Дополнительная литература по информационной безопасности (ИБ), защите информации от угроз, утечек, вирусов, по криптографии (2)

Анализ защищенности и мониторинг компьютерных сетей. Методы и средства

Валерий Бондарев, МГТУ им. Н. Э. Баумана, 2017, 228 с.

В последнее время большое внимание уделяется новому направлению в области защиты информации - адаптивной безопасности компьютерной сети. Это направление включает в себя две основные технологии: анализ защищенности (Security Assessment) и обнаружение атак (Inti-usion Detection). Целью учебного пособия Валерия Бондарева 'Анализ защищенности и мониторинг компьютерных сетей' является ознакомление студентов с теоретическими вопросами, связанными с архитектурой и принципами работы систем обнаружения атак злоумышленников, а также приемами и инструментами, применяемыми при защите компьютерных систем и сетей от атак. Пособие предназначено для студентов, обучающихся по направлению подготовки 'Информационная безопасность' (комплексное обеспечение информационной безопасности автоматизированных систем - КОИБАС, организация и технология защиты информации и т. д

PDF 41,1 Mb **СКАЧАТЬ**

Аудит безопасности информационных систем

Никита Скабцов, Питер, 2017, 272 с.

Основная цель книги Никиты Скабцова 'Аудит безопасности информационных систем' — не привести готовые примеры настройки брандмауэров, сетевых сервисов, оборудования и прочих столь милых сердцу администратора вещей, а познакомить читателя с основными принципами защиты сети. В частности, в книге рассматривается, как уберечь свою инфраструктуру от того, другого читателя, которой более чем внимательно изучил разделы этой же книги по взлому систем. Как и в некоторых других книгах начинается описание с базовых, не технических понятий. Затем затрагивается обучение пользователей основам безопасности, а после чего изложение плавно переходит к техническим мерам. Рассматриваются принципы работы и настройки основных систем, а также возможные проблемы, связанные с их использованием.

PDF 17,3 Mb **СКАЧАТЬ**

Информационная безопасность: защита и нападение. 2-е издание

Андрей Бирюков, ДМК-Пресс, 2017, 434 с.

2-е издание книги Андрея Бирюкова 'Информационная безопасность: защита и нападение' предназначена прежде всего для системных администраторов и специалистов по информационной безопасности, которые хотели бы разобраться в практических аспектах защиты корпоративных ресурсов от различных угроз. Основной упор при написании книги автор сделал именно на практические аспекты, то есть здесь вы не обнаружите «размышлений на тему». Вместо пространных размышлений автор постарался сделать основной упор на практические способы решения проблем информационной безопасности, то есть в книге описываются различные сценарии и настройки приложений и сетевого оборудования, работа со средствами по поиску уязвимостей и многое другое.

PDF 91,3 Mb **СКАЧАТЬ**

Лаборатория хакера

Сергей Бабин, БХВ-Петербург, 2016, 240 с.

В отличие от множества других изданий на тему хакинга, в книге Сергея Бабина 'Лаборатория хакера' сделан уклон не на программирование, а на вопросы сетевого взаимодействия. Именно поэтому она никоим образом не является 'конкуренткой' подобным публикациям. Собственно, книга о том, что не обязательно писать программы! Как правило, на все случаи жизни уже есть готовые решения. Хотя именно вот такой подход зачастую и раздражает профессиональных программистов. Казалось бы, как можно, не имея базовых знаний по программированию, научиться разбираться в основах создания фишингового сайта или еще круче - в приемах атак с инъекцией Java-скриптов? Оказывается, можно.Книга как раз и доказывает, что на первом этапе любому, даже школьнику, запросто можно обойтись без этого... Мало того, на вопрос 'Как изучать настройку оборудования, стоящего отни тысяч рублей, не имея на это средств и возможностей?' так же с уверенностью ответим — и это можно!

PDF 33 Mb **СКАЧАТЬ**

Основы веб-хакинга. Более 30 примеров уязвимостей

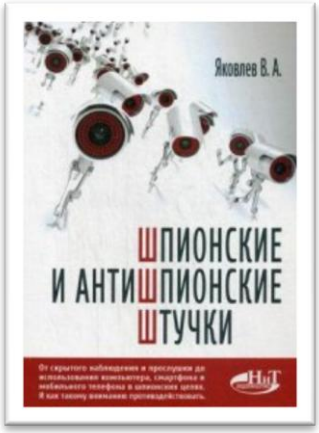
Питер Яворски, Leanpub, 2016, 201 с.

