3 Забезпечення захисту інформації в системах зв'язку. Технічні засоби системи захисту інформації

УДК 681.3.06:519.248.681

МЕХАНИЗМЫ И КРИТЕРИИ БЕЗОПАСНОСТИ СИСТЕМ БЕСПРОВОДНОЙ СВЯЗИ

Евгений Гулак
Закрите акціонерне товариство "Українські Сателітарні Системи"

Аннотация: **Предложен подход к оценке уровня защищенности информации в системах транкинговой связи на основе действующих в Украине нормативных документов для автоматизированных систем (АС). Проведен сравнительный анализ систем TETRA и TETRAPOL, определены основные угрозы безопасности информации и соответствующие механизмы защиты. Разработан критерий выбора криптоалгоритма, который учитывает потенциальные возможности роста производительности электронно-вычислительной техники.**
Summary: **Approach to the evaluation of protection information level in system of tranking communications based on the used Ukrainian normative documents for automated system (AS) are proposed. The comparative analysis of system TETRA and TETRAPOL is made, defined based threat to information security and corresponding security mechanism. Criteria of choice for cryptoalgorithm which whill allow potential possibility of increase productivity of the computer system is developed.**
Ключевые слова: **Критерии защищенности, транкинговая радиосвязь, угрозы безопасности, механизмы защиты, математическое ожидание, криптоалгоритм.**

В настоящее время широкие возможности мобильных систем связи, включая средства на базе стандартов транкинговой связи, привлекают все большее внимание пользователей ведомственных сетей подвижной связи, среди которых преобладают службы общественной безопасности, милиция, пожарные, спасатели, скорая помощь и др.

Кроме таких специфических требований этих групп абонентов, как гарантированный и быстрый доступ в систему, приоритетные вызовы, прямая связь между абонентами и т. д., цифровые транкинговые системы обеспечивают возможность передачи данных, увеличение зон покрытия, экономию частотного ресурса, интеграцию с существующими системами связи, а также повышенный уровень защиты информации, включая такие важнейшие ее характеристики как конфиденциальность, целостность и доступность.

Вместе с тем, системы мобильной (или беспроводной) связи потенциально уязвимы по отношению к реализации угроз со стороны различного рода нарушителей.

Вопросам обеспечения безопасности информации при ее передаче в каналах транкинговой связи посвящено ряд работ отечественных и зарубежных авторов [1–3].

В данной работе изучается классификация угроз безопасности информации, а также подходы к оценке защищенности системы с учетом требований действующих в Украине нормативных документов по вопросам криптографической и технической защиты информации [6–13].

Угрозы безопасности информации в системе беспроводной связи

Анализ известных нарушений безопасности функционирования систем беспроводной связи (СБС) позволяет выделить ряд типовых угроз, которым должны быть противопоставлены адекватные механизмы защиты.

Соответствующие критериям защищенности функции противодействия возможным угрозам приведены на рис. 1.

Угрозы информационной и технической безопасности представлены на рис. 2.

Угрозы, указанные на рис. 2, в свою очередь делятся на:

- перехват: перехват в радиоинтерфейсе, перехват в кабельном интерфейсе, несанкционированное воспроизведение;
- манипуляции: простые изменения информации, удаление или вставка частей сообщения, вставка новых данных, маскировка под базовую станцию, запрос новой передачи сообщений, переустановка данных;

