КРИПТОГРАФИЧЕСКИЕ ПРОТОКОЛЫ
090301 — Компьютерная безопасность

А. В. Черемушкин

1 апреля 2011

Общая концепция дисциплины

- Изложить общие принципы построения протоколов.
- Явно указать основные свойства и уязвимости.
- Привести примеры типовых протоколов и атак на них.
- Не затрагивать вопросов конкретной реализации.

Примерная программа

- Тема 1. Основные понятия
- Тема 2. Схемы цифровой подписи
- Тема 3. Протоколы идентификации
- Тема 4. Инфраструктура открытых ключей
- Тема 5. Протоколы распределения ключей
- Тема 6. Прикладные протоколы
- Тема 7. Протоколы открытых сделок
- Тема 7. Заключение

Примерная программа

Тема 2. Схемы цифровой подписи

Схемы цифровой подписи. Схемы цифровой подписи.
Схемы цифровой подписи на основе симметричных и асимметричных шифрсистем.
Схемы Эль-Гамаля, Фиата – Фейга – Шамира и Шнорра, их свойства Семейство схем типа Эль-Гамаля.
Стандарты США и России электронной цифровой подписи.
Одноразовые подписи.
Схемы конфиденциальной цифровой подписи и подписи вслепую.
Подписи с обнаружением подделки.

Примерная программа

Тема 3. Протоколы идентификации

Протоколы идентификации на основе паролей, протоколы “рукопожатия” и типа “запрос-ответ”.
Идентификация с использованием систем открытого шифрования.
Понятие протоколов интерактивного доказательства и доказательства знания.
Протоколы идентификации на основе протоколов доказательства знания с нулевым разглашением.
Протоколы Фиата – Шамира, Шаума, Шнорра и Окамото.
Связь между протоколами цифровой подписи и протоколами идентификации.
Протоколы с самосертифицируемыми открытыми ключами, построенными на основе идентификаторов.

Примерная программа

Тема 4. Инфраструктура открытых ключей

Управление открытыми ключами.
Основы организации и основные компоненты инфраструктуры открытых ключей.
Сертификат открытого ключа. Стандарт X.509.
Сервисы инфраструктуры открытых ключей.
Удостоверяющий центр. Центр регистрации. Репозиторий.
Архив сертификатов. Конечные субъекты.
Архитектуры инфраструктуры открытых ключей.
Проверка и отзыв сертификата открытого ключа.

Примерная программа

Тема 5. Протоколы распределения ключей

Протоколы генерации и передачи ключей на основе симметричных и асимметричных шифрсистем.
Двух- и трехсторонние протоколы передачи и распределения ключей.
Функции доверенной третьей стороны и выполняемые ею роли.
Схемы предварительного распределения ключей. Неравенство Блома.
Схемы предварительного распределения ключей Блома и на основе пересечений множеств.
Протокол открытого распределения ключей Диффи – Хэллмана и способы его защиты от атаки “противник в середине”.
Аутентифицированные протоколы открытого распределения ключей.
Групповые протоколы. Протоколы разделения секрета и распределения ключей для телеконференции.

Примерная программа

Тема 6. Прикладные протоколы

Построение семейства протоколов KriptoKnight на основе базовых протоколов взаимной аутентификации и распределения ключей.
Особенности построения семейства протоколов IPsec.
Протоколы Oakley, ISAKMP, IKE.
Протоколы SKIP, SSL/TLS и особенности их реализации.

Примерная программа

Тема 7. Протоколы открытых сделок

Протоколы битовых обязательств и их свойства.
Протоколы подбрасывания монеты и “игры в покер” по телефону.
Забывающая передача информации.
Протокол подписания контракта.
Протокол сертифицированной электронной почты.
Протоколы электронного голосования.
Свойства неотслеживаемости и несвязываемости.
Протоколы электронных платежей и цифровых денег.

