УДК 681.324

РАЗРАБОТКА МОДЕЛИ НЕТРАДИЦИОННОГО ИНФОРМАЦИОННОГО КАНАЛА И МЕТОДОВ ПРОТИВОДЕЙСТВИЯ НЕТРАДИЦИОННЫМ ИНФОРМАЦИОННЫМ КАНАЛАМ В СЕТЯХ ПАКЕТНОЙ ПЕРЕДАЧИ ДАННЫХ

Назаров И.В., – адъюнкт
Краснодарское высшее военное училище имени генерала армии Штеменко С.М.

В статье предлагается модель, с помощью которой возможно определить основные свойства нетрадиционных информационных каналов (НИК) в сетях пакетной передачи данных, а также методы противодействия НИК, разработанные на основе предложенной модели. Приводится пример реализации сетевой атаки на автоматизированную систему с использованием НИК.

1. Уязвимости протокола IP и возможности злоумышленников по их использованию для организации сетевых атак

В настоящее время создание и развитие отечественных информационно-компьютерных технологий характеризуется широким применением зарубежного технического и программного обеспечения, как общесистемного, так и специального. При этом в основу межсетевого взаимодействия положено применение протоколов стека TCP/IP, разработанного по инициативе Министерства обороны США (Department of Defence, DoD) более 20 лет назад для связи экспериментальной сети ARPAnet с другими сателлитными сетями как набор общих протоколов для разнородной вычислительной среды.

Несмотря на то, что разработка TCP/IP финансировалась Министерством обороны США, данный стек протоколов не обладает абсолютной защищенностью и допускает различные типы сетевых атак. При осуществлении сетевых атак злоумышленник имеет возможность использовать уязвимости, выраженные в недостаточно продуманной реализации данного протокола для определенной операционной системы.

Протоколы стека TCP/IP распределены по уровням, каждый из которых независимо от других выполняет определенную задачу по доставке данных пользователя (рис. 1).

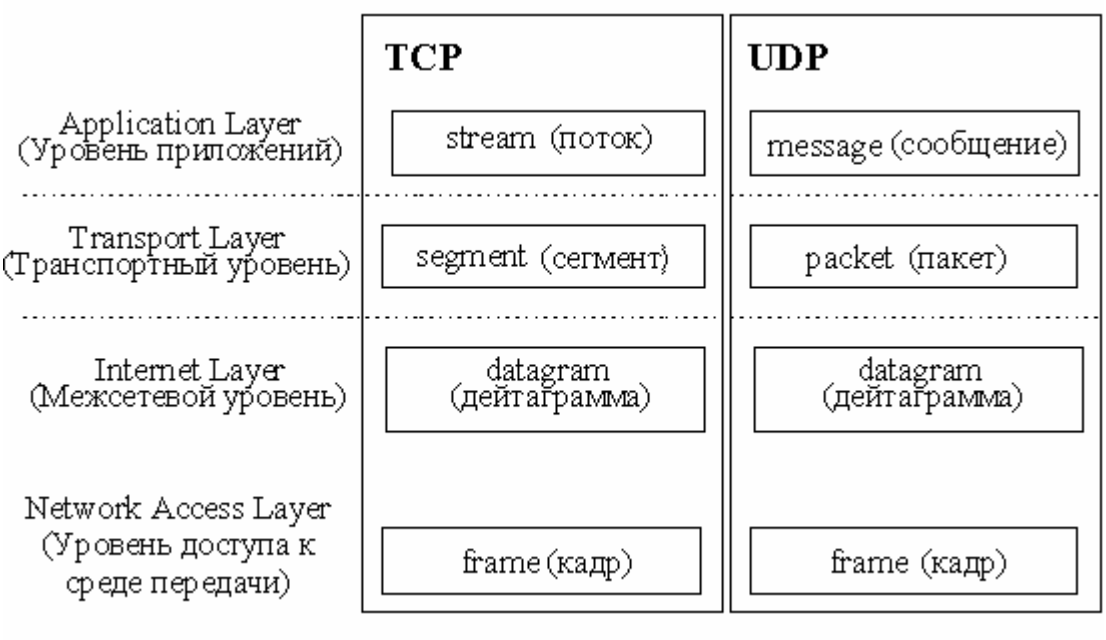

Рис. 1. Уровни и единицы данных стека протоколов TCP/IP

Ни один из протоколов стека TCP/IP не относится к уровню доступа к среде передачи, но данный уровень принято включать в стек как неотъемлемую составляющую межсетевого взаимодействия. Таким образом, протоколы стека TCP/IP распределены по трем уровням – межсетевому, транспортному и уровню приложений.

За все время использования протоколов стека TCP/IP, специалистами в области информационной безопасности, в том числе и злоумышленниками (которых принято называть «хакерами»), было обнаружено множество уязвимостей в реализации протоколов данного стека.

Учитывая главную особенность применения протоколов стека TCP/IP – осуществление инкапсуляции единицы данных протокола (PDU, Protocol Data Unit) верхнего уровня в PDU протокола нижнего уровня, сетевые атаки также носят иерархический характер. Уязвимость протокола нижнего уровня позволяет получить доступ к уязвимости протокола верх-

него уровня, при этом успех в проведении сетевой атаки на каждом из уровней позволяет получить определенный результат (рис. 2).

