УДК 004.056.5:621.39:681

Б. И. Мороз, доктор технических наук,
декан технического факультета
Университета таможенного дела и финансов
Д. И. Прокопович-Ткаченко, кандидат
технических наук, доцент кафедры
информационных систем и технологий
Университета таможенного дела и финансов
И. В. Петренко, старший преподаватель
кафедры информационных систем
и технологий Университета таможенного
дела и финансов

УСОВЕРШЕНСТВОВАНИЕ ПРОТОКОЛА АВТОРИЗАЦИИ МАРШРУТИЗАТОРОВ БЕСПРОВОДНЫХ СЕТЕЙ С ЦЕЛЬЮ УМЕНЬШЕНИЯ ВЕРОЯТНОСТИ НЕГАТИВНОГО ВОЗДЕЙСТВИЯ

Рассмотрены проблемы информационно-телекоммуникационных систем и сетей как кибербезопасность. Анализируются преимущества и недостатки беспроводных маршрутизаторов в кибербезопасности. Одним из важных элементов негативного воздействия считаются протоколы авторизации беспроводных сетей, которые дают потенциальному злоумышленнику полный доступ к информационному ресурсу.

Возникает необходимость изменения протоколов авторизации с целью качественного понижения вероятности вскрытия их алгоритма и идентификации.

Для решения этой проблемы в статье предложено применение в алгоритме формирования ключа авторизации дополнительного функционального элемента, представляющего собой генератор псевдослучайных последовательностей.

В алгоритме генерации ключа авторизации введены два новых элемента. В качестве же дополнительного элемента, положительно влияющего на вероятностные и периодические характеристики алгоритма авторизации, применён упрощенный вариант генератора Голлмана.

Повышение безопасности беспроводных сетей, построенных на традиционных технологиях, – актуальное и перспективное решение для дальнейших исследований проблем информационно-телекоммуникационных систем.

Ключевые слова: *информационно-телекоммуникационные системы; сети; кибербезопасность; протокол авторизации.*

Розглянуто проблеми інформаційно-телекомунікаційних систем і мереж як кібербезпека. Проаналізовано переваги і недоліки безпровідних маршрутизаторів у кібербезпеці. Одним із важливих елементів негативної дії вважаються протоколи авторизації безпровідних мереж, які дають потенційному зловмиснику повний доступ до інформаційного ресурсу.

Виникає необхідність зміни протоколів авторизації з метою якісного зниження вірогідності розкриття їх алгоритму та ідентифікації.

Для розв'язання цієї проблеми авторами пропонується застосування в алгоритмі формування ключа авторизації додаткового функціонального елемента, що є генератором псевдовипадкових послідовностей.

В алгоритмі генерації ключа авторизації введено два нових елементи. В якості ж додаткового елемента, що позитивно впливає на ймовірнісні та періодичні характеристики алгоритму авторизації, застосовано спрощений варіант генератора Голлмана.

Підвищення безпеки безпровідних мереж, побудованих на традиційних технологіях, – актуальне і перспективне розв'язання проблем інформаційно-телекомунікаційних систем для подальших досліджень.

Ключові слова: *інформаційно-телекомунікаційні системи; мережі; кібербезпека; протокол авторизації.*

The article examines this problem in the information and telecommunica-tion systems and networks, as cybersecurity. Analyzes the advantages and disad-vantages of wireless routers in cybersecurity.

Considered a priority element of the negative impact of – wireless authentication protocols. This element allows a potential attacker full access to the information resource.

There is a need to change the authentication protocols with the aim of reducing the probability of opening a quality authentication and identification algorithm.

To solve this problem, the article suggests the use of the algorithm of forming an authorization key additional functional element. Element is a random sequences. Article two new elements introduced in the authorization key generation algorithm.

As an additional element, a positive effect on the probability characteristics of the algorithm and periodic authorization applied simplified version of the Gollman generator.

Improved safety wireless network built on traditional technology is relevant and it becomes promising for further research.

