Уфа : УГАТУ, 2010 Вестник УГАТУ Т. 14, № 2 (37). С. 245–250



УДК 004.7

**И. И. БЕЗУКЛАДНИКОВ, Е. Л. КОН**

# СКРЫТЫЕ КАНАЛЫ В РАСПРЕДЕЛЕННЫХ АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ

Предложен универсальный подход к созданию скрытых каналов. Проанализированы особенности функционирования типового интернет-шлюза LonWorks-Internet, отвечающего требованиям современных стандартов ИБ. Предложен способ организации скрытого канала в распределенной автоматизированной системе управления интеллектуальным зданием, использующей такой шлюз. Произведена оценка основных качественных показателей полученного скрытого канала. Приведен один из методов разрушения подобного канала. *Информационная безопасность*; *информационная система*; *скрытые каналы*; *LON*; *распределенные системы*

В последнее время все большее внимание начинает уделяться проблемам информационной безопасности (ИБ) в сложных информационно-управляющих системах (ИУС). Особенно актуальна проблема ИБ для разнообразных распределенных автоматизированных систем, в которых, как правило, отследить наличие или отсутствие на всех узлах АС программно-аппаратных агентов, используемых злоумышленником для осуществления атаки, не представляется возможным для требуемого уровня достоверности, либо является экономически нецелесообразным. Одними из наиболее уязвимых являются разнообразные системы управления «интеллектуальными зданиями». Это происходит по причине того, что зачастую с целью обеспечения функций удаленного управления и мониторинга в таких системах организуется шлюзование с внешними сетями, в том числе сетью Интернет. Для успешного осуществления атаки на такую систему злоумышленник должен обладать средствами коммуникации, позволяющими осуществлять обмен информацией между ним и программно-аппаратными агентами внутри АС. Функционирование такого канала связи в условиях активного противодействия со стороны средств защиты возможно при выполнении агентами необходимых условий, при которых нелегальная передача данных будет незаметна для действующей политики ИБ. Одним из наиболее эффективных вариантов реализации таких условий является использование агентами для осуществления коммуникаций между собой нетрадиционных каналов связи, являющихся принципиально невидимыми для имеющихся средств защиты. В рамках настоящей статьи будет рассмотрена реализация такого нетрадиционного скрытого канала связи, функционирующего в типовой распределенной системе управления интеллектуальным зданием, построенной в соответствии со стандартом ИБ NIST draft 800-82 [1], и рассчитаны его основные технические характеристики.

## 1. ПОДХОД К ПОСТРОЕНИЮ СКРЫТЫХ КАНАЛОВ

В общем виде для создания скрытого канала необходимо выполнить следующие основные действия.

1. Проанализировать принцип действия и особенности технологии, используемой на соответствующем уровне легальной системы. Предложить принцип, который может быть использован для скрытого переноса информации.

2. Оценить действующую политику информационной безопасности и выделить ее аспекты, относящиеся к выбранному уровню, а также выделить иные действующие в системе ограничения, препятствующие реализации скрытой передачи информации при помощи предлагаемого принципа.

3. Проанализировать выполнение необходимых условий существования скрытого канала [2].

4. Предложить конкретную реализацию скрытого канала, использующего предлагаемый принцип передачи информации.

5. Оценить основные технические характеристики полученной реализации скрытого канала.

Контактная информация: newschannel@pstu.ru

## 2. ПОСТРОЕНИЕ СКРЫТОГО КАНАЛА В РАСПРЕДЕЛЕННОЙ УПРАВЛЯЮЩЕЙ СИСТЕМЕ

### 2.1. Анализ особенностей типовой системы управления интеллектуальным зданием

На рис. 1 представлена упрощенная схема, отражающая типовую структуру современной распределенной системы управления интеллектуальным зданием. Нижний уровень системы представляет собой fieldbus-сеть интеллектуальных датчиков и исполнительных механизмов, построенную в соответствии со стандартом Echelon LonWorks. На верхнем уровне находится корпоративная локальная вычислительная сеть (ЛВС), имеющая выход в Интернет. В рамках корпоративной ЛВС функционирует HTTP-сервер, отвечающий за предоставление web-интерфейса для удаленного мониторинга и управления. Взаимодействие уровней системы осуществляется с помощью стандартного LonWorks-IP шлюза производства Echelon [3].

