

Пярин В. А., Кузьмин А. С., Смирнов С. Н.

) Безопасность электронного бизнеса / Под ред. действительного члена РАЕН д.т.н., проф. *В. А. Минаева*. — М.: Гелиос АРВ, 2002. — 432 с., ил.

Предисловие.....	3
Часть I. Введение.....	13
Глава 1. Объективные предпосылки возникновения электронного бизнеса и угрозы его функционированию.....	15
§ 1. Изменение инфраструктуры субъектов экономической деятельности и информационное обеспечение бизнеса.....	17
§ 2. Структурные изменения потребительской базы.....	21
§ 3. Нормативная база и электронный бизнес.	23
§ 4. Технологические решения электронного бизнеса.	26
Глава 2. Безопасность электронного бизнеса ...	29
§ 1. Оформление договоров в электронном виде.....	33
§ 2. Работа с клиентами.....	35
§ 3. Доставка товаров и услуг.....	37
§ 4. Расчетная система.....	39
§ 5. Управление предприятием.....	42
§ 6. Кредитование организаций и предприятий.....	44
§ 7. Технологическая основа для производства продукции и услуг в сфере обработки и передачи информации.....	45

§ 8. Система безопасности электронного бизнеса.....	48
§ 9. Страхование информационных рисков.....	49

Часть II. Основы электронного бизнеса.....51

Глава 1. Основные понятия электронного бизнеса.....53

§ 1. Основные способы формирования цепочек добавления потребительской стоимости в киберпространстве.....	57
§ 2. Компоненты бизнес-решения в сфере электронного бизнеса.....	60
2.1. Предпринимательское решение.....	62
2.2. Содержательное решение.....	65
2.3. Управленческое решение.....	66
2.4. Технологическое решение.....	68
§ 3. Уровни интеграции электронного бизнеса.....	70
§ 4. Методы повышения потребительской ценности товаров и услуг в электронном бизнесе.....	75

Глава 2. Основные модели электронного бизнеса.....79

§ 1. Электронная реклама.....	84
§ 2. Электронная торговля.....	86
§ 3. Информационные услуги.....	96
§ 4. Электронное здравоохранение.....	98
§ 5. Управление взаимоотношениями с клиентами.....	101
§ 6. Электронное управление закупками.....	105
§ 7. Электронные аукционы.....	110

§ 8. Электронные биржи.....	112
§ 9. Порталы.....	117
Часть III. Информационные технологии электронного бизнеса.....	121
Глава 1. Информационная инфраструктура электронного бизнеса.....	123
§ 1. Источники и потребители данных	129
§ 2. Информационные серверы и универсальные клиенты.....	136
§ 3. Сетевой транспорт. Адресация.....	142
3.1. Отображение локальных адресов на IP-адреса: протоколы АКР иКАКР.....	144
3.2. Отображение символьных адресов на IP-адреса: служба БК8.....	147
3.3. Автоматизация процесса назначения IP-адресов узлам сети: протокол БНСР.....	149
§ 4. Форма представления информации.....	151
4.1. Протокол передачи гипертексто- вых данных.....	152
4.2. Универсальный локатор ресурса ...	153
§ 5. Методы интеграции в информационную инфраструктуру серверов баз данных	155
5.1. Интеграция универсального кли- ента с сервером баз данных.....	155
5.2. Интеграция информационных структур предприятия с информационным сервером.....	157

Глава 2. Платежные системы электронного бизнеса.....	159
§ 1. Электронные платежные системы.....	161
1.1. Эмитенты и эквайеры.....	163
1.2. Платежная система.....	164
1.3. Кредитные и дебетовые платежные системы.....	167
§ 2. Магнитные и микропроцессорные пластиковые карты.....	168
2.1. Виды пластиковых карт.....	171
2.2. Смарт-карты.....	175
2.3. Соотношение стоимость/эффективность.....	178
2.4. РОЗ-терминалы.....	180
§ 3. Принципы создания платежных систем на микропроцессорных картах.....	182
3.1. Эволюция платежных систем.....	182
3.2. Электронные наличные деньги.....	186
3.3. Принципы построения платежных систем на микропроцессорных картах.....	189
§ 4. Технологические основы и технические средства создания платежных систем.....	194
4.1. Организация оплаты с использо- ванием кредитной карты.....	199
4.2. Эффективность организации платежных систем на базе пласти- ковых карт.....	213
4.3. Платежные системы с предвари- тельной авторизацией.....	215
4.4. Платежные системы для микроплатежей.....	220
4.5. Перспективы электронных платежных систем.....	225
§ 5. Стандарты электронных расчетов.....	229

