

Геннадий Федорович
Вильдяйкин

**АППАРАТЫ
И СРЕДСТВА
ПЕРЕХВАТА
ИНФОРМАЦИИ**

для студентов технических
специальностей

Геннадий Вильдяйкин

**Аппараты и средства перехвата
информации. Для студентов
технических специальностей**

«Издательские решения»

Вильдяйкин Г. Ф.

Аппараты и средства перехвата информации. Для студентов
технических специальностей / Г. Ф. Вильдяйкин —
«Издательские решения»,

ISBN 978-5-00-500021-7

В данном пособии рассмотрены аппараты и средства съема информации с
позиции регистрации физических полей и их взаимодействие.

ISBN 978-5-00-500021-7

© Вильдяйкин Г. Ф.
© Издательские решения

Содержание

1. ВВЕДЕНИЕ. ОСНОВНЫЕ ПОНЯТИЯ	6
2. АСП ЭЛЕКТРОМАГНИТНОГО ПОЛЯ	8
2.1. Аппаратура и средства перехвата информации от информационных систем различного назначения	10
2.2. Снятие информации по каналу побочных электромагнитных излучений	11
2.3. Измерительная техника для измерения ПЭМИН и получение информации от ИС.	14
2.4. АСП в виде аппаратной и программной закладок	15
Конец ознакомительного фрагмента.	17

Аппараты и средства перехвата информации Для студентов технических специальностей

Геннадий Федорович Вильдяйкин

© Геннадий Федорович Вильдяйкин, 2019

ISBN 978-5-0050-0021-7

Создано в интеллектуальной издательской системе Ridero

1. ВВЕДЕНИЕ. ОСНОВНЫЕ ПОНЯТИЯ

Аппаратура и средства перехвата информации (АСП) можно рассматривать с различных позиций.

Как пример, выделяются технические каналы утечки информации, и для этих каналов определяется аппаратура и средства.

Иногда же рассматривают различные системы обработки, хранения, передачи информации, а так же технические средства и аппаратура для съема информации.

В данном сборнике рассматривается АСП предназначенные для сбора, и получения информации в зависимости от вида физического поля: акустического (АП), электромагнитного (ЭМП) и линейного и нелинейного взаимодействия этих полей: электромагнитного поля (ЭМП), электрического поля (ЭП), магнитного поля (МП), гидроакустического поля (ГАП), акустического поля (АПВ), вибрационного поля (ВП).

На рисунке 1 представлены классы физических полей и их взаимодействия, которые будут использованы при рассмотрении АСП. Показаны суперпозиция и нелинейные взаимодействия составляющих физических полей.

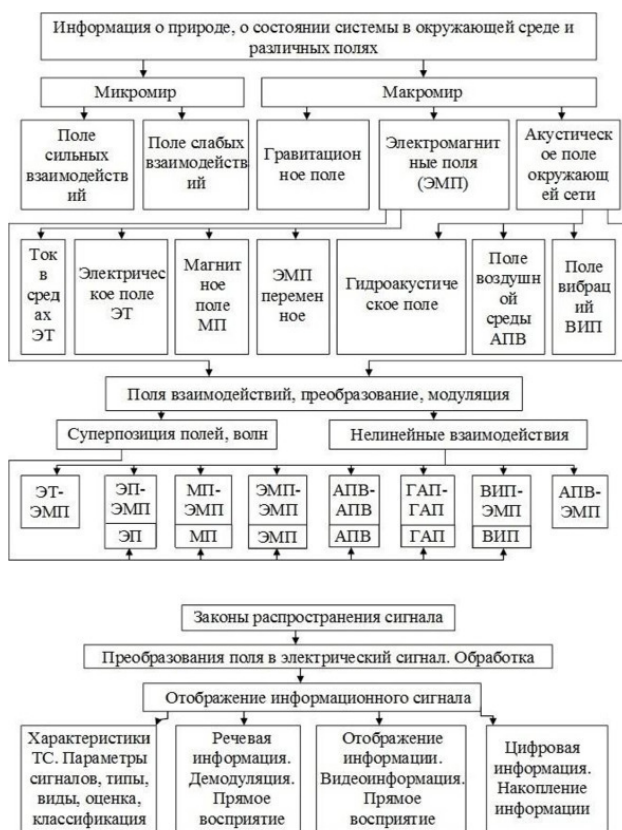


Рисунок 1 – Классы физических полей и их взаимодействия

Итак, определим и охарактеризуем АСП, исходя из тех физических полей и их взаимодействий, которые они перехватывают и регистрируют.