В соответствии с рекомендациями NIST 800-82 в системе установлены следующие элементы обеспечения информационной безопасности: брандмауэр между глобальной сетью и корпоративной ЛВС, брандмауэр между корпоративной промышленной сетью, монитор обращений.

Интерфейс управления и мониторинга, реализуемый при помощи HTTP-сервера с соответствующим программным обеспечением, имеет как минимум 2 уровня доступа:

- только мониторинг – доступен незарегистрированным в системе пользователям;
- мониторинг и управление – доступен пользователям, прошедшим проверку.

Все виды попыток НСД, описанные в NIST 800-82, протоколируются установленным в системе монитором обращений.

Будем считать, что на уровне fieldbus-сети уже существует одна или несколько закладок, предварительно внедренных злоумышленником. Данное допущение является вполне вероятным, поскольку проектирование таких сетей может выполняться силами сторонних организаций с использованием сложных комплектов программного обеспечения иностранного производства. Это, в свою очередь, обуславливает возможность появления программной закладки в элементах fieldbus-инфраструктуры как преднамеренно, путем ее внедрения в исходный код соответствующего проекта, так и непреднамеренно, на этапе компиляции – в этом случае может быть внедрена закладка, созданная производителем программного обеспечения для разработки.

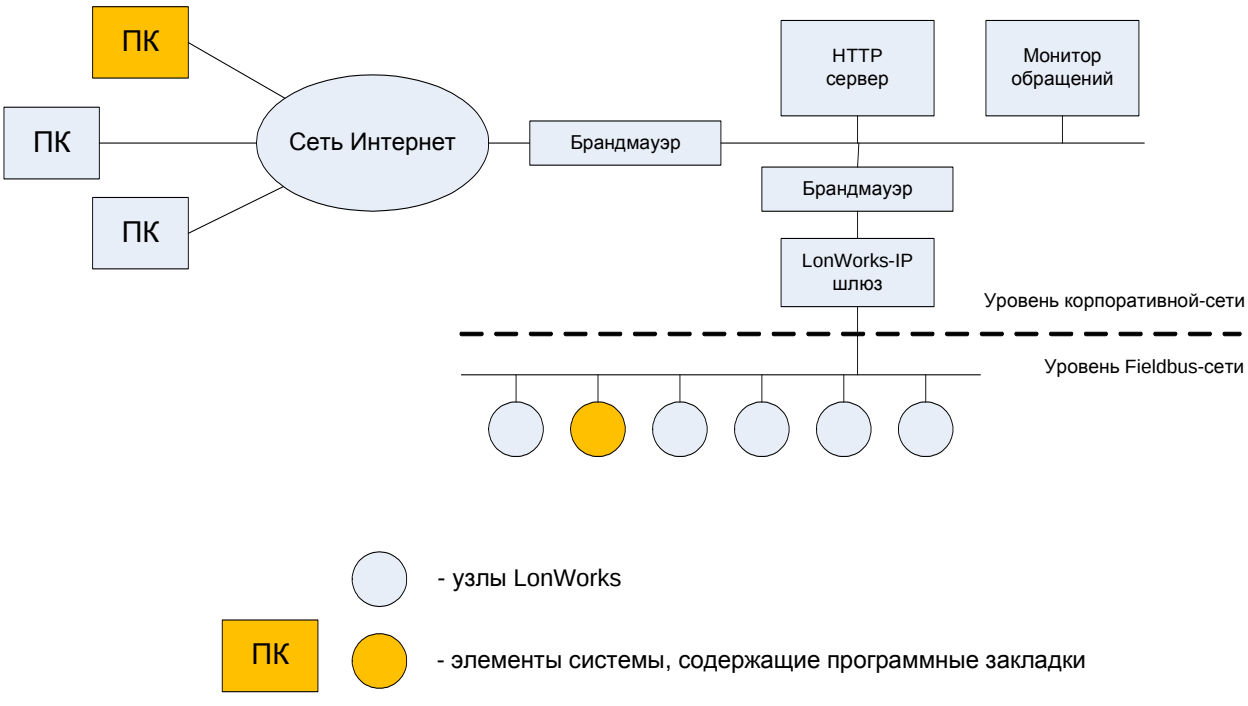


**Рис. 1**

Таким образом, по итогам анализа приведенной системы с точки зрения потенциальной скрытой передачи информации можно сделать следующие выводы:

- в системе находится одна или несколько предварительно внедренных программных закладок на уровне fieldbus-сети (одно из возможных расположений закладок показано на рис. 1);
- злоумышленник имеет возможность создания одного или нескольких программных агентов на узлах внешней сети;
- злоумышленник не имеет возможности влиять на функционирование описанных элементов ИБ, имеющихся в системе;
- злоумышленник имеет возможность доступа к интерфейсу мониторинга из внешней сети.

