СОДЕРЖАНИЕ

ОТ АВТОРОВ 13

ВМЕСТО ПРЕДИСЛОВИЯ 15

С. Д. Рябко: два достоинства книги 15

В. А. Конявский: как нам жить здесь и сейчас — вот основной пафос работы 17

А. В. Морозов: Книга заставляет взглянуть на проблемы ИБ совсем с другой, не столь технологической стороны 19

И. А. Трифаленков: Полнота набора вопросов, рассматриваемых авторами, делает книгу своеобразной энциклопедией информационной безопасности 20

ГЛАВА I. ФИЛОСОФСКАЯ 22

Об информации: от философии к практике 22

Предметная область: где границы? 22
Философия информации 23
Идеальное или материальное? 23
Статика и динамика: сведения и сообщения 25
Данные: новая форма? 27
Информационные ресурсы: общее или частное? 28
Лирическое отступление: курьезы определений 29
Важное свойство: легкость копирования 30
Мера: цена и ценность 31
Мера: системы счислений 31
Цена: «Сколько вешать граммов»? 33
Сухой остаток: для тех, у кого мало времени 34

Информация как объект защиты 34

Важнейший вопрос: защищать информацию или информационную систему? 35
Единство формы и содержания 35
Старая притча и выводы из нее 36
Три кита безопасности информации: конфиденциальность, целостность, доступность 37
Конфиденциальность 37
Целостность 38
Доступность 39
Попытки расширения классической триады 40
Открытая информация: надо ли защищать? 41
Общедоступная информация государственных органов 42
Информация о государственных услугах 43
Информация как товар (коммерческий интерес) 43
Критически важная (технологическая) информация 45
Инфраструктура и технологии: надо ли защищать? 46
Точка приложения усилий 46
Границы дозволенного 48
Безопасность информации и информационные технологии: конфликт интересов 49
Сухой остаток: для тех, у кого мало времени 50

Заказать книгу на сайте издательства Медиа Группы «АВАНГАРД»

О роли права и нормативов 52
Информация как объект права 52
Собственник и обладатель: в чем разница? 54
Границы информации, как объекта права 57
Оборотоспособность информации: что это такое? 60
Применимость имущественного права 63
Применимость интеллектуального права 66
О юридической значимости информации 67
Лирическое отступление: немного истории 68
Собственно о самой проблеме 69
Можно ли сделать электронный автограф? 71
О роли даты 72
Как решать проблему юридически 73
Структура нормативной базы 75
Право: отрасли, формы и нормы 75
Принципы правового регулирования 78
Система информационного законодательства 79
Международные правовые акты 81
Всеобщая Декларация прав человека 82
Международный Пакт о гражданских и политических правах 82
Римская Конвенция 83
Основные положения ОЭСР о защите частной жизни 84
Страсбургская Конвенция 84
Директива № 95/46/ЕС 85
Вассенаарские договоренности 86
Лирическое отступление: ВТО — к добру или к худу? 87
Конституция Российской Федерации 89
Кодифицированные акты (Кодексы Российской Федерации) 90
Гражданский Кодекс РФ 90
Трудовой и Налоговый Кодексы РФ 92
Уголовный кодекс и Кодекс об административных правонарушениях РФ 93
Лирическое отступление: О кодификации преступлений и роли мошенничества 95
Федеральные законы 100
Федеральный закон № 149-ФЗ, 2006 г. 100
Закон Российской Федерации № 5485–1, 1993 г. 102
Федеральный закон № 98-ФЗ, 2004 г. 103
Федеральный закон № 63-ФЗ, 2011 г. 105
Федеральный закон № 152-ФЗ, 2006 г. 108
Лирическое отступление: О критике закона «О персональных данных» 112
Иные Федеральные законы 117
Указы Президента РФ и акты федеральных органов власти 122
Концептуальные документы 122
Общие вопросы обеспечения безопасности информации 127
Безопасность информации при обработке персональных данных 135
Безопасность информации при оказании госуслуг 142
Безопасность информации в национальной платежной системе 146
Кто регулирует отношения в сфере безопасности информации 150
Федеральное собрание (Государственная Дума, Совет Федерации) 150
Президент Российской Федерации 151
Совет безопасности Российской Федерации 151
Правительство Российской Федерации 152
ФСТЭК России 153
ФСБ России 155
Роскомнадзор 157
Банк России 158

