

The background of the entire image is a high-contrast, black and white photograph of a massive explosion. A bright, glowing white core of fire and smoke is at the center, with numerous sharp, white streaks radiating outwards in all directions, creating a sense of intense energy and movement. The overall effect is one of a powerful, chaotic event.

Андрей Сажин

**Записки телеграфиста
спецсвязи. Невидимый
фронт Чечни.**

Андрей Сажин

**Записки телеграфиста спецсвязи.
Невидимый фронт Чечни.**

«Автор»

2026

Сажин А.

Записки телеграфиста спецсвязи. Невидимый фронт Чечни. /
А. Сажин — «Автор», 2026

«Я не герой. Я не брал "языков", не командовал ротой, не закрывал амбразуру. Я сидел в палатке в аэропорту Грозного, набирал телеграммы, чинил кабели зубами и топил буржуйку. Это книга о спецсвязи в Чечне. О тех, кто обеспечивал ту самую "кнопку", по которой командиры отдавали приказы. О победах и потерях, о дружбе и предательстве, о технике и человеческой глупости. Без героического пафоса. Без пропаганды. Без вранья».

© Сажин А., 2026

© Автор, 2026

Содержание

«Мирный воин: Спецсвязь 46 ОБРОН в аэропорту Грозный. 2000-2001»	6
Записки телеграфиста СПС. 353-й отдельный батальон связи, в/ч 6784	6
Аннотация	7
Краткая аннотация (для обложки)	9
СОДЕРЖАНИЕ	10
«Мирный воин: Спецсвязь 46 ОБРОН в аэропорту Грозный. 2000-2001»	10
Записки телеграфиста СПС. 353-й отдельный батальон связи, в/ч 6784	10
Введение	10
Часть 1. Что такое СПС	10
Часть 2. СПС в бою	11
Часть 3. Вместо послесловия	12
Приложения	13
ВВЕДЕНИЕ	14
От автора (техническое примечание)	16
ГЛАВА 1	17
«Свои» и «чужие» в эфире	17
Проблема, которую нельзя было игнорировать	17
Немного истории: как немцы слушали наших	18
Афганистан: японские рации на базарах	18
Первая чеченская: шок и прозрение	19
Вторая чеченская: игра на опережение	19
«Эй, русские! Сдавайтесь!»	20
Почему это важно для нашей книги	20
ГЛАВА 2	21
Разговор, который никто не должен слышать	21
Обычная связь: как её перехватывают	21
Что такое «закрытая связь»	22
Аналоговые ЗАС: «Гранит» и его предки	22
Цифровые ЗАС: «Акведук» и «Арбалет»	23
Скорость vs защита: вечный компромисс	23
«Криптошлюз»: что внутри АРМ	23
«Тапик» и «полёвка»: ручная работа	24
Зачем всё это знать	24
Послесловие к главе: один эпизод	25
ГЛАВА 3	26
Кто пользуется СПС? От президента до рядового	26
Первый уровень: президент и его «Чегет»	26
Второй уровень: правительственная связь	27
Третий уровень: военная спецсвязь (Минобороны)	27
Четвёртый уровень: спецсвязь ФСБ	28
Пятый уровень: батальоны и полки (наша работа)	28

Шестой уровень: тупик. Почему солдаты не пользуются СПС	29
Одна история о неравенстве	29
Что я хотел сказать этой главой	29
ГЛАВА 4	31
Почему эта книга — не учебник	31
Техника как судьба	31
Что вы найдёте в этой книге	31
Чего в этой книге нет	32
Как читать эту книгу	33
Одна история, которая всё объясняет	33
ГЛАВА 5	34
Шифрование: «секретно», «совершенно секретно», «особой важности»	34
Как всё начиналось: советская система секретности	34
Три группы допуска: 3, 2, 1	34
Моя третья группа: как это было	35
Что означают грифы на практике	36
Журналы, подписи, ответственность	36
Одна история о забытом полковнике	37
Послесловие к главе	37
ГЛАВА 6	39
Аналоговая эпоха: «Гранит» и его предки	39
Как работали аналоговые скремблеры	39
Почему «Гранит» был уязвим	39
«Гранит» в моей практике	40
Что было до «Гранита»	40
Почему аналоговые системы дожили до 2000-х	41
Одна история о «Граните»	41
Что осталось от аналоговой эпохи	42
Конец ознакомительного фрагмента.	43

Андрей Сажин
Записки телеграфиста спецсвязи.
Невидимый фронт Чечни.

**«Мирный воин: Спецсвязь 46 ОБРОН
в аэропорту Грозный. 2000-2001»**

**Записки телеграфиста СПС. 353-
й отдельный батальон связи, в/ч 6784**

Аннотация

О чём эта книга

Это не учебник по спецсвязи. Не мемуары генерала. Не героическая эпопея.

Это — окопная правда. Рассказ рядового телеграфиста специальной правительственной связи (СПС) о том, как он служил в Чечне в 2000–2001 годах. Без прикрас, без лжи, без попытки «сохранить лицо».

Вы узнаете:

Как устроена СПС — от аналоговых «крякалок» до цифровых АРМ с криптошлюзами.

Кто пользовался спецсвязью — от президента до рядового телеграфиста.

Как работали связисты в ППД аэропорта «Северный» — суточные дежурства, телеграммы, обрывы кабеля, борьба со вшами и грязью.

Чем отличалась связь боевиков («Моторолы») от нашей СПС — скорость против защиты, тактика против стратегии.

Как боевики перехватывали наши переговоры и вклинивались в эфир с ложными приказами.

Какие технические и человеческие проблемы преследовали нас — устаревшая техника, нехватка запчастей, алкоголь, показуха, небоевые потери.

Кто был рядом — Дэн, Петля, Андрей Петухов, контрабасы, офицеры Некрасов, Зверев, Голодяков, замполит-казак, капитан с узла связи.

Что мы видели — перестрелку у ворот, трупы в вертолёте, президентскую охрану, которая едва не нажала на курок.

Что мы чувствовали — страх, усталость, горечь от несправедливости, радость от салюта из трассеров в новогоднюю ночь.

Что изменилось за 20 лет — и что осталось тем же.

Для кого эта книга

Для тех, кто служил в спецсвязи — вы узнаете себя, своих сослуживцев, свою войну.

Для тех, кто интересуется историей Второй чеченской кампании — вы увидите её с неожиданной стороны.

Для тех, кто хочет понять, что такое СПС на самом деле — без секретности, но с полным погружением.

Для тех, кто просто любит читать правду о войне — без героического пафоса, без пропаганды, без «интернет-экспертов».

Почему стоит прочитать

Потому что это — единственная книга о спецсвязи в Чечне, написанная не историком и не журналистом, а рядовым телеграфистом. Тем, кто сидел на «Пеленге», принимал телеграммы, чинил кабель зубами и топил буржуйку.

Потому что это — правда. Иногда неудобная, иногда страшная, иногда смешная, но — правда.

Потому что это — память. О тех, кто не вернулся. О тех, кто вернулся другим. О тех, кто остался в горах, в госпиталях, в цинковых гробах.

Цитаты из книги

«Я не герой. Я не совершал подвигов. Я просто делал свою работу — иногда плохо, иногда хорошо, иногда спустя рукава, иногда на пределе сил. Как все».

«Когда я перемахнул через забор, то сразу попал в руки местного патруля».

«БТРы. Ими оказались бельевые вши».

«Вдруг загорается индикатор "Входящие". Срочная телеграмма из Ханкалы. Гриф — "Совершенно секретно"».

«Носилки. Двое. Накрытые окровавленными простынями. Я сел рядом. Смотрел на них. Думал: "Там — ребята. Такие же, как я. Тоже ждали дембеля. Тоже хотели домой. Не доехали"».

Об авторе

Андрей Сажин — рядовой телеграфист специальной правительственной связи (СПС), служил в отдельном батальоне связи (в/ч 6784) 46-й отдельной бригады оперативного назначения внутренних войск МВД России в 2000–2001 годах. Участник контртеррористической операции на Северном Кавказе. Награждён овсяным печеньем за 3-е место в конкурсе военных песен. Живёт в Ноябрьске. Пишет правду.

Краткая аннотация (для обложки)

«Я не герой. Я не брал "языков", не командовал ротой, не закрывал амбразуру. Я сидел в палатке в аэропорту Грозного, набирал телеграммы, чинил кабели зубами и топил буржуйку. Это книга о спецсвязи в Чечне. О тех, кто обеспечивал ту самую "кнопку", по которой командиры отдавали приказы. О победах и потерях, о дружбе и предательстве, о технике и человеческой глупости. Без героического пафоса. Без пропаганды. Без вранья».