5.1. Протокол 88Б.....	229
5.2. Протокол 3ЕТ.....	232
5.3. Расширения протокола 8ЕТ.....	238
5.4. Универсальный формат электронного кошелька.....	241
5.5. Новые стандарты электронных расчетов.....	244

Часть IV. Безопасность электронного бизнеса.....247

Глава 1. Технологии защиты информации.....249

§ 1. Обеспечение конфиденциальности информации.....	252
1.1. Понятие шифра.....	253
1.2. Об оценке качества криптографической защиты.....	256
§ 2. Контроль целостности информации.....	258
2.1. Понятие хеширования.....	260
2.2. Ключевые и бесключевые функции хеширования.....	262
§ 3. Аутентификация информации.....	264
3.1. Понятие аутентификации.....	265
3.2. Способы аутентификации информации.....	267
§ 4. Идентификация.....	268
4.1. Понятие протокола идентификации.....	270
4.2. Пароли.....	271
4.3. Идентификация типа «запрос-ответ».....	274
4.4. Протоколы с нулевым разглашением.....	276
§ 5. Электронная цифровая подпись.....	277

5.1. Понятие электронной цифровой подписи.....	278
5.2. Особенности инфраструктуры открытых ключей для цифровой подписи.....	280
5.3. Основные подходы к созданию схем цифровой подписи.....	281
5.4. Примеры алгоритмов цифровой подписи.....	283
5.5. Российский стандарт электронной цифровой подписи (ГОСТ Р 34.10-2001).....	285
5.6. Федеральный закон «Об электронной цифровой подписи».....	289
§ 6. Управление ключами.....	291
§ 7. Инфраструктура открытых ключей.....	300
7.1. Понятие инфраструктуры открытых ключей.....	302
7.1.1. Сертификаты открытых ключей.....	302
7.1.2. Центр сертификации открытых ключей.....	302
7.1.3. Система управления сертификатами.....	303
7.2. Федеральная инфраструктура открытых ключей.....	304
7.2.1. Компоненты ФИОК.....	305
7.2.2. Структура ФИОК.....	307
7.2.3. Нормативное обеспечение ФИОК.....	311
7.2.4. Требования по информационной безопасности ФИОК ..	312
§ 8. Страхование информационных рисков ..	313

8.1. Влияние свойств информации на страхование информационных рисков.....	315
8.2. Страхование информационных рисков.....	317
8.3. Проблемы современной законодательной базы в отношении страхования информационных рисков.....	320
8.4. О системе обязательного страхования информационных рисков.....	323

Глава 2. Методы и средства обеспечения безопасности программных систем ...325

§ 1. Основные требования обеспечения безопасности данных в программных системах.....	328
§ 2. Средства и методы защиты данных прикладного программного обеспечения.....	329
2.1. Ключевая система и ключевые носители.....	332
2.2. Контроль целостности программного обеспечения.....	334
§ 3. Технологии, используемые в СУБД для идентификации и подтверждения подлинности.....	336
§ 4. Методы и средства обеспечения информационной безопасности распределенных баз данных.....	339
4.1. Анализ включающей инфраструктуры.....	340
4.2. Статические средства разграничения доступа.....	343
4.2.1. Привилегии.....	343

4.2.2. Представления (y/e/y).....	346
4.2.3. Роли	347
4.3. Динамические средства	
разграничения доступа.....	348
4.3.1. Триггер и пользовательские процедуры.....	348
4.3.2. Типы данных, определяемые пользователями.	350
4.4. Средства аудита.....	350
4.5. Управление загрузкой системы.	352
Заключение.....	353
Приложение.....	359
П. 1. Алгоритм шифрования данных (ГОСТ 28147-89).....	361
П.2. Алгоритм формирования и проверки электронной цифровой подписи.....	364
П.2.1. Математические понятия.....	365
П.2.2. Параметры цифровой подписи.....	367
П.2.3. Формирование цифровой подписи —	369
П.2.4. Проверка цифровой подписи.....	370
П.3. Формат электронного сертификата X.509 версии 3.....	374
П.4. Нормативные акты.....	387
П.5. Некоторые международные стандарты в области магнитных и интеллектуальных карт.....	408
П.6. Словарь терминов.....	411
Список литературы.	421
Содержание.	423