В результате изучения дисциплины студенты должны

знать:

- криптографические стандарты;
- типовые криптографические протоколы и основные требования к ним;
- основные схемы цифровой подписи;
- протоколы идентификации;
- протоколы передачи и распределения ключей;

В результате изучения дисциплины студенты должны

уметь:

- формулировать задачу по оцениванию безопасности криптографического протокола применительно к конкретным условиям;
- использовать симметричные и асимметричные шифрсистемы для построения криптографических протоколов;
- формулировать свойства безопасности криптографических протоколов;
- проводить сравнительный анализ криптографических протоколов, решающих сходные задачи;

владеть:

- криптографической терминологией;
- простейшими подходами к анализу безопасности криптографических протоколов.

Цели изучения дисциплины

Вид занятий	Всего часов	Семестры
Общая трудоемкость	108+36	9
Аудиторные занятия	60	60
Лекции	30	30
Практические занятия (ПЗ)	34	34
Контрольные работы	2	2
Самостоятельная работа	48	48
Проработка учебного материала	18	18
Домашняя работа (задание)	30	30
Вид итогового контроля	36	(Экзамен)

Основные понятия

Протокол

— описание распределенного алгоритма, в процессе выполнения которого участники последовательно выполняют определенные действия и обмениваются сообщениями.

Предполагается, что все участники выполняют в нем какую-либо активную роль, а пассивные наблюдатели не являются участниками протокола.

Протокол 1: (схематическая запись)

$$(1)\ A \rightarrow B:\ E_{k_{AB}}(M_1),$$
$$(2)\ A \leftarrow B:\ E_{k_{BA}}(M_2).$$

Понятия цикла, шага, роли и сеанса.

- Цикл (проход) протокола (*round*) — в криптографических протоколах с двумя участниками — временной интервал, в котором активен только один из участников.

Понятия цикла, шага, роли и сеанса.

- Цикл (проход) протокола (*round*) — в криптографических протоколах с двумя участниками — временной интервал, в котором активен только один из участников.
- Шаг (*step of a protocol, protocol action*) — конкретное законченное действие, выполняемое участником во время одного цикла (прохода) протокола.

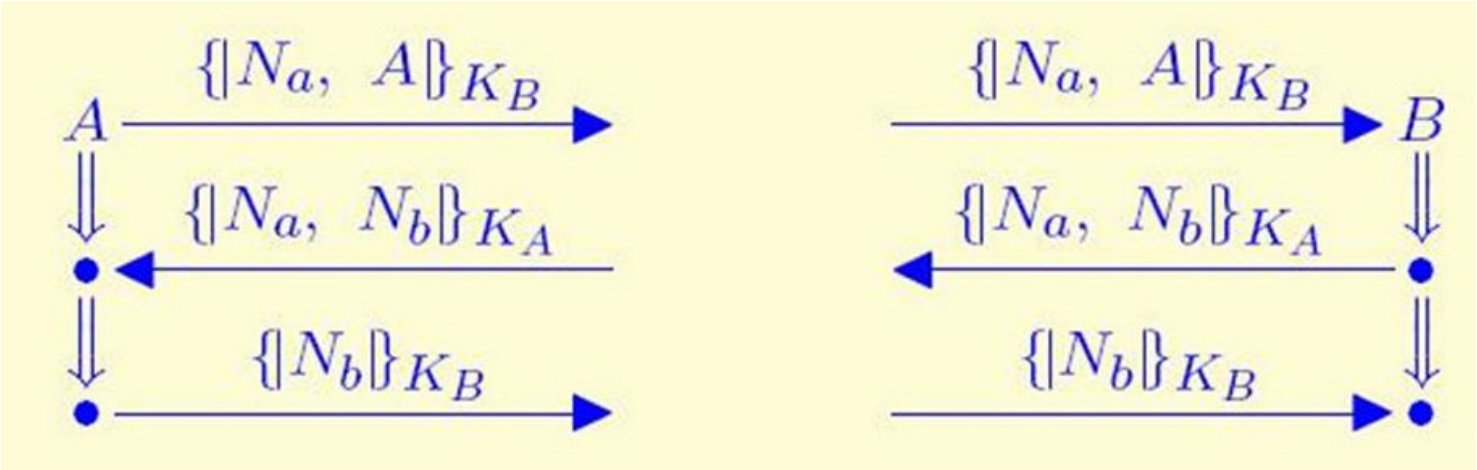
Понятия цикла, шага, роли и сеанса.