СОДЕРЖАНИЕ

«Мирный воин: Спецсвязь 46 ОБРОН в аэропорту Грозный. 2000-2001»

Записки телеграфиста СПС. 353- й отдельный батальон связи, в/ч 6784

Введение

Часть 1. Что такое СПС

№

Название главы

1

«Свои» и «чужие» в эфире

2

Разговор, который никто не должен слышать

3

Кто пользуется СПС? От президента до рядового

4

Почему эта книга — не учебник

5

Шифрование: «секретно», «совершенно секретно», «особой важности»

6

Аналоговая эпоха: «Гранит» и его предки

7

Цифровая эпоха: «Акведук», «Арбалет»

8

ЛТА и РТА: телеграф, который не взломать

9

АРМ: компьютер в спецсвязи

10

УПС: невидимый герой

11

Каналы связи СПС: провод, радио, тропосфера, спутник

12

Боевое дежурство: сутки на узле

13

Как становятся связистами

14

Допуск: разговор с майором из ФСБ

15

Быт связиста в ППД

16

Линейщики: работа на проводе

17

Телеграфисты: «летать как пчёлке»

18

Офицеры СПС: между долгом и солдатами

Часть 2. СПС в бою

№

Название главы

19

Боевики и их связь: «Моторолы» на каждый карман

20

Радиоперехват как оружие

21

Сравнение: связь боевиков и СПС федералов

22

Технические проблемы СПС в Чечне

23

Человеческие проблемы: алкоголь, небрежность, показуха

24

Отдельный батальон связи: структура и задачи

25

ППД аэропорт «Северный»: палатки, стройка, обстрелы

26

Узел «Пеленг»: будни телеграфиста

27

Сослуживцы: Дэн, Петля, Андрей Петухов

28

ЧП у ворот: перестрелка между своими

29

Президентская охрана: «Открываю огонь на поражение»

30

Ошибка в телеграмме: забытый полковник

31

Небоевые потери: трагедии, которых могло не быть

32

Новый год в Чечне: салют из трассеров

33

Выход из ворот: трупы в вертолёте

Часть 3. Вместо послесловия

№

Название главы

34

Уроки для будущего

Приложения

№

Название

1

Словарь терминов СПС

ВВЕДЕНИЕ

Эта книга — о невидимом фронте.

О нём не снимают фильмов. В новостях о нём не говорят. Солдаты этого фронта не ходят в атаку с криками «Ура!», их портреты не печатают на первых полосах газет. О них вспоминают только тогда, когда связь пропадает. И тут же забывают, когда она появляется снова.

Они — связисты специальной правительственной связи. СПС.

Те, кто обеспечивает ту самую «кнопку», по которой президент разговаривает с командармом. Те, кто передаёт приказы, от которых зависят тысячи жизней. Те, кто сидит в душных палатках под обстрелами, чинит кабель зубами, потому что пассатижи — одни на всех, и тот, кому они достались, пьёт чай где-то в другом месте.

Их работа — скучная, монотонная, нервная. Но без неё армия слепнет и глохнет.

Я пишу эту книгу не как историк и не как журналист. У меня нет учёной степени по военному делу и доступа к закрытым архивам. Я пишу как человек, который сам сидел на боевом дежурстве в узле связи «Пеленг» в аэропорту «Северный» города Грозного в 2000–2001 году. Рядовой телеграфист отдельного батальона связи (воинская часть 6784) 46-й отдельной бригады оперативного назначения внутренних войск МВД России.

Я бегал по ППД с катушками полевого кабеля, потом набивал телеграммы на ленточном аппарате ЛТА, потом — на автоматизированном рабочем месте (АРМ), потом топил буржуйку в офицерской палатке, потому что кто-то ошибся в телеграмме, а виноватым назначили меня.

Я был свидетелем, как офицер расстрелял свой наряд. Видел, как контрактник играл с гранатой и остался без хозяйства. Видел, как сослуживца чуть не убил снайпер — зажёг сигарету на посту, и пуля прилетела в бронежилет. Видел трупы в вертолёте, когда летел на дембель. И сам стоял перед стволом автомата президентской охраны за то, что пошёл не той дорогой.

Всё это — правда. Не приукрашенная, иногда глупая, иногда страшная, иногда смешная. Армейская правда.

Но эта книга — не только мои воспоминания.

Я хочу рассказать о том, что такое специальная правительственная связь вообще. Как она устроена. Кто ею пользуется. Какая техника работает. Как шифруют голос и данные. Почему телеграф был важнее телефона. Почему одна ошибка в телеграмме могла стоить карьеры, а иногда и жизни.

Я хочу объяснить, почему во Вторую чеченскую кампанию боевики говорили по «Моторолам» мгновенно, но беззащитно, а федеральные силы передавали приказы по СПС медленно, но надёжно. Кто выигрывал в тактике, а кто — в стратегии. И почему без СПС победа была бы невозможна.

Я буду рассказывать о людях. О связистах, которые таскали катушки под обстрелами. О телеграфистах, которые засыпали над клавиатурой. О линейщиках, которые чинили обрывы полевого осколком стекла, вместо нажа, а иногда и зубами. О командирах, которые прикрывали солдат — и о тех, кто их подставлял.

Без них — без нас — не было бы связи. Без связи — не было бы победы.

Эта книга — не учебник.

В ней нет формул, чертежей и секретных данных. Я не буду писать актуальные частоты, коды и протоколы шифрования — во-первых, потому что не знаю (моя группа допуска была только «секретно», а не «совершенно секретно»), а во-вторых, потому что это до сих пор охраняется законом.

Но я расскажу достаточно, чтобы вы поняли: как это работает, насколько это сложно и насколько это важно.

Книга построена так, что её можно читать с любой главы. Хотите узнать про шифрование — глава 5. Про боевиков и их «Моторолы» — глава 19. Про Андрея Петухова, который в 14 лет вытолкнул снайпершу из окна — глава 27. Про то, как автор чуть не погиб от руки президентской охраны — глава 29.

Но если читать подряд — вы пройдёте путь от азов спецсвязи до окопов Чечни, от теории до практики, от спокойных учебных классов до палаток под артобстрелом.

Я не герой. Я не совершал подвигов. Я просто делал свою работу — иногда плохо, иногда хорошо, иногда спустя рукава, иногда на пределе сил. Как все.

Но я вернулся. И теперь, спустя больше двадцати пяти лет, я хочу рассказать о том, что видел, что делал и что понял.

О невидимом фронте специальной правительственной связи.

Андрей Сажин
г. Ноябрьск
2026 год

От автора (техническое примечание)

В книге использованы реальные имена сослуживцев, реальные названия воинских частей (по состоянию на 2000–2001 годы) и реальные события, которые я зафиксировал в памяти и письмах домой.

Некоторые фамилии офицеров изменены по этическим соображениям — время стёрло точные имена, а выдумывать я не хочу. Но все ключевые эпизоды — правда. Даже те, в которые трудно поверить.

Технические описания аппаратуры проверены по открытым источникам (руководства по эксплуатации, отраслевые журналы «Связист», мемуары других ветеранов). Там, где моя память расходится с документами, я указываю это в примечаниях.

Фотографии, использованные в книге, — из моего личного архива, из архива сослуживца Юры Агеева, а также из открытых источников (с указанием авторства, где это возможно).

ГЛАВА 1

«Свои» и «чужие» в эфире

Ночь. Где-то в Чечне. Блокпост федеральных сил.

Солдат в бронежилете и каске сидит у радиостанции. Наушники на голове, микрофон у губ. В эфире — шипение, треск, обрывки чужих переговоров. Вдруг сквозь помехи прорывается голос. Чёткий, спокойный, с лёгким кавказским акцентом, но почти без акцента:

— «Волга»? Я — «Грозный». Приём.

Солдат настораживается. Позывные чужие. Не наши.

— «Волга» на связи. Кто вызывает?

— Свои, свои. У нас тут обстановка. Докладываю: в квадрате три-семь-ноль-два замечено движение. Человек пятнадцать, вооружены. Идут с юга на север. Похоже, готовят прорыв.

Солдат лихорадочно соображает. Квадрат три-семь-ноль-два — это как раз их сектор. Но откуда доклад? Разведка должна была выйти на связь через час. И позывные не те. И голос... голос знакомый, но не свой.

— Уточните, кто докладывает. Назовите код.

— Код? — в голосе лёгкая заминка. — Код «Буран». Приём.

Кода «Буран» не существует. Солдат холодеет. Он понимает: в эфире — чужой.

— Вас понял. Работаем. Конец связи.

Он отключается и тут же набирает другой канал. Прямой, закрытый. Докладывает дежурному офицеру: в эфире обозначился боевик. Назвал наш квадрат. Сказал, что идут пятнадцать человек с юга на север.

Через полчаса по тому же квадрату бьёт артиллерия. Своих там нет. Боевики, если они действительно были, уходят или остаются лежать в воронках.

А через час тот же голос возвращается:

— «Волга»! Почему вы стреляли? Там же были свои! Мы не успели отойти! У нас потери!

Солдат молчит. Он уже знает: в эфире — враг. Враг, который говорит на чистом русском, знает военную терминологию, угадывает позывные и пытается заставить федералов бить по своим.

Но не выходит.

Эта история — не из моего дневника. Я не был тем солдатом у рации. Я сидел в узле спецсвязи, где такие голоса не проходили. Но эту историю мне рассказывали разведчики, которые слышали такое своими ушами. И не один раз.

Вторая чеченская кампания стала войной не только пуль и снарядов. Она стала войной голосов. Войной эфира. Войной за то, кто кого услышит первым, кто кого обманет, кто кому прикажет.

Проблема, которую нельзя было игнорировать

Представьте себе, что вы — командир роты. У вас в подчинении сто двадцать человек. Где-то в горах, в лесу, в разрушенном городе засел противник. Вы должны координировать движение своих групп, вызывать огонь артиллерии, запрашивать подкрепление.

И всё, что вы говорите в рацию, может услышать враг.

Не просто услышать — записать, проанализировать, понять ваш замысел. А потом — ударить первым. Или, что ещё хуже, вклиниться в эфир и отдать вашему взводу ложный приказ: «Отходите!», «Ложись!», «Вас обходят с тыла!».

Паника, хаос, свои убивают своих.

Это не фантастика. Так работала радиосвязь в Первую чеченскую кампанию. Так работала она и во Вторую — там, где не было СПС.

Немного истории: как немцы слушали наших

Радиоперехват — ровесник радио. Как только появилась возможность передавать сигнал без проводов, сразу же нашлись желающие его перехватить.