Заказать книгу на сайте издательства Медиа Группы «АВАНГАРД»

Преступление и наказание ... 158
Превентивно-репрессивная защита интересов субъектов ... 159
Постфактум-репрессивная защита интересов субъектов ... 162
Роль доказательной базы ... 164
О стандартах, спецификациях и «Best Practices» ... 167
Сухой остаток: для тех, у кого мало времени ... 171

Об институте тайн и безопасности: одна или много? ... 174

Тайна в «бытовом» понимании и в юридическом смысле ... 174
Состав тайн и их взаимосвязь (классификация) ... 176
Государственные секреты ... 177
Тайна частной жизни ... 179
Профессиональная тайна ... 182
Коммерческая тайна ... 185
И все-таки: одна или несколько? ... 189
Статус информационных ресурсов и режим защиты ... 192
Режим тайны ... 192
Роль обладателя ... 195
Особенности государственных информационных систем ... 198
О субъектах правоотношений ... 200
Категории субъектов правоотношений ... 201
Российская Федерация ... 203
Государственные органы ... 203
Субъекты Российской Федерации ... 205
Государственные унитарные предприятия и учреждения ... 207
Должностные лица и сотрудники государственных органов ... 208
Юридические и физические лица ... 208
Сухой остаток: для тех, у кого мало времени ... 209

Последний аккорд ... 212

I постулат. Защищаем информацию ... 213
II постулат. Процедура — все, тайна — ничто ... 213
III постулат. Обладатель — важнейший субъект ... 214
IV постулат. Идеальное в материальном ... 214
V постулат. Целое равно частному ... 215
VI постулат. Надо учитывать конфликт интересов ... 215

ГЛАВА II. ТЕОРЕТИЧЕСКАЯ ... 216

О роли терминов: основа взаимопонимания ... 216

Зри в корень ... 217
Источники терминологии ... 217
Лирическое отступление: следуя духу и букве закона ... 219
О сокращениях и аббревиатурах ... 222
Начало начал: политика безопасности информации ... 223
Лирическое отступление: лингвистика и безопасность ... 223
Теперь о сути политики безопасности информации ... 225
Называем вещи своими именами ... 227
Как правильно: Безопасность информации или Информационная безопасность? ... 227
Не путаться в трех соснах: информационная
или автоматизированная система, объект информатизации ... 232
Вирусы и вредоносные программы ... 237
Аудит и контроль ... 241
Лирическое отступление о том, чего нет: операторы и обработчики ... 243
Сухой остаток: для тех, у кого мало времени ... 249

Заказать книгу на сайте издательства Медиа Группы «АВАНГАРД»

Начинаем ваять 252
Что будем защищать 252
Ревизуем информационные ресурсы 252
Критерии ревизии информации 253
Ревизия информационных технологий 255
Так кто же «vis-à-vis»? 256
Угрозы безопасности информации 257
Реализация угрозы или как это происходит 263
Источники угроз 264
Уязвимости (факторы) 265
Методы реализации 268
Вспомогательные технические средства: уязвимости или источники? 271
Модель угроз: что это такое? 272
Лирическое отступление: чем модель нарушителя отличается от модели угроз 275
От концепции «изолированной среды» к концепции «доверенной среды» 277
Парадигма концепции доверенной среды 279
Локализация информационных ресурсов 283
Счетность субъектов информационных отношений и объектов защиты 284
Доверенность конфигурации и настроек
программного обеспечения и технических средств 285
Подконтрольность действий и документированность событий 286
Принципы построения защиты информации 286
Как организовать защиту 290
Состав системы обеспечения безопасности информации 290
Организационная база 295
Лирическое отступление: «Who is who?» 297
Исполнительный механизм 300
Механизм поддержки 306
Управление безопасностью информации 308
Сухой остаток: для тех, у кого мало времени 312

Копаем глубже 316
Организационная база (архитектура компонент) 316
Компонента «Политика» 316
Компонента «Персонал» 323
Исполнительный механизм (архитектура компонент) 328
Компонента «Техническая» 329
Компонента «Программно-аппаратная» 330
Механизм поддержки (архитектура компонент) 335
Сухой остаток: для тех, у кого мало времени 337