### 3.2. Анализ особенностей политики информационной безопасности

В настоящее время в используемых для подобного класса систем типовых политиках информационной безопасности отсутствуют положения, относящиеся к противодействию НСД, осуществляемому при помощи метода скрытых каналов. Тем не менее, несмотря на их отсутствие, в некоторых случаях в системе могут существовать ограничения, которые не позволят организовать тот или иной тип скрытого канала либо затруднят его функционирование. Кроме того, нарушение каких-либо контролируемых параметров системы может привести к ее детальной проверке и, как следствие, к выявлению скрытого канала. К таким параметрам можно отнести коэффициент битовых / символьных ошибок, задержку при передаче/приеме сигнала, вариацию времени задержки сигнала, изменение скорости передачи, ограниченность аппаратных ресурсов и т. д.

Следует отметить, что в рассматриваемом классе систем, как правило, осуществляется строгий контроль приведенных ограничений, что в сочетании с небольшой избыточностью используемых протоколов (отсутствие «лишних» или «неиспользуемых» полей, малая структурная сложность) может значительно затруднить либо даже сделать невозможным реализацию скрытых каналов. Тем не менее, зачастую определенные особенности используемых протоколов передачи данных и их сочетаний позволяют организовать скрытый канал, использующий альтернативный способ функционирования. Один из таких способов мы и приведем далее.

Таким образом, на основании анализа существующих для подобных систем типовых политик безопасности можно сделать следующие выводы:

- в политиках ИБ для подобных информационных систем отсутствуют правила и нормы, непосредственно обеспечивающие контроль и противодействие скрытым каналам;
- в системе могут существовать дополнительные ограничения, препятствующие организации скрытого канала; такие ограничения зависят от области применения системы и должны быть сформулированы применительно к ее конкретной реализации.

### 3.3. Анализ выполнимости необходимых условий реализации СК

Как уже было сказано выше, для создания скрытого канала любого типа необходимо обеспечить выполнение определенного набора условий. К ним относятся:

- Наличие в системе ресурсов, достаточных для реализации алгоритмов, обеспечивающих функционирование скрытого канала.

Здесь и далее при описании примера авторы будут подразумевать, что у системы достаточно ресурсов для реализации алгоритмов скрытого канала, и что злоумышленник имел необходимый для внедрения в элементы системы уровень доступа.

- Наличие общего разделяемого ресурса между субъектами информационного обмена по скрытому каналу.

Рассмотрим более подробно взаимодействие узлов сети, показанной на рис. 1, содержащих программные закладки, внедренные злоумышленником. На рис. 2 показана модель такого взаимодействия, включающая все узлы, участвующие в типовом сеансе обмена мониторинговой информацией. Сеанс связи проходит по следующим этапам:

**1-2:** атакующий ПК осуществляет HTTP-запрос через сеть Интернет к серверу, содержащему команду на чтение параметра интересующего LON-узла,

**2-3:** HTTP-запрос на чтение обрабатывается корпоративным брандмауэром,

**3-5:** HTTP-сервер генерирует OPC-запрос к шлюзу,

**5-6:** OPC-запрос на чтение данных из промышленной сети обрабатывается брандмауэром,

**6-7:** OPC-запрос обрабатывается LonWorks-IP шлюзом и преобразуется в SNVT-запрос, отправляемый непосредственно на узел в сети LonWorks.