- Цикл (проход) протокола (*round*) — в криптографических протоколах с двумя участниками — временной интервал, в котором активен только один из участников.
- Шаг (*step of a protocol, protocol action*) — конкретное законченное действие, выполняемое участником во время одного цикла (прохода) протокола.
- Сеанс (*session*) — это конкретная реализация протокола с конкретными участниками.

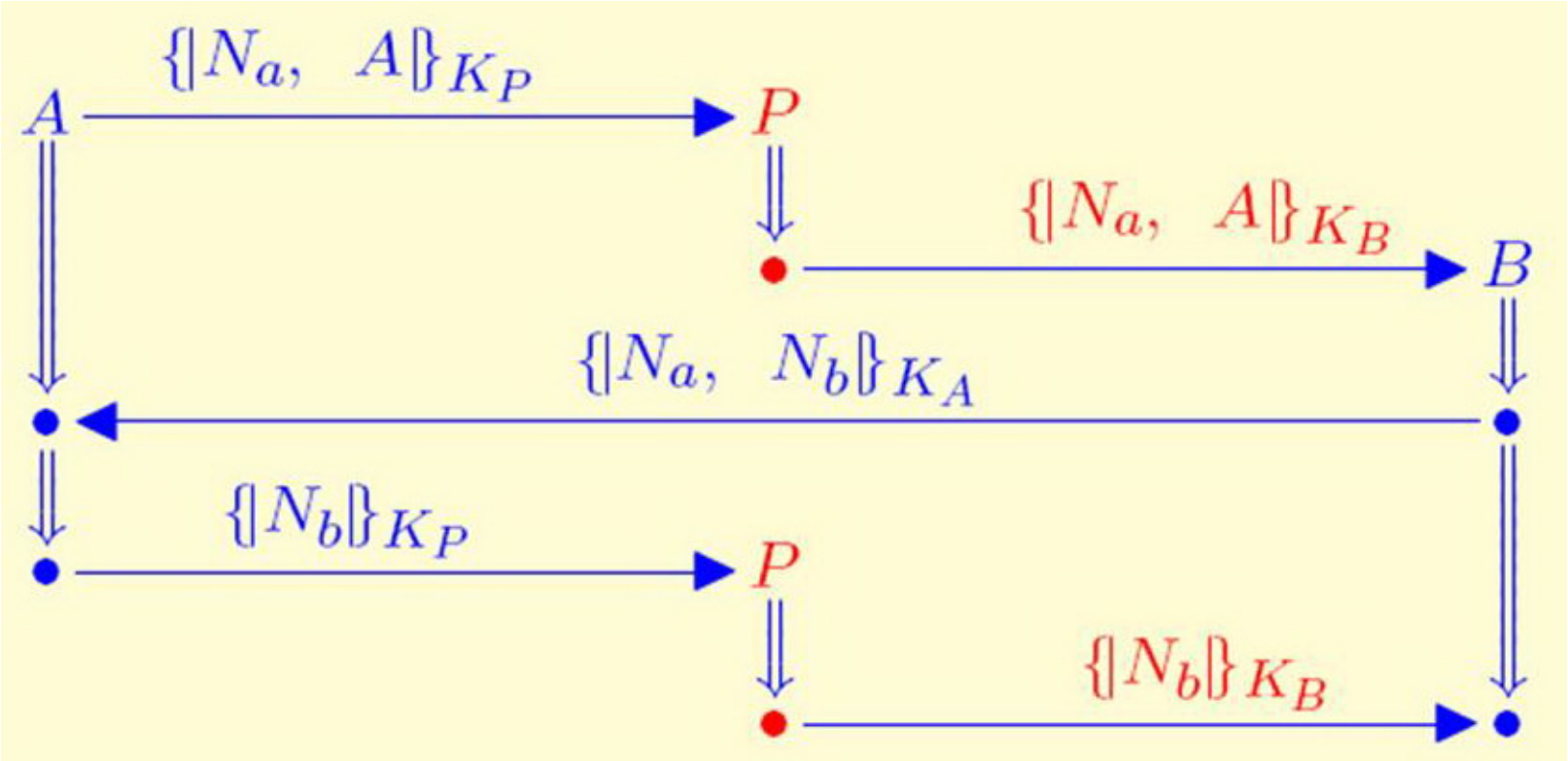
Понятия цикла, шага, роли и сеанса.