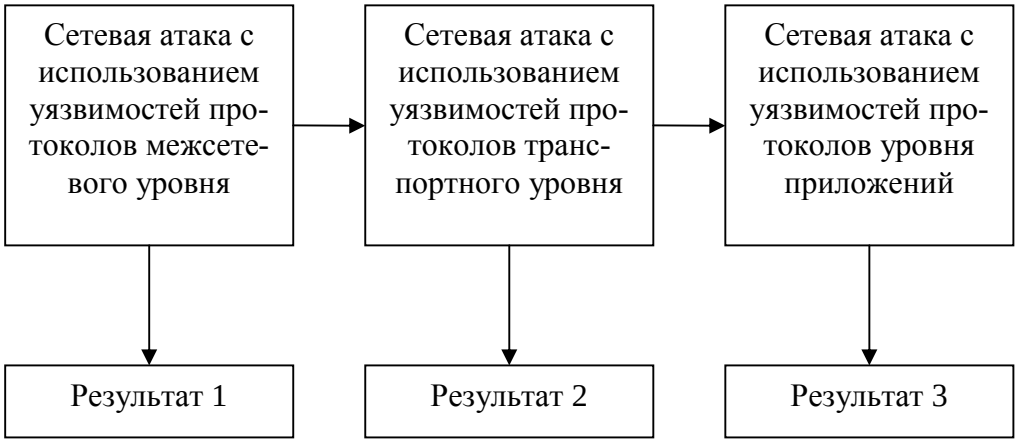

Рис. 2. Схема организации сетевых атак в стеке протоколов TCP/IP

Любая сетевая атака с использованием уязвимостей протоколов стека TCP/IP начинается с использования уязвимостей протокола IP (Internet Protocol), относящегося к межсетевому уровню. В результате анализа различных источников, автор статьи пришел к выводу, что все известные на сегодняшний день сетевые атаки основаны на использовании трех базовых уязвимостей протокола IP:

- возможность назначения адреса отправителя, не являющегося истинным, в заголовке IP-дейтаграммы (рис. 3);
- возможность осуществления инкапсуляции PDU в IP-дейтаграмму, в том числе не предусмотренной стандартом протокола IP (рис. 4);
- возможность осуществления фрагментации IP-дейтаграмм, не предусмотренной стандартом протокола IP (рис. 4).

На рисунках 3 и 4 показано, что использование перечисленных уязвимостей протокола IP позволяет организовывать сетевые атаки с использованием уязвимостей протоколов сетевого и транспортного уровней стека TCP/IP.

Успешное проведение различных атак, приведенных на рисунках 3 и 4, на сетевом уровне, может привести к следующим результатам:

– несанкционированному перенаправлению IP-дейтаграмм;

– отказу в обслуживании.

Успешное проведение различных атак, приведенных на рисунках 3 и 4, на транспортном уровне, может привести к следующим результатам:

– несанкционированному подключению к TCP- или UDP-порту;

– отказу в обслуживании.

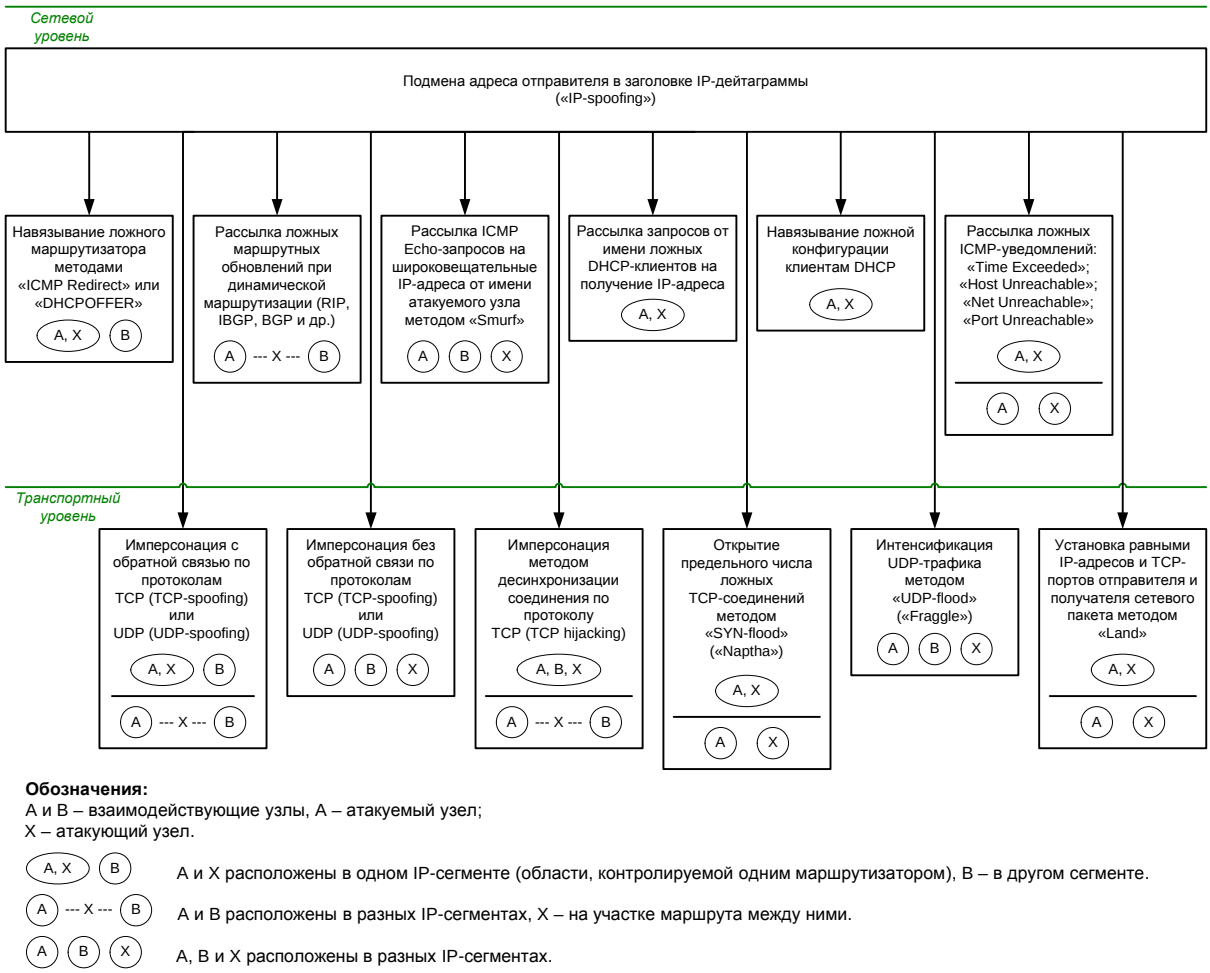

Рис. 3. Схема использования уязвимостей протоколов сетевого и транспортного уровней стека TCP/IP с целью организации атак при подмене адресов отправителей в заголовках IP-дейтаграмм

Разработчики средств защиты информации от сетевых атак ориентируются на противодействие всем производным от трех базовых уязвимостей протокола IP сетевым атакам. Для осуществления этих атак должен

быть соблюден ряд условий, сводящийся к определенному соотношению ошибок в реализации сетевых протоколов и ошибок в реализации и (или) конфигурации средств защиты.