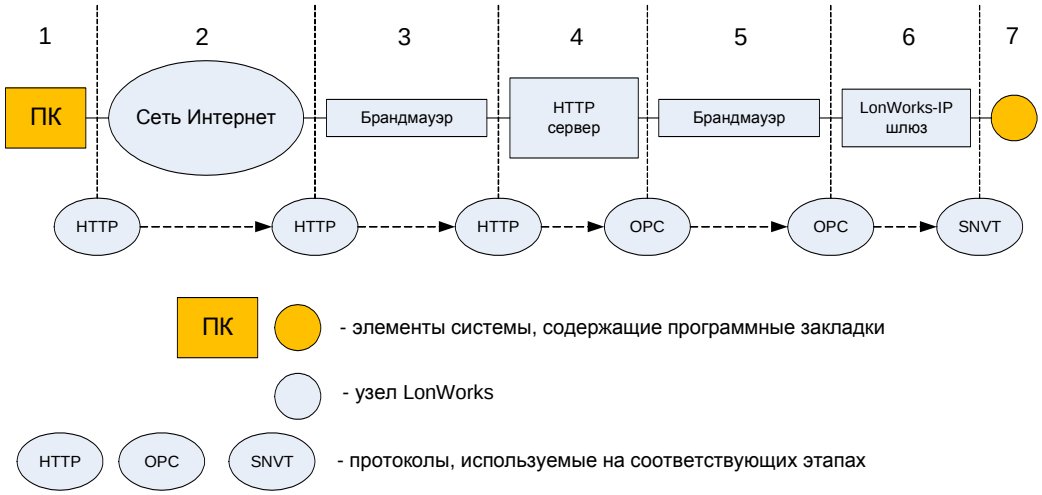


**Рис. 2**

Как видно из приведенных этапов, на пути следования запроса производится несколько преобразований используемых протоколов. В сочетании с малой избыточностью используемых в промышленных сетях протоколов это приводит к невозможности организации скрытого канала при помощи одного из наиболее популярных методов: передачи информации в неиспользуемых протокольных полях.

Тем не менее, возможна реализация некоторых из приведенных в [2] способов организации скрытого канала. К таким способам, в частности, относится модуляция интервалов времени между протокольными единицами или изменение их порядка следования.

В силу ограниченности объема статьи, далее авторами будет более подробно рассмотрен лишь один из вариантов – передача информации при помощи модуляции временных интервалов между запросами. Для успешного использования временных интервалов между запросами в качестве общего ресурса необходимо проанализировать влияние на них всех промежуточных этапов прохождения запроса. Авторами настоящей статьи был проведен такой анализ для показанной на рис. 2 модели, который показал, что в такой системе принципиально возможно детектирование вносимой передатчиком задержки на приемной стороне при выполнении следующего условия [4]:

$$T_{\text{пер}} > n \cdot (T_{13} + T_3 + T_4 + T_5 + T_6),$$

где $T_{\text{пер}}$ – задержка, вносимая передатчиком скрытой информации; $n$ – натуральное число; $T_{13}$ – задержка транспортировки по сети Интернет; $T_3$ – задержка обработки запроса корпоративным брандмауэром; $T_4$ – задержка обработки запроса HTTP-сервером; $T_5$ – задержка обработки запроса IP-Fieldbus брандмауэром; $T_6$ – задержка обработки запроса LonWorks-IP шлюзом.

● Обеспечение скрытности канала в условиях действующей в системе политики информационной безопасности.

Обеспечение скрытности канала зависит от особенностей конкретной системы и действующей политики информационной безопасности. В рамках данной статьи авторы будут в качестве примера оценивать скрытность при помощи анализа задержки, вносимой функционированием алгоритма СК на узлах LonWorks, поскольку из-за ограниченности ресурсов соответствующих аппаратных контроллеров внесение дополнительных задержек может привести к сбоям в работе основного алгоритма, что немедленно будет выявлено.

Следует отметить, что действующая в соответствии со стандартом NIST 800-82 система ИБ не осуществляет мониторинга и/или активного противодействия подобным угрозам, поэтому в данном случае дополнительные ограничения, порождаемые соответствующей ПИБ, отсутствуют. Таким образом, можно сделать вывод, что все необходимые для реализации СК условия удовлетворены.