Key words: *information and telecommunication systems; networks; cybersecurity; authentication protocols.*

Постановка проблемы. Обеспечение кибербезопасности – наиболее актуальная проблема в информационно-телекоммуникационных системах и сетях (далее – ИТС). Широко распространенными элементами ИТС стали беспроводные маршрутизаторы, у которых есть свои как неоспоримые преимущества (мобильность, низкие затраты при развертывании и использовании таких сетей), так и существенные недостатки (неограниченные возможности доступа к ним посредством беспроводных технологий со стороны заинтересованных лиц, что может привести к нарушению целостности хранимых данных, а также значительным материальным и юридическим негативным последствиям).

Анализ последних исследований и публикаций. На протяжении нескольких лет массовое производство беспроводных маршрутизаторов привело к насыщению рынка сетевого оборудования на различных уровнях пользования устройствами, не обеспечивающими основные требования по кибербезопасности ресурсов.

В ходе их технологического эволюционирования основные алгоритмы и технологии беспроводных маршрутизаторов стандартизированы, изучены и популяризированы, что привело к массовому созданию алгоритмов и технологий по их взлому с целью дальнейшего воздействия на информационные ресурсы как отдельных пользователей, так и сетевых ресурсов различных уровней сложности.

Приоритетным элементом негативного воздействия являются протоколы авторизации беспроводных сетей. Этот элемент позволяет обеспечить потенциальному злоумышленнику полный доступ к информационному ресурсу. Возникает необходимость изменения протоколов авторизации с целью качественного снижения вероятности вскрытия алгоритма авторизации и идентификации.

Цель статьи – как вариант технологического решения предлагается применение в алгоритме формирования ключа авторизации дополнительного функционального элемента.

Изложение основного материала. Элемент представляет собой генератор псевдослучайных последовательностей (далее – ПСП). Структурная схема изображена на рис. 1.

