На правах рукописи

УСПЕНСКИЙ Александр Юрьевич

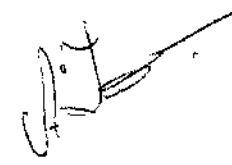
ЗАЩИТА ИНФОРМАЦИИ В РАДИОКАНАЛАХ МОБИЛЬНЫХ РОБОТОТЕХНИЧЕСКИХ КОМПЛЕКСОВ

Специальность 05.13.19 — Методы и системы защиты информации, информационная безопасность.

АВТОРЕФЕРАТ

диссертации на соискание ученой степени

кандидата технических наук



Москва - 2006

Работа выполнена в Московском государственном техническом университете имени Н.Э. Баумана

Научный руководитель:	кандидат технических наук, доцент **Медведев Николай Викторович**
Официальные оппоненты:	доктор технических наук, **Сычев Михаил Павлович** кандидат технических наук, **Скиба Владимир Юрьевич**
Ведущая организация:	Институт автоматизации проектирования Российской академии наук (г. Москва)

Защита состоится «14» 12 2006 г. на заседании диссертационного совета Д 219.007.02 в ФГУП «Всероссийский научно-исследовательский институт проблем вычислительной техники и информатизации (ВНИИПВТИ)» по адресу: 115114, г. Москва, 2-ой Кожевнический пер., д.8.

С диссертацией можно ознакомиться у ученого секретаря диссертационного совета.

Просим принять участие в работе Совета или прислать отзыв в одном экземпляре, заверенный печатью организации.

Автореферат разослан « __ » _____ 2006 г.

Ученый секретарь
диссертационного совета Д.219.007.02
кандидат технических наук. М. Б. Гордон

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность работы. В настоящее время, как в России, так и за рубежом ведутся активные работы по созданию мобильных робототехнических комплексов (МРК). Сфера применения комплексов обширна, первоочередными являются задачи, в ходе которых мобильный робот действует в условиях, опасных для нахождения человека. Перспективным является использование автоматизированных робототехнических комплексов в боевых условиях, когда имеется прямая угроза жизни оператора. В составе поисковой группы МРК могут осуществлять функции дистанционной разведки, действуя автономно и передавая данные по беспроводному каналу.

В МГТУ им. Баумана ведутся работы по созданию МРК, предназначенных для выполнения разнообразных задач в экстремальных условиях. Обычно в состав комплекса входит мобильный робот, который имеет на борту специальное оборудование, и система управления, которая, среди прочих устройств, включает пультовую ЭВМ, установленную на посту управления – рабочем месте оператора, а также бортовую ЭВМ, установленную на борту мобильного робота. Связь между пультовой и бортовой ЭВМ осуществляется посредством беспроводного канала стандарта IEEE 802.11.

При разработке МРК одной из важнейших задач является обеспечение необходимого условия защищенности информации. Наиболее уязвимыми являются данные, передаваемые через радиоканал. От поста управления на бортовую ЭВМ передаются команды управления, от бортовой ЭВМ на пультовую ЭВМ возвращаются данные по статусу систем мобильного комплекса и информация от датчиков (видео камеры, радар, приповерхностный сканер и т.д.). Команды, передаваемые роботу по беспроводному каналу, могут быть перехвачены и модифицированы. Данные, передаваемые от мобильного робота на пункт управления, так же могут быть перехвачены и модифицированы.

К системе аутентификации в беспроводной сети предъявляются повышенные требования по безопасности. Необходимо использовать

криптографически стойкие алгоритмы, позволяющие осуществить взаимную аутентификацию сторон.

Отдельной важной задачей является локализация активной станции-нарушителя в пределах защищенной беспроводной сети. Необходимо разработать технологию, позволяющую осуществлять эффективный поиск неавторизованной станции.

Настоящая диссертационная работа посвящена решению задачи защиты информации в радиоканалах мобильных робототехнических комплексов, путем применения комплексных мер по защите от возможных атак направленных на перехват и подмену передаваемых данных.

Целью диссертационной работы является исследование и разработка комплекса методов и средств защиты информации в радиоканалах стандарта IEEE 802.11b, применяемых в мобильных робототехнических комплексах.