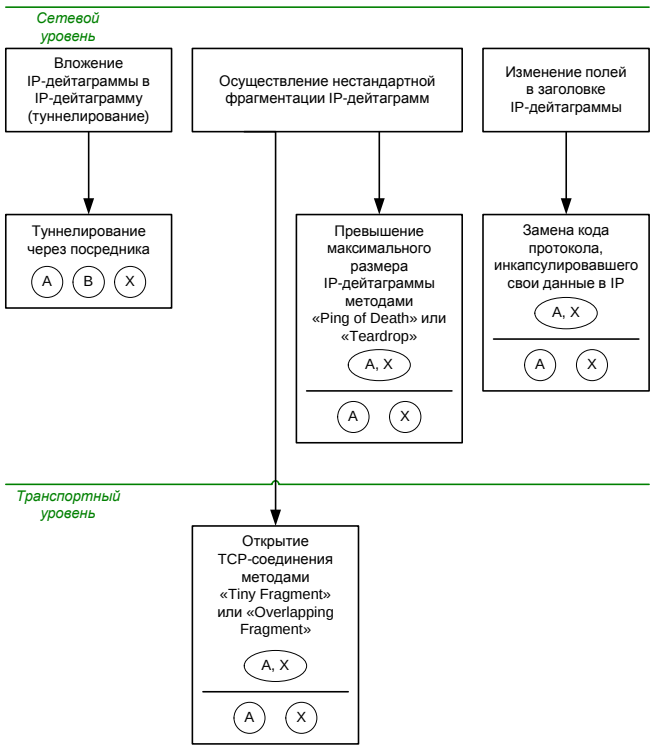

Рис. 4. Схема использования уязвимостей протоколов сетевого и транспортного уровней стека TCP/IP с целью организации атак при нестандартном проведении инкапсуляции и фрагментации IP-дейтаграмм

Современные средства защиты информации, построенные на основе технологии виртуальных частных сетей (VPN, Virtual Private Network) позволяют обеспечить высокий уровень конфиденциальности информации, передаваемой через информационно-вычислительные сети общего пользования (ИВС ОП) путем шифрования полей данных IP-дейтаграмм. При этом протоколы верхних уровней модели TCP/IP, начиная с транспортного, изолированы от потенциально опасных субъектов ИВС ОП. Взаимодействие узлов автоматизированной системы (АС) через каналы ИВС ОП с применением технологии VPN обеспечивается установкой пограничных узлов защиты (УЗ), состоящих из шифровального средства (ШС) и межсетевого экрана (МЭ) (рис. 5).

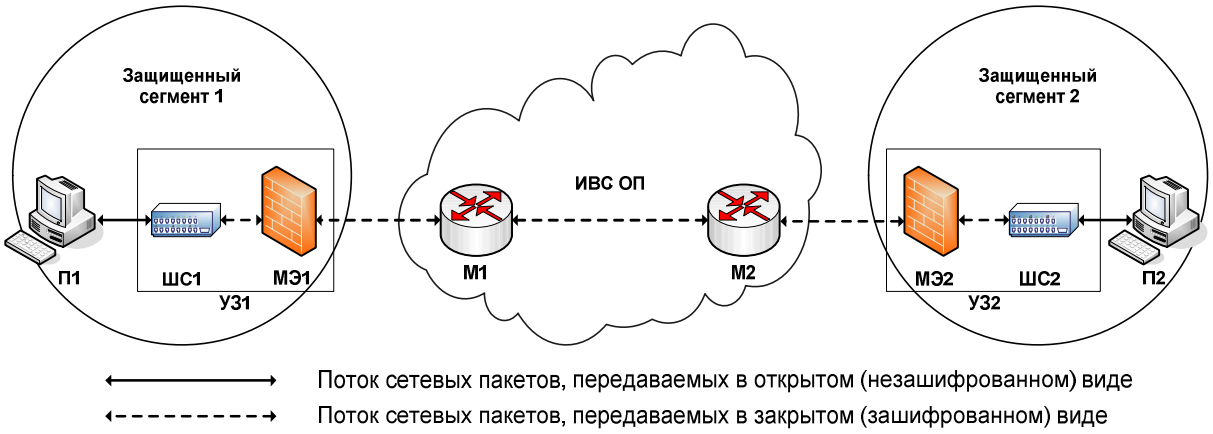

Рис. 5. Схема взаимодействия узлов АС через каналы ИВС ОП с применением технологии VPN

Данная схема взаимодействия не предусматривает обращения пользователей защищенных сегментов 1 и 2 к информационным ресурсам ИВС ОП, которая используется только в качестве среды передачи данных, что можно рассматривать как недостаток в ситуациях, когда взаимодействие с информационными ресурсами ИВС ОП необходимо. Существуют комплексные решения, позволяющие решить эту задачу.

В данной статье будет рассматриваться схема, приведенная на рисунке 5, как обеспечивающая наибольшую защищенность от сетевых атак, представленных на рисунках 3 и 4.

Предположим, что злоумышленник, находящийся в ИВС ОП, решил предпринять сетевую атаку на узел П2 защищенного сегмента 2 (рис. 5). С применением «традиционных» методов организации сетевых атак (рис. 3, 4), существует возможность вызвать «отказ в обслуживании» УЗ2, но при этом не существует никаких путей доступа к сетевому интерфейсу узла П2, следовательно, злоумышленник не способен решить поставленную задачу. Главным препятствием для злоумышленника в данной схеме построения АС, является уничтожение узлом ШС2 всех незашифрованных пакетов, пришедших из ИВС ОП, а также пакетов, не подлежащих расшифрованию на узле ШС. Незнание ключа шифрования является основ-

ным фактором, препятствующим злоумышленнику формировать собственные пакеты протоколов транспортного и прикладного уровней стека TCP/IP для последующей передачи в защищенный сегмент 2.