В Первую мировую войну радиостанции были громоздкими и маломощными. Перехватывали в основном телеграфные сообщения (азбука Морзе). Немцы регулярно слушали русские радиogramмы, и наоборот.

Но настоящий расцвет радиоперехвата пришёлся на Вторую мировую.

Немецкая служба радиоперехвата (называлась она, если по-немецки, Funkaufklärung — «радиоразведка») работала блестяще. Они прослушивали советские переговоры на всех уровнях — от штабов армий до полков. И не просто слушали, а анализировали, накапливали базы данных по голосам командиров, по позывным, по стилю речи.

Бывали случаи, когда немецкие радисты вклинивались в советский эфир и отдавали ложные приказы. Правда, с советскими войсками это проходило реже — у нас была довольно жёсткая дисциплина связи, кодовые таблицы менялись часто. Но на других фронтах, например, в Северной Африке, англичане таким страдали постоянно.

Главный урок Второй мировой: если твоя связь не защищена — ты воюешь с включённым микрофоном, а противник сидит в наушниках и записывает.

Афганистан: японские рации на базарах

В Афганистане (1979–1989) проблема стала ещё острее.

Моджахеды не имели своей радиоэлектронной промышленности. Но они имели деньги — от американцев, от саудитов, от наркотрафика. И на эти деньги они покупали на базарах в Пакистане и Иране портативные радиостанции.

Самые популярные — японские Kenwood и американские Motorola (тогда они ещё не были символом спецсвязи боевиков, но уже были хорошими). Эти рации были лёгкими, надёжными, работали в широком диапазоне частот. И стоили недорого.

Советские войска использовали радиостанции Р-105, Р-123, Р-159 — надёжные, но старые, громоздкие. И главное — почти все переговоры велись открыто. Шифрование было, но аппаратура засекречивания (ЗАС) ставилась только на уровне штаба дивизии и выше. До роты она не доходила.

Моджахеды слушали советские переговоры постоянно. Они знали, когда начнётся арт-подготовка, куда пойдут колонны, где слабые места. И действовали на опережение.

Бывало и хуже. В некоторые рации советских солдат моджахеды встраивали радиозакладки. Микроскопические передатчики, которые работали даже когда рация была выключена. И слушали разговоры в палатках, в штабах, даже в туалетах.

Армия училась. К концу войны в Афганистане ужесточили дисциплину связи, ввели обязательную смену частот, кодовые фразы. Но кардинально проблему не решили.

Потому что для кардинального решения нужна была СПС на каждом узле связи — от штаба армии до отдельного батальона. А это дорого, сложно и требует квалифицированных кадров.

Первая чеченская: шок и прозрение

Когда в декабре 1994 года федеральные силы вошли в Чечню, связь оказалась катастрофической.

Старые радиостанции, отсутствие шифрования, необученные радисты. Боевики, к тому времени, имели на вооружении современные «Моторолы» (серии HT и GP), купленные на чёрном рынке или полученные от зарубежных спонсоров. Они говорили открыто, но быстро. Координация у них была отличная — потому что каждый командир имел рацию в кармане.

Что происходило в эфире, описывали потом многие ветераны.

Боевики слушали переговоры федералов, записывали, анализировали. А иногда — вклинивались.

Я не был в первую чеченскую, но слышал рассказы от тех, кто там был. Один из самых страшных — про колонну, которая шла на помощь окружённому блокпосту. Боевики перехватили переговоры, назвались «своими» и увели колонну в засаду. Погибли почти все.

Командование было в шоке. Как так? Почему противник знает наши планы? Почему он говорит нашим голосом?

Ответ был прост: потому что у нас нет защищённой связи.

Вторая чеченская: игра на опережение

Когда началась Вторая чеченская кампания (август 1999 года — формально, активная фаза до 2001 года), уроки первой были усвоены. Частично.

Связи стало больше. Появились новые радиостанции — например, Р-168 «Акведук» (не путать с одноимённой ЗАС — в армии любили одинаковые названия для разной техники). Появилась спутниковая связь — ограниченно, но появилась. И, главное, начали массово внедрять СПС — специальную правительственную связь.

Что это дало?

Те переговоры, которые велись по СПС, боевики не слышали. Вообще. Шифрование было достаточно стойким. Перехватить зашифрованный сигнал — мало. Его ещё нужно расшифровать. А без ключей — это годы работы самых мощных компьютеров (на тот момент).

Но СПС была не везде. И не для всех.

Солдаты на блокпостах, разведчики в рейдах, экипажи БТРов — они говорили по обычным радиостанциям. Открыто, или с простым кодированием, которое боевики взламывали за минуты.

И в этом эфире продолжалась война голосов.

«Эй, русские! Сдавайтесь!»

У меня самого есть такой эпизод.

В 2000 году, в ППД аэропорта «Северный», я иногда работал на приёмно-передающей аппаратуре (хочется так написать, но на самом деле тянул полевик к палатке разведки). И вот в эфире, между обрывками наших переговоров, вдруг ворвался чужой голос:

— Эй, русские! Сдавайтесь, пока не поздно! Если не сдадитесь, мы вас всех перережем, как баранов!

Голос был уверенный, почти без акцента. Он говорил по-русски лучше многих моих сослуживцев.

Я замер. Рядом сидевший сержант выругался, переключил частоту. Чужой голос пропал.

— Это они, — сказал сержант. — Каждый день так делают. Психологическая атака.

— И часто это срабатывает?

— На новеньких — иногда. Потом привыкают.

Я не привык. Я запомнил этот голос на всю жизнь. Не потому, что испугался. А потому, что осознал: враг не только там, за бетонным забором, с автоматом и гранатой. Враг — ещё и в эфире. И он говорит на твоём языке.

Почему это важно для нашей книги

Весь этот долгий рассказ — не просто исторический экскурс. Он нужен, чтобы вы поняли главное.

Специальная правительственная связь — это не про удобство. И не про секретность ради секретности. СПС — это про то, чтобы ваши приказы дошли до своих, а до чужих — не дошли. Это про то, чтобы враг не узнал ваш замысел. Это про то, чтобы он не смог сказать вашим солдатам: «Отходите, вас обходят», и они не поверили.

В Первую чеченскую такой защиты не было. И это сильно усложняло борьбу с боевиками.

Во Вторую чеченскую — она появилась. Не везде, не полностью, не идеально. Но появилась. И это изменило ход войны.

Как именно — об этом следующие главы.

А пока запомните: когда вы слышите слово «СПС», не думайте о чиновниках в кабинетах. Думайте о солдате, который в наушниках слышит чужой голос и не знает — свой или враг. И о том, кто этот голос отсекает, не даёт ему пройти.

Вот о ком эта книга.

ГЛАВА 2

Разговор, который никто не должен слышать

Представьте себе, что вы идёте по улице и разговариваете с другом. Громко, не стесняясь. О погоде, о работе, о том, что купить на ужин. Вокруг идут люди. Они слышат обрывки вашего разговора. Кому-то всё равно, кто-то невольно подслушивает, кто-то прислушивается специально.

А теперь представьте, что вы обсуждаете не ужин, а военную операцию. Координаты удара. Время атаки. Коды запуска ракет.

И вокруг — не случайные прохожие, а вражеские разведчики. У каждого в ухе наушник, у каждого в руках приёмник. Они не просто «могут» подслушать — они делают это профессионально, круглосуточно, с одной целью: узнать ваш план и помешать ему.

Это — разговор в открытом эфире. Разговор, который слышат все.

СПС — специальная правительственная связь — превращает этот громкий разговор на улице в шёпот в запертой комнате с зашторенными окнами. А потом — в зашифрованную записку, которую везёт запечатанный курьер. А потом — в нечто, что нельзя даже сравнить с обычным разговором, потому что принцип здесь совсем другой.

Давайте разбираться по порядку.

Обычная связь: как её перехватывают

Начнём с простого. Обычная телефонная связь — проводная или сотовая — это аналоговый или цифровой сигнал, который идёт от вас к собеседнику по проводам или по радио.

Если это провод — чтобы перехватить, нужно физически подключиться к линии. Сложно, но можно. В военных условиях — запросто: противник за ночь подключается к вашему кабелю, и наутро вы говорите прямо в его наушники.

Если это радио — ещё проще. Радиосигнал распространяется во все стороны. Любой приёмник, настроенный на ту же частоту, примет ваш разговор. Дальность перехвата может быть больше, чем дальность вашей связи, потому что у разведчика антенна мощнее.

В военных радиостанциях есть режим «скачкообразной перестройки частоты» (ППРЧ) — когда передатчик и приёмник прыгают с частоты на частоту по определённому алгоритму. Перехватчику нужно знать этот алгоритм, иначе он потеряет сигнал. Но в 1990-е годы такие системы были только в дорогой военной технике, а у боевиков и у нас — не всегда.

И даже ППРЧ не спасает от записи: перехватчик может просто записать весь диапазон частот, а потом прокрутить и найти ваш разговор. Это требует мощных компьютеров, но в 2000 году это уже было реально.

Итог: любой разговор по обычной связи — проводной или радио — может быть перехвачен. Вопрос только в ресурсах перехватчика.

Что такое «закрытая связь»

Закрытая связь — это связь, при которой содержание разговора (или данных) недоступно перехватчику.

Обратите внимание: я сказал «содержание», а не «сам факт передачи». Перехватчик может знать, что вы с кем-то говорите. Он может засечь время, продолжительность, направление сигнала. Но что именно вы сказали — нет.

Как это достигается?

Два основных способа: скремблирование и шифрование.