Авторы книги 'Основы веб-хакинга: Более 30 примеров уязвимостей' верят, что эта книга будет потрясающим руководством на протяжении всего вашего пути. Она изобилует полноценными примерами отчетов об уязвимостях из реального мира, эти отчеты принесли их авторам реальные деньги. Так же в этой книге вы найдете полезный анализ и обзор от Питера Яворски, автора и хакера. Он ваш помощник на пути обучения, и это бесценно. Еще одна причина, по которой эта книга так важна, заключается в том, что она фокусируется на том, как стать этичным хакером. Освоение искусства хакинга может быть чрезвычайно мощным навыком, который, мы надеемся, будет использован во благо. Самые успешные хакеры умеют во время хакинга балансировать на тонкой линии между правильным и неправильным. Многие люди могут ломать вещи, и даже пытаются извлечь из этого быструю выгоду. Но только представьте, вы можете сделать Интернет безопаснее, работать с потрясающими компаниями со всего мира и даже получать за все это деньги. Ваш талант потенциально может сохранить миллиарды людей и их данные в безопасности.

PDF 11 Mb **СКАЧАТЬ**

Шпионские и антишпионские штучки

В.А. Яковлев, Наука и техника, 2015, 320 с.



Данная книга В.А. Яковлева 'Шпионские и антишпионские штучки' рассказывает об организации скрытого видеонаблюдения, выбора видеокамер, регистраторов и другого оборудования. В книге освещаются правовые вопросы создания, приобретения и использования шпионских штучек в нашей стране. Также в данном издании рассматриваются и различные антишпионские гаджеты, такие, как индикаторы поля, обеспечивающие обнаружение жучков, постановщики помех, «глушилки», созданные для предупреждения утечки информации. Но главными шпионскими штучками нашего века безусловно являются персональные компьютеры, ноутбуки, нетбуки, планшеты, смартфоны и мобильные телефоны. В книге описываются различные программные комплексы, осуществляющие слежение за абонентом или пользователем. Многие такие программы предусматривают запись и прослушку телефонных разговоров, прослушивание окружения, перехват SMS или сообщений электронной почты, контроль местоположения, выявление паролей и многое другое.

WinDjvu 24,3 Mb **СКАЧАТЬ**

Математики, шпионы и хакеры. Кодирование и криптография

Жуан Гомес, ООО 'Де Агостини', 2014, 144 с.

Книга Жуана Гомеса 'Математики, шпионы и хакеры: Кодирование и криптография' является попыткой рассказать историю секретных шифров с точки зрения наиболее квалифицированного из гидов: математики. При взрывном росте вычислительной мощности именно шифры, а не традиционные соображения секретности играют ведущую роль в передаче информации. Универсальный язык современного общества использует не буквы или иероглифы, а только две цифры — 0 и 1. Это двоичный код. Какая из сторон выиграла от прихода новых технологий: криптографы или криптоаналитики? Возможна ли безопасность в наш век вирусов, информационных краж и суперкомпьютеров? Ответ на второй вопрос в значительной степени положителен, и снова мы должны сказать спасибо математике, а именно простым числам и их особенным свойствам. Как долго продержится временная победа криптографии? Ответ на этот вопрос уведет нас к самой дальней границе современной науки — теории квантовой механики, поразительные парадоксы которой подведут итог нашему захватывающему путешествию по разделу математики, отвечающему за безопасность и секретность.

PDF 50,2 Mb **СКАЧАТЬ**

Управление рисками информационной безопасности. 2-е издание

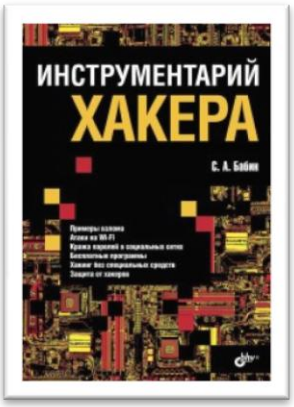
Наталья Милославская, Михаил Сенаторов, Горячая линия-Телеком, 2014, 130 с.