Несмотря на множество способов и средств противодействия «традиционным» сетевым атакам, существует возможность преодоления наиболее эффективных средств защиты информации с использованием таких свойств протокола IP, которые не контролируются данными средствами. В частности, ими являются:

– возможность осуществления перестановок IP-дейтаграмм (рис. 6);
– возможность изменения временных интервалов между IP-дейтаграммами (рис. 6).

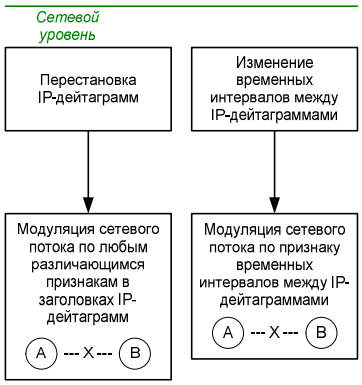

Рис. 6. Схема использования уязвимостей протокола IP для организации сетевых атак по нетрадиционным информационным каналам

Данные возможности получили название нетрадиционных информационных каналов (НИК) [1], применительно к сетям пакетной передачи данных.

Нетрадиционный информационный канал (Unusual channel; covert channel; subliminal channel) – несанкционированный способ скрытой передачи не легитимной информации по действующим («традиционным») каналам связи, нарушающий системную политику безопасности [3].

2. Пример реализации сетевой атаки с использованием НИК

Рассмотрим пример реализации сетевой атаки на узел П2 защищенного сегмента 2 с использованием НИК. Предположим, что злоумышленнику удалось разместить на узле П2 закладочное устройство ЗУ2 (рис. 7). Также, злоумышленник контролирует маршрутизатор М2, находящийся в ИВС ОП. Предположим, что злоумышленнику удалось перенаправить весь трафик, входящий в защищенный сегмент 2, а также весь трафик, исходящий из данного сегмента, через маршрутизатор М2, в который внедрено закладочное устройство ЗУ1. Перечисленные условия являются необходимыми и достаточными для организации атаки с использованием НИК применительно к рассматриваемой схеме взаимодействия узлов АС.

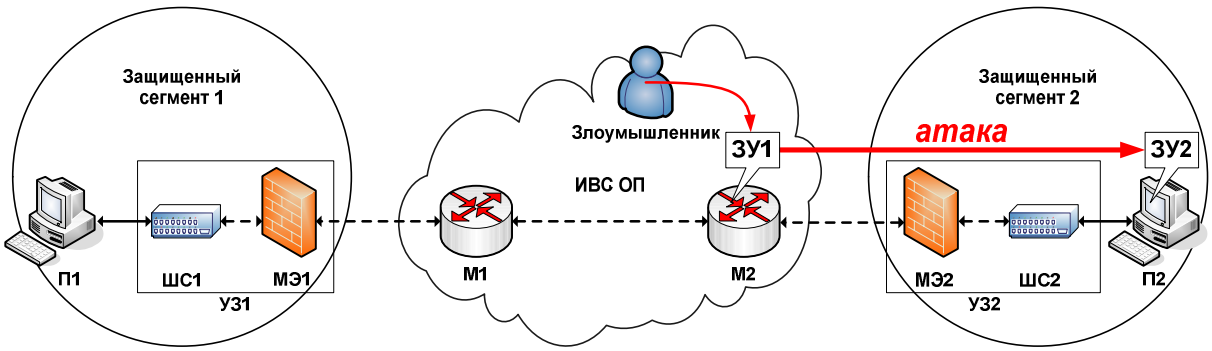

Рис. 7. Схема организации атаки с использованием НИК в АС, построенной с применением технологии VPN

Очевидно, что создание условий для атаки с использованием НИК сопряжено с некоторыми трудностями, но вполне осуществимо.

Злоумышленник передает ЗУ1 некоторую команду, которая должна быть передана и выполнена ЗУ2 на узле П2. После получения команды злоумышленника ЗУ1 начинает анализировать сетевой поток, направляемый узлом М2 в адрес УЗ2, на предмет наличия различающихся длин IP-дейтаграмм.

Пусть ЗУ1 для модуляции каждого из сигналов «0» и «1» применяет группы из 20 IP-дейтаграмм. Каждая из этих групп условно разделена пополам, т.е. состоит из $2k$ IP-дейтаграмм, где k=10. Пусть k_i является строго

возрастающей последовательностью длин IP-дейтаграмм, а k_j – строго убывающей последовательностью длин IP-дейтаграмм. Модуляция сигналов осуществляется на основе перестановок IP-дейтаграмм внутри каждой группы, при этом биту «0» соответствует перестановка $\{k_i, k_j\}$, а биту «1» соответствует перестановка $\{k_j, k_i\}$ (рис. 8).

