

# Оглавление

От авторов .....	3
Введение .....	5
<b>ГЛАВА 1. Структурные компоненты сети GSM/GPRS как объекты защиты от НСД.</b> .....	<b>11</b>
1.1. Сетевая инфраструктура GSM/GPRS .....	11
1.1.1. Структура сети сотовой подвижной связи стандарта GSM для реализации речевых услуг .....	11
1.1.2. Расширение базовой конфигурации сети GSM/GPRS .....	14
1.1.3. Интерфейсы сетей GSM/GPRS .....	16
1.1.4. Канальное кодирование в сетях связи стандарта GSM .....	19
1.2. Эволюция сетей СПС ОП к сетям 3G .....	21
1.3. Абонентские терминалы и абонентский радиointерфейс. ....	23
1.4. Биллинговая система .....	26
1.5. Цифровая транспортная сеть .....	30
1.5.1. Технологии xDSL .....	30
1.5.2. Беспроводный доступ с использованием PPL .....	32
1.5.3. Цифровые системы передачи ВОЛС .....	32
1.5.4. Спутниковые системы связи .....	33
1.6. WAP-платформа .....	34
1.6.1. Мобильный доступ к сети Интернет .....	34
1.6.2. Стек протоколов WAP .....	35
1.6.3. Спецификация приложений беспроводного доступа (WAE) .....	36
1.7. SMS-платформа .....	38
1.8. MMS-платформа .....	41
1.9. Pre-paid-платформа .....	44
1.10. WEB-платформы .....	47
1.11. Карточная платформа оплаты услуг .....	48
1.12. Элементы конвергентных решений .....	49
1.12.1. Гибридная сеть GPRS/WLAN (Wi-Fi) .....	49
1.12.2. Сеть FMC (Fixed-Mobile Convergence) .....	53
1.13. Корпоративная телекоммуникационная сеть и информацион- ные ресурсы предприятия-оператора .....	56
Выводы .....	59
<b>ГЛАВА 2. Анализ методов и алгоритмов обеспечения инфор- мационной безопасности в сетях СПС ОП стандарта GSM/ GPRS</b> .....	<b>61</b>
2.1. Механизмы защиты от НСД, предусмотренные стандартом GSM/GPRS .....	61
2.1.1. Механизмы аутентификации .....	61

2.1.2. Секретность передачи данных .....	62
2.1.3. Обеспечение секретности абонента .....	63
2.1.4. Обеспечение секретности в процедуре корректировки местоположения .....	63
2.1.5. Общий состав секретной информации и ее распределение в аппаратных средствах GSM .....	64
2.1.6. Обеспечение секретности при обмене сообщениями между HLR, VLR и MSC .....	65
2.1.7. Модуль подлинности абонента .....	66
2.1.8. Механизмы защиты от НСД в сети передачи данных GPRS .....	67
2.2. Эволюция механизмов защиты от НСД, реализованных в сетях СПС стандарта GSM .....	69
2.3. Анализ уязвимости механизмов защиты от НСД, предусмотренных стандартом GSM .....	72
2.3.1. Уязвимости механизма аутентификации абонента .....	72
2.3.2. Уязвимости алгоритмов шифрования информации .....	73
2.3.3. Анализ уязвимости механизма использования TMSI .....	74
2.3.4. Уязвимости технологии GPRS .....	77
2.4. Обобщение перечня угроз информационной безопасности сети СПС стандарта GSM/GPRS .....	78
Выводы .....	82
<b>ГЛАВА 3. Методические рекомендации для разработки концепции информационной безопасности компании – оператора сети СПС .....</b>	<b>84</b>
3.1. Классификация концепций информационной безопасности ..	85
3.2. Выбор типа концепции информационной безопасности для компании – оператора сети СПС .....	87
3.3. Составные части концепции информационной безопасности .	88
3.4. Этапы разработки концепции информационной безопасности	89
3.5. Жизненный цикл концепции информационной безопасности .	91
3.6. Пример концепции информационной безопасности .....	94
Выводы .....	94
Приложение к главе 3. Типовые разделы концепции информационной безопасности .....	95
<b>ГЛАВА 4. Методические рекомендации по разработке организационно-режимных процессов защиты информации в компаниях – операторах услуг подвижной связи на сетях СПС стандарта GSM .....</b>	<b>110</b>
4.1. Требования к разработке организационно-режимных процессов защиты информации .....	111
4.2. Перечень основных организационно-режимных процессов по обеспечению информационной безопасности в компаниях – операторах сети СПС стандарта GSM.....	114
4.3. Организационно-режимные процессы по обеспечению информационной безопасности от угроз «конкурентной разведки» .	117
4.4. Организационно-режимные процессы по противодействию «легальному» съему информации .....	118

