первичная последовательность является последовательностью независимых одинаково распределенных случайных величин, то необходимо подтвердить данный факт с помощью статистического тестирования. Если первичная последовательность проходит статистическое тестирование, то применяется алгоритм построения оценки минимальной энтропии для последовательности независимых одинаково распределенных случайных величин. В противном случае полагается, что она не является последовательностью независимых одинаково распределенных случайных величин и для построения оценки минимальной энтропии применяется второй алгоритм.

Тестирование независимости и одинаковой распределенности как первичной, так и выходной последовательности осуществляется с использованием статистических критериев хи-квадрат и перестановочных тестов [4]. Перестановочные тесты опираются на тот факт, что выборка, полученная перестановкой наблюдений исходной выборки, должна иметь те же свойства, что и исходная выборка.

Выходная последовательность обязательно должна быть последовательностью независимых одинаково распределенных случайных величин, поэтому она всегда проходит статистическую проверку на независимость и одинаковую распределенность. Если выходная последовательность не проходит статистическое тестирование, это означает, что генератор не прошел испытания.

При отсутствии дополнительного функционального преобразования первичной последовательности оценки минимальной энтропии выходной и первичной последовательностей совпадают. При реализации функционального преобразования на основе сертифицированных криптографических алгоритмов и функций проверяется корректность реализации. В случае корректности оценка минимальной энтропии рассчитывается по следующей формуле:

$$H = \min\{H_{in}, W_{out}\},$$

где H_{in} – энтропия, поступившая на вход преобразования, W_{out} – длина битовой строки на выходе.

В случае использования других алгоритмов и функций или некорректной реализации сертифицированных алгоритмов и функций применяется алгоритм построения оценки энтропии для последовательности независимых одинаково распределенных случайных величин.

Список использованных источников

1. National Institute of Standards and Technology special publication (SP) 800-22 A statistical test suite for random and pseudorandom number generators for cryptographic applications. – 2000.

2. Federal Information Processing Standard 140-2, Security requirement for cryptographic modules. – 2001.

3. *Knuth, D.* The art of computer programming / D. Knuth. – Vol. 2, 3rd ed. – Boston, USA, 1998.

4. National Institute of Standards and Technology special publication (SP) 800-90B Recommendation for the entropy sources used for random bit generation. – 2012.

НАУЧНО-МЕТОДИЧЕСКАЯ ПОДДЕРЖКА ДИСЦИПЛИНЫ «КРИПТОГРАФИЧЕСКИЕ ПРОТОКОЛЫ» В РАМКАХ СПЕЦИАЛЬНОСТИ «КОМПЬЮТЕРНАЯ БЕЗОПАСНОСТЬ»

Е. Н. МЕЛЬНИКОВА

Криптографические протоколы представляют собой сравнительно молодое направление исследований в теоретической криптографии. Первые работы, посвященные

криптографическим протоколам, появились примерно в конце 70-х гг. XX столетия. К настоящему времени это направление образует вполне сложившийся раздел теоретической криптографии, имеющий достаточно много практических приложений.

Криптографические методы и, в частности, криптографические протоколы все более активно используются в банковских технологиях, при создании информационных систем для обеспечения электронной коммерции и электронного документооборота [1; 2; 6]. Интенсивное развитие сетевых технологий ставит перед многими пользователями ряд вопросов, связанных с обеспечением безопасности при работе в сети. Помимо обеспечения конфиденциальности информации, актуальными являются и такие задачи, как проверка подлинности сторон (идентификация и аутентификация), передача и распределение ключей, обеспечение целостности сообщений, обеспечение невозможности отказа от авторства, анонимность (обеспечение неотслеживаемости).

Если задача обеспечения конфиденциальности решается с помощью криптосистем, то для решения других задач разрабатываются криптографические протоколы. Поэтому криптографические протоколы представляют собой один из важнейших элементов распределенных систем, и их применяют для того, чтобы обеспечить защищенное взаимодействие (обмен информацией) удаленных пользователей компьютерной сети, использующих, как правило, для передачи сообщений открытые каналы связи.

В настоящий момент имеется уже достаточно много различных типов криптографических протоколов, предназначенных для разных целей и обеспечивающих разный уровень безопасности. Все эти типы можно условно разделить на две группы: прикладные протоколы и примитивные. Прикладные протоколы решают конкретные задачи, которые возникают или могут возникнуть на практике. Примитивные протоколы используются как базовые модели при разработке прикладных протоколов.

Учитывая важность раздела современной теоретической криптографии, посвященного изучению криптографических протоколов, на факультете прикладной математики и информатики Белорусского государственного университета для студентов 5-го курса (при пятилетней форме обучения) специальности «Компьютерная безопасность» специализации «Математические методы защиты информации» разработан курс лекций «Криптографические протоколы», рассчитанный на 36 лекционных часов. Этот курс основывается на знаниях студентов, полученных при изучении таких дисциплин, как «Криптографические методы», «Теоретические основы компьютерной безопасности», «Системы и сети передачи информации».

Поскольку объем аудиторных часов небольшой, целью курса является ознакомление с основными принципами разработки, анализа, реализации и применения криптографических протоколов в современных информационных системах и компьютерных сетях, а также рассмотрение методов оценки их стойкости. При подготовке курса была использована литература, представленная в [1–11].