Мысли мудрого читателя о сказанном 339
VII постулат. Плясать надо от печки 341
VIII постулат. Основа — доверенная среда 341
Мысли мудрого читателя о сказанном 341
IX постулат. Система защиты подобна слоеному пирогу 342
X постулат. Система защиты должна быть индифферентной 342

ГЛАВА III. ПРАКТИЧЕСКАЯ 343

Порядок действий 343
Этапность, или с чего начать 344
Step by step или следуем ГОСТу 344
А так ли нужна концепция? 347
Лирическое отступление: об обследовании и ревизии 349
Ищем подрядчика 352

Заказать книгу на сайте издательства Медиа Группы «АВАНГАРД»

Формируем требования ... 355
Как определить актуальные угрозы ... 356
Какие методы парирования угроз применимы ... 357
Взаимосвязь: модель угроз — требования ... 361
Определяем базовый уровень защищенности ... 363
Очень важное замечание: необходимые и достаточные требования ... 365
Общие требования к системе защиты информации ... 367
Особенности использования технологий виртуализации ... 369
Особенности использования криптографических средств ... 372
Сухой остаток: для тех, у кого мало времени ... 376

Локализуем информационные ресурсы ... 380

Правила деления ... 380
Вдоль или поперек ... 381
Виртуально или реально ... 382
Типы сегментов ... 383
Закрытые сегменты ... 384
Открытые сегменты ... 384
Буферные сегменты ... 385
Удаленные сегменты ... 386
Правила сопряжения ... 387
Правила доступа пользователей ... 389
Интернет: три задачи, три подхода ... 390
Общие правила подключения к Интернету ... 392
Решение транспортной задачи ... 393
Решение портальной задачи ... 395
Решение информационной задачи ... 396
Сухой остаток: для тех, у кого мало времени ... 399

Решаем частные задачи ... 402

Защищаемся от вирусов ... 402
Как распространяются вирусы ... 403
Концепция многорубежной защиты ... 405
Первый рубеж обороны ... 407
Второй рубеж обороны ... 407
Третий рубеж обороны ... 408
Профилактика заражения или организационные меры ... 408
Коротко о программно-аппаратных средствах защиты ... 410
Защищаем периметр системы ... 410
Межсетевое экранирование ... 411
Обнаружение и предотвращение вторжений ... 415
Контролируем содержимое ... 416
Организуем доступ и наделяем правами ... 419
Управляем учетными записями ... 419
Наделяем полномочиями субъектов ... 422
Идентифицируем и аутентифицируем ... 424
Контролируем выдачу печатных форм ... 428
Управляем безопасностью ... 430
Когда надо управлять ... 431
Чем надо управлять ... 432
Три кита управления безопасностью ... 434
Обеспечиваем резервное копирование ... 435
Копирование одно, подходы — разные ... 436
Какие методы резервного копирования бывают ... 437
Правила резервного копирования ... 438
Храним резервные копии ... 442

Заказать книгу на сайте издательства Медиа Группы «АВАНГАРД»

Организуем эксплуатацию . . . 444
Какая эксплуатация бывает . . . 445
Тестовая эксплуатация . . . 445
Опытная эксплуатация . . . 446
Нормальная (штатная) эксплуатация . . . 447
Сухой остаток: для тех, у кого мало времени . . . 449

ГЛАВА IV. ПРАГМАТИЧЕСКАЯ . . . 454

Персональные данные — это важно для всех! . . . 455

Для кого закон не писан . . . 456
Личные нужды . . . 456
Архивы . . . 457
Суды и судейские . . . 458
Какие персональные данные бывают . . . 459
Идентификационные персональные данные . . . 459
Биометрические персональные данные . . . 464
Общедоступные персональные данные . . . 472
Обезличивание данных . . . 474
О роли согласия . . . 477
А что нам скажет великий и могучий? . . . 478
А как на это смотрит закон? . . . 479
А в чем прагматизм? . . . 480
Трансграничная передача персональных данных . . . 481
Что влияет на организацию трансграничной передачи данных . . . 482
Адекватно — это как? . . . 484
Как избавиться от сомнений . . . 486
Аутсорсинг обработки персональных данных . . . 489
Почему это стало возможным . . . 491
Как строить отношения с аутсорсером . . . 492
Что включать в договор с аутсорсером . . . 493
О проверках регулятора . . . 494
Какие бывают проверки . . . 495
Какие документы надо готовить . . . 497
Коротко о технических проверках . . . 498

