

ЗМІСТ

Вступ	7
Розділ 1. Загальні положення	9
1.1. Вступ до технології захисту інформації	9
1.2. Стан захисту інформації в Україні	11
1.3. Потенційні загрози	12
1.3.1. Доступ до інформації через термінали захищеної системи	14
1.3.2. Отримання пароля на основі помилок адміністратора та користувачів	15
1.3.3. Отримання пароля на основі помилок у реалізації	16
1.4. Соціальна психологія та отримання конфіденційної інформації	17
1.5. Принципи забезпечення інформаційної безпеки	21
1.6. Комплексний підхід до забезпечення інформаційної безпеки	24
1.6.1. Законодавчі (правові) заходи	24
1.6.2. Морально-етичні заходи	28
1.6.3. Організаційні (адміністративні) заходи	29
1.6.4. Технічні заходи	31
1.6.5. Програмні засоби	31
1.7. Державний стандарт із захисту інформації в Україні	31
1.8. Інформаційне та правове забезпечення електронних видань в Україні	39
1.9. Вирішувані завдання з огляду на потенційні загрози	43
Питання для самоперевірки	44
Розділ 2. Стандарти інформаційної безпеки	45
2.1. Критерії оцінки комп'ютерних систем	45
2.1.1. Критерії оцінки надійних комп'ютерних систем	45
2.1.2. «Європейські критерії»	49
2.1.3. «Федеральні критерії» безпеки інформаційних технологій	50
2.1.4. «Єдині критерії безпеки інформаційних технологій»	52
2.1.5. Стандарт Open Web Application Security Project (OWASP)	55
2.2. Політика безпеки та розмежування доступу	62
2.2.1. Дискреційне розмежування доступу	65
2.2.2. Мандатне розмежування доступу	67
2.2.3. Управління доступом на основі ролей	69
2.2.4. Контроль доступу на основі атрибутів	72
2.2.5. Політики безпеки контролю цілісності інформаційних ресурсів	75
2.3. Стандартизація у сфері захисту інформації	80
2.3.1. Принципи архітектури безпеки ISO 7498-2	80
2.3.2. Принципи архітектури безпеки DoD (Department Of Defense)	83

2.3.3. Принципи архітектури безпеки Internet IETF (Internet Engineering Task Force)	86
Питання для самоперевірки	98
Розділ 3. Перевірка справжності користувачів	90
3.1. Поняття ідентифікації, автентифікації та авторизації	90
3.2. Парольні системи ідентифікації та автентифікації користувачів	92
3.2.1. Однобічна парольна ідентифікація / автентифікація	94
3.2.2. Двобічна парольна ідентифікація / автентифікація	96
3.2.3. Одноразові паролі	100
3.3. Хешування паролів	105
3.3.1. Способи зламу хешованих значень	106
3.3.2. Способи мінімізації зламу хешованих значень	108
3.3.3. Поняття стретчингу, технології обходу	112
3.4. Програмна автентифікація	112
3.4.1. Автентифікація з поданням цифрового сертифіката	112
3.4.2. Автентифікація за допомогою Cookies	115
3.4.3. Автентифікація на основі токенів	118
3.4.4. Стандарти OAuth 2.0 та OpenID Connect	121
3.4.5. Децентралізована автентифікація	125
3.5. Апаратна автентифікація	131
3.5.1. Контактні смарт-карти з інтерфейсом ISO 7816	132
3.5.2. Контактні смарт-карти з USB-інтерфейсом	135
3.5.3. Безконтактні смарт-карти	136
3.6. Протоколи ідентифікації з нульовим передаванням знань	138
Питання для самоперевірки	142
Розділ 4. Методи захисту програмного забезпечення	143
4.1. Вступ до захисту програмного забезпечення	143
4.2. Засоби захисту програмного забезпечення	144
4.3. Методологія та інструменти аналізу програм	147
4.4. Структура захищеної програми	149
4.5. Захист від дизасемблювання	152
4.5.1. Шифрування коду	153
4.5.2. Модифікація заголовка виконавчого файлу	155
4.5.3. Захист програм шляхом обфускації	157
4.5.4. Поняття недосяжного, мертвого та надлишкового коду	160
4.6. Методи захисту від копіювання	164
4.6.1. Криптографічні методи	164
4.6.2. Апаратний захист	168
4.6.3. DRM (Digital Rights Management)	170
4.6.4. Динамічні способи зняття захисту програм від копіювання	171
4.7. Захист із використанням електронних ключів-токенів	173