4.5. Система сбора данных для расследования инцидентов нарушения информационной безопасности .....	119
4.6. Организационно-режимные аспекты политики информационной безопасности .....	120
4.7. Организационно-режимный аспект в программе управления информационной безопасностью .....	121
4.8. Управление персоналом — составная часть организационно-режимных процессов по обеспечению информационной безопасности .....	121
4.9. Организационно-режимные процессы по планированию восстановления информационной безопасности .....	122
4.10. Контроль и мотивация сотрудников — составная часть организационно-режимных процессов по защите информации .....	123
4.11. Обучение персонала информационной безопасности .....	124
<b>ГЛАВА 5. Рекомендации по нормативному обеспечению мероприятий в области информационной безопасности в компаниях – операторах сетей СПС стандарта GSM .....</b>	<b>126</b>
5.1. Анализ нормативного обеспечения информационной безопасности в РФ .....	127
5.1.1. Законодательный уровень и общедоказательный уровень .....	127
5.1.2. Уровень нормативных документов министерств и ведомств .....	130
5.1.3. Нормативные документы коммерческих компаний .....	131
5.2. Типовой состав нормативной документации по обеспечению информационной безопасности .....	134
5.2.1. Общая структура документации .....	134
5.2.2. Характеристика отдельных документов .....	136
5.3. Анализ деятельности операторской компании по обоснованию состава документов для обеспечения информационной безопасности .....	140
5.3.1. Типовые процессы, требующие нормативного обеспечения .....	140
5.3.2. Процессы, специфические для компании – оператора сети СПС .....	140
5.4. Уточненный перечень нормативных документов по информационной безопасности для компании – оператора сети СПС ..	142
Выводы .....	144
Приложение к главе 5 .....	145
<b>ГЛАВА 6. Рекомендации по обеспечению защиты от НСД средств и сооружений связи в сетях СПС стандарта GSM ..</b>	<b>157</b>
6.1. Общие принципы построения систем защиты объектов связи ..	159
6.1.1. Специфика защиты сетей и сооружений связи .....	159
6.1.2. Классификация методик для построения систем защиты объектов связи от НСД .....	160
6.1.3. Использование интегрального метода для построения системы защиты объекта связи от НСД .....	161
6.2. Подсистемы, входящие в систему комплексной защиты объектов связи .....	164
6.3. Технические средства, используемые для физической защиты объектов связи .....	168