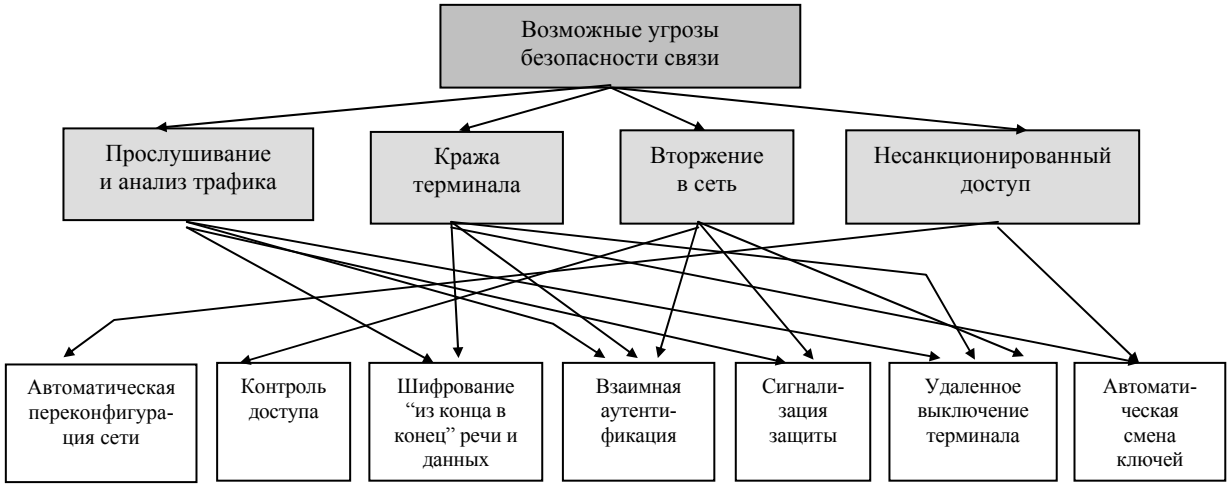

Рисунок 1 – Возможные угрозы безопасности связи и способы защиты

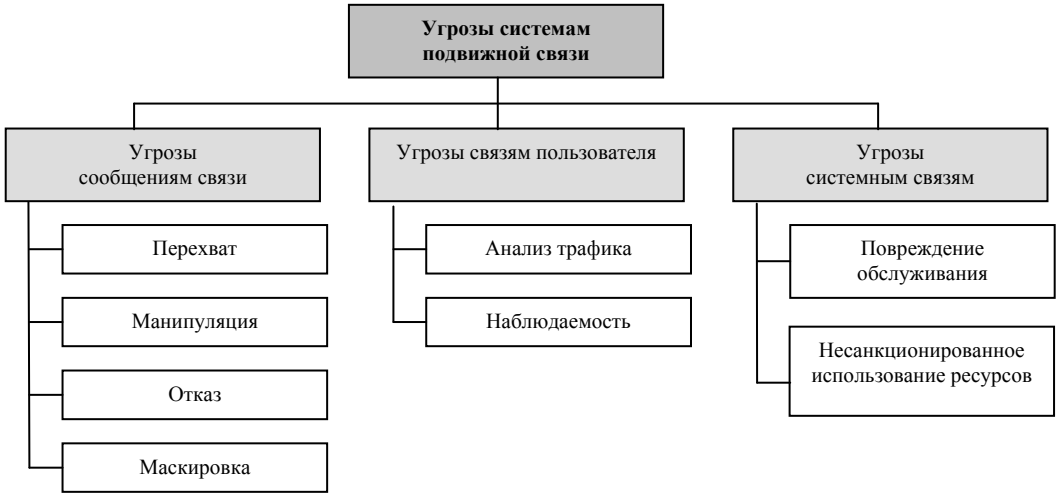

Рисунок 2 – Классификация угроз в системах подвижной связи

- отказ: отказ от получения информации, отказ от посылки информации;
- маскировка: маскировка под другого пользователя, маскировка под базовую станцию;
- анализ информационного трафика: скорость передачи сообщений, длина сообщений, идентификация отправителя и получателя;
- наблюдаемость: местоположение пользователя, принадлежность к абонентским группам, уровень приоритета обслуживания;
- нарушение обслуживания: удаление сообщений, задержка сообщений, изменение сетевой конфигурации системы, преднамеренное создание "заторов", злоупотребление дополнительным обслуживанием;
- несанкционированное использование ресурсов: использование запрещенных ресурсов (маскировка, использование украденного оборудования, дополнительные права доступа), использование неуполномоченных ресурсов (злоупотребление служебной информацией, неуполномоченное использование оборудования, манипуляции с доступом).

Сосредоточим внимание на двух технологиях: TETRA и Tetrapol. На первой потому, что это действующий общеевропейский стандарт, а на второй потому, что она создана с целью удовлетворения специфическим требованиям сил безопасности.

Вопросам анализа угроз безопасности информации в СБС посвящено большое число работ [1–3]. Поэтому не будем останавливаться на теоретическом описании угроз и рассмотрим лишь их классификацию и меры противодействия, предусмотренные в протоколах TETRA и Tetrapol.

Механизмы защиты от вышеперечисленных угроз на примере стандартов TETRA и Tetrapol приведены в табл. 1.

