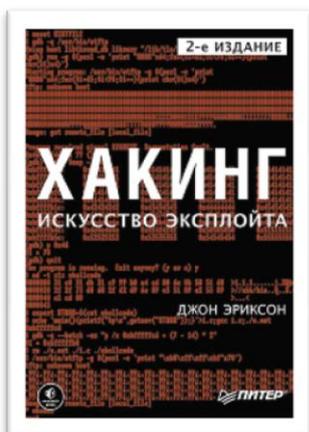


Дополнительная литература по информационной безопасности (ИБ), защите информации от угроз, утечек, вирусов, по криптографии (1)

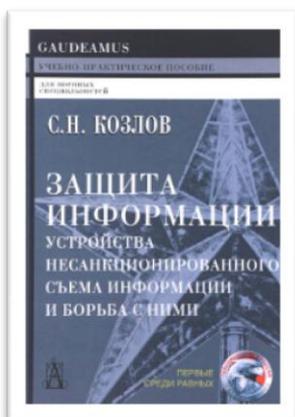
В современном информационном обществе информация превратилась в особый ресурс любой деятельности, следовательно, как и всякий другой ресурс, нуждается в защите от угроз, в обеспечении ее сохранности, целостности и безопасности. В конкурентной борьбе широко распространены разнообразные действия, направленные на получение (добывание, приобретение) конфиденциальной информации самыми различными способами, вплоть до прямого промышленного шпионажа с использованием современных технических средств разведки. В этих условиях защите информации от неправомерного овладения ею должно отводиться весьма значительное место в деятельности любой организации. На этой странице вы можете ознакомиться и скачать книги и литературу по информационной безопасности (ИБ), защите информации, защите деловой переписки, защите от компьютерных вирусов и других угроз совершенно бесплатно.



Хакинг. Искусство эксплойта, Питер, 2018, 498 с.

Понимание принципов программирования помогает находить уязвимости, а навыки обнаружения уязвимостей помогают создавать программы, поэтому многие хакеры занимаются тем и другим одновременно. Интересные нестандартные ходы есть как в техниках написания элегантных программ, так и в техниках поиска слабых мест. С чего начать? Чтобы перезаписывать память с помощью переполнения буфера, получать доступ к удаленному серверу и перехватывать соединения вам предстоит программировать на Си и ассемблере, использовать шелл-код и регистры процессора, познакомиться с сетевыми взаимодействиями и шифрованием и многое другое.

PDF 20 Мб [СКАЧАТЬ](#)



Защита информации. Устройства несанкционированного съема информации и борьба с ними

Козлов Сергей, Трикста, 2018, 289 с.

Благодаря представленным в пособии материалам читатель не только сможет ознакомиться с каналами утечки информации, устройствами ее несанкционированного съема (УНСИ) и тактикой преступных элементов при установке и контроле этих устройств, но и получит наглядный и эффективный практикум по организации поиска и локализации УНСИ.

PDF 15 Мб [СКАЧАТЬ](#)

Вскрытие покажет. Практический анализ вредоносного ПО

Майкл Сикорски, Эндрю Хониг, Питер, 2018, 768 с.



На самом деле это даже две книги в одной. В первой читатель учится анализировать современные вредоносные программы — уже только это оправдывает покупку. Но авторы решили не останавливаться и фактически написали второй том, который можно было бы озаглавить как «Прикладной анализ вредоносного ПО». Он состоит из лабораторных работ, кратких ответов и развернутого анализа, представленного в конце каждой главы и в приложении В. Кроме того, авторы сами написали все вредоносные образцы, которые используются в примерах, подготовив для вас разнообразную, но при этом безопасную среду для обучения. Таким образом, вместо того чтобы сетовать на очевидную асимметричность с точки зрения систем защиты, скажите спасибо, что вредоносное ПО обрело именно такую форму. Вооружившись книгами, подобными этой, вы получите фору, необходимую для обнаружения и устранения вторжений в вашу организацию или организации ваших клиентов.

PDF 15,6 Mb [СКАЧАТЬ](#)

Искусство легального, анонимного и безопасного доступа к ресурсам Интернета

Райтман М., БХВ-Петербург, 2017, 624 с.

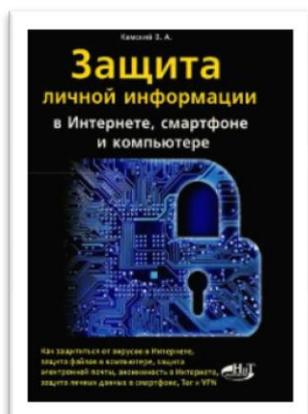


Описан ряд приемов защиты персональных данных с помощью шифрования, паролей, многофакторной аутентификации, приватного обмена, бесследного удаления информации и других доступных обычному пользователю средств. Приведены способы конспиративного общения по защищенным каналам связи и подключения к анонимным сетям, таким как Tor, I2P RetroShare и др. Описаны способы получения инвайтов в закрытые сообщества и доступа к таким ресурсам, как Pandora и Hulu. Представлено подробное руководство по операционной системе Tails, обеспечивающей максимальный уровень анонимизации и безопасности. В качестве приложения приведен экскурс в Даркнет - теневую сторону Интернета, а также сведения о 'варезной' сцене и демосцене, разновидности компьютерного искусства.

PDF 40,6 Mb [СКАЧАТЬ](#)

Защита личной информации в интернете, смартфоне и компьютере

В. Камский, Наука и Техника, 2017, 274 с.



По статистике большинство пользователей персональных компьютеров и Интернета сами позволяют похищать/использовать свои личные данные злоумышленникам или просто подкованным в техническом плане третьим лицам. И ущерб от таких противоправных действий колеблется от незначительного до катастрофического. Никто не поможет лучше всего защитить ваши данные чем... вы Сами! И эта книга вам в этом поможет. Простым и понятным языком здесь рассказано как эффективно защитить свою электронную почту, какими способами лучше воспользоваться для этой цели, а также приведены примеры взлома электронной почты. Вы узнаете как стать анонимным в Интернете, чтобы вас не беспокоили назойливые правила форумов, как защититься от вирусов в Интернете, что такое проект Tor

PDF 61 Mb [СКАЧАТЬ](#)

Взламываем Хакера. Часть 1-3

Роджер А. Граймс, Самиздат, 2017, 259 с.



Цель книги Роджера А. Граймса 'Взламываем Хакер' - оценить по достоинству людей из сферы компьютерной безопасности, рассказать об одних из лучших в мире «белых шляпах», специалистах по безопасности, преподавателей и писателей. Большая часть этой книги состоит из глав, в которых кратко описывается, как осуществляется определенный вид взлома. После глав приводится один или несколько эталонных примеров борьбы с этими уязвимостями от экспертов из этой области. Приводится попытка выбрать представителей из разных сфер: легенд индустрии, светил, и даже некоторых относительно неизвестных людей, которые, тем не менее, внесли выдающийся вклад. Автор постарался выбрать разных академиков, корпоративных поставщиков, учителей, лидеров, писателей и честных сотрудников, живущих по всему миру. Читатели, желающие связать свою жизнь с информационной безопасностью, смогут найти ту же мотивацию, которую нашел автор, чтобы помочь сделать компьютерную индустрию значительно безопаснее.

PDF 3 Mb [СКАЧАТЬ](#)