Скремблирование (от английского *scramble* — перемешивать) — это аналоговый метод. Ваш голос разбивается на частотные компоненты, и эти компоненты перемешиваются по определённому закону. На приёме — собираются обратно. Перехватчик слышит бессмысленный шум, похожий на шипение или на «кряканье» (отсюда сленговое название таких аппаратов — «крякалки»).

Проблема скремблирования: оно не очень стойкое. К 1990-м годам существовали методы его взлома, особенно если перехватчик имеет образец чистой речи (например, запись приветствия «Алло, проверка связи»). Некоторые скремблеры взламывались за минуты.

Шифрование — это цифровой метод. Ваш голос оцифровывается (превращается в набор нулей и единиц), а затем эти нули и единицы математически преобразуются по секретному ключу. Без ключа — только перебор. А перебор современных ключей (длиной 128 бит и более) занимает миллиарды лет даже на самых мощных компьютерах.

Шифрование — это надёжно. Но оно требует вычислительной мощности. В 1990-е годы для шифрования голоса в реальном времени нужен был специальный процессор. Такой процессор стоял в аппаратуре ЗАС — засекречивающей аппаратуре связи.

Аналоговые ЗАС: «Гранит» и его предки

Советская промышленность начала разрабатывать аппаратуру засекречивания ещё в 1960-е годы. Первые образцы были громоздкими, капризными, работали только на проводных линиях.

К 1970-м годам появились ЗАС для радиосвязи. Самые массовые — серия «Гранит».

«Гранит» — это аналоговый скремблер. Он работал по принципу инвертирования спектра: высокие частоты становились низкими, низкие — высокими. Если знать алгоритм инвертирования (а он был стандартным для всей серии), взломать «Гранит» мог радиолюбитель с осциллографом.

Тем не менее, «Гранит» стоял на многих узлах связи вплоть до конца 1990-х. Почему? Потому что он был простым, дешёвым и ремонтпригодным. В полевых условиях это важнее стойкости: лучше иметь хоть какую-то защиту, чем никакой.

К 2000 году «Гранит» уже безнадёжно устарел. Но его всё ещё использовали на второстепенных каналах.

Цифровые ЗАС: «Акведук» и «Арбалет»

В середине 1990-х годов на вооружение начала поступать цифровая аппаратура засекречивания. Самая известная серия — «Акведук».

«Акведук» — это уже настоящее шифрование. Голос оцифровывался, шифровался по алгоритму, который в открытой печати не публиковался (и не публикуется до сих пор), и передавался по цифровым каналам связи.

Стойкость «Акведука» была высокой. Настолько высокой, что даже спустя десятилетия нет публичных сообщений о его взломе. Это не значит, что его нельзя взломать — это значит, что ни одна из сторон, которые пытались, не сообщила об успехе.

«Акведук» устанавливался на стационарных узлах связи — в штабах округов, в Генштабе, на крупных узлах в зоне КТО (в Ханкале, например).

Но была проблема: «Акведук» был большим, тяжёлым и требовал квалифицированного обслуживания. Для полевых условий он не годился.

Поэтому для подвижных узлов связи (на КШМ, в палатках) разработали «Арбалет» — полевую версию цифровой ЗАС. Она была компактнее, легче, но чуть менее стойкой (хотя всё равно на порядок лучше «Гранита»).

Вот такой «Арбалет» и стоял на узле связи «Пеленг» в аэропорту «Северный». По крайней мере — должен был стоять. Хватало ли его на всех — большой вопрос. В мемуарах я не упоминаю конкретную модель ЗАС, но по косвенным признакам (работа с АРМ, шифрование телеграмм) — это была цифра, а не аналог.

Скорость vs защита: вечный компромисс

Шифрование — медленное. В 2000 году шифровать голос в реальном времени было уже не проблема: процессоры справлялись. Но шифровать большие объёмы данных (например, телеграммы на несколько страниц) — всё равно требовало времени.

Поэтому в СПС был компромисс.

Речевая связь (по телефону) использовалась только на высшем уровне — президент — командующий, командующий — командарм. Ниже — экономили ресурсы шифрования и использовали телеграф.

Телеграмма — это текст. Текст можно зашифровать, передать, расшифровать. Это медленнее разговора, но надёжнее. И главное — телеграмму можно перечитать, проверить, подписать.

В бою, конечно, хочется говорить. Но если говорить нельзя — пиши. Так работала СПС.

«Криптошлюз»: что внутри АРМ

Когда я работал на АРМ — автоматизированном рабочем месте — я не задумывался, как именно шифруется моя телеграмма. Для меня это была кнопка «Отправить» и ожидание, пока на другой стороне напечатается ответ.

Но устройство АРМ было примерно таким.

Обычный компьютер — в нашем случае, скорее всего, 486-й или Pentium, с DOS (Norton Commander) или Windows 95. Внутри — плата криптошлюза. Это специальный процессор,

который и занимался шифрованием. Плата была съёмной, с защитой от вскрытия (при попытке открыть корпус — стирала ключи).

Когда я набирал телеграмму в текстовом файле и нажимал «Отправить», происходило следующее:

Файл подавался на криптошлюз.

Криптошлюз разбивал его на блоки (обычно по 64 или 128 бит).

Каждый блок шифровался по секретному алгоритму с использованием ключа, который был загружен в аппарат.

Зашифрованные блоки упаковывались в сетевые пакеты (по протоколу, который тоже был секретным) и отправлялись в канал связи.

На принимающей стороне — обратный процесс: приём, распаковка, расшифровка, вывод на печать.

Весь этот процесс занимал от нескольких секунд до минуты — в зависимости от длины телеграммы и загрузки канала.

Ключи шифрования менялись регулярно. В стационарных узлах — должны были раз в сутки. В полевых — реже, потому что достать новый ключ было проблемой. Ключи передавались на бумаге (распечатка длинной цифровой последовательности) или на дискетах, под расписку. Потеря ключа — ЧП уровня «сажают всех».

Я не помню, чтобы мы меняли ключи. Скорее всего, их хватало на неделю или на месяц. Но это уже детали, которые я мог забыть.

«Тапик» и «полёвка»: ручная работа

Не всё в СПС было высокотехнологичным.

Внутри ППД (пункта постоянной дислокации) связь часто была проводной. Простой полевой кабель П-274, в просторечии «полёвка». Две медно-стальные жилы в пластмассовой (не виниловой) оболочке. Тяжело, но надёжно.

К кабелю подключались полевые телефонные аппараты ТА-57 — «тапики». Коробка из прочного пластика, внутри — трубка, сбоку — ручка генератора. Крутишь ручку — вырабатывается электрический импульс, звонок на другом конце. Связь как в старых фильмах: кручу-верчу, говорить хочу.

«Тапик» не давал никакой защиты. Разговор по нему мог перехватить любой, кто подключится к линии. Поэтому по «полёвке» говорили только о несекретных вещах: «пришлите обед», «подгоните грузовик», «дневальный, где ты, чёрт тебя дернул!». Всё секретное — по СПС, через ЗАС и АРМ.

Но «полёвка» рвалась постоянно. Её перерубали лопатой, наматывали на колёса грузовики, использовали как бельевую верёвку. Чинить — линейщикам. Инструмент не выдавали, поэтому осколком стекла, а если его нет — зубами.

Это уже не высокие технологии. Это рутина войны.

Зачем всё это знать

Я задержался на технических деталях не случайно.

Когда я служил, я не задумывался о разнице между «Гранитом» и «Акведуком». Для меня была ЗАС — и всё. Я знал, что если телеграмма шифруется, её не прочтает враг. А как именно — неважно.

Но когда я начал писать эту книгу, я понял: без понимания «как» вы не поймёте «почему».

Почему СПС была медленной? Потому что шифрование требует времени, особенно в 2000 году.

Почему СПС была не везде? Потому что цифровые ЗАС стоили дорого, а аналоговые — не давали полной защиты.

Почему офицеры иногда говорили открыто? Потому что не хватало аппаратуры или они её берегли для важных переговоров.

Почему связь в Чечне всё равно была лучше, чем в Первую кампанию? Потому что появились «Акведук» и «Арбалет», потому что АРМ заменили ЛТА на ответственных направлениях.

Техника определяет тактику. Тактика определяет исход боя. Исход боя определяет ход войны.

Поэтому в этой книге будет много техники. Не перегруженно, не сухо — но будет. Потому что без неё вы не поймёте, что на самом деле происходило в тех палатках, в тех КШМ, на том узле «Пеленг».

Послесловие к главе: один эпизод

Когда я учился на телеграфиста в Екатеринбурге, нас водили в штаб округа — показывать настоящую работу.

Там сидели девушки-телеграфистки. Печатали на ЛТА, перематывали ленты, отправляли в аппарат. Всё быстро, чётко, без суеты.

Я тогда спросил у одной:

— А страшно? Ну, что враг перехватит?

Она посмотрела на меня с лёгкой усмешкой:

— Перехватит — не расшифрует. А расшифрует — не поверит. А поверит — уже будет поздно.

Мне этот ответ показался загадочным. Но теперь я понимаю, что она имела в виду.

Надёжная криптография — это когда враг может иметь ваши зашифрованные сообщения, но не может их прочитать. И даже если каким-то чудом прочитает — к тому времени, как он это сделает, информация уже потеряет актуальность.

Так работает СПС.

ГЛАВА 3

Кто пользуется СПС? От президента до рядового

В предыдущей главе я рассказывал о том, как устроена специальная правительственная связь. О шифровании, о ЗАС, об АРМ и «полёвке». Всё это — техника. Железо. Провода и микросхемы.