При подготовке данного учебного пособия были поставлены следующие задачи: определить основные понятия, относящиеся к управлению рисками информационной безопасности (ИБ), детально рассмотреть составляющие процесса управления рисками ИБ, описать различные подходы к анализу и оценке рисков ИБ, проанализировать систему управления рисками ИБ (СУРИБ), рассмотреть необходимое документальное обеспечение и применяемые в настоящее время инструментальные средства управления рисками ИБ. Материалы, вошедшие в учебное пособие «Управление рисками информационной безопасности» обеспечивают учебно-методической базой любую учебную дисциплину, относящуюся к управлению ИБ. Однако в полной мере данное учебное пособие может быть востребовано при подготовки профессионалов в области управления ИБ.

PDF 68,5 Mb **СКАЧАТЬ**

Инструментарий хакера

Сергей Бабин, БХВ-Петербург, 2014, 240 с.



Книга Сергея Бабина 'Инструментарий хакера' может быть использована в качестве практического руководства для начальной подготовки специалистов информационной безопасности. В книге описывается типичный инструментарий современного хакера. Приводится множество примеров взлома и сокрытия следов: перехват паролей, атаки на Wi-Fi-роутеры, подмена MAC-адресов, способы оставаться невидимым в Интернете. Книга будет полезна всем: начиная от интересующегося старшеклассника, студента (причем любого факультета, даже не связанного с информационной безопасностью), каждого пользователя домашнего компьютера (в особенности, если он применяет систему 'клиент — банк'), программиста (в том числе занимающегося обслуживанием компьютеров в различных фирмах) и заканчивая специалистами, связанными с областью защиты информации. Даже бизнесмен, который применяет в своей практике компьютер, задействованный в дистанционном банковском обслуживании, найдет здесь все необходимое, что требуется сделать для того, чтобы у него элементарно не украли все нажитое непосильным трудом.

PDF 19,3 Mb **СКАЧАТЬ**

Управление инцидентами информационной безопасности и непрерывностью бизнеса. 2-е издание

Наталья Милославская, Михаил Сенаторов, Горячая линия-Телеком, 2014, 160 с.

Учебное пособие «Управление инцидентами информационной безопасности и непрерывностью бизнеса», разработанное Натальей Милославской, Михаилом Сенаторовым и Александром Толстым, является третьей частью серии учебных пособий «Вопросы управления информационной безопасностью». При подготовке данного учебного пособия были поставлены следующие задачи: 1) описать процесс управления инцидентами информационной безопасности (ИБ). 2) определить особенности системы управления инцидентами ИБ и рассмотреть ее основные характеристики. 3) дать основные определения, относящиеся к проблеме обеспечения непрерывности бизнеса (ОНБ). 4) рассмотреть основные аспекты управления непрерывностью бизнеса (УНБ).

WinDjvu 10 Mb **СКАЧАТЬ**

Информационные операции в сети Интернет

С.П. Расторгуев, М.В. Литвиненко, АНО ЦСОиП, 2014, 128 с.

Книга известных специалистов в области информационной безопасности и психологического воздействия на массы С.П. Расторгуева и М.В. Литвиненко 'Информационные операции в сети Интернет' предназначена главным образом для военных экспертов и специалистов, работающих в сфере информационно-психологического воздействия. Она также безусловно будет интересна широкому кругу читателей, интересующихся вопросами развития кибернетических систем и сетевых технологий. В данной книге предлагается обоснованный подход к построению систем выявления информационных угроз, даются базовые определения и проводится исследование специальных действий, присущих информационным операциям в сети Интернет. В книге четко показывается, что производство практически всех компонент информационной операции уже поставлено на промышленную основу: от вирусов, нацеленных на автоматизированные объекты военного и промышленного назначения, до генераторов сообщений в виде текстов, голосовых сообщений по заданной голосовой характеристике или видеосюжетов по заданной исходной «картинке».

PDF 2,3 Mb **СКАЧАТЬ**

Защита в операционных системах

Вадим Проскурин, Горячая линия-Телеком, 2014, 192 с.

В книге подробно рассмотрены основные средства и методы обеспечения информационной безопасности в современных операционных системах: управление доступом, аутентификация, аудит и обнаружение вторжений. Кроме того, отдельно рассматриваются некоторые специфические вопросы, косвенно связанные с обеспечением безопасности операционных систем: централизованное управление политиками безопасности в доменах Windows, особенности обеспечения безопасности операционных систем мобильных устройств, концепция виртуализации операционных систем и ее влияние на информационную безопасность. Изложение теоретического материала иллюстрируется практическими примерами. В конце каждой главы приведен перечень вопросов для самопроверки, в конце пособия методические рекомендации по его изучению.

PDF 11,3 Mb **СКАЧАТЬ**