Таблица 1 – Механизмы защиты

Виды угроз	**TETRA**	**Tetrapol**
Перехват в радиоинтерфейсе	1. взаимная аутентификация через интерфейс между БС и МС; 2. шифрование интерфейса между БС и МС; 3. шифрование между оконечными точками; 4. механизм передачи ключей шифрования по интерфейсу между БС и МС (OTAR)	1. взаимная аутентификация через интерфейс между БС и МС; 2. шифрование интерфейса между БС и МС; 3. шифрование между оконечными точками; 4. механизм передачи ключей шифрования по интерфейсу между БС и МС (OTAR)
Перехват в кабельном интерфейсе	1. шифрование между оконечными точками; 2. обеспечение защиты информации на БС	1. шифрование между оконечными точками
Несанкциониро-ванное воспроизведение информации	1. использование ключей шифрования; 2. механизм автоматической смены ключей по интерфейсу между БС и МС (OTAR)	1. использование ключей шифрования; 2. механизм автоматической смены ключей по интерфейсу между БС и МС (OTAR)
Маскировка	1. взаимная аутентификация через интерфейс между БС и МС; 2. шифрование интерфейса между БС и МС; 3. шифрование между оконечными точками; 4. механизм передачи ключей (OTAR)	1. взаимная аутентификация через интерфейс между БС и МС; 2. шифрование интерфейса между БС и МС; 3. шифрование между оконечными точками; 4. механизм передачи ключей (OTAR)
Отказ от участия в связи	1. взаимная аутентификация через интерфейс между БС и МС; 2. использование криптографических алгоритмов; 3. всесторонняя регистрация трафика	1. взаимная аутентификация через интерфейс между БС и МС; 2. использование криптографических алгоритмов; 3. всесторонняя регистрация трафика
Манипуляция в радиоинтерфейсе	1. взаимная аутентификация через интерфейс между БС и МС; 2. шифрование интерфейса между БС и МС; 3. шифрование между оконечными точками; 4. механизм передачи ключей (OTAR)	1. взаимная аутентификация через интерфейс между БС и МС; 2. шифрование интерфейса между БС и МС; 3. шифрование между оконечными точками; 4. механизм передачи ключей (OTAR)
Манипуляция в кабельном интерфейсе	1. взаимная аутентификация через интерфейс между БС и Центром коммутации; 2. шифрование между оконечными точками;	1. взаимная аутентификация через интерфейс между БС и Центром коммутации; 2. шифрование между оконечными точками;
Анализ трафика	1. взаимная аутентификация через интерфейс между БС и МС; 2. шифрование интерфейса между БС и МС; 3. шифрование между оконечными точками; 4. механизм передачи ключей шифрования по интерфейсу между БС и МС (OTAR); 5. вставка фиктивных сообщений; 6. дополнение сообщений	1. взаимная аутентификация через интерфейс между БС и МС; 2. шифрование интерфейса между БС и МС; 3. шифрование между оконечными точками; 4. механизм передачи ключей шифрования по интерфейсу между БС и МС (OTAR); 5. вставка фиктивных сообщений; 6. дополнение сообщений
Наблюдаемость	1. применение временных идентификаций (псевдонимов)	1. применение временных идентификаций (псевдонимов)

Продолжение Таблицы 1

Повреждение обслуживания	1. применение информационной избыточности; 2. обеспечение гибкости системы; 3. всесторонняя ревизия функционирования сети	1. применение информационной избыточности; 2. обеспечение гибкости системы; 3. всесторонняя ревизия функционирования сети
Использование запрещенных и неуполномоченных ресурсов	1. взаимная аутентификация через интерфейс между БС и МС; 2. управление доступом; 3. всесторонняя ревизия работы системы	1. взаимная аутентификация через интерфейс между БС и МС; 2. управление доступом; 3. всесторонняя ревизия работы системы

Построение критериев защищенности информации

В настоящее время в Украине отсутствуют нормативно-правовые акты, регулирующие вопросы создания и эксплуатации СБС, предназначенных для передачи конфиденциальной информации, проверки достаточности реализованных в таких системах методов и средств защиты информации.

Наиболее эффективным, а в случае использования радиоканала практически единственным методом надежной защиты конфиденциальности передаваемой в канале связи информации является криптографическая защита. При наличии возможности мобильные компоненты системы связи (транспортные средства) должны быть защищены от утечки по акустическим каналам.

Для стационарного оборудования транкинговых систем связи должны быть выполнены в полном объеме меры по технической защите от побочных электромагнитных излучений и наводок (ПЭМИН).

В настоящее время в нормативно-правовых актах ДСТСЗИ СБ Украины [8–13] достаточно полно проработаны вопросы создания, разработки и проведения исследований (экспертизы) комплексной системы защиты в автоматизированных системах, автоматических коммутационных системах, определен порядок создания и требования к средствам криптографической защиты информации.

Вместе с тем, как уже было отмечено выше, надежную защиту в СБС трудно создать без применения криптографических методов; в то же время, задачи по защите информации в СБС аналогичны тем, которые приходится решать в автоматизированных системах обработки информации с ограниченным доступом.

С учетом изложенного предлагается до создания соответствующих нормативных документов по СБС использовать для классификации степени их защищенности нормативные документы Департамента в сфере криптографической и технической защиты информации.

Сравнительный анализ терминов, определений и характера их использования в области защиты информации в АС и соответствующих понятий в научных публикациях [1–3] по вопросам защищенных СБС свидетельствует зачастую или о тождественном смысле термина, или о незначительных специфических аспектах его применения в сфере радиосвязи. В свою очередь это позволяет говорить о потенциальной применимости критериев защищенности АС для классификации угроз безопасности информации, циркулирующей в СБС, и оценки защищенности СБС.