4.7.1. Типи захисту програмного забезпечення з допомогою ключів.....	175
4.7.2. Робота з платформою Sentinel LDK	176
4.7.3. Методи компрометації захисту електронних ключів	180
4.8. Стандарт Universal 2nd Factor	182
Питання для самоперевірки	187
Розділ 5. Біометричні методи ідентифікації.....	188
5.1. Вступ до біометрії	188
5.2. Параметри систем біометричної ідентифікації.....	190
5.3. Біометрична ідентифікація за відбитками пальців	192
5.3.1. Підходи до автоматичної класифікації	193
5.3.2. Оптичні пристрої отримання відбитків пальців.....	195
5.3.3. Напівпровідникові пристрої отримання відбитків пальців.....	197
5.3.4. Ультразвукові пристрої отримання відбитків пальців	199
5.3.5. Обмеження технології розпізнавання за відбитками пальців.....	201
5.4. Біометрична ідентифікація за геометрією руки.....	202
5.5. Біометрична ідентифікація за венами руки.....	204
5.6. Біометрична ідентифікація за параметрами вуха	205
5.7. Біометрична ідентифікація на основі райдужної оболонки ока	207
5.8. Біометрична ідентифікація за серцевим ритмом	209
5.9. Біометрична ідентифікація за параметрами обличчя	211
5.9.1. Двовимірна ідентифікація за параметрами обличчя.....	211
5.9.2. Тривимірна ідентифікація за параметрами обличчя.....	214
5.9.3. Ідентифікація обличчя за тепловізійним зображенням.....	216
5.10. Динамічні методи біометричної ідентифікації	218
5.11. Біометрична ідентифікація за допомогою голосу	218
5.11.1. Фізіологічні та артикуляційні ознаки	219
5.11.2. Методи та механізми голосової ідентифікації.....	220
5.11.3. Алгоритм голосової ідентифікації	221
5.11.4. Перспективи та особливості використання	223
5.12. Біометрична ідентифікація за рукописним підписом	223
5.13. Біометрична ідентифікація за клавіатурним почерком	225
5.14. Перспективні методи біометричної ідентифікації.....	226
Питання для самоперевірки	219
Розділ 6. Мережева безпека.....	230
6.1. Вступ до мережевої безпеки	230
6.2. Проксі-сервери.....	231
6.3. Міжмережевий екран (фаєрвол, брандмауер).....	233
6.3.1. Класифікація міжмережевих екранів залежно від рівня OSI.....	234
6.3.2. Функції міжмережевих екранів	237
6.3.3. Принципи побудови оточення міжмережевого екрану	239
6.3.4. Схеми під'єднання міжмережевих екранів	240

6.3.5. Варіанти готових рішень	245
6.4. Системи виявлення та запобігання вторгнень.....	248
6.4.1. Системи виявлення вторгнень	249
6.4.2. Системи запобігання вторгнень	254
6.4.3. Типові представники систем виявлення та запобігання вторгнень	255
6.5. Віртуальні приватні мережі.....	257
6.5.1. Концепція побудови захищених віртуальних приватних мереж	257
6.5.2.Тунелювання інформації	259
6.5.3. Класифікація VPN-мереж за рівнем моделі OSI.....	261
6.5.4. Класифікація VPN за архітектурою технічного рішення	264
6.6. Захист безпроводних мереж.....	267
6.6.1. Протокол WEP (Wired Equivalent Privacy)	269
6.6.2. Протокол WPA (Wi-Fi Protected Access)	271
6.6.3. Наявні технології та рішення	273
Питання для самоперевірки.....	276
Глосарій термінів	277
Перелік тестових питань	291
Список літератури	311