- Цикл (проход) протокола (*round*) — в криптографических протоколах с двумя участниками — временной интервал, в котором активен только один из участников.
- Шаг (*step of a protocol, protocol action*) — конкретное законченное действие, выполняемое участником во время одного цикла (прохода) протокола.
- Сеанс (*session*) — это конкретная реализация протокола с конкретными участниками.
- Роль — это та функция, которую выполняет конкретный участник в конкретном сеансе.

Роли протокола NSPK



Атака Lowe на протокол NSPK



Криптографический протокол

Безопасность протокола выражается в обеспечении гарантий выполнения таких свойств, характеризующих безопасность, как: доступность, конфиденциальность, целостность и др.

Защищенный или, протокол обеспечения безопасности

(*security protocol*) — протокол, обеспечивающий поддержку хотя бы одной из функций безопасности.

Криптографический протокол

— протокол, предназначенный для выполнения функций криптографической системы, в процессе выполнения которого участники используют криптографические алгоритмы.

Свойства/цели безопасности

Обычно свойства протоколов, характеризующие их стойкость к различным атакам, формулируют как цели (goals), или требования к протоколам.

Трактовка этих целей со временем меняется и уточняется.

Под свойствами (целями, требованиями) безопасности в документах IETF в настоящее время понимаются следующие 20 целей, сгруппированные в 10 групп:

Свойства/цели безопасности

№	Код	Название
1	G1	Аутентификация субъекта
	G2	Аутентификация сообщения
	G3	Защита от повтора
2	G4	Неявная (скрытая) аутентификация получателя
	G5	Аутентификация источника
3	G6	Авторизация (доверенной третьей стороной)
4	G7	Аутентификация ключа
	G8	Подтверждение правильности ключа
	G9	Защищенность от чтения назад
	G10	Формирование новых ключей
	G11	Защищенная возможность договориться о параметрах

Свойства/цели безопасности

№	Код	Название
5	G12	Конфиденциальность
6	G13	Анонимности при прослушивании (несвязываемость)
	G14	Анонимности при работе с другими участниками
7	G15	Ограниченная защищенность от DoS атак
8	G16	Неизменность отправителя
9	G17	Подотчетность
	G18	Доказательство отправки
	G19	Доказательство получения
10	G20	Безопасное временное свойство

Примеры свойств безопасности

Протокол \ Цель G	1	2	3	4	5	6	7	8	9	10	11	12
EAP-IKEv2	×	×	×			×	×			×		
EKE	×	×										×
IKE	×	×	×				×		×	×	×	
IKEv2	×	×	×				×		×	×	×	
DHCP-IPSec-tunnel	×	×										×
kerberos	×	×	×			×	×			×		
SSH	×	×	×				×			×	×	
TLS	×	×	×				×			×	×	
TLS-v1.1	×	×	×				×			×	×	
TLS-SRP	×	×	×				×			×	×	
tls-sharedkeys	×	×	×				×			×	×	
SET	×	×	×									

Атаки на протокол

Атака на протокол

— попытка проведения анализа сообщений протокола и/или выполнения не предусмотренных протоколом действий с целью нарушения работы протокола и/или получения информации, составляющей секрет его участников.