Отметим, что критерии защищенности АС, установленные нормативным документом системы ТЗИ 2.5-004-99 [11], определяют:

1) сравнительную шкалу для оценки надежности механизмов защиты информации от несанкционированного доступа, реализованных в компьютерных системах;

2) базу для разработки компьютерных систем, в которых должны быть реализованы функции защиты информации.

Критерии являются методологической базой для определения требований по защите информации в компьютерных системах (КС) от несанкционированного доступа; создания защищенных КС и средств защиты от НСД; оценки защищенности информации в КС и их пригодности для обработки информации, требующей защиты.

Указанный документ устанавливает, что *критерии могут использоваться применительно ко всему спектру КС, включая однородные системы, многопроцессорные системы, базы данных, встроенные системы, распределенные системы, сети, объектно-ориентированные системы и др.*

Нормативным документом системы ТЗИ 2.5-004-99 установлено пять групп критериев защищенности информации, в т. ч. критерии конфиденциальности, целостности, доступности, наблюдаемости и критерии гарантий.

Сравнительный анализ стандартов TETRA и Tetrapol в соответствии с критериями защищенности информации

Исходя из изложенного выше анализа угроз [3], а также на основании данных из соответствующих источников [11, 16–18] проведем сравнительный анализ стандартов TETRA и Tetrapol на предмет соответствия критериям защищенности информации.

Так как критерии защищенности информации являются многоуровневыми, то для полноценной оценки системы на соответствие критериям конфиденциальности необходимы подробные внутрисистемные спецификации. Но поскольку данная информация является закрытой для общественности и доступна лишь для ограниченного контингента (производители, разработчики, соответствующие органы, уполномоченные проводить подобную проверку), сравнительный анализ будем проводить без учета уровней защищенности, т. е. будем регистрировать только их наличие/отсутствие. В том случае, когда нельзя будет однозначно ответить, имеется ли реализация данной функции в системах TETRA и Tetrapol – из-за неполноты информации, либо из-за отсутствия аналогичной функции в СБС как таковой — будем ставить знак “?”.

Согласно критериям защищенности информации, можно выделить четыре основных типа угроз. Для удобства последующего анализа пронумеруем эти группы:

1) угрозы, которые относятся к несанкционированному ознакомлению с информацией, составляют угрозы конфиденциальности;

2) угрозы, которые относятся к несанкционированной модификации информации, составляют угрозы целостности;

3) угрозы, которые относятся к нарушению возможности использования КС или обрабатываемой информации, составляют угрозы доступности;

4) угрозы несанкционированного использования ресурсов системы, которым противодействует идентификация, контроль за действиями пользователей и управляемость компьютерной системой, составляющие предмет услуг наблюдаемости и управляемости.

Таким образом, приведенную ранее классификацию угроз можно представить в следующем виде:

Группа	Виды угроз
1	перехват, маскировка, анализ трафика, наблюдаемость
2	манипуляции
3	нарушение обслуживания
4	отказ, несанкционированное использование ресурсов

Результаты соответствия методов противостояния угрозам информации, реализуемых в протоколах TETRA и Tetrapol, критериям защищенности приведены в табл. 2.

Таблица 2 – Соответствие критериям защищенности технологий TETRA и Tetrapol

Критерии	**TETRA**	**Tetrapol**
1. Критерии конфиденциальности:		
доверительная конфиденциальность	**?**	**?**
административная конфиденциальность	+	+
повторное использование объектов	**?**	**?**
анализ скрытых каналов	+	+
конфиденциальность при обмене	+	+
2. Критерии целостности:		
доверительная целостность	**?**	**?**
административная целостность	+	+
откат	+	+
целостность при обмене	+	+
3. Критерии доступности:		
использование ресурсов	+	+
стойкость к отказам	+	+
горячая замена	+	+
восстановление после сбоев	+	+

Продолжение Таблицы 2

4. Критерии наблюдаемости:		
регистрация	+	+
идентификация и аутентификация	+	+
достоверный канал	**?**	**?**
распределение обязанностей	**?**	**?**
целостность комплекса средств защиты	+	+
самотестирование	+	+
идентификация и аутентификация при обмене	+	+
аутентификация отправителя	+	+
аутентификация получателя	+	+
5. Критерии гарантий:		
архитектура	+	+
среда разработки	+	+
последовательность разработки	**?**	**?**
среда функционирования	+	+
документация	+	+
испытания комплекса средств защиты	+	+