АСП физических полей построена на едином принципе. Схема (рисунок 2) выглядит просто:

1. Любой датчик поля (ЭМП, АП, ГД) под действием поля вырабатывает аналоговый сигнал независимо от того какой сигнал присутствует в исследуемом поле. Это относится

и к оптоволоконному, и радиочастотному кабелю. Для ЭМП датчиками поля являются антенны, индуктивные съемники, преобразователи. Для АП – микрофоны, для ВП – вибродатчики, акселерометры и др.

Если датчик (только щуп) подключен в проводную сеть (витая пара или провод), где присутствует цифровой сигнал, он будет регистрировать цифровой сигнал.

2. Усилитель, или же преобразователь, непосредственно усиливает или преобразовывает сигнал низкого уровня до величины (амплитуда, мощность) и вида (частота и время), достаточно для дальнейшей обработки.

3. Устройство обработки сигнала выделяет информативный сигнал с использованием современных методов анализа, синтеза обработки сигнала для отображения, регистрации.

4. Устройство отображения и регистрации доводит информацию до пользователя.



Рисунок 2 – Классы физических полей и их взаимодействия

2. АСП ЭЛЕКТРОМАГНИТНОГО ПОЛЯ

Рассмотрим АСП ЭМП, к которым относятся **линейное и нелинейное взаимодействие этих полей**. АСП ЭМП охватывает широкий класс технических средств, в том числе и средства разведки. В зависимости от частотного диапазона, спектра ЭМВ и от характера добываемой информации средства технической разведки подразделяются следующим образом.

Средства **радиоэлектронной разведки (РЭР)**. РЭР обеспечивает перехват электромагнитного поля ЭМП в радиодиапазоне или электрический ток. РЭР подразделяется на радиоразведку, радиотехническую разведку, радиолокационную разведку, радиотепловую разведку, разведку побочных электромагнитных излучений и наводок (ПЭМИН).

Радиоразведка добывает в большинстве случаев семантическую, то есть символьную или знаковую информацию путем перехвата радиосигналов с конфиденциальной информацией.

Радиотехническая разведка добывает информацию о параметрах (признаках) радиотехнических сигналов.

Радиолокационная разведка добывает информацию о дальности и направлении движения объекта, о видовых признаках радиолокационного изображения объекта на экране радиолокатора.

Радиотепловая разведка добывает информацию о признаках объектов, проявляющихся через их собственные электромагнитные излучения в радиодиапазоне.

Разведка ПЭМИН использует ту же радиоаппаратуру и методы, что и радиоразведка.

Средства оптической разведки (ОР). АСП ОР работают в видимом и инфракрасном диапазонах ЭМП. Оптическая разведка включает в себя визуально-оптическую, фотографическую. Оптическая разведка обеспечивает добывание информации с помощью оптических ТСР, обеспечивающих прием электромагнитных колебаний инфракрасного, видимого и ультрафиолетового диапазонов, излучаемых или отраженных интересующими объектами наблюдения и местными предметами. Ведется с использованием оптических приборов наблюдения (бинокли, перископы, монокуляры, в том числе панхроматические) и специальной фотоаппаратуры.

Средства **оптико-электронной разведки (ОЭР)**. Средства ОЭР это АСП ЭМП. В состав ТСР ОЭР входят: телевизионная, лазерная и инфракрасная разведки и разведка лазерных излучений. Оптико-электронная разведка (ОЭР) обеспечивает получение информации с помощью ТСР, имеющих входную оптическую систему с фотоприемником и электронными схемами обработки электрического сигнала, которые обеспечивают прием электромагнитных волн видимого и инфракрасного диапазонов, излученных или отраженных объектами наблюдения и местностью.

ТСР ОЭР подразделяются на активные и пассивные. Пассивная аппаратура ОЭР основана на приеме собственных или переотраженных излучений объектами наблюдения. К ТСР пассивной ОЭР относятся приборы ночного видения (ПНВ), тепловизоры, тепlopеленгаторы и радиометры.

С помощью аппаратуры телевизионной разведки осуществляется добывание информации за счет приема сигналов в видимом и ближнем ИК диапазонах, отраженных объектами наблюдения и элементами окружающей среды.

Лазерная разведка решает две группы задач: получение информации по результатам облучения объекта лазерным лучом (для подсветки, измерения дальности, дистанционного физического и химического анализа) и для определения источников и характеристик лазерного излучения.