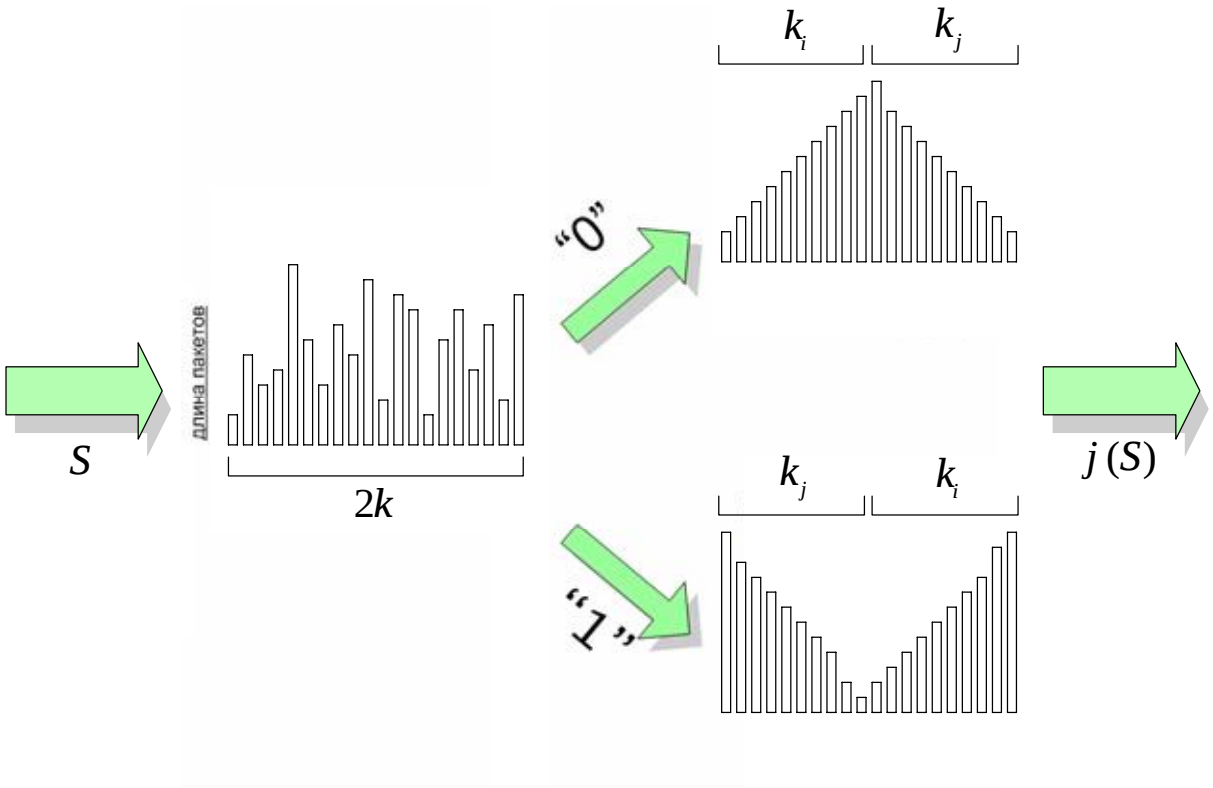

Рис. 8. Схема модуляции сигналов «0» и «1»

Пусть S – множество всех возможных 20-дейтаграммных групп, каждая из которых уникальна расположением IP-дейтаграмм по признаку длин. Пусть $\varphi(S)$ – множество всех возможных 20-дейтаграммных групп, являющихся перестановками $\{k_i, k_j\}$ и $\{k_j, k_i\}$, при этом $\varphi(S) \subset S$.

Таким образом, при модуляции сигналов «0» и «1» осуществляется преобразование элементов множества S в элементы множества $\varphi(S)$.

Пусть множество $\varepsilon_1(S)$ – множество всех возможных 20-дейтаграммных групп, являющихся перестановками $\{k_i, k_j\}$, а множество

$\varepsilon_2(S)$ – множество всех возможных 20-дейтаграммных групп, являющихся перестановками $\{k_j, k_i\}$, при этом:

$$\varphi(S) = \varepsilon_1(S) \cup \varepsilon_2(S), \qquad \varepsilon_1(S) \cap \varepsilon_2(S) = \varnothing.$$

Кодирование данных с использованием модуляции по принципу, показанному на рисунке 8, может быть основано на потенциальном коде NRZ (Non Return to Zero), в котором сигнал не возвращается к нулю в течение такта (рис. 9).

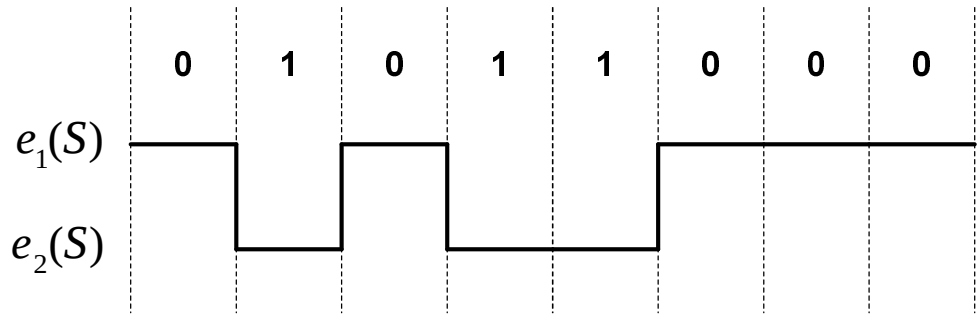

Рис. 9. Кодирование данных на основе потенциального кода NRZ с использованием элементов множеств $\varepsilon_1(S)$ и $\varepsilon_2(S)$.

ЗУ1 и ЗУ2 располагают данными о признаке модуляции (модуляция по признаку длин IP-дейтаграмм), его величине (кодирование с применением потенциального кода NRZ), и о параметрах модуляции (элементах множеств $\varepsilon_1(S)$ и $\varepsilon_2(S)$).

ЗУ1 интегрирована с модулем маршрутизации узла М2 так, что осуществляет контроль потока IP-дейтаграмм и способна изменять порядок их следования. Получая IP-дейтаграммы от модуля маршрутизации, ЗУ1 помещает их в буфер, пока не накопится серия, содержащая 20 различных по длине IP-дейтаграмм. После этого ЗУ1 выполняет перестановку IP-дейтаграмм в соответствии с модулируемым сигналом и отправляет получившуюся последовательность на сетевой интерфейс МЭ2.

Для сообщения ЗУ2 о начале передачи команды злоумышленника, ЗУ1 выполняет отправку обучающей последовательности, состоящей из чередующихся бит «0» и «1». ЗУ2, для обеспечения скрытого взаимодей-

ствия с ЗУ1, постоянно находится в готовности к приему и выполняет анализ входящего сетевого потока на предмет наличия обучающей последовательности.

Средства УЗ2 не контролируют свойства *S* сетевого потока, поэтому обучающая последовательность беспрепятственно проникает в защищенный сегмент 2 и поступает на сетевой интерфейс узла П2, где считывается ЗУ2.