На основании проведенного анализа нельзя однозначно ответить, какая система все же лучше или предпочтительнее для украинского рынка транкинговых систем, поскольку для получения сертификата в ДСТСЗИ необходимо выполнение системой всех изложенных критериев. Однако, необходимо отметить, что:

1) для оценки защищенности систем TETRA и Tetrapol показана практическая возможность использования шкалы критериев для АС; вместе с тем, невозможность однозначно ответить на некоторые требования критериев, разработанных для автоматизированных систем, требует их частичной модификаци для оценки защищенности СТС или разработки для данного вида связи отдельных критериев оценки;

2) для детального анализа системы на предмет соответствия критериям необходимо соответствующее оборудование и техническая документация на тестируемые алгоритмы и протоколы;

3) системы TETRA и Tetrapol соответствуют большей части критериев, ориентированных на основные виды угроз.

Если предположить, что вскоре могут появиться нормативные документы, учитывающие всю специфику транкинговых радиосистем, то при общей схожести этих систем для конечного пользователя, следует учитывать и другие аспекты.

Оценка применимости криптоалгоритмов для защищенных СТС

Известно [4, 5], что безопасность информации, защищаемой с помощью средств криптографической защиты при обеспечении необходимого уровня секретности ключа, в основном зависит от криптостойкости примененных криптоалгоритмов.

Положение о порядке криптографической защиты информации (КЗИ) в Украине [6] определяет, что требования к разработке, производству, эксплуатации и сертификации средств КЗИ устанавливаются Департаментом. В частности, в положении о порядке разработки, производства и эксплуатации средств криптографической защиты конфиденциальной информации (утверждено приказом ДСТСЗИ СБ Украины от 30.11.99 № 53) установлено, что для защиты конфиденциальной информации в Украине используются криптографические алгоритмы, являющиеся государственными стандартами или рекомендованные Департаментом.

В настоящее время в Украине действует три государственных стандарта для криптоалгоритмов:

- ГОСТ 28147-89, определяющий алгоритм шифрования;
- ГОСТ 34.310-95, устанавливающий алгоритм электронной цифровой подписи (ЭЦП) и
- ГОСТ 34.311-95, определяющий функцию хеширования, используемую совместно с алгоритмом ЭЦП.

Что касается алгоритмов, рекомендованных Департаментом, то на основе нормативных документов, определяющих порядок сертификации и экспертизы [8, 10] средств КЗИ, можно говорить о следующей процедуре для указанных выше алгоритмов. Разработанный алгоритм по решению Департамента исследуется независимой организацией, материалы исследований направляются для экспертизы в Департамент, на основании которой делается вывод о возможности/невозможности применения этого криптоалгоритма в конкретных условиях (определенном изделии).

Таким образом, можно предполагать, что для тех или иных практических применений Департаментом потенциально могут быть рекомендованы широко используемые в мире алгоритмы, включая DES, Triple DES, IDEA, RSA, AES (новый американский стандарт) и др. При этом видимо главными критериями применимости алгоритмов будут их криптографическая стойкость, длина ключа, возможность обеспечения необходимой скорости криптопреобразования и т. п.

Оценка криптографической стойкости того или иного криптоалгоритма в общем случае является очень сложной математической задачей, требующей применения современных математических методов [14].

Рассмотрим оценку применимости криптоалгоритма на основе анализа вычислительной сложности метода опробования ключей [14].

Суть метода заключается в следующем. Для "перехваченного" шифрованного сообщения осуществляется попытка расшифровать его с помощью последовательного перебора всех возможных вариантов множества ключей – W_k : $ord\ W_k=K$.

В ряде случаев вместо всего множества допустимых ключей используется его подмножество не эквивалентных ключей, т. е. применение которых дает при одинаковых открытых сообщениях одинаковые зашифрованные сообщения.

Кроме того, для сокращения вариантов перебора могут быть использованы иные особенности построения криптоалгоритмов. В частности, криптоалгоритм DES обладает свойством дополнения [4]. Последнее означает, что для любого открытого сообщения x и любого ключа шифрования k справедливо соотношение:

$$DES(\overline{x}, \overline{k}) = \overline{DES(x, k)}, \tag{1}$$

где $DES(\overline{x}, \overline{k})$ – обозначает функцию, реализуемую алгоритмом DES; $\overline{x}$, $\overline{k}$ – инвертированные значения открытого сообщения и ключа, т. е. $x = \overline{x} \oplus 1$ (1 – единичный вектор).

Из соотношения (1) следует, что при подборе ключа нарушитель может сократить вдвое объем перебора, т. е. ключ можно искать с точностью до инверсии.