Средства радиационной разведки (РДР). РДР использует АСП ЭМП. **Радиационная разведка** предназначена для обнаружения, локализации, определения характеристик ЭМП и измерения уровней энергии в верхней части спектра ЭМВ, то есть регистрация радиационного α , β , γ – излучения.

Магнитометрическая разведка (ММР). ММР использует АСП составляющую ЭМП магнитное поле. Магнитометрическая разведка позволяет получать информацию об объекте путем обнаружения и анализа локальных изменений поля Земли под воздействием объектов с большой магнитной массой.

Компьютерная разведка (КР). Компьютерная разведка осуществляет несанкционированный доступ к информации, обрабатываемой средствами вычислительной техники, и также прием электромагнитных излучений компьютеров и наводок электромагнитных излучений, распространяющихся по соединительным кабелям.

2.1. Аппаратура и средства перехвата информации от информационных систем различного назначения

К ИС относятся КИИ, АСУ ТП, ГИС, АС различного назначения, АРМ.

АСП информации от ИС это аппаратура регистрации ЭМП, ЭП, МП, электрического тока и их взаимодействия. К средствам перехвата относятся программные продукты, которые применяет разведка используя уязвимости при не эффективной защите ИС от НСД, МЭ, СОВ и антивирусе, уязвимости ОС Windows и ЗУ в ПО приложений.

Для перехвата ЭМП и наводок используются средства КР.

Основным способом добывания информации КР является перехват сигналов в компьютерах и их сетях. Учитывая, что компьютеры становятся основным средством обработки и хранения информации, возможности ее непрерывно растут.

Технические средства разведки ПЭМИН обеспечивают добывание информации в формируемых, передаваемых или отображаемых сообщениях (телефонных, телеграфных, телеметрических и так далее) и документах (телевизионных изображений, изображений с экранов ПЭВМ, текстах, таблицах, снимках и тому подобное) за счет регистрации электромагнитных излучений (ЭМИ) и электрических сигналов, наводимых первичными ЭМИ в токопроводящих цепях различных технических устройств и конструкций зданий.

АСП ПЭМИН использует радиоаппаратуру и средства радиоэлектронной разведки. Только эта аппаратура предназначена для улавливания очень слабых сигналов, то есть она более чувствительная.

По материалам зарубежных публикаций можно составить таблицу (рисунок 3) основных характеристик средств РР и РТР для получения информации от ИС через ПЭМИН.

№ п/п	Наименование характеристик	Значения характеристик на частотах, ГГц		
		0.03 - 0.1	0.1 - 1.0	1.0 - 18.0
1	Чувствительность приемника средства разведки, ДБ (отн. Вт/Гц)	-158	-165	-170
2	Коэффициент усиления приемной антенны портативной носимой портативной возимой	1	5	12
		8	12	18

Рисунок 3 – Таблица основных характеристик средств радиоразведки и радио-технической разведки

Предназначение оборудования для перехвата информации может быть идентифицировано по маркировке «TEMPEST screened». AST утверждает, что «*оборудование используется для сбора сигналов с зарубежных средств телекоммуникаций правительством США*». Одни ведущий специалист по криптографии емко описал корпорацию AST как «*магазин «Все для ЭШЕЛОНА»*».

Следует отдельно выделить вид АСП программный Tempest Soft.

ЗУ могут функционировать постоянно, с помощью ВЧ навязывания, ВЧ облучения.

Конкретные модели АСП, которые реализуют получение информации по схеме «**РС – излучение – прием – обработка – видеорегистрация**», в иностранной и отечественной литературе, а так же в Интернете отсутствуют. Имеются модели АСП и характеристики аппаратуры для регистрации ЭМП, измерения уровня ЭМП, методики расчета зон излучений. Описание АСП, ее характеристики, методика получения изображения от монитора на больших расстояниях (более 50 метров) в литературе отсутствует.

2.2. Снятие информации по каналу побочных электромагнитных излучений

При комплексном подходе к защите информационных систем (защита от НСД, шифрование, межсетевое экранирование, система обнаружения вторжений, антивирусная защита) использование АСП ПЭМИН остается актуальной.

Кроме того, не регламентируются требования к защите «Tempest Soft» как к разновидности ПЭМИН и разновидности уязвимости при отсутствии сертификации по НДВ.