Решение этой важной научной задачи требует проведения следующих научных исследований:

- Анализ структуры системы управления МРК;
- Формулирование основных требований к системе защиты данных в радиоканалах МРК;
- Исследование возможностей по защите информации, заложенных в протоколе стандарта IEEE 802.11b, применяемом при передаче данных по радиоканалу;
- Выявление недостатков в системе безопасности протокола IEEE 802.11b;
- Исследование и классификация возможных видов атак на информацию, передаваемую по радиоканалу;
- Анализ безопасности системы аутентификации, реализованной на основе протокола SPEKE;
- Разработка методов защиты информации от атак на систему аутентификации SPEKE;

- Разработка усовершенствованной системы защиты информации в радиоканале;
- Исследование методов обнаружения неавторизованной беспроводной станции;
- Разработка технологии, позволяющей осуществлять эффективный поиск и локализацию активной станции-нарушителя в защищенной беспроводной сети.

Объектом исследования являются радиоканалы стандарта IEEE 802.11b, применяемые в мобильных робототехнических комплексах.

Предметом исследования являются методы и средства защиты информации в радиоканалах стандарта IEEE 802.11b.

Методология исследования. Результаты диссертационной работы получены на основе методов защиты информации в радиоканале с применением криптографии и стойких алгоритмов защищенного обмена ключами по методу Диффи-Хелмана. Комплексный подход основан как на применении стандартных, хорошо зарекомендовавших себя методах защиты, так и на новых разработанных технологиях. Использованы научные положения теории вычисления дискретных логарифмов и операций на мультипликативных группах целых чисел поля Галуа.

Научная новизна. В диссертации лично автором получены следующие новые научные результаты:

- Разработана методика защиты от атак на стандартный протокол потокового шифрования WEP, применение которой значительно повышает уровень безопасности информации в радиоканале;
- Создана система аутентификации и обмена ключами для радиоканала на основе алгоритма SPEKE, превосходящая с точки зрения безопасности стандартные средства и добавляющая новые возможности для защищенного обмена сессионными ключами;
- Впервые предложена методика создания комплексной усовершенствованной системы безопасности данных в радиоканалах

802.11, объединяющая в себе шифрование данных, аутентификацию сторон и обмен ключами, применение которой значительно повышает уровень защиты данных, по сравнению со стандартными средствами;

- Разработана технология, использующая особенности протокола 802.11, с помощью которой осуществляется локализация активной станции-нарушителя, что позволяет устранить угрозу атак на информацию в защищенной сети.

Практическая ценность работы. Полученные теоретические и практические результаты рекомендуются к внедрению в организациях, использующих радиоканалы для передачи конфеденциальной информации с повышенными требованиями к безопасности.

Стандартная система защиты информации протокола 802.11 обладает рядом недостатков в области безопасности. Для практического использования в составе мобильных робототехнических комплексов создана усовершенствованная система защиты информации в радиоканалах, позволяющая значительно снизить риск утечки конфиденциальной информации и повысить степень защиты от несанкционированного доступа к данным. В усовершенствованную систему входят методы взаимной аутентификации, значительно превосходящие стандартные, а так же средства защищенного обмена сессионными ключами, отсутствующие в стандартной системе. Разработана технология, использующая особенности протокола 802.11, которая позволяет осуществить поиск активной станции-нарушителя, это позволяет снизить угрозу атак на информацию в защищенной сети.

Усовершенствованная система защиты информации успешно внедрена на МРК, разрабатываемом в МГТУ им. Баумана.

Апробация работы. Материалы работы были изложены автором на следующих конференциях и семинарах:

- Научно-техническая конференция «Информационная безопасность 2002» - М., 2002;

– 2-я международная научная конференция «Ракетно-космическая техника: фундаментальные и прикладные проблемы» - М., 2005;

Публикации. Основные результаты диссертационной работы опубликованы в 6 печатных работах.

Структура и объем работы. Диссертационная работа состоит из введения, четырех глав и заключения, изложенных на 149 страницах, содержит список литературы из 61 наименования, 9 таблиц и 31 рисунок.

На защиту выносятся следующие основные результаты работы:

- Методика защиты от атак на стандартный протокол потокового шифрования WEP, применение которой значительно повышает уровень безопасности информации в радиоканале;
- Система аутентификации и обмена ключами для радиоканала, превосходящая стандартные средства и добавляющая новые возможности для защищенного обмена сессионными ключами;
- Методика создания комплексной усовершенствованной системы безопасности данных в радиоканалах 802.11, объединяющая в себе шифрование данных, аутентификацию сторон и обмен ключами, применение которой значительно повышает уровень защиты данных, по сравнению со стандартными средствами;
- Технология, использующая особенности протокола 802.11, с помощью которой осуществляется локализация активной станции-нарушителя, что позволяет устранить угрозу атак на информацию в защищенной сети.

СОДЕРЖАНИЕ РАБОТЫ

Во введении отражены актуальность темы, сформулированы цели и задачи исследования. Приводится краткое содержание диссертации по главам.