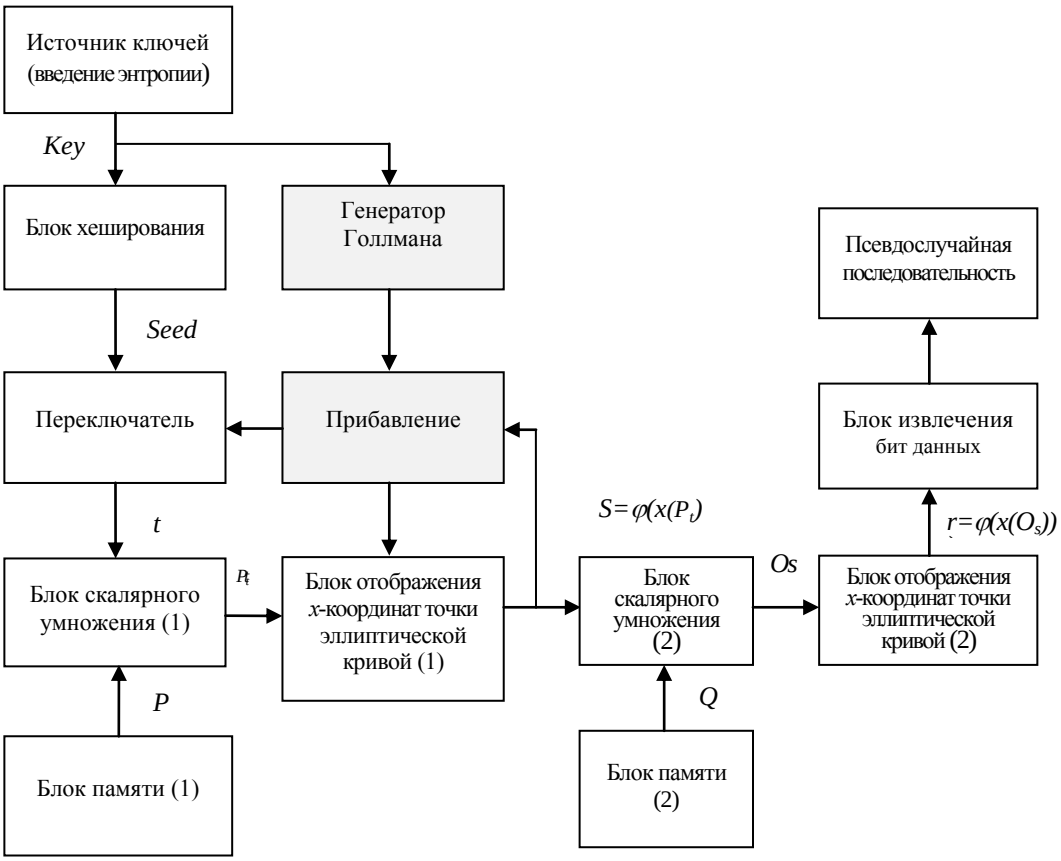

Рис. 1. Структурная схема алгоритма формирования ключей авторизации

В структурной схеме приведен алгоритм формирования ключей авторизации, находящихся в открытом доступе и широко использующихся в беспроводных маршрутизаторах и клиентских устройствах практически всех основных производителей беспроводного оборудования. Но в этой схеме мы вносим два новых элемента, которые качественно влияют на вероятностные и периодические характеристики этих алгоритмов.

В качестве дополнительного элемента, положительно влияющего на вероятностные и периодические характеристики алгоритма авторизации, применён упрощенный вариант генератора Голлмана.

Основным элементом каскада Голлмана является LFSR.

Регистр сдвига с линейной обратной связью (далее – РЛСОС, англ. Linear feedbackshift register, LFSR) – регистр сдвига битовых слов, у которого значение входного (вдвигаемого) бита равно линейной булевой функции от значений остальных битов регистра до сдвига. Может быть организован как программными, так и аппаратными средствами. Применяется для генерации псевдослучайных последовательностей битов, что находит применение, в частности, в криптографии.

Каскад Голлмана включает несколько регистров сдвига LFSR. Первый регистр движется равномерно с шагом 1. Сдвиг каждого последующего регистра управляется предыдущим так, что изменение состояния последующего регистра в такте происходит, если в такте с предыдущего регистра снимается 1. Иначе состояние последующего регистра не изменяется (рис. 2).

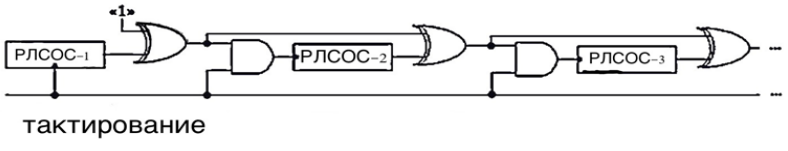

Рис. 2. Каскад Голлмана

Типичным примером комбинирования регистров сдвига является схема чередующегося “старт-стоп” генератора (Alternating Stop-and-Go Generator).

У этого генератора большой период и высокая линейная сложность, но несложная схема реализации алгоритма.

Программные реализации РЛСОС достаточно медленны и работают быстрее, если они написаны на ассемблере. Одно из решений – параллельное использование 16 РЛСОС (или 32, в зависимости от длины слова в архитектуре компьютера). В такой схеме используется массив слов, размер которого равен длине регистра сдвига, а каждый бит слова относится к своему РЛСОС. Так как используются одинаковые номера отводных последовательностей, то это может дать заметный выигрыш производительности генератора.

Как вариант программного решения представим использование регистров, называемое конфигурацией Фибоначчи. Рассмотрим 32-битовый сдвиговый регистр. Для него имеется отводная последовательность (32, 31, 30, 28, 26, 1). Это означает, что для генерации нового бита необходимо с помощью операции XOR просуммиро-

вать 31, 30, 29, 27, 25, 0-й биты. Полученный РСЛОС имеет максимальный период 2 32 1. На рис. 3 формализовано представлен код на языке программирования Си:

```
int LFSR_Galois (void)
{
    static unsigned long S = 0x00000001;
    if (S & 0x00000001) {
        S = (S ^ 0x80000057 >> 1) | 0x80000000;
        return 1;}
    else {
        S >>= 1;
        return 0;}
}
```