Как показывают результаты исследований, разнообразие современных ОТСС ИС, их информативные ЭМП и наводки могут регистрироваться на значительных расстояниях от ИС. На современном этапе остается актуальным сбор информации от ПЭМИН ИС. Компрометирующие излучения продолжают оставаться интереснейшей областью исследований, хотя по большому счету они не изучены в научной литературе. Высокая стоимость физического экранирования и постоянно растущие тактовые частоты современных компьютеров гарантируют, что данную проблему быстро не преодолеть. Одновременно, появление мощных программных радиоприемников на любительском рынке способно лишь ухудшить ситуацию.

ПЭМИН – это не только излучения и сигналы в линиях. Программные методы могут существенно изменить картину: их можно применять для новых атак, создавать новые средства защиты и совершенно новые приложения. Технология «Программный Темпест» может существенно развить данную область исследований.

Динамика изменения требований.

Требования к ПЭМИН и TEMPEST в нашей стране и в США развивались одинаково по времени и по качеству, начиная с 70 годов. Нормы на начальном этапе были жесткие. В последующие годы методы, методики и нормы по защите ПЭМИН КИ корректировались, изменялись. Причем эти изменения были как в сторону послабления так и ужесточения.

С развитием технологии «Tempest Soft», наличие явных зон, территорий возможного снятия информации по ТКУ возникает необходимость изменения требований к ПЭМИН.

Первые демонстрации перехвата смысловой информации ПЭМИН в СССР демонстрировались в начале семидесятых годов ГТК СССР. Все последующие, в том числе современные зарубежные и отечественные публикации и материалы по данной теме, принципиально ничем не отличаются. Прием рядом с монитором, качество низкое, предложения и варианты увеличения уровня сигнала.

ТКУ информации – ПЭМИН.

Обработка информации в ИС проходит, как правило, с подключением в ИС к международным каналам связи. И хотя каналы связи защищены, этапы (участки) прохождения, обработки информации в АРМ или ЛВС создают ПЭМИН до их защиты в каналах связи.

ПЭМИН обладают любые радиоэлектронные средства.

Если рассматривать ИС с использованием средств вычислительной техники, то побочные электромагнитные излучения возникают при выводе информации на экран монитора, вводе данных с клавиатуры, при записи и чтении информации на накопителях, при передачи данных в каналы связи, при выводе данных на периферийные печатные устройства.

Создают ПЭМИН мониторы, системные блоки, видеокарты, соединительные кабели, флэш накопители.

Излучения устройств Wi-Fi можно также отнести к ПЭМИН.

Наводки от ИС АСП снимает в электрических цепях питания, на электрошитах, подстанциях в цепях заземления и сетях коммуникаций.

Случайные антенны, сосредоточенные и распределенные, линии коммутации и различные проводные линии это источник получения информации АСП.

Важную роль в перекрытие утечка информационного электрического сигнала играет качественное технологическое заземление.

Расчет потенциальной максимальной зоны регистрации ПЭМИ.

$$N_0 = kT_0 = 4 \cdot 10^{-21} \text{ Вт/Гц}$$

Рисунок 4 – Минимальный уровень спектральной плотности шума

Это физический предел спектральной мощности, которую могут технические средства регистрировать. Этот уровень включает все возможности приема и обработки информации (помехи, антенны, спектральные и корреляционные методы, накопление и другое).

Этот входной уровень соответствует спектральным значениям мощности и напряжению (рисунок 5):

$$P_{\text{сп}} = -204 \text{ Дб}, U_{\text{сп}} = -178 \text{ Дб}$$

Рисунок 5 – Спектральное значение мощности и напряжения

Если принять за чувствительность технического средства значение N_0 и действующую длину антенны $h_d=1\text{м}$, то спектральная напряженность электрической составляющей поля равна формуле, представленной на рисунке 6.

$$E_{\text{сп}_M} = 4,47 \cdot 10^{-10} \frac{\text{В}}{\text{м}} \cdot \text{Гц}^{1/2}$$

Рисунок 6 – Спектральная напряженность электрической составляющей поля

При коэффициенте калибровки антенны, равной 20 Дб, спектральная напряженность электрической составляющей поля равняется формуле их рисунке 7.

$$E_{\text{сп}_M} = 13,4 \cdot 10^{-10} \text{ В/М} \cdot \text{Гц}^{1/2} \cdot E_{\text{сп}_M} = 13,4 \cdot 10^{-10} \frac{\text{В}}{\text{М}} \cdot \text{Гц}^{1/2}$$

Рисунок 7 – Спектральная напряженность электрической составляющей поля при коэффициенте калибровки антенны, равной 20 Дб

С учетом измеренных уровней ПЭМИ и их расчетов для ближней, промежуточной и дальней зон максимальное значение, где **теоретически** можно регистрировать излучения, могут быть величины от 10 м до 30000 м в зависимости от частоты и h_d .