Но техника сама по себе не работает. За ней стоят люди. И эти люди — абоненты СПС. Те, кто говорит, кто слушает, кто отдаёт приказы и кто их получает.

Абоненты СПС — это не «все военные». Это строго определённый круг лиц, организованный в жёсткую иерархию. От президента в Кремле до рядового телеграфиста в палатке в Грозном. Между ними — десятки ступеней, сотни узлов связи, тысячи километров кабелей и радиоволн.

Давайте пройдем по этой иерархии сверху вниз. Не как по учебнику — сухо и перечисляя должности. А как по живой цепи, где на каждом уровне свои люди, свои проблемы и свои истории.

Первый уровень: президент и его «Чегет»

На самом верху пирамиды СПС — президент России.

Его связь — самая защищённая, самая надёжная, самая дорогая. О ней говорят «связь особой важности». К ней имеют доступ единицы — не больше десяти человек во всей стране.

Как она устроена?

У президента есть несколько каналов связи. Самый известный — «Чегет». Это не телефон и не рация, а целая система, включающая в себя стационарные узлы в Кремле, в Белом доме, в загородных резиденциях (в Ново-Огарёве, например), а также подвижные узлы — в машинах, в поездах, в самолётах.

«Борт №1» — это не просто самолёт с президентом на борту. Это летающий узел связи. Там есть всё: спутниковая связь (через российские военные спутники), радиорелейная связь (для связи с землёй при взлёте и посадке), КВ-связь (на всякий случай) и, конечно, защищённые каналы через наземные станции.

Шифрование на этом уровне — многоконтурное. Голос шифруется несколько раз разными алгоритмами. Ключи меняются после каждого сеанса связи. Аппаратура — полностью российская, секретная, разработанная в НИИ ФСО. Никто за пределами этой системы не знает, как она работает.

Кто обслуживает эту связь? Офицеры ФСО — Федеральной службы охраны. Не путать с ФСБ. ФСО — отдельная структура, которая занимается охраной высших должностных лиц и их связью. Их подготовка — годы. Их техника — последнее слово. Их режим секретности — абсолютный.

Про одного такого офицера я слышал историю. Он работал на узле связи в Кремле. Однажды ночью, в дежурной смене, зазвонил спецтелефон. Он поднял трубку. Голос сказал: «Соедините с премьер-министром». Офицер выполнил процедуру аутентификации — спросил код. Голос назвал код. Офицер соединил.

Через час пришёл вызов от президента — тоже по спецтелефону. Оказалось, что первый звонок был учебной тревогой — проверка реакции. Офицер всё сделал правильно. Но осадок

остался: а вдруг это был не учебный, а настоящий? И код украден? И премьер на самом деле не тот, за кого себя выдаёт?

В СПС высшего уровня паранойя — часть профессии.

Второй уровень: правительственная связь

Чуть ниже президента — остальное высшее руководство: премьер-министр, главы обеих палат парламента, председатели Конституционного и Верховного судов, генеральный прокурор, руководители ключевых министерств (обороны, иностранных дел, внутренних дел, МЧС).

Их связь тоже защищена, но уже не так «толсто», как президентская. У них нет «борта №1» с тройным шифрованием. Но у каждого есть спецтелефон — в кабинете, в машине, дома.

Эту связь обеспечивает не ФСО, а другая структура — в разное время она называлась по-разному. В СССР — 8-е Главное управление КГБ. В 1990-е — ФАПСИ (Федеральное агентство правительственной связи и информации). С 2003 года — снова в составе ФСО, но как отдельное управление.

Аппаратура на этом уровне — тоже секретная, но менее экзотическая. Используются те же ЗАС, что и в армии — например, «Акведук» в стационарном исполнении. Каналы — в основном проводные (волоконно-оптические, защищённые от прослушки) и спутниковые (через гражданские спутники, но с шифрованием).

Интересная деталь: в 1990-е годы, когда экономика рухнула и денег на связь не хватало, некоторые министры пользовались обычными телефонами. Их, конечно, ругали — но не всегда могли запретить. Потому что альтернативы не было.

К 2000 году эта практика прекратилась. Появились деньги — появилась и нормальная связь.

Третий уровень: военная спецсвязь (Минобороны)

Теперь перейдём к самому массовому сегменту СПС — военной спецсвязи.

Здесь абонентов — тысячи. Штабы военных округов, штабы армий, штабы дивизий, штабы бригад, штабы отдельных полков. У каждого штаба — свой узел связи. Узел — это комната или несколько комнат, где стоят аппаратура ЗАС, АРМ, ЛТА, коммутаторы.

Задачи военной СПС:

Обеспечение связи между вышестоящим штабом и нижестоящими (Генштаб — штаб округа, штаб округа — штаб армии, и так далее).

Передача боевых приказов, донесений, разведданных.

Координация действий разных родов войск.

Связь с союзниками (по отдельным каналам).

В отличие от правительственной связи, военная СПС должна работать в полевых условиях. Поэтому аппаратура — возимая или переносимая. Палатки, КШМ, контейнеры. Дизель-генераторы вместо городской электросети. Полевые кабели вместо волоконной оптики.

И персонал — не офицеры ФСО с десятилетней подготовкой, а срочники (как я) и контрактники (кто постарше). Обучение — недели или месяцы. Качество — разное.

Именно к этому уровню относился наш батальон связи (в/ч 6784) в составе 46-й отдельной бригады оперативного назначения ВВ МВД.

Мы обеспечивали связь между штабом бригады (аэропорт «Северный», Грозный) и вышестоящим штабом в Ханкале. А также внутреннюю связь внутри бригады — между штабом, батальонами, КПП, автопарком.

Нас было человек сорок-пятьдесят срочников и контрактников. Мы не были элитой. Мы были работягами спецсвязи. Но без нас бригада не могла воевать.

Четвёртый уровень: спецсвязь ФСБ

Отдельная история — связь Федеральной службы безопасности.

ФСБ — не военная организация. Формально — гражданская. Но у неё есть свои воинские подразделения (погранвойска, например, тогда ещё были в составе ФСБ). И у неё есть свои оперативные задачи, требующие защищённой связи.

Спецсвязь ФСБ — самая закрытая после президентской. Потому что ФСБ занимается контрразведкой, борьбой с терроризмом, разведкой. Их переговоры — если они станут известны противнику — могут стоить жизни агентам, провалить операции, разрушить сети.

Аппаратура — своя, не похожая на военную. Каналы — часто арендованные у гражданских операторов, но с двойным шифрованием. Персонал — офицеры с допуском «особой важности», многие — с опытом работы за границей.

В Чечне связь ФСБ работала отдельно от военной. У них были свои узлы, свои частоты, свои ключи. С военными они стыковались через специальные узлы сопряжения — обычно в штабе группировки в Ханкале.

Я с ними почти не пересекался. Один раз — тянул кабель в их палатку. Срочники из их палатки оказались «редкими ублюдками», осознали себя выше остальных в ППД, но речь сейчас не об этом.

Пятый уровень: батальоны и полки (наша работа)

Спустимся ещё ниже. К тем, кто непосредственно обеспечивал связь на уровне бригады — и к тем, кто этой связью пользовался.

Кто пользовался СПС на уровне бригады?

Командир бригады (полковник Зубарев, например)

Начальник штаба бригады

Начальники служб (разведка, артиллерия, тыл)

Командиры батальонов (в том числе наш комбат — майор Некрасов)

Они отдавали приказы, получали донесения, запрашивали информацию. Их голоса и телеграммы шли по СПС — зашифрованные, зарегистрированные, проверенные.

Кто эту связь обеспечивал?

Операторы узла связи (телеграфисты) — мы с Петлёй, Дэном, другими ребятами.

Линейщики — те, кто тянул и чинил кабели.

Техники ЗАС — отвечали за шифровальную аппаратуру (их было мало, и они были невидны).

Дежурные офицеры и прапорщики — контролировали смену, несли ответственность.

Мы — не абоненты. Мы — обслуживающий персонал. Мы не говорили по СПС (у нас не было таких прав). Мы только передавали то, что сказали другие. Но без нас они бы не сказали ничего.

Шестой уровень: тупик. Почему солдаты не пользуются СПС

А теперь важный момент. Почему солдаты — рядовые и сержанты — не пользуются СПС?

Потому что СПС — это дорого, сложно и не нужно на уровне взвода-роты.

Солдату в окопе не нужна шифрованная связь. Ему нужно быстро крикнуть в рацию: «Справа, в подвале, двое!» — и услышать ответ: «Понял, работаем». Пока он будет набирать телеграмму на АРМе, шифровать, отправлять — его уже убьют.

Для тактического уровня есть обычная радиосвязь. Открытая, быстрая, мобильная. Да, её перехватывают. Да, её могут заглушить. Но альтернативы нет.

Поэтому СПС — для штабов. Для планирования. Для стратегии. А в окопах — «Моторолы» и «Кенвуды». У нас и у боевиков — одинаковые, только у нас с перепутанными частотами, а у них — настроенные как надо.

Парадокс: мы защищали свои штабы от прослушки — но солдаты на передовой говорили открыто. И боевики это слышали.

Одна история о неравенстве

В нашем батальоне ходила одна байка. Говорили, что в другом батальоне служил парень — Санек из Узбекистана. Контрактник. Он должен был получить допуск к СПС, потому что работал на узле. Но ему не дали. Почему? Потому что он был гражданином Узбекистана (на момент службы — не гражданин РФ, а «лицо без гражданства», если точно, но для ФСБ это было неважно).

Ему сказали: «Ты не можешь работать с секретными документами, потому что ты — иностранец».