6.4. Методика применения интегрального подхода к построению системы защиты объектов связи от НСД .....	173
6.4.1. Обследование объекта .....	173
6.4.2. Построение модели угроз и модели нарушителя .....	176
6.4.3. Решение по защите объекта .....	177
6.4.4. Общая схема разработки ИСБ для объекта связи .....	179
6.5. Взаимосвязь системы защиты объектов связи от НСД с действиями внутренних нарушителей .....	180
6.5.1. Категорирование внутреннего нарушителя .....	181
6.5.2. Внедрение и интеграция системы контроля и учета материальных ценностей в систему физической защиты предприятия .....	182
Выводы .....	182
<b>ГЛАВА 7. Рекомендации по использованию алгоритмов шифрования и аутентификации в сетях СПС стандарта GSM ...</b>	<b>186</b>
7.1. Общее описание характеристик безопасности в стандарте GSM	187
7.2. Возможные последствия использования ненадежных алгоритмов шифрования .....	189
7.2.1. Клонирование SIM-карт .....	190
7.2.2. Перехват трафика .....	191
7.3. Рекомендации Международной ассоциации GSM .....	193
7.3.1. Рекомендации по использованию алгоритмов A3 и A8 .....	194
7.3.2. Рекомендации по использованию алгоритма A5 .....	194
7.4. Перечень алгоритмов защиты, используемых в сетях СПС стандарта GSM .....	195
7.4.1. Краткая характеристика алгоритмов .....	196
7.4.2. Возможность использования алгоритмов .....	200
7.5. Перспективные алгоритмы .....	202
7.5.1. Алгоритм A5/3 .....	202
7.5.2. Алгоритмы спецификации G-Milenage .....	203
7.6. Атаки на алгоритмы со стороны злоумышленника .....	203
7.6.1. Эфирные атаки .....	203
7.6.2. Атаки с доступом к терминалу .....	204
7.6.3. Атаки с доступом к SIM-карте .....	204
7.7. Рекомендации по использованию встроенных алгоритмов шифрования и аутентификации .....	205
7.7.1. Рекомендации Международной ассоциации GSM .....	205
7.7.2. Дополнительные рекомендации по использованию алгоритмов A3 и A8 .....	206
7.8. Рекомендации по использованию дополнительных алгоритмов шифрования и аутентификации .....	207
Выводы .....	208
<b>ГЛАВА 8. Разработка методических рекомендаций по борьбе с рисками НСД .....</b>	<b>211</b>
8.1. Взаимосвязь традиционных рисков и рисков НСД .....	212
8.2. Типы рисков .....	215

8.2.1. Риски НСД и классификация рисков .....	215
8.2.2. Финансовые риски .....	216
8.2.3. Юридические риски .....	217
8.2.4. Технологические риски .....	217
8.2.5. Имиджевые риски .....	218
8.2.6. Прочие риски .....	218
8.3. Взаимосвязь рисков .....	118
8.3.1. Взаимосвязь между различными видами финансовых рисков ..	219
8.3.2. Взаимосвязь между различными типами рисков. Риски НСД как катализатор рисков .....	219
8.4. Модели рисков .....	220
8.5. Выбор модели рисков для операторской компании сети СПС стандарта GSM с учетом оценки рисков НСД .....	220
8.6. Содержание управления рисками .....	221
8.7. Система управления рисками .....	222
8.7.1. Понятие системы управления рисками .....	222
8.7.2. Планирование управления рисками .....	224
8.7.3. Идентификация рисков .....	224
8.7.4. Оценка рисков .....	224
8.7.5. Планирование реагирования на риски .....	226
8.7.6. Мониторинг и контроль .....	227
8.7.7. Современные методы управления рисками НСД .....	228
8.7.8. Использование системы на основе Business Unit Management ..	229
8.7.9. Практические рекомендации по управлению рисками НСД и генерируемыми ими рисками .....	231
Выводы .....	233
<b>ГЛАВА 9. Механизмы информационной безопасности в системах широкополосной связи WI-MAX и WI-FI.....</b>	<b>235</b>
9.1. Общие сведения о Wi-MAX .....	236
9.2. Физический уровень IEEE 802.16 (Wi-MAX) .....	237
9.3. Сетевой уровень безопасности IEEE 802.16 (Wi-MAX) .....	241
9.3.1. Шифрование пакетов данных .....	242
9.3.2. Протокол управления ключами .....	242
9.3.3. Ассоциация безопасности (Security Associations) .....	243
9.3.4. Назначение соответствия соединений SA .....	244
9.3.5. Криптографический инструментарий .....	244
9.3.6. Аутентификация СП и обмен авторизованным ключом .....	244
9.3.7. Передача ключей шифрования пакетов с данными .....	246
9.3.8. Выбор средств безопасности .....	247
9.3.9. Механизм управления авторизацией .....	248
9.3.10. Механизм управления КШД .....	248
9.4. Безопасность беспроводных локальных сетей стандарта 802.11	248
Выводы .....	250
<b>ГЛАВА 10. Модель защиты СЕТИ GSM от НСД с учетом методов борьбы с мошенничеством .....</b>	<b>252</b>