В первой главе (Анализ структуры системы управления мобильным робототехническим комплексом) выполнен анализ структуры системы управления мобильным робототехническим комплексом. Рассмотрено взаимодействие между вычислительными задачами, функционирующими на пультовых и бортовых ЭВМ, реализованное посредством системной сетевой среды.

В состав комплекса входит мобильный робот, имеющий на борту специальное оборудование, оснащенный манипулятором, и система управления, в состав которой входят пульт дистанционного управления и каналы связи с мобильным роботом (см. рис. 1).

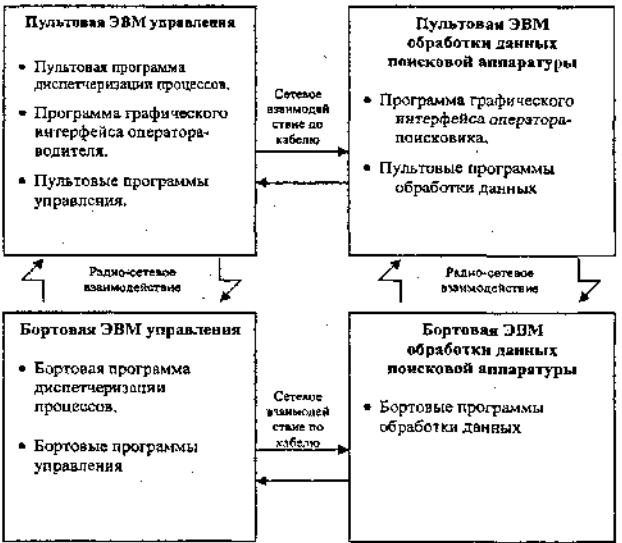


Рис. 1. Структурная схема системы управления и обработки данных поисковой аппаратуры МРК

Требования к защищенности информации, передаваемой по радиоканалу, прежде всего, определяются физическими принципами функционирования. Так как имеет место беспроводный способ передачи данных, то значительно увеличивается вероятность перехвата и модификации данных. В отличие от проводных сетей радиоканал может быть прослушан и сетевой трафик может быть перехвачен и проанализирован атакующей стороной с помощью пассивного приемника, настроенного на частоту передающего устройства. Факт перехвата при этом установить невозможно. Однако возможно установить факт активности неавторизованной беспроводной карты стандарта 802.11 в пределах сети, которую необходимо защитить. Это может быть проделано с помощью программного обеспечения, позволяющего осуществить мониторинг пакетов стандарта 802.11, а так же просмотр содержимого фреймов с целью обнаружения широковещательных рассылок с неавторизованных беспроводных карт.

Проведенный анализ публикаций по теме защиты информации и специфика применения (невозможность использования отдельного сервера сертификации в полевых условиях, повышенные требования к безопасности и т.д.) позволяет выделить перечень требований, определяющих качество защиты радиоканалов МРК. Данные в радиоканале считаются защищенными, если выполнены все требования, приведенные в таблице 1.

Таблица 1

Требования к защищенному радиоканалу МРК

1.	Создать защиту от несанкционированного расшифрования и изменения информации, передаваемой по радиоканалу МРК
2.	Обеспечить целостность данных при передаче
3.	Реализовать средства, обеспечивающие невозможность раскрытия внутренней структуры сети при перехвате сообщений
4.	Использовать надёжную систему аутентификации и обмена ключей
5.	Использовать криптографически стойкий алгоритм аутентификации
6.	Применить методы, позволяющие осуществить взаимную аутентификацию обоих сторон
7.	Реализовать механизм смены секретных ключей
8.	Использовать надежные средства передачи секретных сеансовых ключей
9.	Разработать технологию, позволяющую обнаружить и локализовать активную неавторизованную беспроводную станцию в пределах радиосети

В конце главы, на основе проведенного исследования выполнена формальная постановка задачи диссертационной работы, включающая в себя требования и ограничения.

Во второй главе (Исследование проблем защиты информации в радиоканале) рассмотрены особенности структуры беспроводных сетей стандарта IEEE 802.11b с точки зрения защиты информации. Проанализированы стандартные средства и методы защиты информации в

радиоканале 802.11b. Проведена оценка механизма аутентификации. Проведен анализ уязвимостей в службах контроля доступа. Исследованы методы защиты информации в протоколе WEP. Приведена задача дискретного логарифмирования в применении к криптографическим приложениям. Проанализированы элементы теории групп, связанные с методами Диффи-Хелмана. Проведено исследование алгоритмов аутентификации и обмена SPEKE и DH-EKE. Составлена сводная характеристика возможных атак на беспроводную сеть, описаны основные классы атак.