Конечно же Санек обиделся. Он служил, рисковал, хотел делать настоящее дело — а его отодвинули в сторону.

В итоге он работал на узле, но не на шифровании, а на вспомогательных задачах — приносил телеграммы, помогал с бумагой, следил за порядком.

Но правила есть правила. Допуск к СПС — это не только проверка твоей биографии. Это проверка твоих родителей, дедушек, бабушек. Всех, кто когда-то жил на территории СССР. Если среди них есть «неблагонадёжные» — всё, доступа нет.

В системе СПС нет демократии. И не может быть.

Что я хотел сказать этой главой

Я хотел показать, что СПС — это не «волшебная трубка», которая есть у всех военных. Это сложная, дорогая, иерархическая система. У неё есть привилегированные пользователи (президент, правительство) и непривилегированные (рядовые связисты, которые эту систему обслуживают). Есть уровни, где связь шифруется максимально, и уровни, где она работает почти открыто.

И каждый уровень — это люди. Со своими заботами, проблемами, радостями.

Президент — о войне.

Командующий — о выполнении приказа.

Командир бригады — о потерях.

Начальник узла связи — о том, чтобы аппаратура не сломалась.

Рядовой телеграфист — о том, чтобы не ошибиться в телеграмме и успеть на ужин.

Мы все — звенья одной цепи. Без одного звена цепь рвётся.

ГЛАВА 4

Почему эта книга — не учебник

Я должен сразу предупредить читателя. Эта книга не научит вас работать на АРМ, не расскажет, как настраивать тропосферную связь, и не даст готовых рецептов «как стать лучшим связистом». Это не учебное пособие для военных кафедр. Это не секретный документ с грифом «Совершенно секретно» и не аналитический доклад для Генштаба.

Это — книга о людях.

О тех, кто сидел в душных палатках под канонаду артобстрела, чинил кабель зубами и засыпал над клавиатурой. О тех, кто ошибался, плакал, злился, смеялся и ждал дембеля. О тех, кто вернулся — и о тех, кто не вернулся.

Техника как судьба

В армии — особенно в такой специфической сфере, как спецсвязь — техника определяет всё. Не характер, не воспитание, не приказы командиров. Техника.

Если у тебя есть АРМ — ты работаешь быстро, чисто, почти без ошибок. Если АРМ сломался — ты садишься за ЛТА и набиваешь телеграммы буква за буквой, и каждый твой палец помнит тяжесть клавиш.

Если у тебя есть ЗАС — твои переговоры не услышит враг. Если ЗАС нет — ты говоришь открыто, и каждый твой приказ может стать достоянием противника.

Если у тебя есть пассатижи — ты чинишь обрыв за пять минут. Если пассатижи у кого-то другого — ты зачищаешь провода осколком стекла или зубами, и это не героизм, а необходимость.

Техника не просто помогает или мешает. Техника формирует твою жизнь. Твои победы и поражения. Твои успехи и провалы.

Поэтому, когда я пишу про ЛТА — я пишу не про железо. Я пишу про усталость. Про то, как болят пальцы после восьмичасовой смены. Про страх ошибиться, когда каждое нажатие клавиши — это чья-то судьба.

Когда я пишу про ЗАС — я пишу про уверенность. Про то, что враг не слышит. Про то, что ты защищён. И одновременно — про тревогу: а вдруг ЗАС сломается? Вдруг ключ шифрования устарел? Вдруг тот, кто сидит на другом конце, — не тот, за кого себя выдаёт?

Когда я пишу про «полёвку» и «тапики» — я пишу про простоту и уязвимость. Про то, как надёжно работает проводная связь — пока её не перерубят лопатой. Про то, как легко говорить по полемому телефону — пока в трубку не ворвётся чужой голос.

Техника в этой книге — не самоцель. Это фон. Это сцена, на которой разворачивается человеческая драма.

Что вы найдёте в этой книге

Итак, если это не учебник — что здесь есть?

Истории. Реальные истории людей, которые служили в спецсвязи. Мои истории. Истории моих сослуживцев. Истории, которые я слышал от других ветеранов. Некоторые из них смешные, некоторые страшные, некоторые трагические. Но все — правдивые.

Быт. Как жили связисты в Чечне. В чём спали, что ели, как мылись, чего боялись, о чём мечтали. Без прикрас и без героизации. Иногда стыдно, иногда противно, иногда смешно до колик.

Техника в действии. Как работала спецсвязь не в теории, а на практике. Что делали, когда аппаратура ломалась. Как обходились без инструментов. Как учились на ходу. Как ошибались и как исправляли ошибки.

Контекст. Война в Чечне глазами не героя-спецназовца, а простого солдата из батальона связи. Не штурмы и засады, а рутина. Стройка, наряды, отравление в столовой, борьба со вшами. И редкие минуты, когда война врывается в эту рутину — обстрелы, перестрелки у ворот, пуля в бронежилет сослуживца.

Выводы. Не военно-стратегические — я не имею права делать такие выводы. А человеческие. Что такое война. Что такое служба. Что такое дружба и предательство. Что остаётся в душе через двадцать пять лет.

Чего в этой книге нет

А теперь — честно. Чего вы не найдёте на этих страницах.

Секретных данных. Никаких действующих частот, кодов, ключей шифрования, протоколов. Во-первых, я их не знаю — моя группа допуска была только третья, «Секретно», а не «Совершенно секретно». Во-вторых, то, что я знал, устарело двадцать лет назад. В-третьих, даже устаревшая информация может быть закрытой. Я не хочу иметь проблем с законом, и вам не советую.

Точных технических характеристик. Я не инженер. Я пользователь. Я могу рассказать, как выглядит ЛТА, как он работает, какие у него плюсы и минусы. Но не спрашивайте меня о количестве транзисторов, ёмкости конденсаторов и типе разъёмов. Я этого не помню — и никогда не знал.

Политических оценок. Эта книга не о том, правильной или неправильной была война в Чечне. Не о том, хороший или плохой был президент. Не о том, кто прав, а кто виноват. Я солдат, а не политик. Моё дело — выполнять приказы. А оценивать их — удел историков. Я просто рассказываю, что видел. А выводы пусть каждый делает сам.

Героического пафоса. Я не герой. Я не совершал подвигов. Я не выносил раненых с поля боя, не брал «языков», не закрывал амбразуры. Я сидел в палатке и набивал телеграммы. Это не героично. Это работа. Скудная, монотонная, иногда опасная — но работа. И я её делал. Так же, как делали тысячи других солдат. Не надо из меня делать Рэмбо. Я — обычный человек. Со своими слабостями, ошибками, страхами.

Точности абсолютной. Прошло больше двадцати лет. Моя память — не видеомэгнитофон. Я мог перепутать даты, имена, последовательность событий. Где-то я пишу «кажется», где-то «по-моему», где-то «если не ошибаюсь». Я старался быть максимально точным, сверял свои воспоминания с фотографиями, письмами, рассказами сослуживцев. Но абсолютная точность в мемуарах невозможна. Простите.

Как читать эту книгу

Я построил книгу так, чтобы её можно было читать с любой главы. Не нужно продирааться от корки до корки, если вас интересует что-то конкретное.

Хотите узнать про шифрование — глава 2 и 5–7. Хотите про боевиков и их связь — глава 19. Хотите про Андрея Петухова — глава 27. Хотите про то, как я чуть не погиб от руки президентской охраны — глава 29.

Но если вы прочитаете книгу от начала до конца, вы увидите, как постепенно, глава за главой, из технических деталей, человеческих историй и военных эпизодов складывается общая картина.

СПС — это не просто «закрытая связь». Это мир. Со своими законами, традициями, жаргоном, героями и антигероями. Мир, который остаётся невидимым для посторонних. Мир, без которого современная армия не может воевать.

Я хочу показать вам этот мир. Изнутри. Без прикрас. Без купюр.

Одна история, которая всё объясняет

Когда я вернулся из армии, ко мне подошла тётя Таня — родственница, которая меня не видела два года.

— Андрей, — спросила она шёпотом, оглядываясь по сторонам, — ты много бандитов убил?

Её вопрос привёл меня в лёгкое замешательство. Я ей попытался объяснить, что я не спецназ, не разведчик, не снайпер. Я телеграфист. Я набивал телеграммы. Я чинил кабели. Я топил буржуйку.

— А-а-а, — протянула тётя Таня, — я поняла. Ну, не хочешь — не говори.

Она не поверила. Она была уверена, что я герой, а скромничаю, как тот парень из фильма «Брат» — «писарем в штабе отсиживался».

Я не стал спорить.

Но теперь, через двадцать лет, я пишу эту книгу, чтобы объяснить: да, я не герой. Да, я не убивал бандитов. Да, я «отсиживался» в штабе — точнее, в палатке, в узле связи «Пеленг», под артобстрелами, под прицелом снайперов, под пристальным взглядом чёрных человечков из президентской охраны.

И это — тоже война. Другая. Невидимая. Без выстрелов, но со смертью. Без атак, но с ошибками, которые стоят жизни.

Об этой войне я и хочу рассказать.

ГЛАВА 5

Шифрование: «секретно», «совершенно секретно», «особой важности»

В предыдущих главах я рассказывал о том, что такое СПС, кому она нужна и почему эта книга — не учебник. Теперь пришло время поговорить о том, что лежит в основе любой защищённой связи. О том, без чего СПС была бы просто дорогой и бесполезной игрушкой.

О шифровании.

Но прежде чем говорить о шифровании как о техническом процессе, нужно понять другое. В армии, в спецсвязи, в любой системе, имеющей дело с секретами, информация делится на категории. На грифы секретности.