Таким образом в случае использования метода "опробования" ключей целесообразно оперировать не с полным множеством ключей алгоритма W_k, а с некоторым его подмножеством W_{nk}, имеющим вообще говоря меньшую мощность, существенно зависящую от "индивидуальных" особенностей криптоалгоритма:

$$K = ord\ W \geq ord\ W_{nk} = k. \tag{2}$$

В частности, для алгоритма DES длина ключа шифрования l=56 бит, тогда $ordW_k = 2^{56}$ а с учетом сделанного выше замечания

$$k=ordW_{nk} \leq 2^{55}.$$

Отметим, что в последнем выражении мы не используем знака равенства, так как мощность множества W_{nk} может быть еще и меньше.

Далее оценим сложность решения задачи перебора вариантов ключа для произвольного криптоалгоритма. Очевидно, что время перебора всего множества ключей прямо пропорционально мощности множества ключей K и обратно пропорционально производительности используемой злоумышленником вычислительной техники v.

Для опробования одного варианта ключа необходимо выполнить некоторую последовательность операций, в т. ч.:

- к каждому символу (блоку бит) зашифрованного сообщения применить обратную процедуру криптоалгоритма с проверяемым ключом;
- полученную последовательность символов (блоков) проверить на осмысленность полученного текста (критерий открытого сообщения).

Именно такую схему используют программы восстановления утерянных ключей программных средств архивирования файлов.

Указанную процедуру можно значительно ускорить за счет реализации указанных преобразований и проверок (полностью или частично) аппаратным путем. В частности целым рядом фирм выпускаются микросхемы, работающие на тактовых частотах порядка десятков мегагерц и позволяющие за один такт реализовать зашифрование (расшифрование) по алгоритму DES одного блока текста длиной 64 бит.

Поскольку предметом исследования является только оценка возможности применения алгоритма и ориентировочной стойкости шифрования, а не оптимизация процедуры криптоанализа, то будем полагать, что одной элементарной операции компьютера соответствует проверка одного варианта ключа.

Нужно иметь также в виду, что для равновероятного и случайного применения ключей из множества ключей W_k $(P(k \in W_k)=K^{-1})$ математическое ожидание (среднее значение) Ms числа шагов опробования ключей до нахождения истинного ключа равно [15]:

$$\mathrm{M}s = \sum_{S=1}^{K} s \cdot K^{-1} = K^{-1} \sum_{S=1}^{K} s = \frac{(K+1)K}{2} \cdot \frac{1}{K} = \frac{K+1}{2}. \quad (3)$$

При $K \to \infty$, $\mathrm{M}s \approx \frac{K}{2}$, таким образом, при больших K, в среднем перебрав половину ключей, злоумышленник найдет истинный ключ.

С учетом изложенного выше для математического ожидания времени нахождения истинного ключа можно получить выражение:

$$\mathrm{M}t = C \cdot \frac{K}{2vG}, \quad (4)$$

где C – коэффициент сокращения времени нахождения ключа за счет распараллеливания процессов вычислений (например, для 1000 компьютеров $C = 0.001$); v – быстродействие компьютера, количество операций в секунду; G – продолжительность года в секундах ($G \approx 3.2 \cdot 10^7$ с).

Для простоты суждений будем полагать, что для поиска ключа будет использоваться компьютер с максимальной тактовой частотой, так что $v = f_{max}$ (в настоящее время $f_{max} = 2.5$ ГГц).

Результаты вычислений математического ожидания времени подбора ключа для одного компьютера с неизменной производительностью для различных криптоалгоритмов приведены в колонке 4 табл. 3.

Предположим, что ежегодно тактовая частота удваивается. и злоумышленник использует новейший компьютер. С учетом данного обстоятельства выведем формулу числа лет, необходимого для перебора ключей.

Так как при переменной производительности компьютера злоумышленника на i-ом году может быть выполнено $v_i G$ операций (перебранных ключей), то за n лет может быть выполнена проверка $K/2$ ключей:

$$\frac{K}{2} = v_1 G + v_2 G + \ldots + v_n G. \quad (5)$$

С учетом предположения, что тактовая частота ежегодно удваивается, уравнение (5) можно переписать в следующем виде

$$\frac{K}{2} = (f_m + 2f_m + 4f_m + \ldots + 2^{n-1} f_m)G = G\sum_{i=1}^{n} f_m \cdot 2^{i-1} = G \cdot f_m \sum_{i=1}^{n} 2^{i-1}. \quad (6)$$

Сумма членов в правой части выражения (6) представляет сумму n членов геометрической прогрессии, вследствие чего получим

$$\frac{K}{2} = G \cdot f_m \cdot (2^n - 1). \quad (7)$$

Для достаточно больших n правую часть (7) можно считать равной $G{\cdot}f_m{\cdot}2^n$, поэтому после соответствующих преобразований можно получить формулу для расчета числа лет работы компьютера с переменной производительностью в следующем виде:

$$\frac{K}{2} = 2^n \cdot f_m \cdot G \Rightarrow 2^n = \frac{K}{2 f_m G} \Rightarrow n \lg 2 = \lg \frac{K}{2 f_m G}. \quad (8)$$

Откуда окончательно получим выражение

$$n = \lg^{-1} 2 \cdot \lg \frac{K}{2 f_m G}. \quad (9)$$

На основе формулы (9) произведен расчет числа лет, необходимых для вскрытия ключа при возрастающей производительности компьютера. Результаты расчета приведены в колонке 5 табл. 3.