ЗУ2 статистическими методами определяет скрытую передачу через НИК и принимает решение о наличии обучающей последовательности, после чего передает ЗУ1 ответ о завершении обучения, аналогичным методом модулируя сетевой поток, исходящий из защищенного сегмента 2 в ИВС ОП.

После получения ответа о завершении обучения, ЗУ1 отправляет ЗУ2 синхронизационную последовательность, состоящую из серии сигналов «1» и завершающуюся сигналом «0». После сигнала «0» начинается передача команды злоумышленника, по окончании которой передается серия сигналов «0», являющаяся признаком завершения передачи.

ЗУ2 выполняет полученную команду злоумышленника, при этом может инициировать процесс передачи ЗУ1 результата. Таким образом, цель злоумышленника достигнута.

3. Разработка модели НИК в сетях пакетной передачи данных

Пусть φ – функция несанкционированного воздействия на сетевой поток, обладающий ограниченным набором свойств *S*. Данная функция выполняется ЗУ1, внедренным в М2.

Пусть ψ – функция обеспечения безопасности информации, выполняемая каждым узлом защиты по отношению к сетевому потоку, обладающему ограниченным набором свойств *S*. Данная функция выполняется УЗ1 и УЗ2.

Тогда сетевой поток, поступающий на УЗ2 обладает набором свойств $\varphi(S)$, вместо «ожидаемого» на данном участке набора свойств S. Следовательно, УЗ2 применяет по отношению к входящему потоку функцию $\psi(\varphi(S))$ вместо $\psi(S)$.

Предположим, что если $\psi(\varphi(S))=\psi(S)$, сетевой поток проходит через УЗ2, не нарушая существующих правил разграничения доступа, и поступает на узел П2.

Пусть ψ_r – функция несанкционированного анализа сетевого потока на предмет определения элементов, входящих в состав множеств $\varepsilon_1(S)$ и $\varepsilon_2(S)$, где

$$\varphi(S)=\varepsilon_1(S)\,\mathbf{U}\,\varepsilon_2(S), \qquad \varepsilon_1(S)\,\mathbf{I}\,\varepsilon_2(S)=\varnothing.$$

Функция ψ_r выполняется ЗУ2, внедренным в П2. Данная функция возвращает успешный результат при $\psi_r(\varphi(S))$ и неудачный результат при $\psi_r(S)$.

Модель НИК в сетях пакетной передачи данных построена с учетом всех этапов скрытой передачи между закладочными устройствами (рис. 10).

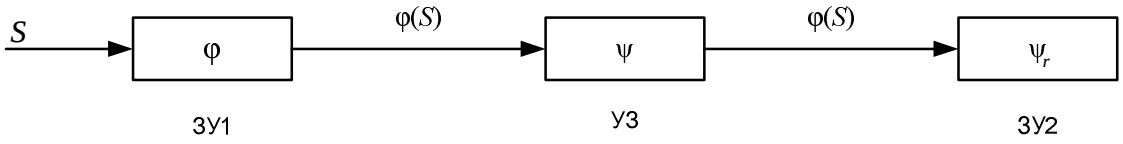

Рис. 10. Модель НИК в сетях пакетной передачи данных

Рассмотрим сетевую атаку на АС при использовании НИК с модуляцией потока пакетов по признаку длин применительно к показанной схеме взаимодействия (рис. 7) и разработанной модели.

В отношении свойств S сетевого потока сделаны следующие допущения:

– сетевой поток содержит только IP-дейтаграммы с длинами четырех различающихся видов – a, b, c, d;

– в сетевом потоке не могут следовать подряд два и более IP-дейтаграмм с длинами одного вида.

Исходя из указанных допущений, все IP-дейтаграммы сетевого потока можно условно разделить на группы по 4 пакета с различающимися длинами. Каждая группа содержит определенную комбинацию длин IP-дейтаграмм. Количество возможных комбинаций определяет состав множества *S*.

Таким образом, множество *S* состоит из перестановок длины 4, каждая из которых содержит элементы *a*, *b*, *c*, *d*. При этом $|S| = 4! = 24$.

Перестановка *abcd* является строго возрастающей последовательностью длин сетевых пакетов (рис. 11).

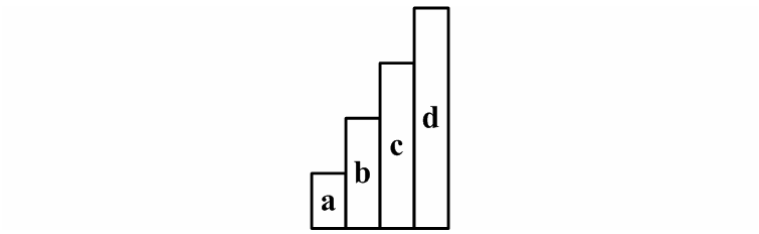

Рис. 11. Строго возрастающая последовательность длин *abcd*

Элементы множества *S* могут быть использованы для модуляции сигналов «0» и «1».

Пусть, для модуляции сигнала «0» будут использоваться перестановки *acdb*, *bdca*, *adcb*, *bcda* (рис. 12), а для модуляции сигнала «1» будут использоваться перестановки *cabd*, *dbac*, *dabc*, *cbad* (рис. 13).