Причиной рисков, связанных с безопасностью информации, при использовании сетевой инфраструктуры стандарта 802.11b являются атаки на конфиденциальность информации (перехват и анализ трафика), целостность (подмена адреса, повтор и модификация сообщения) и атаки типа «Отказ в обслуживании» (см. рис. 2).

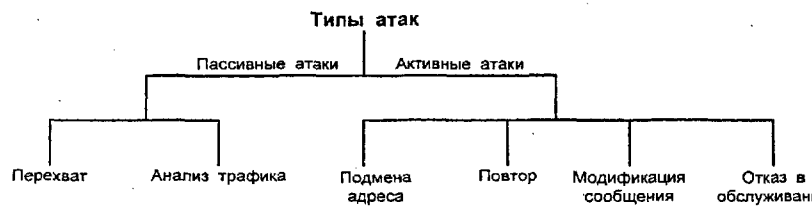


Рис. 2. Типы атак на беспроводную сеть стандарта 802.11

В третьей главе (Разработка комплекса методов и средств защиты информации в радиоканалах) созданы методы улучшения стандартной системы безопасности основанной, на алгоритме WEP. Проведена оценка системы аутентификации на основе алгоритма SPEKE, показаны источники потенциальных угроз безопасности и разработаны средства защиты. Разработаны методы оптимизации алгоритма SPEKE по быстродействию. Обоснована возможность применения стойких гибридных систем, которые могут использовать для дополнения друг друга независимые методы, как базирующиеся на ключах, так и основанные только на паролях. На основе полученных результатов создана усовершенствованная система безопасности МРК.

Пассивная атака с целью расшифровки трафика

Вектор инициализации (далее IV) является 24 разрядным числом, которое используется совместно с секретным 40 битным ключом для генерации ключевой последовательности. Таким образом, каждая станция, участвующая в сеансе связи на скорости 11 Мбит/с, может исчерпать все комбинации чисел IV в течение пяти часов:

$$\frac{1500\ \text{байт}}{\text{пакет}} \times \frac{8\ \text{бит}}{1\ \text{байт}} \times \frac{1\ \text{сек}}{11\ \text{Мбит}} \times \frac{1\ \text{Мбит}}{10^6\ \text{бит}} \times 2^{24}\ \text{пакетов} \approx 18{,}300\ \text{сек} \approx 5\ \text{часов}$$

Далее возможен статистический анализ для восстановления исходного незашифрованного теста, содержащегося в одном из сообщений. В случае удачного подбора, проведя операцию «исключающее ИЛИ» (XOR, $\oplus$) над зашифрованным сообщением и распознанным текстом злоумышленник восстанавливает соответствующую ключевую последовательность k, позволяющую ему просматривать все остальные зашифрованные сообщения, зашифрованные с помощью данного IV:

$$M \oplus C = M \oplus (M \oplus RC4(IV, K)) = RC4(IV, K)$$

Так как злоумышленник имеет два или несколько пакетов зашифрованных одним и тем же IV, он имеет возможность применить операцию XOR к содержимому и выявить различия и совпадения в структуре:

$$C_1 = M_1 \oplus RC4(IV, K);$$

$$C_2 = M_2 \oplus RC4(IV, K),$$

где C_1 и C_2 - сообщения зашифрованные с помощью одного IV. Тогда

$$C_1 \oplus C_2 = (M_1 \oplus RC4(IV, K)) \oplus (M_2 \oplus RC4(IV, K)) =$$

$$= M_1 \oplus M_2$$

Применение операции XOR над двумя такими зашифрованными сообщениями позволяет исключить влияние ключевой последовательности и анализировать разницу незашифрованных данных ($M_1 \oplus M_2$), что может позволить раскрыть содержимого пакетов методом статистического анализа.

Активная атака с целью подмены трафика

В случае если злоумышленник не достиг полной расшифровки содержимого пакета, он может произвольно изменять значение битов в сообщении, затем добавлять пересчитанное значение контрольной суммы ICV для имитации корректной версии модифицированного пакета. Операция XOR обладает свойством дистрибутивности: $c(x \oplus y) = c(x) \oplus c(y)$ для любых x и y. Рассмотрим ситуацию, в которой произведён перехват пакета с данными, где C – зашифрованные данные:

$$A \rightarrow (B) : (IV \,||\, C)$$

При этом C соответствует некому зашифрованному сообщению P:

$$C = (P \,||\, c(P)) \oplus RC4(IV, K)$$

Возможно создание такого зашифрованного сообщения C' которое соответствует P', где $P' = P + \Delta$, причём Δ может быть подобрана атакующей стороной. Далее появляется возможность подмены пакета с данными:

$$(A) \rightarrow B : (IV \,||\, C')$$

В этом случае станция B получит изменённый пакет данных P' с корректным значением контрольной суммы.

