакеты на основе критериев сетевого и канального уровня иерархической модели OSI. По сути, фильтр учитывал только IP-адреса источника и назначения, флаг фрагментации, номера портов. Собственно, классические межсетевые экраны, которые и сейчас можно встретить практически в каждой сети, работают по аналогичному принципу. Такой подход позволяет предотвратить только самые простые сетевые атаки, такие как сканирование портов, обращение к определенным сегментам сети. Это первое поколение межсетевых экранов.

Второе поколение представляет собой шлюзы сеансового уровня, называемые также фильтрами контроля состояния канала (stateful firewall). Этот функционал позволил проверять принадлежность пакетов к активным TCP-сессиям.

Современные межсетевые экраны – это преимущественно физические устройства, объединяющие в себе несколько функций. В частности, в бюджетных моделях функция межсетевого экранирования встроена в беспроводные точки доступа, ADSL-модемы или маршрутизаторы.

Еще одно замечание по поводу межсетевых экранов. В последнее время большую популярность приобрели комплексные решения, включающие в себя и межсетевой экран и антивирус. Зачастую такие решения представляют из себя хороший антивирус и слабый брандмауэр или, наоборот, мощный файрвол и не слишком мощный антивирус.

Межсетевые экраны имеют различный интерфейс и различную систему команд конфигурирования. Однако принципы их работы, как правило, одинаковы. Поэтому я не буду приводить здесь примеров настройки какого-то конкретного межсетевого экрана.

Тем, кто интересуется внутренним устройством программных межсетевых экранов, рекомендую ознакомиться с исходным кодом МЭ iptables, который можно найти по адресу: ftp://ftp.netfilter.org/pub/iptables/iptables-1.4.1.tar.bz2.

Если межсетевой экран является статичным элементом защиты, действующим только в соответствии с заданными политиками, то средства обнаружения и предотвращения вторжений являются, по сути, динамичным элементом, способным оперативно реагировать на новые сетевые угрозы.

Система обнаружения вторжений (СОВ) – это программное или аппаратное средство, предназначенное для выявления фактов неавторизованного доступа в компьютерную систему или сеть либо несанкционированного управления ими в основном через Интернет.

Системы обнаружения вторжений используются для обнаружения некоторых типов вредоносной активности, которая может нарушить безопасность компьютерной системы. К такой активности относятся сетевые атаки против уязвимых сервисов, атаки, направленные на повышение привилегий, неавторизованный доступ к важным файлам, а также действия вредоносного программного обеспечения (компьютерных вирусов, троянов и червей).

Обычно архитектура СОВ включает:

- сенсорную подсистему, предназначенную для сбора событий, связанных с безопасностью защищаемой системы;
- подсистему анализа, предназначенную для выявления атак и подозрительных действий на основе данных сенсоров;
- хранилище, обеспечивающее накопление первичных событий и результатов анализа;
- консоль управления, позволяющую конфигурировать СОВ, наблюдать за состоянием защищаемой системы и СОВ, просматривать выявленные подсистемой анализа инциденты.

Существует несколько способов классифицировать СОВ в зависимости от типа и расположения сенсоров, а также методов, используемых подсистемой анализа для выявления подозрительной активности. Во многих простых СОВ все компоненты реализованы в виде одного модуля или устройства.

Виды систем обнаружения вторжений

В сетевой СОВ сенсоры расположены на важных для наблюдения точках сети, часто в демилитаризованной зоне или на границе сети. Сенсор перехватывает весь сетевой трафик и анализирует содержимое каждого пакета на наличие вредоносных компонентов. Протокольные СОВ используются для отслеживания трафика, нарушающего правила определенных протоколов либо синтаксис языка (например, SQL). В хостовых СОВ сенсор обычно является программным агентом, который ведет наблюдение за активностью хоста, на который установлен. Также существуют гибридные версии перечисленных видов СОВ.