Технологии облачных вычислений — это что-то новенькое! . . . 500

Какие облака бывают . . . 501
Проблемы безопасности в «облаках» . . . 503
Нормативно-правовые проблемы . . . 504
Технологические проблемы . . . 506
Доверенная среда облачных вычислений . . . 509
Концепция «доверенного облака»: триединая задача . . . 509
Доверие к провайдеру — через сегрегацию информации пользователя . . . 512
Система доверенного контроля целостности . . . 513
Система контролируемого пользователем шифрования . . . 514
Что включать в SLA . . . 515
Суммируя сказанное . . . 519

Коротко о разном . . . 521

О перлюстрации, конституционных правах и коммерческой тайне . . . 521
Суть спорной ситуации . . . 521
А была ли тайна? . . . 522
А было ли преступление? . . . 524
А была ли законность? . . . 525
А нужно ли согласие? . . . 526

Заказать книгу на сайте издательства Медиа Группы «АВАНГАРД»

О сертификации: добро или зло? . . . 527
Зачем она нужна? . . . 528
Так ли она хороша? . . . 529
Кому она нужна? . . . 532
Учимся правильно читать сертификат . . . 536
Заметки на полях: о качестве и «глюкавости» . . . 539
Суммируя сказанное . . . 542
Как обмениваться секретами . . . 543
Кому обязаны предоставить информацию . . . 544
Какую информацию обязаны предоставлять . . . 545
Об обязанностях соблюдать конфиденциальность . . . 548
Об ответственности и возмещении убытков . . . 550
Суммируя сказанное . . . 553

ВМЕСТО ЗАКЛЮЧЕНИЯ . . . 555

ПРИЛОЖЕНИЯ . . . 558

Приложение 1. Перечень основных нормативных правовых актов в сфере обеспечения безопасности информации . . . 558
Международные нормативные правовые акты . . . 558
Федеральные Конституционные законы . . . 558
Федеральные законы . . . 558
Федеральные законы, ограничивающие доступ к информации и императивно предписывающие обеспечение ее конфиденциальности (режим тайны) . . . 559
Указы и распоряжения Президента Российской Федерации . . . 560
Распоряжения Правительства Российской Федерации . . . 560
Постановления Правительства Российской Федерации . . . 561
Нормативные и методические документы федеральных органов государственной власти . . . 562
Нормативные и методические документы Банка России . . . 563
Приложение 2. Перечень национальных стандартов в области обеспечения безопасности информации (на декабрь 2012 г.) . . . 564
Национальные стандарты на базе международных стандартов . . . 564
Национальные стандарты . . . 565
Некоторые международные стандарты . . . 566
Планируемые к разработке национальные стандарты на базе международных стандартов (ТК 362) . . . 567
Планируемые к разработке национальные стандарты (ТК 362) . . . 567
Приложение 3. Основные термины и определения в области информационной безопасности (краткий тезаурус) . . . 568
Общие понятия . . . 568
Общие понятия (виды тайн) . . . 573
Общие понятия (объекты) . . . 574
Общие понятия (субъекты) . . . 575
Общие понятия (организация защиты) . . . 576
Виды и способы защиты информации . . . 576
Воздействие на информацию . . . 578
Доступ к информации . . . 578
Оценка соответствия . . . 579
Государственная тайна . . . 581
Коммерческая тайна . . . 581
Персональные данные . . . 582
Электронная подпись . . . 583
Средства защиты информации . . . 583
Угрозы и уязвимости . . . 584

Заказать книгу на сайте издательства Медиа Группы «АВАНГАРД»