Рассмотрим механизм получения значения C', которое соответствует M'. Так как алгоритм RC4, применяющийся в WEP, использует для преобразований линейные функции, становится возможным следующее преобразование – применение XOR $(\Delta \,||\, c(\Delta))$ к информационному пакету, с целью получить значение C':

$$C' = C \oplus (\Delta \,||\, c(\Delta)) =$$
$$= RC4(IV, K) \oplus (P \,||\, c(P)) \oplus (\Delta \,||\, c(\Delta)) =$$
$$= RC4(IV, K) \oplus ((P \oplus \Delta) \,||\, (c(P) \oplus c(\Delta))) =$$
$$= RC4(IV, K) \oplus (P' \,||\, c(P \oplus \Delta)) =$$
$$= RC4(IV, K) \oplus (P' \,||\, c(P'))$$

В данном случае мы использовали тот факт, что преобразование CRC линейно и, следовательно, $c(P) \oplus c(\Delta) = c(P \oplus \Delta)$. В результате, становится

возможным преобразовать зашифрованное сообщение C в C', которое соответствует открытому сообщению $P \oplus \Delta$, т.е. изменённому атакующей стороной. Таким образом, возможно невыявляемое нарушение целостности информационных пакетов, причем требуется лишь частичное знание содержимого пакета для его модификации.

Активная атака с подменой адреса

Для осуществления данной атаки недостаточно просто заменить IP адрес получателя пакета, необходимо чтобы контрольная сумма изменённого пакета была корректной. Предположим, что D_L и D_H – это две 16-битные части исходного IP адреса получателя, их необходимо заменить на D'_L и D'_H. Обозначим значение исходной контрольной суммы как S, причём ее значение не обязательно должно быть известно. Тогда новое значение вычисляется по формуле:

$$S' = S + D_L + D_H - D'_L - D'_H$$

Если значение S заранее известно, то несложно вычислить значение S' и модифицировать пакет операцией XOR со значением $S \oplus S'$. Если S заранее не известно, то задача гораздо сложнее. Известно значение $E = S' - S$, необходимо вычислить $\Delta = S \oplus S'$. При использовании методов статистического анализа и имея представления о возможной структуре сообщения, велика вероятность подбора нужного значения.

В результате, можно переправить сообщение адресату за пределами защищенной сети.

Атака на основе составления таблицы

Относительно малое количество возможных значений IV позволяют атакующей стороне построить таблицу расшифровки. При достаточно хорошо отработанной технологии статистического анализа злоумышленник может построить таблицу соответствия IV векторов и соответствующих им ключевых последовательностей. Такая таблица будет содержать порядка 2^{24} (более 16 миллионов) записей, что составит объём порядка 24 Гб. Пользуясь этой

таблицей, злоумышленник сможет расшифровать любой пакет без усилий, достаточно выяснить только значение ключевой последовательности по его IV.

Система аутентификации

Система аутентификации для радиоканала стандарта 802.11b построена на основе стандарта IEEE 802.1x. Среди EAP методов, разработанных специально для беспроводных сетей, стоит особо выделить семейство, основанное на стойких паролях. Алгоритм SPEKE был разработан с целью преодолеть проблемы, связанные с неудовлетворительным уровнем безопасности и высокой сложностью в реализации, присущие методам аутентификации, основанным на сертификатах.

Алгоритмы SPEKE и DH-EKE базируются на методе обмена ключей Диффи-Хелмана. Классический обмен по алгоритму DH позволяет двум сторонам без предварительной договоренности создать общий секретный ключ сессии.

Алгоритмы используют арифметику внутри большой конечной группы. Несколько видов таких групп могут быть использованы в DH, однако мы ограничимся рассмотрением Z_m^*, где m является большим простым числом.

Определим термины (см. таблицу 2).

Таблица 2

Таблица терминов

S	Секретный общий пароль для сторон A и B небольшого размера
m	Большое простое число, подходящие для использования в алгоритме Диффи-Хелмана
q	Большой простой множитель числа m -1
g	Подходящий генератор порядка большого простого числа
G_x	Подгруппа Z_m^* порядка x. Где x – множитель m-1.
$f(S)$	Функция, которая конвертирует S в соответствующий базис DH
R_A, R_B	Случайные числа, выбранные сторонами A и B
Q_A, Q_B	Значения, посланные сторонами A и B

$E_k(t)$	Симметричная функция шифрования от *t*, используя ключ *k*.
$h(t)$	Стойкая односторонняя хеш-функция от *t*
$A \rightarrow B$: *t*	Сторона А посылает *t* стороне В
K	Порожденный ключ сессии

В алгоритме SPEKE сторона В получает запрос от стороны А, создаёт большое случайное число R_B и вычисляет:

$$Q_B = f(S)^R{}_B \bmod m \text{ , } B \rightarrow A\text{: } Q_B, m,$$

где *m* – большое простое число, используемое как модуль.