### 3.4. Пример реализации скрытого канала, использующего описанный принцип

Перенос информации по скрытому каналу в предлагаемом варианте его реализации обеспечивается за счет модуляции интервала времени между несколькими последовательными HTTP-запросами к web-интерфейсу мониторинга. Такое изменение интервалов, как было показано в предыдущем пункте, в конечном

итоге приводит к соответствующему изменению интервала между SNVT-запросами от LonWorks-IP шлюза к конкретному промышленному контроллеру, находящемуся на fieldbus-уровне системы. В табл. 1 приведены критерии, в соответствии с которыми обеспечивается интерпретация полученной задержки.

Таблица 1

**Интерпретация задержек между SNVT-запросами**

| | |
|---|---|
| лог. «0» | задержка между SNVT-запросами находится в интервале от 0 до $T_a$ |
| лог. «1» | задержка между SNVT-запросами находится в интервале от $T_a$ до $T_b$ |
| старт/стоп передачи | задержка между SNVT-запросами больше, чем $T_b$ |

При этом параметры $T_a$ и $T_b$ должны удовлетворять условию успешного детектирования, описанному в предыдущем пункте. В качестве примера можно рассмотреть вариант использования в качестве границ интервалов значений, полученных при $n = 1$ и $n = 2$. Для успешного выделения сигнала необходимо обеспечить на приемной стороне реализацию таймера, отслеживающего задержку между соседними SNVT-сообщениями. При этом разрешение такого таймера должно составлять не менее 2 отсчетов на каждый из временных интервалов, описанных в табл. 1. Для исключения ложного срабатывания закладки авторами предлагается ввести дополнительный маркер начала и конца передачи данных длиной 8 бит, представляющий собой последовательность вида «10101010».

### 3.5. Анализ основных параметров скрытого канала

Проведем оценку основных технических характеристик полученного скрытого канала связи. С точки зрения злоумышленника основными техническими характеристиками создаваемого канала связи будет время, затрачиваемое на проведение успешной атаки с его использованием, а также количество необходимых для этого запросов (сообщений).

Максимальное время передачи произвольного сообщения по описанному каналу зависит от содержания в этом сообщении «0» и «1» и в общем виде может быть выражено следующим образом:

$$T_{\text{передачи}} = T_a \cdot N_0 + T_b \cdot N_1,$$

где $T_{\text{передачи}}$ – время передачи сообщения; $T_a$ – верхняя граница задержки при передаче лог. «0»; $T_b$ – верхняя граница задержки при передаче лог. «1»; $N_0$ – количество нулей в передаваемой последовательности; $N_1$ – количество единиц в передаваемой последовательности.

Для расчета конкретных показателей воспользуемся следующим примером. Пусть конечной целью злоумышленника является изменение одного параметра атакуемой системы (например, температуры в помещении со скоропортящимися товарами). Для успешного осуществления такой атаки необходима передача закладке, работающей на уровне fieldbus-сети, одного полного SNVT-сообщения длиной 96 байт, состоящего из 64 нулей и 32 единиц. Для организации скрытого канала выбраны граничные интервалы $T_a$ = 10 с, $T_b$ = 20 с, заведомо большие, чем возможные задержки при транспортировке сигнала. Помимо информационного сообщения требуется также передача маркеров начала и конца передачи общей длиной 16 байт, содержащих по 4 нуля и единицы каждый. В этом случае максимальное время осуществления такой атаки будет следующим:

$$T_{\text{атаки}} = T_a \cdot (N_{0\text{С}} + N_{0\text{П}}) + T_b \cdot (N_{1\text{С}} + N_{1\text{П}});$$
$$T_{\text{атаки}} = 10 \cdot (64 + 8) + 20 \cdot (32 + 8) = 1520\,\text{с},$$

где $T_{\text{атаки}}$ – время осуществления атаки; $T_a$ – верхняя граница задержки при передаче лог. «0»; $T_b$ – верхняя граница задержки при передаче лог. «1»; $N_{0\text{С}}$ – количество нулей в передаваемой последовательности; $N_{1\text{С}}$ – количество единиц в передаваемой последовательности; $N_{0\text{П}}$ – количество нулей в маркерах начала/конца передачи; $N_{1\text{П}}$ – количество единиц в маркерах начала/конца передачи.

Следовательно, можно сделать вывод о том, что при таких исходных данных успешная атака злоумышленника на автоматизированную систему возможна менее чем за 26 минут.