Атака считается *успешной*, если нарушено хотя бы одно из заявленных свойств, характеризующих безопасность протокола.

В основе атак могут лежать различные *методы анализа протоколов*.

Стойкость протокола

Стойкость протокола

— способность противостоять атакам.

Определяется конкретным набором свойств протокола.

Стойкость протокола зависит от многих факторов:
— от надежности криптографических механизмов,
— от правильности реализации,
— от точности выполнения порядка предписанных действий участниками протокола,
— и др.

Стойкость протокола

Рассматриваем только те слабости протоколов,

которые обусловлены способом формирования и порядком отправки сообщений участниками, то есть ошибками, допущенными при синтезе самих протоколов, представляющих собой предписания, определяющие порядок действий всех участников.

Основные предположения

Предположение 1. *Perfect cryptography assumption* — все стандартные криптографические примитивы удовлетворяют условию совершенной стойкости, слабости могут быть вызваны только непродуманным порядком действий, предписанных самим протоколом;

Предположение 2. *Strong typing assumption* (строгое соблюдение типов) — все участники правильно понимают форматы получаемых сообщений и корректно распознают типы полей в записи передаваемых сообщений;

Предположение 3. *Honest participants* (честность участников) — все участники точно выполняют предписанный согласно протоколу порядок действий.

Предположение 4. *Bounded number of sessions* (ограниченное число сеансов) — для сведения задачи к конечному числу состояний.

При неограниченном числе сеансов проблема безопасности протокола неразрешима (S. Even, O. Goldreich, 1983).

Подходы к классификации атак

- по способу воздействия;
- по цели;
- по области применения;
- по классу протоколов;
- по применяемому математическому аппарату;
- по способу применения;
- по требуемым ресурсам;
- по наличию и характеру дополнительной информации, и т.д.

Известные атаки

- 1. *Подмена (impersonation)* — попытка подменить одного пользователя другим.
- 2. *Повторное навязывание сообщения* (*replay attack*).
- 3. *Атака отражением* (*reflection attack*).
- 4. *Задержка передачи сообщения* (*forced delay*).
- 5. *Комбинированная атака* (*interleaving attack*) — комбинация данных из ранее выполненных протоколов, в том числе протоколов, ранее навязанных противником.

Известные атаки

- 6. *Атака с параллельными сеансами* (*parallel-session attack*).
- 7. *Атака с использованием специально подобранных текстов*.
- 8. “*Противник в середине*” (“*men in the middle*”) .
- 9. *Атака с известным сеансовым ключом* (*known-key attack*).
- 10. *Атака с неизвестным общим ключом* (*unknown key-share attack*)

Атака UKS на протокол STS

Протокол STS:

$$A \to B: \ A, B, m_A = \alpha^x \bmod p,$$
$$A \leftarrow B: \ B, A, m_B = \alpha^y \bmod p, E_k(Sig_B(m_B, m_A)),$$
$$A \to B: \ A, B, E_k(Sig_A(m_A, m_B)).$$

Здесь Sig_A и Sig_B — цифровые подписи пользователей A и B соответственно, $k = \alpha^{xy} \bmod p$ — искомый общий ключ.

Атака UKS на протокол STS

Атака:

(Lowe G., 1996) (*атака с неизвестным общим ключом*)
(unknown key-share attack)

$$
\begin{array}{lll}
A \rightarrow & C(B): & A, B, m_A, \\
 & C \rightarrow B: & C, B, m_A, \\
 & C \leftarrow B: & B, C, m_B,\ E_k(Sig_B(m_B, m_A)), \\
A \leftarrow & C(B): & B, A, m_B,\ E_k(Sig_B(m_B, m_A)), \\
A \rightarrow & C(B): & A, B, E_k(Sig_A(m_A, m_B)).
\end{array}
$$

Нарушитель C, используя свой законный обмен с участником B, в результате атаки убеждает A в том, что он выступает от имени B.