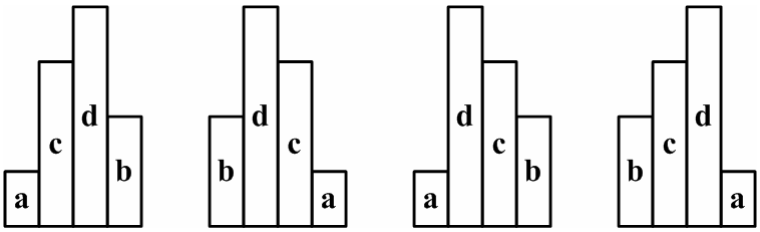

Рис. 12. Перестановки длины 4, используемые для модуляции сигнала «0»

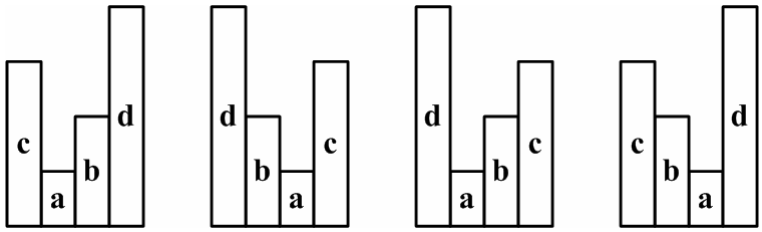

Рис. 13. Перестановки длины 4, используемые для модуляции сигнала «1»

Пусть $\varepsilon_1(S)$ – множество всех перестановок, которые могут быть использованы для модуляции сигнала «0», и $\varepsilon_2(S)$ – множество всех перестановок, которые могут быть использованы для модуляции сигнала «1».

Тогда,

$$\varepsilon_1(S)=\{acdb, bdca, adcb, bcda\}, \qquad \varepsilon_2(S)=\{cabd, dbac, dabc, cbad\}.$$

Таким образом, в данном примере, $|\varphi(S)|=8$, $|\varepsilon_1(S)|=|\varepsilon_2(S)|=4$.

Пусть функция ψ, выполняемая УЗ2, не учитывает порядок следования пакетов. Тогда будем считать, что каждый элемент $s\in S$ интерпретируется УЗ2 как сочетание ***abcd***, в котором порядок следования элементов не имеет значения, $\psi(S)=\psi(\varphi(S))=\{abcd\}$, $|\psi(S)|=|\psi(\varphi(S)|)=1$.

Равенство $\psi(S)=\psi(\varphi(S))$ обозначает, что УЗ2 не способен отличить сетевой поток, обладающий набором свойств *S*, от сетевого потока, обладающего набором свойств $\varphi(S)$.

Если результатом отображения ψ для любой перестановки $s\in S$ является сочетание ***abcd***, то перестановка без изменений передается в защищенный сегмент 2, где поступает на узел П2, в который внедрено ЗУ2.

ЗУ2 осуществляет несанкционированный анализ сетевого потока, применяя функцию ψ_r, с помощью которой определяет состав множеств $\varepsilon_1(S)$ и $\varepsilon_2(S)$. Таким образом, ЗУ2 переходит в состояние готовности приема от ЗУ1 определенной команды для выполнения несанкционированного воздействия на АС.

В [2] определено, что пара отображений (φ,ψ), где $\varphi,\psi\in C(S)$, где *C*(*S*) – множество всех отображений множества *S* в себя, называется ин-

формационным протоколом на S. Протокол (φ,ψ) называется прозрачным, если $|\varphi(S)|=|\psi(\varphi(S))|$, и мутным, если $|\varphi(S)|>|\psi(\varphi(S))|$.

Применительно к разработанной модели НИК, функции φ и ψ представляют информационный протокол (φ,ψ), как определенные правила, которые описывают функции обеспечения безопасности информации ψ по отношению к сетевому потоку, обладающему свойствами $\varphi(S)$, и содержащему сигнал, передаваемый с применением НИК.

Прозрачный протокол – это протокол (φ,ψ), свойства которого недостаточны для организации передачи сигналов с применением НИК, т.е. если $|S|=1$, то $|\varphi(S)|=1$, следовательно, $|\varphi(S)|=|\psi(\varphi(S))|$.

Мутный протокол – это протокол (φ,ψ), свойства которого достаточны для организации передачи сигналов с применением НИК, т.е. если $|S|\geq 2$, то $|\varphi(S)|\geq 2$, следовательно, $|\varphi(S)|>|\psi(\varphi(S))|$.

4. Разработка методов противодействия НИК в сетях пакетной передачи данных

Анализ разработанной модели НИК в сетях пакетной передачи данных АС показал, что условиями существования НИК являются:

- отсутствие в составе средств обеспечения безопасности информации АС функции, способной выявить отличие между S и $\varphi(S)$;
- наличие в сетевом потоке свойств, с применением которых возможно осуществлять модуляцию $\varphi(S)$ сигналов «0» и «1».

Следовательно, для обеспечения противодействия НИК, необходимо исключить возможность выполнения одного из перечисленных условий.

Для включения в состав средств обеспечения безопасности информации АС функции, способной выявить отличие между S и $\varphi(S)$, необходимо обеспечить непрерывный анализ свойств S сетевого потока, в реальном времени, с применением статистических методов.

Недостатками данного решения следует считать:

- высокую сложность реализации, поскольку функция обеспечения безопасности информации АС должна отслеживать изменение параметров модуляции для каждого из возможных признаков модуляции, а также уметь принимать правильное решение;
- высокие требования к вычислительной мощности ПЭВМ, на базе которой реализованы функции системы обеспечения безопасности информации;
- возможность недостаточно своевременного обнаружения начала передачи сигналов с применением НИК.

Наличие в сетевом потоке свойств, с применением которых возможно осуществлять модуляцию $\varphi(S)$ сигналов «0» и «1», в большинстве случаев (для большинства признаков модуляции), является неотъемлемой составляющей сетевого протокола, необходимой для обеспечения межсетевого взаимодействия. Следовательно, необходимо решение, препятствующее применению противником свойств S сетевого потока, для организации скрытой передачи сигналов по НИК. При этом, для обеспечения межсетевого взаимодействия в соответствии с установленным протоколом, необходимые свойства S сетевого потока должны оставаться неизменными, даже если они могут быть применены противником для организации скрытой передачи сигналов по НИК.

Таким образом, возникает задача разработки методов противодействия НИК в сетях пакетной передачи данных. В результате решения данной задачи разработаны три метода:

- метод приведения мутного протокола к прозрачному протоколу при изменении количества свойств сетевого потока;
- метод приведения мутного протокола к прозрачному протоколу без изменения количества свойств сетевого потока;

– метод применения мутного протокола с восстановлением его первоначальных свойств.