Сторона В пересылает *m* и Q_B пользователю в теле запроса. Сторона А создаёт ещё одно большое случайное число R_A и вычисляет:

$$Q_A = f(S)^R{}_A \bmod m, \; A \rightarrow B\text{: } Q_A$$

На следующем шаге пользователь вычисляет:

$$K = h(Q_B{}^R{}_A \bmod m),$$

где *K* – вычисленный пользователем основной ключ сессии, Q_B – значение, полученное от стороны В.

В таблице 3 приведены методы защиты от атак для алгоритмов SPEKE и DH-EKE, знак √ отмечает подверженность алгоритма данному виду атак.

Таблица 3

Методы защиты для алгоритмов SPEKE и DH-EKE

	Метод защиты	**Предотвращаемая атака**	**SPEKE**	**DH-EKE**
1.	Модуль *m* должен быть большим числом	Атака на основе быстрого вычисления дискретного логарифма	√	√
2.	Проверка на Q_x ! = 0, в случае не зашифрованных значений	Форсирование значения *K* = 0	√	√
3.	Значение *m* - 1 должно иметь большой простой множитель *q*.	Вычисление логарифма по методу Поллинга-Хэлмана	√	√

	Метод защиты	Предотвращаемая атака	SPEKE	DH-EKE
4.	Шифрование Q_x, разбитого на части и собранного в случайном порядке	Утечка информации из значения $E_S(Q_x)$		√
5.	База g должна быть первообразным корнем от m.	Распределенная атака на $E_S(Q_x)$		√
6.	База должна быть генератором для q	Распределенная атака на Q_x	√	
7.	База в виде $S_x \bmod p$	Атака типа «пароль-в-экспоненте»	√	
8.	Требуется шифровать Q_x при проверке K	Подбор пароля S используя R_x, Q_x, $E_K(x)$ и словаря паролей		√
9.	Использование одностороннего хеширования значения K	Атака на ограничение значений	√	√
10.	Первый бит m должен равняться 1	Распределенная атака на $E_K(Q_x)$		√
11.	Шифрование значений Q_A, Q_B	Ограничение по подгруппам для K		√
12.	Прерывание работы, если K малого порядка	Ограничение по подгруппам для K	√	

Возможные атаки на процесс DH-обмена можно условно разделить на следующие классы:

– Быстрое вычисление дискретного логарифма (1, 3);

– Утечка информации (2, 4-8, 10);

– Ограничение по небольшим подгруппам (9, 11, 12).

В атаке «Быстрое вычисление дискретного логарифма» производится обратное преобразование от возведения в степень по модулю m, с целью восстановления показателя степени и, в конечном счете, пароля S. Трудность этих вычислений зависит от размера и свойств числа m. Устойчивость алгоритма к данной атаке основывается на практической невозможности подобного вычисления.

Необходимо отметить, что перехват значений экспоненты, возможно зашифрованной, не приводит к утечке информации о пароле S. Утечка даже одного бита информации о пароле может быть критичной. В случае применения атаки с подбором по словарю, позволяет разделить возможные пароли на две группы: подходящие и заведомо неправильные.

Наконец, атакующая сторона, которая знает структуру Z_m^* , может быть способна ограничить область возможных значений K до размера небольшой подгруппы, которая позволяет догадаться о значении или применить атаку перебором. При проведении анализа безопасности алгоритма Диффи-Хелмана предполагается, что K всегда расположено с равномерной вероятностью в Z_m^* . Это предположение является неверным, так как, начиная с первого возведения g в степень, являющуюся случайным числом, происходит попадание результатов в меньшую подгруппу, по крайней мере, в половине случаев. На этой закономерности основывается атака «Ограничение по небольшим подгруппам».

Усовершенствованная система защиты информации

Слабые стороны стандартной системы безопасности протокола 802.11b вызваны как чисто физическими факторами, так и особенностями реализации. Основными недостатками являются:

- Недостатки, связанные с шифрованием;
- Недостаточно надежная система аутентификации;
- Отсутствие системы безопасного обмена ключами.

Стандартная система безопасности стандарта IEEE 802.11 нуждается в серьезном улучшении. Для этого необходимо применить комплексный подход к данной проблеме. Комплексная усовершенствованная система защиты информации в радиоканале 802.11b показана на рис. 3.