Таблица 3 – Время вскрытия ключа

Алгоритм	Разработчик	Количество ключей, *Wk*	Матожидание времени вскрытия ключа, M_t (лет)	Среднее время вскрытия ключа при возрастании производительности ЭВТ (лет)
1	2	3	4	5
DES	Стандарт США	$7.2 \cdot 10^{16}$	**0.45**	**0.45**
DVP	Фирма Motorola	$2.4 \cdot 10^{21}$	**$1.5 \cdot 10^{3}$**	**14**
DVP-XL	Фирма Motorola	$7.9 \cdot 10^{28}$	**$4.9 \cdot 10^{11}$**	**39**
IDEA	Стандарт ISO	$2.5 \cdot 10^{38}$	**$1.6 \cdot 10^{21}$**	**70**

Продолжение Таблицы 3

1	2	3	4	5
ГОСТ 28147-89	Межгосударственный стандарт СНГ	$6.3 \cdot 10^{76}$	**$3.9 \cdot 10^{59}$**	**198**

Анализ приведенных в табл. 3 результатов расчетов по формулам (4) и (9) показывает, что:

- полученные результаты неплохо согласуются с сообщениями о том, что для "взлома" методом перебора ключа алгоритма DES с длиной ключа 40 бит потребовалось около одного месяца работы и до 1000 компьютеров, объединенных сетью Internet;
- весьма низкий уровень криптографической стойкости алгоритмов DES и DVP не позволяет сделать вывод о возможности их использования в перспективных системах транкинговой связи; алгоритмы с мощностью ключевого пространства $10^{16} \le W_{nk} \le 10^{28}$ можно рекомендовать лишь для систем с временной стойкостью (с защитой в течение относительно небольшого промежутка времени);
- для защиты конфиденциальной информации в перспективных системах транкинговой связи силовых структур целесообразно использовать криптоалгоритмы с мощностью ключевого пространства W_{nk} не менее $2^{128}=2.5 \cdot 10^{38}$.

Приведенные расчеты наводят на мысль о необходимости дополнительного уточнения критериев защищенности информации в АС с учетом специфики обеспечения безопасности информации в криптосистемах.

В частности, представляется целесообразным учет модели безопасности информации в соответствии с моделями нарушителей и классификацией защищенности криптосистем, разработанными в Системе сертификации СКЗИ РОСС RU.0001.030001.

В указанной системе рассматривается три возможных модели нарушителя:

Первый уровень: нарушитель самостоятельно создает методы нападения и реализует атаки на шифрсредства и защищенные ИТКС;

Второй уровень: нарушитель корпоративного типа, реализующий атаки с НИ организаций;

Третий уровень: нарушитель — специальная служба научно-технически развитой страны.

Система сертификации различает две категории средств криптографической защиты информации:

1. средства для защиты государственной тайны;
2. средства для защиты конфиденциальной информации.

Для средств второй категории предполагается три уровня сертификации:

- уровень "А" – сертификат на систему защиты в целом;
- уровень "В" – сертификат на систему защиты, включающую шифрсредства и их окружение;
- уровень "С" – сертификат только на шифрсредства.

В зависимости от выбранного уровня сертификации определяется один из шести классов сертификатов.

Уровень "А"

Класс КА1 – обеспечение стойкости шифра, когда возможности нарушителя ограничены только современным состоянием науки и техники.

Уровень "В"

Класс КВ2 – сохранение стойкости шифра при наличии недокументированных возможностей в прикладном программном обеспечении.

Класс КВ1 – сохранение стойкости шифра при перехвате ПЭМИН от технических средств.

Уровень "С"

Класс КС3 – обеспечение стойкости шифра при атаке со стороны пользователя системы.

Класс КС2 – обеспечение стойкости шифра при неквалифицированном доступе технического персонала к средствам КЗИ.

Класс КС1 – обеспечение стойкости криптоалгоритма и правильности реализации самого шифрсредства.

Таким образом учитываются основные специфические характеристики средств криптографической защиты информации и пользователь криптосистемы достаточно точно знает уровень ее стойкости по отношению к возможным атакам.