4.1. Метод приведения мутного протокола к прозрачному протоколу при изменении количества свойств сетевого потока

Для приведения мутного протокола к прозрачному протоколу при изменении количества свойств сетевого потока необходимо и достаточно включить в состав средств обеспечения безопасности информации функцию δ_x, обеспечивающую изменение свойств S сетевого потока таким образом, что

$$|\delta_x(S)| = |\delta_x(\varphi(S))| = Z, \qquad Z \cap S = \varnothing.$$

Применительно к приведенному выше примеру НИК с модуляцией сетевого потока по признаку длин IP-дейтаграмм, применение функции δ_x обеспечит выравнивание их длин таким образом, что

$$\delta_x(S) = \delta_x(\varphi(S)) = Z = \{d\}.$$

Поскольку УЗ2 проверяет пакеты входящего сетевого потока на предмет соответствия правилу ψ, и данное правило не учитывает порядок следования пакетов, то

$$\psi(\delta_x(S)) = \psi(\delta_x(\varphi(S))) = \psi(Z) = \{d\}.$$

Тогда,

$$|\delta_x(\varphi(S))| < |\varphi(S)| \le |S|,$$

$$|\delta_x(\varphi(S))| = |\psi(\delta_x(\varphi(S)))| = |\psi(\varphi(S))|,$$

следовательно, протокол (φ,ψ) прозрачен и передача сигналов «0» и «1» с применением модуляции пакетов по признаку длины невозможна.

Таким образом, разработан метод противодействия НИК в сетях пакетной передачи данных АС, основанный на применении прозрачного протокола (φ,ψ), с изменением количества свойств S сетевого потока.

Прозрачность протокола (φ,ψ) следует рассматривать относительно применяемого признака модуляции. Например, протокол (φ,ψ) может яв-

ляться прозрачным относительно признака модуляции по длинам сетевых пакетов, но при этом являться мутным относительно признака модуляции по адресам в заголовках сетевых пакетов.

4.2. Метод приведения мутного протокола к прозрачному протоколу без изменения количества свойств сетевого потока

Для приведения мутного протокола к прозрачному протоколу без изменения количества свойств сетевого потока необходимо и достаточно включить в состав средств обеспечения безопасности информации функцию δ_y, обеспечивающую изменение свойств S сетевого потока таким образом, что

$$\left|\delta_y(S)\right| = \left|\delta_y(\varphi(S))\right| = 1.$$

Применительно к приведенному выше примеру НИК с модуляцией сетевого потока по признаку длин IP-дейтаграмм, применение функции δ_y обеспечит равномерное распределение длин внутри каждой группы из четырех IP-дейтаграмм так, что $\delta_y(S) = \delta_y(\varphi(S)) = \{abcd\}$.

Поскольку УЗ2 проверяет пакеты входящего сетевого потока на предмет соответствия правилу ψ, и данное правило не учитывает порядок следования сетевых пакетов, то

$$\psi(\delta_y(S)) = \psi(\delta_y(\varphi(S))) = \{abcd\}.$$

Тогда,

$$\left|\delta_y(\varphi(S))\right| < \left|\varphi(S)\right| \le \left|S\right|,$$

$$\left|\delta_y(\varphi(S))\right| = \left|\psi(\delta_y(\varphi(S)))\right| = \left|\psi(\varphi(S))\right|,$$

следовательно, протокол (φ,ψ) прозрачен и передача сигналов «0» и «1» с применением модуляции пакетов по признаку длины невозможна.

Таким образом, разработан метод противодействия НИК в сетях пакетной передачи данных АС, основанный на применении прозрачного протокола (φ,ψ), без изменения количества свойств S сетевого потока.

4.3. Метод применения мутного протокола с восстановлением первоначальных свойств сетевого потока

Для применения мутного протокола с восстановлением первоначальных свойств S сетевого потока необходимо и достаточно включить в состав средств обеспечения безопасности информации функцию δ_z, обеспечивающую изменение свойств S сетевого потока таким образом, что

$$\delta_z(S) = \delta_z(\varphi(S)) = \varphi^{-1}(S) = S.$$

Применительно к приведенному выше примеру НИК с модуляцией потока по признаку длины, применение функции δ_z обеспечит восстановление порядка следования сетевых пакетов, что является восстановлением свойств S сетевого потока, которые были изменены в результате преобразования $\varphi(S)$.

Поскольку узел защиты УЗ2 проверяет IP-дейтаграммы входящего сетевого потока на предмет соответствия правилу ψ, и данное правило не учитывает порядок следования сетевых пакетов, то

$$|\psi(\delta_z(S))| = |\psi(\delta_z(\varphi(S)))| = |\psi(S)| = |\psi(\varphi(S))| = 1.$$

Протокол (φ,ψ) является мутным, поскольку

$$|\delta_z(\varphi(S))| = |\delta_z(S)| = |S| \geq |\varphi(S)| > |\psi(\varphi(S))|$$

ЗУ2 реализует функцию ψ_r, при этом успешное принятие решения возможно только при $\psi_r(\varphi(S))$, следовательно, передача сигналов «0» и «1» с применением модуляции пакетов по признаку длины невозможна, поскольку

$$\psi_r(\delta_z(\varphi(S))) = \psi_r(S).$$

Таким образом, разработан метод противодействия НИК в сетях пакетной передачи данных АС, основанный на применении мутного протокола (φ,ψ), с восстановлением первоначальных свойств S сетевого потока.

Разработанные модель и методы противодействия НИК были применена автором при разработке методики противодействия НИК в сетях пакетной передачи данных АС.

Литература:

1. Научно-исследовательская работа «Апология-2003»: Отчёт / ИТМ и ВТ РАН; Руководитель Д. А. Ловцов; М., 2003.
2. Ронжин А. Ф. Расширения информационных протоколов, основанных на отображениях конечных множеств // Дискретная математика. – 2004. – Т. 16. – Вып. 2. – С. 11 – 16.
3. Ловцов Д. А. Информационная теория эргасистем: Тезаурус. – М.: Наука, 2005.