10.1. Определение и классификация мошенничества (фрода) в сетях СПС .....	252
10.1.1. Определение мошенничества .....	252
10.1.2. Классификация мошенничества .....	253
10.2. Методы обнаружения и предотвращения мошенничества (фрода) в сетях СПС стандарта GSM .....	258
10.2.1. Методы обнаружения мошенничества Post Factum (Post call) ...	258
10.2.2. Методы обнаружения мошенничеств непосредственно в момент их совершения .....	259
10.2.3. Использование автоматизированных систем обнаружения фрода	260
10.3. Методы предотвращения мошенничества .....	262
10.3.1. Законодательные методы .....	262
10.3.2. Организационные методы .....	263
10.4. Формальные модели защиты от НСД .....	266
10.4.1. Модели предоставления прав .....	266
10.4.2. Множественно-графовые математические модели обеспечения безопасности .....	267
10.4.3. Информационные и вероятностные модели .....	268
10.4.4. Модель на основе анализа угроз, выявления нарушения безопасности и обнаружения атак .....	269
10.4.5. Сравнительный анализ моделей защиты их достоинств и недостатков .....	271
10.5. Модель защиты сети GSM от НСД с учетом методов борьбы с мошенничеством .....	275
10.5.1. Концептуальный уровень: взаимосвязь угроз, объектов и субъектов информационной безопасности, действий злоумышленника и атак .....	275
10.5.2. Функциональный уровень (уровень функциональных систем сети GSM) .....	278
10.5.3. Компонентный уровень (уровень отдельных компонентов сети GSM) .....	282
Выводы .....	285

## **ГЛАВА 11. Методологические рекомендации по проведению аудита информационной безопасности компании – оператора сети GSM .....**

293

11.1. Цели и задачи аудита информационной безопасности .....	295
11.1.1. Задачи, решаемые при проведении аудита информационной безопасности .....	295
11.1.2. Цели аудита информационной безопасности .....	296
11.1.3. Понятие контролируемых параметров .....	298
11.1.4. Внешний контроль параметров .....	299
11.1.5. Соотношение параметров информационной безопасности при внешнем контроле и аудите .....	300
11.2. Классификация видов аудита информационной безопасности	301
11.2.1. Пассивный аудит .....	301
11.2.2. Активный аудит .....	305
11.2.3. Экспертный аудит .....	307

11.2.4. Аудит на соответствие стандартам .....	308
11.3. Мероприятия по аудиту информационной безопасности .....	310
11.3.1. Инициирование процедуры аудита .....	311
11.3.2. Сбор исходных данных .....	311
11.3.3. Анализ данных аудита .....	315
11.3.4. Использование методов анализа рисков .....	316
11.3.5. Оценка соответствия требованиям стандарта .....	317
11.3.6. Выработка рекомендаций .....	317
11.3.7. Подготовка отчетных документов .....	318
11.4. Жизненный цикл услуг информационной безопасности .....	318
11.4.1. Уровень безопасности .....	318
11.4.2. Уровень безопасности и время жизни системы .....	319
11.4.3. Окно безопасности .....	320
11.4.4. Задачи аудита в терминах окна безопасности .....	321
Выводы .....	325
<b>ГЛАВА 12. Примеры программных и аппаратных средств за- щиты информации в сетях СПС .....</b>	<b>326</b>
12.1. Обзор программных продуктов, предназначенных для анализа и управления рисками .....	326
12.1.1. Метод GRAMM .....	326
12.1.2. Метод RiskWatch .....	329
12.1.3. Система COBRA .....	330
12.1.4. Программный продукт Buddy System .....	330
12.2. Технические средства, используемые для физической защиты объектов сотовой подвижной связи .....	330
12.2.1. Средства контроля доступа .....	331
12.2.2. Замки .....	331
12.2.3. Автоматизированные системы контроля доступа .....	332
12.2.4. Средства сигнализации .....	335
12.2.5. Средства наблюдения .....	336
12.2.6. Оборудование пункта централизованного наблюдения .....	337
12.3. Система контроля и управления доступа помещений на объекте оператора СПС .....	338
12.4. Биометрические методы защиты абонентских терминалов по- движной связи .....	342
Выводы .....	347
Список сокращений .....	349