Литература: ***1.*** *Жуков В. А., Климашов И. А. Транкинговая связь в правоохранительных органах. // Системы связи, – 2001, – № 37, с. 65–69.* ***2.*** *Костров Д. В. Безопасность – ключевой фактор в успехе TETRA // Технологии и средства связи, – 1998, – № 6, с. 103–105.* ***3.*** *Иванов В. А. Информационная и техническая безопасность цифровых тракинговых систем. – О.: УНИИРТ, 2001. – 13 с.* ***4.*** *Зегжда Д. П., Ивашко А. М. Основы безопасности информационных систем. – М.: Горячая линия – Телеком, 2000. – 452 с.*

5. *Петраков А. В., Основы практической защиты информации. 2-е изд. Учебн. Пособие. – М.: Радио и связь, 2000. – 376 с.* ***6.*** *"Положення про порядок здійснення криптографічного захисту інформації в Україні" затверджене Указом Президента України від 22 травня 1998 року № 505/98.* ***7.*** *Указ Президента України від 6 жовтня 2000 року № 1120 "Питання Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України".* ***8.*** *Порядок проведення сертифікації засобів криптографічного захисту інформації.* ***9.*** *"Положення про порядок розроблення, виготовлення та експлуатації засобів криптографічного захисту конфіденційної інформації", затверджено наказом ДСТСЗІ СБ України від 30.11.99 № 53.* ***10.*** *"Положення про державну експертизу у сфері криптографічного захисту інформації", затверджено наказом ДСТСЗІ СБ України від 25.12.2000 року № 62.* ***11.*** *Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу, НД ТЗІ 2.5-004-99, затверджено наказом ДСТСЗИ СБ України від 28.04.99 № 22.* ***12.*** *Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу, НД ТЗІ 1.1-003-99, затверджено наказом ДСТСЗИ СБ України від 28.04.99 № 22.* ***13.*** *Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі, НД ТЗІ 3.7-001-99, затверджено наказом ДСТСЗИ СБ України від 28.04.99 № 22.* ***14.*** *Харин Ю. С., Берник В. И., Матвеев Г.В. Математические основы криптологии. – Минск.: БГУ, 1999. – 182 с.* ***15.*** *Феллер В. Введение в теорию вероятностей и ее приложения. – М.: Мир, 1964. – 498 с.* ***16.*** *Tetrapol News. PMR: Digital radio standardisation update/ № 6, September 1996.* ***17.*** *Radio Equipment and Systems (RES)/ Trans-European Trunked Radio (TETRA)/Voice plus Data (V+D)/Part 7: Security/ ETS 300 392-7 December 1996.* ***18.*** *Trans-European Trunked Radio (TETRA) systems; Technical requirements specification Part 3: Security aspects ETR 086-3 January 1994.*

УДК 621.395, 621.391.82

ПУТИ ПОВЫШЕНИЯ БЕЗОПАСТНОСТИ РАДИОИНТЕРФЕЙСА В СЕТЯХ ОПОВЕЩЕНИЯ

Александр Романов, Сергей Ливенцев, Игорь Столяр
Научный центр связи и информатизации, г. Киев

Анотація: **Рассмотрены пути повышения безопасности радиоинтерфейса в сетях оповещения. Произведен анализ и систематизация угроз безопасности информации. Предложены методы борьбы с ними.**
Summary: **In the article considered way of raising safety радиоинтерфейса in networks of notification. Made analysis and systematization of threats of safety information.. Offered methods of struggle with them.**
Ключові слова: **система радиосвязи, радиоинтерфейс, защищенность.**

Одной из задач, которая требует своего развития на базе достижений современных телекоммуникационных технологий, является совершенствование сетей передачи сигналов оповещения и сопровождающих их сообщений и команд. Эта задача актуальна для Вооруженных Сил Украины, Министерства по Чрезвычайным ситуациям, Министерства Внутренних дел и ряда других министерств и ведомств.

При решении этой задачи необходимо учитывать ряд особенностей и специфических требований, предъявляемых к функционированию систем такого типа.

1. Для достижения высокой вероятности доведения сигналов с требуемой степенью достоверности целесообразно обеспечивать передачу и прием сигналов параллельно по нескольким каналам связи, образованным различными средствами связи.

2. Сообщения, с помощью которых передаются сигналы оповещения, имеют малый объем. Это дает возможность вводить достаточно большую избыточность с целью достижения высокой надежности и достоверности доведения сигналов до абонентов.

3. Интенсивность возникновения сигналов очень мала, поэтому необходимо применять специальные меры для повышения эффективности использования оборудования.

4. Сигналы несут особо важную информацию, что требует принятия специальных мер по скрытности, достоверности, высокой степени безопасности, надежности и защите передаваемой информации, а так же исключения приема ложных сигналов.

5. Жесткие требования ко времени доставки сообщений и тенденции его уменьшения по мере совершенствования средств поражения и их носителей.