Что касается количества необходимых для осуществления атаки запросов, то оно может быть выражено следующим образом:

$$N_{\text{запросов}} = L_C + mL_{\text{М}} + 1 = 96 + 16 + 1 = 113,$$

где $L_C$ – общая длина передаваемых сообщений; $m$ – общее количество необходимых маркеров; $L_M$ – длина маркера.

Необходимо отметить, что еще одним важным параметром, отражающим технические характеристики данного канала, является задержка, порождаемая выполнением алгоритма закладки, реализующей функциональность скрытого канала. Особенно важен этот параметр в условиях ограниченности ресурсов, характерной для fieldbus-систем. Существует несколько методов оценки задержки, связанной с выполнением произвольных программ. Одним из таких методов является выделение количе-

ства элементарных операций, необходимых для реализации требуемого алгоритма, производимое на основании анализа его реализации на каком-либо языке высокого уровня, и последующего проецирования полученных результатов на выбранный аппаратный базис. Так, в данном случае, необходимые алгоритмы были реализованы авторами на языке C++, после чего проанализированы с целью выделения элементарных операций: сложения, умножения, деления, а также операторов чтения и записи данных, операторов условного перехода. Полученные данные представлены в табл. 2.

Таблица 2

**Количество необходимых элементарных операций**

| Передатчик | |
|---|---|
| Сложение | 23 |
| Умножение | 10 |
| Деление | 0 |
| Чтение | 31 |
| Запись | 18 |
| Переход | 48 |
| Приемник | |
| Сложение | 67 |
| Умножение | 12 |
| Деление | 8 |
| Чтение | 85 |
| Запись | 91 |
| Переход | 54 |

Используя соответствующие данные, можно определить аналитическую задержку для необходимого аппаратного базиса, учитывая выбранную архитектуру команд, тактовую частоту и прочие необходимые параметры. В качестве примера в табл. 3 приведены результаты такого подсчета для нескольких систем различной архитектуры.

Таблица 3

**Результаты оценки задержки выполнения алгоритма скрытого канала для систем с разной архитектурой**

| Система | Задержка (мс) |
|---|---|
| x86, Intel Pentium IV, 3200MHz | 0,0009 |
| RISC, StrongARM, 200MHz | 0,17 |
| RISC, Neuron Chip, 4MHz | 15 |

Следует отметить, что приводимые результаты являются оценочными, поскольку получить реальную информацию о задержке можно только при непосредственном анализе выполнения кода, полученного после компилятора для соответствующей архитектуры. Тем не менее, эти результаты показывают порядок получаемых величин и могут быть использованы для предварительной оценки либо для сравнительного анализа.

## ВЫВОДЫ

1. Предложена концепция скрытого канала, функционирующего в многопротокольной распределенной управляющей системе, основанной на современных стандартах и протоколах.

2. Показана возможность функционирования такого канала без наличия промежуточных программных или аппаратных закладок.

3. Выявлена невозможность противодействия такому каналу со стороны типовых ПИБ для данного класса систем.

4. Предложены аналитические выражения для определения времени передачи произвольного сообщения через описываемый канал, времени, необходимого для осуществления успешной атаки заданного образца, и методика оценки задержки, порождаемой выполнением алгоритма скрытого канала в базисе fieldbus-системы.

## СПИСОК ЛИТЕРАТУРЫ

1. National Institute of Standarts and Technology. NIST800-82. Guide to Industrial Control Systems Security [Электронный ресурс] (src.nist.gov/publications/drafts/800-82/draft_sp800-82-fpd.pdf).

2. **Тимонина Е. Е.** Анализ угроз скрытых каналов и метода построения гарантированно защищенных распределенных автоматизированных систем: Дисс. д-ра техн. наук. М., 2004.

3. LON-технология : построение распределенных приложений / Д. Дитмар [ и др.]. Пермь, 2001.

4. Digital Communications: Fundamentals and Applications. Prentice-Hall PTR, 2001. P. 790–793.

## ОБ АВТОРАХ

**Безукладников Игорь Игоревич,** ст. преп. каф. автоматики и телемеханики ПГТУ. Дипл. инж. по сетям связи и системам коммутации (ПГТУ, 2005). Иссл. в обл. инф. безопасности.

**Кон Ефим Львович,** проф. той же каф. Канд. техн. наук. Иссл. в обл. инф. безопасности.