Это чистая теория. Реальность другая. Теоретический минимальный. уровень может достигается затратами и большими габаритами АСП.

На рисунке 8 приведены спектральные уровни шумов. Поэтому если взять, например, частоту 150 МГц для третьей гармоники и шум, например 1,5 Дб, отношение сигнал шум $q = 10\text{Дб}$, $h_d = 2,2\text{м}$, $T_0 = 100\text{К}$, то $R = 3\text{м}$.

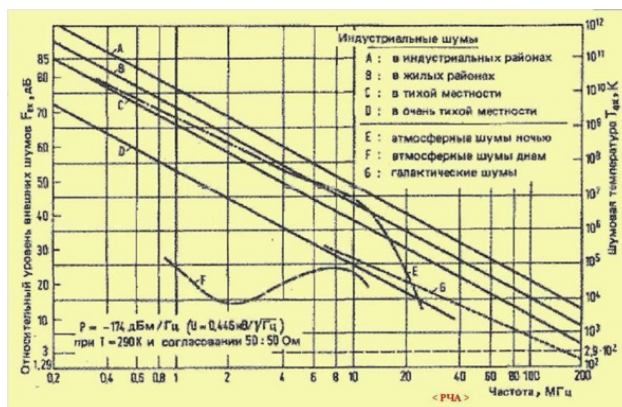


Рисунок 8 – Спектральные уровни шумов

2.3. Измерительная техника для измерения ПЭМИН и получение информации от ИС.

Компания Rohde & Schwarz представляет разнообразные комплексы измерительных приемников электромагнитных (ЭМП) и анализаторы спектра и сигналов высокого класса с большим динамическим диапазоном и уникальными функциональными возможностями. Эти средства можно использовать для измерения и контроля параметров ЭМП (ПЭМИН). Также они могут использоваться в комплексах для получения реальной информации, обрабатываемой ИС в том числе из ПЭМИН. Перечень наиболее приемлемых анализаторов и приемников как АСП для этих целей приводится ниже.

Анализаторы спектра, сигналов и шумов: R&S®FSC, R&S®FSL, R&S®FSV, R&S®FSVA, R&S®FSVR, R&S®FPS, R&S®Spectrum Rider FPH, R&S®FSH, R&S®FSWP.

Приемники измерительные: R&S®ESL, R&S®ESRP, R&S®ESR, R&S®ESU, R&S®ESW.

Программное обеспечение для анализа сигналов и для измерения ЭМС.

Антенные решения для измерения ЭМП.

Основные характеристики перечисленных анализаторов и приемников:

- Перекрывают частотный диапазон от 10 Гц до 40 ГГц, а с расширением до 500 ГГц;
- Уровень собственных шумов в полосе 1 Гц до —168 дБмВт;
- Чувствительность измерений фазовых шумов до -172 дБн.

Кроме того, в настоящее время для измерения ПЭМИН и ЭМИ ИС используются анализаторы и приемники компания Rohde & Schwarz, выпуска предыдущих годов.

Компания Agilent США выпускает анализаторы спектра серий ESA CSA EXA PSA MXA: E444xA, N9020A, 856xEC, N9010A, E44xxB, N1996A, N9320A, N9340A, приемник N9039A, работающие в частотном диапазоне от (10 Гц- 100 кГц) до 26,5 ГГц с внешним преобразователем частоты до 325 ГГц. Средний уровень собственного шума составляет 168 дБм—144 дБм.

Анализаторы компании Hewlett-Packard работают с сигналами частотой от 100 Гц до 40 ГГц, фазовыми шумами меньше 110 дБ/Гц, чувствительностью на полосе 10 Гц не хуже 130 дБм.

Анализаторы спектра и сигналов фирмы Anritsu функционируют в диапазоне до 40 ГГц и имеют чувствительность до -166 дБм в полосе 1 Гц.

2.4. АСП в виде аппаратной и программной закладок

Аппаратной закладкой является скрытое техническое приспособление, который позволяет получить доступ к цели или сведения о ней. Под программной закладкой понимаются скрытые программы, позволяющие получить доступ к цели программным способом, как, например, при помощи троянских коней и бэкдоров.