В результате изучения дисциплины «Криптографические протоколы» студенты должны
знать:

- виды задач, решаемых с использованием криптографических протоколов;
- классификацию криптографических протоколов;
- типовые криптографические протоколы и основные требования к ним;
- основные виды, способы построения и анализа стойкости криптографических протоколов аутентификации;
- основные виды, способы построения и анализа стойкости криптографических протоколов передачи и распределения ключей;
- криптографические стандарты;

уметь:

- формулировать свойства безопасности криптографических протоколов;
- проводить сравнительный анализ криптографических протоколов, решающих схожие задачи;

• анализировать стойкость криптографических протоколов к разным видам атак;

• применять полученные знания при проектировании систем безопасности;

владеть:

• криптографической терминологией;

• простейшими подходами к анализу безопасности криптографических протоколов.

Среди задач, которые решаются с использованием криптографических протоколов, можно, в частности, выделить две наиболее важные.

Первая задача заключается в установлении подлинности пользователей, участвующих в выполнении протокола. Процедуру, позволяющую одному пользователю проверить объявленные свойства другого пользователя, называют аутентификацией, и реализуется она с помощью протоколов аутентификации.

Вторая задача состоит в том, чтобы распределить между пользователями секретный сеансовый ключ для дальнейшего конфиденциального взаимодействия. Хотя успешное выполнение протокола аутентификации и обеспечивает подлинность пользователей, но оно не гарантирует подлинность и конфиденциальность дальнейшего обмена информацией между ними. Для защищенного взаимодействия в будущем, в процессе аутентификации или сразу после него, между пользователями должен быть распределен секретный сеансовый ключ. Распределение секретного ключа обеспечивается протоколами распределения ключевой информации.

На практике, как правило, эти две задачи взаимосвязаны, поскольку, с одной стороны, для безопасного распределения ключей необходимо подтверждение подлинности участников информационного обмена, а с другой – задача надежной аутентификации участников очень часто решается на основе выполнения безопасного распределения секретных ключей. Поэтому один и тот же протокол может применяться для решения нескольких задач. Основное внимание в курсе «Криптографические протоколы» уделено именно протоколам аутентификации пользователей и протоколам распределения секретных ключей.

В рамках предлагаемой дисциплины изучаются и анализируются протоколы из литературных источников по криптографии, которые относятся к учебным протоколам [2–8], рассматриваются конструкции протоколов, которые представлены в Международных стандартах, принятых Международной организацией по стандартизации и Международной электротехнической комиссией (ISO/IEC) [9–11], а также некоторые широко используемые на практике криптографические протоколы.

Примерный тематический план дисциплины включает следующие разделы:

1. Введение в теорию криптографических протоколов, основные понятия и общие положения.

2. Криптографические ключи. Управление ключами в криптографических системах и протоколах.

3. Инфраструктура открытых ключей, формат сертификата открытых ключей X.509, список отозванных сертификатов.

4. Атаки на криптографические протоколы, разновидности атак, взаимодействие атакующего с каналом связи.

5. Криптографические протоколы аутентификации. Простая и строгая аутентификация; односторонняя и взаимная аутентификация.

6. Криптографические протоколы распределения ключей, использующие одноключевую (симметричную) криптосистему.

7. Криптографические протоколы распределения ключей, использующие двухключевую (асимметричную) криптосистему.

8. Обзор практических криптографических протоколов (NTLM 2.0, Kerberos v.5, SSL/TLS, IPSec).

Для всех изучаемых протоколов приводится схема протокола, указывается область применения, формулируются предположения, необходимые для выполнения

протокола, дается описание шагов протокола и проводится анализ его стойкости. Включение перечисленных выше прикладных протоколов обосновано тем, что эти протоколы являются стандартными и широко используются в реальных компьютерных системах и сетях.

Следует отметить, что раздел криптографии, посвященный криптографическим протоколам, очень обширный и многогранный. Естественно, многие темы не вошли в тематический план, поэтому имеется возможность обновлять материал и добавлять новые разделы. Например, можно добавить раздел, изучающий криптографические протоколы на эллиптических кривых, раздел, посвященный протоколам доказательства с нулевым разглашением, раздел, посвященный схемам разделения секрета.

Список использованных источников

1. *Запечников, С. В.* Криптографические протоколы и их применение в финансовой и коммерческой деятельности / С. В. Запечников. – М.: Горячая линия – Телеком, 2007. – 320 с.

2. *Мао, В.* Современная криптография: теория и практика /В. Мао; пер. с англ. – М.: Изд. дом «Вильямс», 2005. – 768 с.

3. *Молдовян, Н. А.* Введение в криптосистемы с открытым ключом / Н. А. Молдовян, А. А. Молдовян. – СПб.: БХВ-Петербург, 2005.

4. *Смит Р. Э.* Аутентификация: от паролей до открытых ключей / Р. Э. Смит; пер. с англ. – М.: Изд. дом «Вильямс», 2005. – 432 с.

5. Криптология / Ю. С. Харин [и др.]. – Минск: БГУ, 2013. – 512 с.

6. *Черемушкин, А. В.* Криптографические протоколы. Основные свойства и уязвимости: учеб. пособие / А. В. Черемушкин. – М.: Изд. центр «Академия», 2009. – 272 с.

7. *Шнайер, Б.* Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке СИ / Б. Шнайер. — М.: Изд-во «Триумф», 2002.

8. *Clark, J.* A Survey of Authentication Protocol Literature: version 1.0, 1997/ J. Clark, J. Jacob. Avail. at www.cs.york.ac.uk/.

9. ISO/IEC 9798-2. Information technology – Security techniques – Entity authentication. Part 2: Mechanisms using symmetric encipherment algorithms // International Standard, 1999-07-15.

10. ISO/IEC 9798-4. Information technology – Security techniques – Entity authentication. Part 4: Mechanisms using a cryptographic check function // International Standard, 1999-12-15.

11. ISO/IEC 11770-2. Information technology – Security techniques – Key management. Part 2: Mechanisms using symmetric techniques // International Standard, 1996-06-01.