Без этих грифов невозможно понять, кто имеет право знать ту или иную информацию, как её передавать, как хранить, как уничтожать. И — что самое важное для нас — кто может работать с ней.

Грифы — это не просто бумажки с надписями «секретно» или «совершенно секретно». Это система. Жёсткая, бюрократическая, иногда бесячая. Но без неё — хаос.

Как всё начиналось: советская система секретности

Система грифов секретности в России — наследница советской. А советская, в свою очередь, складывалась в 1920–1930-е годы, когда молодая страна готовилась к обороне и боялась шпионов.

В СССР было три основных грифа: «секретно», «совершенно секретно» и «особой важности» (иногда — «особой важности» с пометкой «лично»). К ним добавлялись ведомственные пометки: «для служебного пользования» (самый низкий уровень, не совсем секрет, но и не для всех), «не подлежит опубликованию в печати», «снять копии запрещается» и другие.

Допуск к секретным сведениям оформлялся через особые отделы (в армии — через Особый отдел КГБ, позже — через органы ФСБ). Процедура была долгой и унижительной: проверяли не только тебя, но и твоих родственников — родителей, братьев, сестёр, супругов, иногда даже дальних.

Если кто-то из родственников был судим, жил за границей, имел «неблагонадёжных» знакомых — допуска не давали. Или давали, но более низкой категории.

Эта система перекочевала в Российскую Федерацию. Почти без изменений. Даже сейчас, через тридцать пять лет после распада СССР, порядок оформления допуска изменился не сильно.

Три группы допуска: 3, 2, 1

В армии, когда речь идёт о работе с секретной связью, используется не только гриф секретности документов, но и группа допуска у человека.

Группа допуска — это уровень, до которого человек может знать секреты.

Их три.

Третья группа допуска — самая низкая из «настоящих» (не считая «для служебного пользования», которое вообще не считается секретным). С третьей группой можно работать с документами и информацией, имеющими гриф «Секретно».

Что это за информация? Например, оперативные сводки. Планы боевых действий на уровне батальона-полка. Списки личного состава. Координаты полевых лагерей. Ничего сверхсекретного, но и не для открытой печати.

Чтобы получить третью группу, нужно пройти проверку по месту жительства. ФСБ запрашивает характеристики с работы (если работал) и из военкомата, проверяет судимости (свои и родственников), иногда — опрашивает соседей.

Всё это занимает несколько недель. И — вот важный момент — третью группу дают почти всем, кто работает с секретной связью. Даже срочникам. Как мне.

Вторая группа допуска — серьёзнее. С ней можно работать с документами «Совершенно секретно».

Это уже информация государственной важности. Планы крупных операций. Данные разведки. Сведения о потерях (иногда — с разбивкой по частям). Коды и шифры (частично). Списки агентуры (если речь о разведке).

Чтобы получить вторую группу, проверка глубже. Могут проверять не только тебя, но и твоих близких родственников — всех, кто живёт с тобой или часто с тобой общается. Могут приезжать на место жительства, беседовать с участковым, с соседями.

Вторую группу срочникам почти не дают. Только контрактникам и офицерам. И то не всем — а только тем, кому это действительно нужно по службе.

Первая группа допуска — высшая. С ней можно работать с документами «Особой важности».

Это всё, что связано с национальной безопасностью. Ядерное оружие. Стратегическое планирование. Секретные переговоры на высшем уровне. Коды запуска ракет. Агентурные сети за рубежом.

Проверка для первой группы — тотальная. Выезд на место жительства, опрос всех, кто вас знает (соседей, коллег, учителей, друзей). Проверка всех родственников до третьего колена. Проверка заграничных связей. Могут даже попросить пройти полиграф («детектор лжи»).

Первую группу имеют только высшие офицеры и некоторые гражданские специалисты. Срочников — никогда.

Моя третья группа: как это было

Когда я оформлял допуск — это было в Екатеринбурге, во время формирования команды в батальон связи — я не очень понимал, что происходит. Пришёл какой-то офицер (кажется, из ФСБ, но точно не скажу), задал несколько вопросов. Про родителей, про место рождения, про образование, про то, не был ли я судим. Спрашивал, нет ли у меня родственников за границей. У меня не было.

Потом была пауза в несколько дней. Я уже начал волноваться: вдруг не дадут? Вдруг из-за моих приключений в начале службы (самоволки, пьянки) откажут? Но потом нас собрали и объявили: «Рядовому Сажину присвоена третья группа допуска к сведениям, составляющим государственную тайну».

Всё. Никакой торжественной клятвы. Никакого вручения «красной корочки». Просто запись в личном деле и короткое уведомление.

Но — были и ограничения. Нам сказали: после окончания службы вы не имеете права выезжать за границу в течение пяти лет. Подпись под этим обязательством мы поставили. Я тогда не планировал ехать за границу, так что не расстроился.

Честно говоря, я не очень понимал, что мне теперь известно такого секретного, что я не мог ехать за границу. Но правила есть правила.

Потом, уже в Чечне, я понял. Я видел телеграммы с координатами артиллерийских ударов. Я видел донесения о потерях. Я знал, какие подразделения куда выдвигаются. Всё это — «секретно». Враг, получивший эту информацию, мог бы нанести серьёзный урон.

Так что пять лет без загранпоездки — не такая уж большая плата.

Что означают грифы на практике

Теперь — немного конкретики. Что именно означают эти загадочные слова «секретно», «совершенно секретно» и «особой важности»?

«Секретно». Информация, разглашение которой может нанести ущерб интересам ведомства или, в некоторых случаях, государства. Например, если боевики узнают, что в такой-то бригаде такие-то потери, они могут этим воспользоваться — усилить давление, устроить засаду, перехватить колонну.

«Секретно» — это не «смертельно опасно», но и не «можно рассказать друзьям». Хранить такие документы нужно в сейфе. Передавать — по СПС или с фельдгегерем. Уничтожать — через шредер (у нас таких) не было или сжиганием.

«Совершенно секретно». Информация, разглашение которой может нанести серьёзный ущерб интересам государства. Если боевики узнают план крупной операции — они могут сорвать её, нанести большой урон, взять пленных.

С такими документами работают только те, у кого вторая группа. Хранение — в специальных сейфах, в опечатанных помещениях. Передача — только по СПС, с подтверждением получения. Уничтожение — с составлением акта, в присутствии комиссии.

«Особой важности». Информация, разглашение которой может нанести ущерб высшим интересам государства. Если враг узнает, например, о системе шифрования или о планах ядерного удара — последствия могут быть катастрофическими.

С такими документами работают единицы. Их даже не копируют без особого разрешения. Передают только «лично в руки» под расписку. Уничтожают по специальной процедуре, часто — в присутствии представителя вышестоящего штаба.

В своей работе я сталкивался с документами «секретно» и иногда — «совершенно секретно» (например, телеграммы с координатами ударов). «Особой важности» я не видел. И слава богу.

Журналы, подписи, ответственность

Работа с секретными документами — это не только чтение и передача. Это ещё и бесконечная бумажная волокита.

Каждая телеграмма, которую я отправлял или принимал, регистрировалась в журнале.

Журнал исходящих телеграмм: номер, дата, время, адресат, краткое содержание (без секретных подробностей — просто «оперативная сводка» или «боевой приказ»), гриф секретности, подпись оператора.

Журнал входящих телеграмм: номер, дата, время, отправитель, краткое содержание, гриф, кому передана на исполнение, подпись оператора.

Каждый день эти журналы проверял начальник смены — прапорщик или офицер. Каждый месяц — начальник узла связи. Раз в квартал — проверяющий из штаба.

Если в журнале была ошибка — не та цифра, не тот адресат, не тот гриф — это было ЧП. Могли отстранить от работы, понизить в должности, отправить в другое подразделение.

В моём случае с телеграммой на награждение — там была ошибка. Но не в журнале, а в самом тексте. И виноватым назначили меня, хотя ошибся не я. Это — отдельная история. Я расскажу её позже.

Сейчас важно другое: бюрократия в СПС — не прихоть. Это способ контроля. Каждая телеграмма, каждый сеанс связи, каждый оператор — всё учтено, всё подписано, всё можно проверить.

Если что-то пошло не так — всегда можно найти, кто ошибся, когда, в каком месте. И наказать. Или — как в моём случае — наказать невинного, потому что он «молодой и здоровый, а женщину в Урус-Мартан отправлять нельзя».

Бюрократия не спасает от несправедливости. Но она спасает от хаоса.

Одна история о забытом полковнике

Я обещал рассказать эту историю позже. Расскажу сейчас, коротко. Полностью — в главе 23.

Телеграмма на награждение. Список офицеров — человек десять. Набирал кто-то из операторов (не я). Пропустил одну строчку — одного полковника.

Полковник не получил медаль. Разозлился. Приехал в узел связи. Требовал найти виноватого.

Старшая телеграфистка — пожилая женщина, ефрейтор — заплакала. Ей грозила отправка в Урус-Мартан (очень опасное место, постоянные обстрелы).

Начальник узла связи — капитан — вызвал меня. Сказал: «Женщину туда нельзя. Возьми вину на себя».

Я согласился.

Меня отстранили от работы на узле. И чтобы не отправлять меня в Урус-Мартан и спрятать с глаз обиженного полковника перевели в истопники. Дальше — глава 26.

К чему я это рассказываю? К тому, что система грифов и допусков — не бездушная машина. За ней стоят люди. И люди иногда принимают решения, которые не прописаны в инструкциях.

Не всегда справедливые. Не всегда правильные. Но — человеческие.