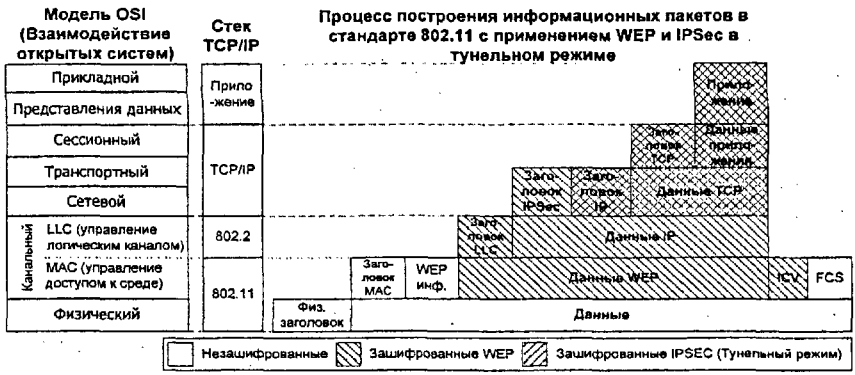


Рис. 3. Усовершенствованная система защиты информации для радиоканала 802.11

Основные настройки и элементы, применяемые в усовершенствованной системе безопасности:

Стандартная система безопасности:

- Активизация протокола WEP;
- Установление длины ключа 104 бит;
- Включение фильтрации MAC адресов.

Система аутентификации:

- Алгоритм аутентификации и распределения ключей SPEKE.

IPSec (Туннельный режим):

- Инкапсуляция зашифрованных данных (ESP) с применением алгоритма 3DES.

Изменение установок по умолчанию для сетевого оборудования:

- ID администратора;
- Пароль администратора;
- Секретный ключ WEP;
- SSID.

Управление секретными ключами WEP:

– Защищённая передача ключа на основе алгоритма SPEKE по заданному расписанию.

В четвертой главе (Обнаружение и локализация станции-нарушителя, атакующей систему безопасности радиоканала) рассмотрены методы и средства обнаружения перехвата информации в беспроводной сети. На основе экспериментальных данных разработана технология, позволяющая осуществлять эффективный поиск и локализацию неавторизованной станции в защищенной беспроводной сети. Выявлены причины возможного возникновения ошибок, приведены методы повышения эффективности определения местоположения станции-нарушителя.

В результате экспериментов и исследований было получено следующее соотношение для распространения радиосигнала в здании на частоте 2,4 ГГц:

$$R_d = C - 35\lg D$$

Где:

D – расстояние (м);

R_d – потери в радиоканале (Дб).

С – константа, определяющая выходную мощность с учетом влияния затуханий, конфигурации антенны и других факторов

Ожидаемая погрешность находиться в диапазоне 13 Дб. Построим функциональную зависимость уровня сигнала от координат, где R_d - уровень полученного сигнала (Дб), N - ненормированное значение уровня полученного сигнала (%), T_x и T_y – координаты передатчика, C – константа, определяющая выходную мощность с учетом влияния затуханий, конфигурации антенны и других факторов.

$$R_d = C - 35\lg\sqrt{(T_x - x)^2 + (T_y - y)^2}$$

$$N = 0{,}83(C - 35\lg\sqrt{(T_x - x)^2 + (T_y - y)^2}) + 83{,}891$$

В таблице 3 приведены реальные значения и наилучшие соответствия, полученные из наборов данных.

Таблица 3

Результаты эксперимента

	Координата передатчика (x)	Координата передатчика (y)	Найденное значение (x)	Найденное значение (y)	Значение константы C (зависит от мощности передатчика)
Cisco AP350s с антенной	5.18	-14.94	5.15986 +/- 0.9969	-14.847 +/- 0.7456	-20.1008 +/- 1.706
Cisco AP350s без антенны	12.50	-18.29	11.3324 +/- 0.2842	-16.2561 +/- 0.55	-50.4432 +/- 0.6815
Orinoco AP-1000 с антенной Lucent	14.17	-13.11	14.6243 +/- 1.3	-21.1688 +/- 2.547	-34.1176 +/- 2.639

Погрешность двух результатов не превышает 2 метров, тогда как погрешность третьего результата больше 8 метров.

В результате проведенного эксперимента разработана технология, позволяющая локализовать неавторизованную активную станцию, размещенную в зоне работы беспроводной сети.

Анализ результатов показал высокую эффективность применения данного комплекса мер для предотвращения возможности атаки на систему защиты информации в радиоканале.