Атака BUKS на модифицированный протокол STS

Модифицированный протокол STS:

$$
\begin{aligned}
A \to B: &\ A, B, m_A = \alpha^x \bmod p, \\
A \leftarrow B: &\ B, A, m_B = \alpha^y \bmod p, Sig_B(m_B, m_A), h_{k_0}(m_B, m_A) \\
A \to B: &\ A, B, Sig_A(m_A, m_B), h_{k_0}(m_A, m_B),
\end{aligned}
$$

где $k_0 = f(k)$, $k = \alpha^{xy} \bmod p$.

Покажем, как участники C и D, вступившие в сговор, могут ввести в заблуждение участников A и B, сформировавших общий ключ.

Двусторонняя атака с неизвестным общим ключом:

$$
\begin{array}{llll}
A \rightarrow & C: & & A, B, m_A, \\
 & C \rightarrow & D: & A, B, m_A, \\
 & & D \rightarrow B: & D, B, m_A, \\
 & & D \leftarrow B: & B, D, m_B, Sig_B(m_B, m_A), h_{k_0}(m_B, m_A), \\
 & C \leftarrow & D: & B, A, m_B, h_{k_0}(m_B, m_A) \\
A \leftarrow & C: & & C, A, m_B, Sig_C(m_B, m_A), h_{k_0}(m_B, m_A), \\
A \rightarrow & C: & & A, C, Sig_A(m_A, m_B), h_{k_0}(m_A, m_B), \\
 & C \rightarrow & D: & A, B, h_{k_0}(m_A, m_B), \\
 & & D \rightarrow B: & D, B, Sig_D(m_A, m_B), h_{k_0}(m_A, m_B).
\end{array}
$$

A уверен, что он сформировал общий ключ с участником C,
B уверен, что он сформировал общий ключ с участником D.

Подходы к классификации протоколов

Классификация *по числу участников*:

- двусторонний,
- трехсторонний и т. п.,
- многосторонний.

Классификация *по числу передаваемых сообщений*:

- интерактивный (есть взаимный обмен сообщениями),
- неинтерактивный (только однократная передача).

Неинтерактивные протоколы часто называют *схемами*.

Подходы к классификации протоколов

Классификация *по целевому назначению* протокола:

- протокол обеспечения целостности сообщений,
  - с аутентификацией источника,
  - без аутентификации источника,
- протокол (схема) цифровой подписи,
  - протокол индивидуальной / групповой цифровой подписи,
  - с восстановлением / без восстановления сообщения,
  - протокол цифровой подписи вслепую,
  - протокол конфиденциальной цифровой подписи,
  - протокол цифровой подписи с доказуемостью подделки,
- протокол идентификации (аутентификации участников),
  - односторонней аутентификации,
  - двусторонней (взаимной) аутентификации,

- конфиденциальная передача,
  - обычный обмен сообщениями,
  - широковещательная / циркулярная передача,
  - честный обмен секретами,
  - забывающая передача,
  - протокол привязки к биту (строке),
- протокол распределения ключей,
  - протокол (схема) предварительного распределения ключей,
  - протокол передачи ключа (обмена ключами),
  - протокол совместной выработки ключа (открытого распределения ключей),
  - протокол парный / групповой,
  - протокол (схема) разделения секрета,
  - протокол телеконференции, и др.

Групповые протоколы (*group-oriented protocol*)

Предполагают одновременное участие групп участников:

- *протокол разделения секрета* (*secret sharing protocol*) — если все группы, имеющие на это право, формируют одинаковые ключи;
- *протокол телеконференции* — если у различных групп должны быть разные ключи;
- *протокол групповой подписи* (*group signature protocol*) — предполагается одновременное участие заранее определенной группы участников, причем в случае отсутствия хотя бы одного участника из группы формирование подписи невозможно.