Рис. 3. Код на языке программирования Си

Этот криптоалгоритм имеет хорошие статистические свойства, он достаточно прост в программной или аппаратной реализаций, может быть использован для генераций псевдослучайных последовательностей большой разрядности и с большими периодами, обладает доказанными на адекватных математических моделях статистическими преимуществами. К недостаткам можно отнести чувствительность к вскрытию, которую называют запиранием (lock-in). Метод, по которому криптоаналитик восстанавливает вход последнего сдвигового регистра в каскаде, а затем эмулирует весь каскад регистр за регистром.

Существуют угрозы, связанные с недостатками интерфейса оборудования. Как правило, интерфейсы основных производителей унифицированы и стандартизированы. Альтернативные интерфейсы не решают проблем безопасности, что зачастую приводит к массовому опосредованному использованию беспроводного оборудования в DDOs воздействиях на другие элементы и ресурсы глобальной сети.

Как частный пример воздействия на беспроводное оборудование рассмотрим GET-запрос (это разновидность HTTP-запроса), с помощью которого браузер запрашивает файлы веб-сервера.

Попробуем описать механизм GET-запроса:

– используется для запроса содержимого указанного ресурса, в нашем прикладном случае – доступ к идентификаторам беспроводного маршрутизатора;

– с помощью метода GET можно инициировать процесс несанкционированной авторизации;

– в этом случае в тело ответного сообщения поступает информация о ходе выполнения процесса идентификации и авторизации;

– клиент может передавать параметры выполнения запроса в URI целевого ресурса после символа “?”:

GET/path/resource?param1=value1&param2=value2 HTTP/1.1

Согласно стандарту HTTP, запросы типа GET считаются идемпотентными, то есть на каждый одинаковый запрос поступает одинаковый ответ.

Кроме обычного метода GET, различают:

– условный GET – содержит заголовки If-Modified-Since, If-Match, If-Range и подобные;

– частичный GET – содержит в запросе Range.

Порядок выполнения подобных запросов определён стандартами отдельно, то есть изменение алгоритма идентификации и авторизации приведёт к уменьшению вероятности использования этих процессов для несанкционированной идентификации и последующей авторизации.

Существует статистика киберинцидентов, когда из-за недостаточных мер по кибербезопасности со стороны провайдера осуществляется несанкционированный доступ к корпоративным сетевым ресурсам и массовому распространению вредоносного программного обеспечения.

Выводы из данного исследования и перспективы дальнейших исследований в данном направлении. Вышеперечисленные угрозы связаны с выявленными недостатками интерфейсов беспроводных маршрутизаторов и свойственны устаревшим типам беспроводного оборудования практически всех основных производителей. Это оборудование имеет широкое распространение в Украине в связи с его низкой себестоимостью и встречается практически во всех информационных ресурсах государственных структур.

Повышение безопасности беспроводных сетей, построенных на традиционных технологиях, в настоящее время весьма актуально и является перспективным для дальнейших исследований в этом направлении.

Список использованной литературы:

1. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си / Шнайер Б. – М. : Триумф, 2013. – 816 с.

2. Габидулин Э. М. Защита информации : учеб. пособие / Габидулин Э. М., Кшевецкий А. С., Колыбельников А. И. – М. : МФТИ, 2011. – 225 с.

3. Ларин А. Л. Основы цифровой электроники / Ларин А. Л. – М. : МФТИ, 2008. – 314 с.

4. Скляр Б. Цифровая связь. Теоретические основы и практическое применение / Скляр Б. – М. : Вильямс, 2007. – 1104 с.

5. Сорока Л. С. Моделі і методи авторизації доступу в безпроводових телекомунікаційних мережах / Л. С. Сорока, О. О. Кузнецов, Д. І. Прокопович-Ткаченко. – Дніпро-петровськ : Пороги, 2013. – 196 с.