Список программных и аппаратных средств из опубликованных Э. Сноуденом.

АСП с компьютеров:

GINSU – техника, позволяющая восстановить программную закладку под названием KONGUR на целевых системах с аппаратной закладкой BULLDOZZER на PCI-шине. Например, в случае обновления или переустановки операционной системы на целевом компьютере. Данные технологии предназначены для получения удаленного доступа к компьютеру под управлением Windows от 9x до Vista.

IRATEMONK позволяет обеспечить присутствие программного обеспечения для слежки на настольных и портативных компьютерах с помощью закладки в прошивке жесткого диска, которая позволяет получить возможность исполнения своего кода путем замещения MBR.

SWAP позволяет обеспечить присутствие программного обеспечения для шпионажа за счет использования BIOS материнской платы и HPA области жесткого диска путем исполнения кода до запуска операционной системы.

HOWLERMONKEY представляет собой радиопередатчик малого и среднего радиуса. Является специальным радиомодулем для других аппаратных закладок.

JUNIORMINT миниатюрная аппаратная закладка на базе ARM-системы, которая может быть сконфигурирована для различных задач.

MAESTRO-II, TRINITY миниатюрная аппаратная закладка на базе ARM-системы, размером в одноцентовую монету.

SOMBERKNAVE программная закладка, работающая под Windows XP предоставляющая удаленный доступ к целевому компьютеру. Использует незадействованные Wi-Fi адаптеры.

COTTONMOUTH-I, -II, -III аппаратные закладки на USB предоставляющие беспроводной мост к целевой сети, а также загрузки эксплойтов на целевой системе. Может создавать скрытый канал связи.

FIREWALK аппаратная сетевая закладка, способная пассивно собирать трафик сети Gigabit Ethernet, а также осуществлять активные инъекции в Ethernet пакеты целевой сети.

SURLYSPAWN – аппаратная закладка (кейлоггер), позволяющая получить по радиоканалу данные от цели (клавиатура, низкоскоростные цифровые устройства). Данные передаются в отраженном сигнале, для активации необходимо облучение закладки радиосигналом от специализированного излучателя. Кейлоггер совместим с USB и PS/2 клавиатурами, в дальнейшем планируется добавление совместимости с клавиатурами ноутбуков.

RAGEMASTER – аппаратная закладка, позволяющая перехватить сигнал от VGA монитора. Закладка прячется в обычный VGA-кабель соединяющий видеокарту и монитор, установлена, как правило, в феррит на видеокабеле. Реализован захват сигнала с красного цветового канала. Активируется при облучении радиосигналом от специализированного излучателя.

Сети Wi-Fi

NIGHTSTAND мобильный комплекс для проведения активных атак на Wi-Fi сети, дальность действия может достигать 13 км.

SPARROW II встраиваемая компьютерная система под управлением Linux. Система для сбора данных о беспроводных сетях.

Серверы:

IRONCHEF обеспечивает доступ к целевым системам при помощи BIOS материнской платы и использования SMM-режима для связи с аппаратной закладкой, предоставляющей двухстороннюю радиосвязь DEITYBOUNCE предоставляет программный доступ к серверам Dell PowerEdge при помощи BIOS материнской платы и использования SMM-режима для получения возможности запуска перед загрузкой системы.

Сетевое оборудование:

JETPLOW – это закладка для прошивки Cisco PIX и ASA (Adaptive Security Appliance) файрволов, способен работать на Cisco PIX 500-й серии и ASA (5505, 5510, 5520, 5540, 5550).

HALLUXWATER – это бэкдор устанавливаемый в качестве обновления загрузчика в файрволы Huawei Eudemon.

FEEDTROUGH представляет собой технику установки двух программных закладок BANANAGLEE и ZESTYLEAK.

GOURMETTROUGH закладка для некоторых моделей Juniper. SOUFFLETROUGH закладка для BIOS файрволов Juniper SSG 500, 300 серий.

Конец ознакомительного фрагмента.

Текст предоставлен ООО «ЛитРес».

Прочитайте эту книгу целиком, [купив полную легальную версию](#) на ЛитРес.

Безопасно оплатить книгу можно банковской картой Visa, MasterCard, Maestro, со счета мобильного телефона, с платежного терминала, в салоне МТС или Связной, через PayPal, WebMoney, Яндекс.Деньги, QIWI Кошелек, бонусными картами или другим удобным Вам способом.