Выявлены наиболее вероятные причины возникновения ошибок при вычислении координат:

- Затухание сигнала от антенны передатчика было велико. На пути сигнала располагались препятствия;
- Передатчик располагался в середине помещения, следовательно, не удалось собрать достоверную информацию о затухании сигнала на предельных расстояниях;
- Передатчик располагался в помещении с большим количеством металлических предметов, что дополнительно ослабляло и экранировало сигнал в определенных направлениях.

К основным ограничениям предложенного метода относятся:

- При использовании данной технологии невозможно определить местоположение неактивной станции;
- Драйвер и сетевая карта Cisco ограничены в возможности сканирования произвольного трафика, таким образом, некоторое количество полезных данных могло быть утеряно в ходе эксперимента;
- Карта Cisco не может сканировать несколько каналов одновременно. При возникновении сигнала от неавторизованной станции, все карты, задействованные для защиты сети, должны приостановить сканирование и переключиться на этот канал, с целью наиболее полного сбора информации.

Выявлены методы повышения эффективности разработанной технологии:

- Поисковая станция должна сканировать все частоты по всему спектру одновременно;
- Включение в состав комплекса GPS навигаций может значительно улучшить результаты и упростить сбор данных;
- Привлечение как минимум 3-х поисковых станций значительно улучшит результаты.

В заключении сформулированы основные теоретические, методические и практические результаты диссертационной работы.

ОСНОВНЫЕ РЕЗУЛЬТАТЫ

Цель, сформулированная в диссертационной работе, по исследованию и разработке комплекса методов и средств защиты информации в радиоканалах МРК, достигнута.

1. Проведено исследование особенностей работы стандартного протокола потокового шифрования WEP. Для каждого из видов атак разработаны методы противодействия, позволяющие повысить степень защиты данных в радиоканале.
2. Разработана система аутентификации, основанная на алгоритме SPEKE. Проведено исследование с точки зрения защиты информации, проанализированы механизмы возникновения атак, созданы методы противодействия. Разработанная система является заменой стандартным средствам аутентификации протокола 802.11, не обладающим достаточным уровнем безопасности.
3. На основе алгоритма SPEKE создан механизм защищенного обмена ключами сессии, отсутствующий в стандартной системе безопасности. Возможность смены ключа сессии позволит снизить вероятность успешных атак на информацию, зашифрованную с помощью алгоритма потокового шифрования WEP.
4. Создана усовершенствованная система защиты информации, передаваемой в радиоканале 802.11, позволяющая значительно повысить уровень защиты информации, по сравнению со стандартной системой, за счет применения комплекса криптографически стойких средств и методов шифрования данных, аутентификации и обмена ключами.
5. Разработана технология, позволяющая использовать особенности протокола 802.11 для локализации станции-нарушителя, размещенной в зоне работы беспроводной сети. Созданы методы повышения эффективности работы системы поиска активных станций-нарушителей.

Это позволит значительно снизить вероятность атак на информацию в радиоканалах.

Достоверность научных положений диссертации подтверждена: выполненными экспериментальными исследованиями, практической реализацией системы защиты данных в радиоканале МРК и результатами внедрения.

Основное содержание диссертации отражено в следующих печатных работах:

1. Успенский А. Ю. Применение интерфейса Photon в системе управления робототехническим комплексом // Компью-Лог, - 2001. - №5. - С. 13-20.
2. Успенский А.Ю., Иванов И.П. Анализ проблем защиты информации в радиоканалах стандарта IEEE 802.11 // Вестник МГТУ. Сер. Машиностроение. - 2002. - №. 4 - С. 102-108.
3. Успенский А.Ю. Исследование возможности и методы противодействия перехвату защищённой при помощи протокола WEP информации в радиоканале стандарта IEEE 802.11 // Студенческая научная весна – 2002. Сборник докладов студенческой научной конференции. – М.: МГТУ им. Н.Э. Баумана, 2002. – С. 89 - 91.
4. Медведев Н.В., Успенский А.Ю. Возможности перехвата защищённой информации в радиоканале стандарта IEEE 802.11 // Сборник докладов к научно-технической конференции «Информационная безопасность 2002» - М. «КомпьюЛог», 2002. – С. 58-63.
5. Иванов И.П., Успенский А.Ю. Модель информационной безопасности радиоканала IEEE 802.11. // Вестник МГТУ. Сер. Машиностроение. - 2003. - №.2(51) – С.89 – 94.
6. Медведев Н.В., Успенский А.Ю. Усовершенствованная система безопасности радиоканала IEEE 802.11. // Вестник МГТУ. Сер. Машиностроение. - 2006. - №.4(71) – С.73 – 78.