Приложение 4. Примерный рекомендуемый перечень организационно-распорядительных документов, которые необходимо разработать при формировании политики обеспечения безопасности информации 587
Документы оперативного уровня 587
Документы исполнительского уровня 587
Приложение 5. Функции, которые должны быть реализованы функциональными контурами исполнительного механизма 588
Контур поддержки доверенной среды (ПДС) 588
Контур идентификации и аутентификации субъектов (ИАС) 590
Контур контроля и управления доступом субъектов (КДС) 592
Контур защиты потоков информации (ЗПИ) 593
Контур регистрации и аудита событий (РАС) 594
Контур управления безопасностью информации (УБИ) 596
Приложение 6. Типовое содержание работ на стадиях создания системы обеспечения безопасности информации 597
Приложение 7. Рейтинг крупнейших компаний, предоставляющих услуги в области безопасности информации 600
Приложение 8. Содержание основных методов парирования угроз безопасности информации 601
Правовые методы 601
Экономические методы 601
Организационные методы 601
Инженерно-технические методы 602
Технические методы 602
Программно-аппаратные методы 602
Приложение 9. Состав средств защиты информации и требования по их размещению на элементах информационных систем 605
Требования, обеспечивающие физический подуровень защиты 605
Требования, обеспечивающие технологический подуровень защиты 605
Требования, обеспечивающие пользовательский подуровень защиты 605
Требования, обеспечивающие сетевой (локальный) подуровень защиты 606
Требования, обеспечивающие канальный подуровень защиты 606
Приложение 10. Краткие сведения о методах обнаружения и распространения вирусов и вредоносных программ 608
Сканирование 608
Эвристический анализ 608
Обнаружение изменений 608
Приложение 11. Соотношение уровней защищенности персональных данных, классов защищенности государственных информационных систем и классов защищенности средств защиты информации 609
Соотношение уровней защищенности персональных данных, установленных Постановлением Правительства РФ от 01.11.2012 г. № 1119 и классов защищенности средств защиты информации, установленных руководящими документами ФСТЭК России 609
Соотношение уровней защищенности персональных данных, установленных Постановлением Правительства РФ от 01.11.2012 г. № 1119 и классов защищенности государственных информационных систем, предназначенных для обработки персональных данных (Приказ ФСТЭК России от 11.02.2013 № 17) 610
Соотношение классов защищенности государственных информационных систем, установленных Приказом ФСТЭК от 11.02.2013 № 17 и классов защищенности средств защиты информации, установленных руководящими документами ФСТЭК России 611
Приложение 12. Справочные материалы для оценки адекватности защиты интересов субъектов при трансграничной передаче персональных данных 612
Перечень государств, в которых действуют законы, регулирующие порядок защиты неприкосновенности частной жизни и персональных данных 612

Заказать книгу на сайте издательства Медиа Группы «АВАНГАРД»

Перечень государств, имеющих специальные государственные структуры, осуществляющие надзор за обработкой персональных данных и защиту интересов субъектов . . . 613
Перечень иностранных государств, не являющихся сторонами Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных и обеспечивающих адекватную защиту прав субъектов персональных данных . . . 613
Перечень государств, ратифицировавших Конвенцию Совета Европы о защите физических лиц в отношении автоматизированной обработки данных личного характера (ETS № 108) . . . 614
Приложение 13. Справочные материалы для подготовки оператора к проверке регуляторами выполнения требований по организации обработки персональных данных . . . 616
Контрольные сроки, определенные Регламентом проверок, о которых нельзя забывать . . . 616
Перечень вопросов проверки юридических лиц и индивидуальных предпринимателей по соблюдению законодательства РФ в области персональных данных . . . 616
Приложение 14. Дополнительные требования, предъявляемые ФСТЭК России при использовании среды виртуализации для обработки конфиденциальной информации . . . 624
Состав компонент виртуальной инфраструктуры, к которым предъявляются требования . . . 624
Базовый набор мер защиты виртуальной среды для соответствующего класса защищенности государственных информационных систем . . . 625
Приложение 15. Классификация и содержание угроз безопасности информации, обрабатываемой с использованием технологий облачных вычислений . . . 626
Угрозы безопасности информации для потребителей облачных услуг . . . 626
Угрозы безопасности информации для поставщиков облачных услуг . . . 627
Угрозы безопасности информации,применительно к моделям предоставления облачных сервисов . . . 629
Приложение 16. Правила выбора мер защиты информации для их реализации в системе обеспечения безопасности информации . . . 631
Общий порядок действий по выбору мер защиты информации . . . 632
Определение базового набора мер защиты информации . . . 632
Адаптация базового набора мер . . . 632
Уточнение адаптированного набора мер . . . 633
Дополнение уточненного адаптированного набора мер . . . 633
Библиография . . . 634
Литература «по теме» . . . 634
Литература не «по теме», но «в тему» (упоминания в книге) . . . 637
Словари и энциклопедии . . . 637

Заказать книгу на сайте издательства Медиа Группы «АВАНГАРД»