- *Примитивный* криптографический протокол (*primitive cryptographic protocol*) — это криптографический протокол, который не имеет самостоятельного прикладного значения, но используется как базовый компонент при построении прикладных криптографических протоколов. Как правило, он решает какую-либо одну абстрактную задачу.
  Примеры: протокол обмена секретами, протокол привязки к биту, протокол подбрасывания монеты (по телефону).
- *Прикладной* криптографический протокол (*application cryptographic protocol*) предназначен для решения практических задач обеспечения функций — сервисов безопасности с помощью криптографических систем. Следует заметить, что прикладные протоколы, как правило, обеспечивают не одну, а сразу несколько функциям безопасности. Более того, такие протоколы, как IPsec, на самом деле являются большими семействами различных протоколов, включающими много разных вариантов для различных ситуаций и условий применения.

Примеры прикладных протоколов:

- система электронного обмена данными:
  - протоколы электронного документооборота,
- система электронных платежей:
  - протоколы систем с виртуальными деньгами,
    - удаленный платеж по электронным чекам,
  - протоколы систем с электронными деньгами,
    - протокол удаленного платежа по кредитным картам,
    - протокол электронного денежного перевода,
    - протокол электронного дебетового поручения,
  - протоколы систем с цифровыми деньгами,
    - протокол снятия со счета цифровой наличности,
    - платежный протокол с цифровыми деньгами,
    - протокол депозита для сдачи цифровых денег в банк,
    - протокол с идентификацией повторной траты монеты.

Примеры прикладных протоколов:

- система электронной коммерции:
  - протокол подписания контракта,
  - протокол сертифицированной электронной почты,
  - протокол электронного аукциона,
- поддержка правовых отношений:
  - протоколы голосования (электронные выборы),
- игровые протоколы,
  - протокол бросания жребия (по телефону),
  - протокол игры в покер (по телефону) и т. д.

Основная литература

- *Алферов А.П, Зубов А.Ю., Кузьмин А.С., Черемушкин А.В.* Основы криптографии. Учебное пособие. 3е изд., доп. Допущено Минобразования. – М.: АРВ – Гелиос, 2005. – 450 с.
- *Черемушкин А.В.* Криптографические протоколы. Основные свойства и уязвимости. Учебное пособие. Допущено УМО. – М.: Изд. центр “Академия”, 2009. – 272 с.
- *Запечников С.В.* Криптографические протоколы и их применение в финансовой и коммерческой деятельности: учеб. пособие: Допущено УМО. – М.: Горячая линия – телеком, 2006. – 319 с.
- *Гашков С. Б., Применко Э.А., Черепнев М.А.* Криптографические методы защиты информации: учеб. пособие: Допущено УМО. – М.: Изд. центр “Академия”, 2010. – 304 с.

Дополнительная литература

- *Под ред. Погорелова Б.А., Сачкова В.Н.* Словарь криптографических терминов. – М.: МЦНМО, 2006.
- *Столлингс В.* Криптография и защита сетей: принципы и практика, 2-е издание. – М.: Вильямс, 2001.
- *Столингс В.* Основы защиты сетей. Приложения и стандарты. – М.: Вильямс, 2002.
- *Горбатов В.С., Полянская О.Ю.* Основы технологии PKI. – М.: Горячая линия – Телеком, 2007.
- *Семенов Ю.А.* Протоколы Internet для электронной торговли. – М.: Горячая линия – Телеком, 2003.
- *Чмора А.* Современная прикладная криптография. – М.: АРВ – Гелиос, 2001.
- *Мао В.* Современная криптография: теория и практика. – М.: Вильямс, 2005.
- *Шнайер Б.* Прикладная криптография. – М.: Триумф, 2002.
- *Stinson D.R.* Cryptography, theory and practice. – London etc., CRC Press, 1995.
- *Menezes A.J., van Oorschot P.C., Vanstone S.A.* Handbook of applied cryptography. – Boca Raton, New York, London, Tokyo: CRC Press, 1997.

Вопросы?