Послесловие к главе

Шифрование, грифы, допуски — всё это звучит скучно и бюрократично. Но за каждым грифом — реальная информация. За каждым допуском — реальный человек. За каждой телеграммой — реальные судьбы.

Когда я ставил свою подпись в журнале исходящих телеграмм, я не думал о государственной тайне. Я думал: «Быстрее бы отправить эту "портянку" с координатами и пойти курить».

Но теперь, через двадцать лет, я понимаю: та «портянка» с координатами — это чей-то приказ артиллеристам. Артиллеристы по этим координатам били по боевикам. Боевики отступали или погибали. Наши солдаты оставались живы.

Вот что такое гриф «секретно» на практике. Не абстракция. Не бумажка. А жизнь.

ГЛАВА 6

Аналоговая эпоха: «Гранит» и его предки

Когда мы говорим о спецсвязи, о засекречивающей аппаратуре, о шифровании — возникает соблазн представить себе что-то футуристическое. Мигающие лампочки, сложные коды, компьютеры, которые считают быстрее, чем враг успевает моргнуть.

До того как в СПС пришли цифровые технологии, основным средством защиты переговоров были аналоговые системы засекречивания. Их называли по-разному: скремблеры, инверторы, «крякалки». В Советской армии самой массовой серией таких аппаратов была «Гранит».

«Гранит» — это не компьютер. Это даже не полупроводниковая электроника в современном понимании. Это — аналоговая техника. Транзисторы, конденсаторы, резисторы. Схемы, которые можно было спаять в полевых условиях, если есть паяльник и прямые руки.

И «Гранит» работал. Плохо, по современным меркам. Уязвимо. Но — работал.

Как работали аналоговые скремблеры

Чтобы понять принцип работы аналогового скремблера, представьте себе обычный разговор. Ваш голос — это звуковая волна. Она имеет определённую форму, определённый частотный состав.

Скремблер берёт эту звуковую волну и... переворачивает её. Буквально. Высокие частоты становятся низкими, низкие — высокими. Или — сдвигает частоты по определённому закону.

На приёме происходит обратное преобразование. Высокие снова становятся высокими, низкие — низкими. И вы слышите нормальный голос.

Перехватчик, если он просто слушает эфир, слышит не голос, а странный шум. Напоминающий кряканье. Отсюда — народное название «крякалка».

Казалось бы — гениально просто. И действительно, в 1960–1970-е годы такие системы были прогрессом. Они позволяли защитить переговоры от случайного прослушивания и от большинства радиолюбителей.

Но у «крякалок» был огромный недостаток. Они были предсказуемы.

Почему «Гранит» был уязвим

Любой аналоговый скремблер — это не шифрование в современном смысле. Это преобразование сигнала по известному алгоритму. Алгоритм — не секрет. Он запаян в схему. И если у перехватчика есть такой же аппарат (или он знает, как работает ваш), он может восстановить исходный голос.

Более того, в 1980-е годы появились методы взлома аналоговых скремблеров без знания алгоритма. С помощью цифровой обработки сигнала. Ты записываешь «крякающий» эфир, прогоняешь через специальную программу — и через несколько минут слышишь чистый голос.

Сначала это было дорого и сложно. Нужны были мощные компьютеры (по тем временам) и квалифицированные специалисты. Но к 1990-м годам такие технологии стали доступны не только спецслужбам, но и хорошо финансируемым боевикам.

В Чечне у боевиков не было своих лабораторий по взлому скремблеров. Но у них были спонсоры. Были связи с зарубежными эмиссарами. И была информация — от перебежчиков, от пленных, от купленных осведомителей.

Поэтому к 2000 году «Гранит» уже не обеспечивал реальной защиты. Его можно было взломать. Вопрос был только во времени и ресурсах.

Но «Гранит» продолжали использовать. Потому что альтернативы не было.

«Гранит» в моей практике

Я работал с аппаратурой, которую называли «ЗАС». Но была ли это конкретно «Гранит» или что-то другое — не знаю. В уставе это называлось «аппаратура засекречивания». Конкретных моделей нам не объявляли. Сказали: «Вот кнопки. Нажимайте так. Не нажимайте эдак. Запомнили? Всё».

Я помню, что аппарат был металлическим, тяжёлым, с тумблерами и лампочками. Зелёный. В старом советском стиле. В нём не было экранов, не было клавиатуры — только кнопки включения, выключения, индикаторы готовности.

Когда он работал, из него доносилось еле слышное гудение. Трансформатор, наверное.

И он периодически ломался. Тогда приходил техник — прапорщик с чемоданчиком. Открывал аппарат, копался внутри, вытаскивал какие-то блоки, вставлял новые. Иногда помогал простой способ: выключить, подождать минуту, включить снова.

Это — классика аналоговой техники. Она не «зависает», как компьютер. Она или работает, или нет. Или гремит, или молчит.

Что было до «Гранита»

До «Гранита» в Советской армии использовались ещё более старые системы.

Например, «Лавина» — одна из первых советских ЗАС для правительственной связи. Громоздкая, капризная, требовала специально обученного персонала. Использовалась в основном в Москве и крупных штабах.

Была «Сосна» — полевая версия, для подвижных узлов. Но к концу 1970-х годов она устарела.

Были и другие, совсем экзотические. Например, системы, основанные не на частотном преобразовании, а на временном — когда голос резался на микроскопические кусочки и эти кусочки передавались в разной последовательности. На приёме — собирались обратно. Это было сложнее в реализации, но и надёжнее.

Однако к 1980-м годам стало ясно: аналоговые методы защиты — тупик. Нужна цифра. Нужно настоящее шифрование. Нужны ключи, которые можно менять, алгоритмы, которые можно усложнять.

Но переход на цифру занял десятилетия. Денег не было. Промышленность не успевала. Квалифицированных кадров не хватало.

Поэтому в 2000 году в Чечне, на многих узлах связи, ещё стоял «Гранит». Или его аналоги. И боевики, возможно, могли их взломать.

Нам об этом не говорили. Мы верили, что ЗАС — надёжна. Что враг не слышит. Что мы защищены.

Верить — это важно на войне. Даже если вера не всегда соответствует реальности.

Почему аналоговые системы дожили до 2000-х

Может возникнуть вопрос: если «Гранит» был так уязвим, почему его не заменили раньше?

Ответ — как всегда в России: денег не было.

В 1990-е годы армия разваливалась. Военные заводы стояли. Зарплаты не платили. Новые разработки замораживались. То, что удавалось произвести, шло в первую очередь в ФСО и Генштаб. В полевые части — только остатки.

Когда в 1999 году началась Вторая чеченская, руководство бросило ресурсы на оснащение войск. Но за год-два невозможно переоснастить всю армию. Поэтому в Чечню поехали с тем, что было.

«Гранит» был. Он был старым, но работал. Он давал хоть какую-то защиту. И его можно было чинить в полевых условиях — паяльником, отвёрткой, прямыми руками.

Цифровые ЗАС («Акведук», «Арбалет») были лучше. Но их было мало. Они доставались приоритетным направлениям — штабу группировки в Ханкале, крупным узлам в Моздоке, возможно — отдельным бригадам.

В нашей 46-й ОБРОН, кажется, были и те, и другие. Я точно не помню. Но я помню, что аппаратура была старой — зелёной, тяжёлой, советской. Значит, «Гранит» или его родственники.

Одна история о «Граните»

Однажды мне рассказал сослуживец. Он не был техником. Он не ремонтировал ЗАС. Но он видел, как это делают.

«Однажды наш «Гранит» (или что там было) перестал работать. В середине смены. Погасли лампочки. Каналы связи пропали.

Я позвал дежурного прапорщика. Он посмотрел, пощёлкал тумблерами — ноль эмоций. — Сгорел блок питания, — сказал он.

Полез в аппарат, вытащил какой-то тяжёлый блок. Металлический, с рёбрами охлаждения. Унёс его в соседнюю палатку — там был склад запчастей.

Через час вернулся с другим блоком. Вставил. Включил. Загорелись лампочки. Каналы связи появились.

— Всё, — сказал прапорщик. — Работайте.

Я спросил: «А часто они горят?»

— Бывает, — ответил он. — Трансформаторы старые. Изоляция сохнет. Конденсаторы текут. Надо бы новые закупить, да где ж их взять...»

Вот так. Война в Чечне, боевое дежурство, секретная связь — а аппаратура на ладан дышит. Трансформаторы сохнут, конденсаторы текут, прапорщик колдует с блоком питания, как сельский электрик с лампочкой в сарае.

Это — не позор. Это — реальность 2000 года. Страна выходила из кризиса. Армия училась воевать по-новому. И техника, с которой мы воевали, была старой, но верной. Она нас не подводила. В самый ответственный момент — не подводила.

Что осталось от аналоговой эпохи

Сегодня, через двадцать с лишним лет, аналоговые скремблеры ушли в прошлое. Даже в самых отсталых армиях их заменили цифровые системы. В России тоже.

Но память о «Граните» и его предках жива. Жива в старых солдатских байках. В учебниках для связистов. В музеях военной связи.

И — в этой книге.

Потому что без «Гранита» не было бы «Акведука». Без аналогового прошлого — цифрового настоящего.

Конец ознакомительного фрагмента.

Текст предоставлен ООО «Литрес».

Прочитайте эту книгу целиком, [купив полную легальную версию](#) на Литрес.

Безопасно оплатить книгу можно банковской картой Visa, MasterCard, Maestro, со счета мобильного телефона, с платежного терминала, в салоне МТС или Связной, через PayPal, WebMoney, Яндекс.Деньги, QIWI Кошелек, бонусными картами или другим удобным Вам способом.