Основы изучения PKI технологий в ФГОСах, как обеспечение потребностей Удостоверяющих центров

Шелупанов Александр Александрович
д.т.н., профессор,
директор УЦ Сибири
проректор по
научной работе ТУСУР
зав. кафедрой КИБЭВС

Направление подготовки «Информационная безопасность» 090000

Наименование специальности	Код	Квалификация
Информационная безопасность	090900	бакалавр
Криптография	090100	специалист
Противодействие техническим разведкам	090200	специалист
Компьютерная безопасность	090301	специалист
Информационная безопасность телекоммуникационных систем	090302	специалист
Информационная безопансость автоматизированных систем	090303	специалист
Информационно-аналитические системы безопасности	090305	специалист

Информационная безопасность 090900

Объекты профессиональной деятельности:

- Объекты информатизации (компьютерные, автоматизированные , телекоммуникационные, информационные системы).
- Технологии обеспечения ИБ.
- Процессы управления ИБ.

Виды профессиональной деятельности:

- эксплуатационная;
- проектно-технологическая;
- экспериментально-исследовательская;
- организационно-управленческая.

Информационная безопасность 090900

Профили:

1. Безопасность компьютерных систем.
2. Организация и технология защиты информации.
3. Комплексная защита объектов информатизации.
4. Безопасность автоматизированных систем.
5. Безопасность телекоммуникационных систем.
6. Информационно-аналитические системы финансового мониторинга.

Информационная безопасность 090900

Дисциплина: Криптографические методы ЗИ

Знать	Уметь	Владеть
Принципы построения криптографических алгоритмов, криптографические стандарты и их использование в информационных системах		

- Способность принимать участие в эксплуатации подсистем управления ИБ предприятия (ПК-9);
- Способность администрировать подсистемы ИБ объекта (ПК-10);
- Способность выполнять работы по установке, настройке и обслуживанию технических и программно-аппаратных СЗИ (ПК-11).

Криптография 090101

Закрытая специальность

Направление подготовки по данной специальности ориентировано на подготовку профессионалов в области **разработки и эксплуатации** криптографических средств защиты информации.

Криптография 090101

Специалисты получают глубокие знания по:

- криптографическим алгоритмам;
- математическое обеспечение криптографических преобразований;
- методы криптографической защиты информации;
- реализация криптографических алгоритмов;
- практическое использование СКЗИ (внедрение и обслуживание).

Противодействие техническим разведкам (ПДТР 090201)

Закрытая специальность!

Направление подготовки по данной специальности ориентировано на подготовку профессионалов в области **противодействия техническим разведкам** преимущественно для органов госвласти и госкорпораций.

Компьютерная безопасность (КБ 090301)

Объекты профессиональной деятельности:

- Защищаемые компьютерные системы.
- Системы управления ИБ.
- Методы и реализующие их СЗИ.
- Математические модели процессов ЗИ.
- Методы и средства контроля эффективности ИБ.
- Технологии создания СЗИ.

Виды профессиональной деятельности:

- научно-исследовательская;
- проектная;
- контрольно-аналитическая;
- организационно-управленческая;
- эксплуатационная.

Компьютерная безопасность 090301

Специализации:

1. Анализ безопасности компьютерных систем;
2. Математические методы ЗИ;
3. Безопасность распределенных компьютерных систем;
4. Разработка защищенного программного обеспечения;
5. Безопасность высокопроизводительных вычислительных систем;
6. Безопасность программного обеспечения мобильных систем;
7. Информационно-аналитическая и техническая экспертиза компьютерных систем;
8. ИБ объектов информатизации на базе компьютерных систем.

Компьютерная безопасность 090301

Дисциплины:

- Криптографические методы ЗИ,
- Криптографические протоколы,
- Теоретико-числовые методы в криптографии.

Компьютерная безопасность 090301

Знать	Уметь	Владеть
- основные виды симметричных и асимметричных криптографических алгоритмов; - математические модели шифров; - криптографические стандарты; - типовые криптографические протоколы и основные требования к ним; - алгоритмы проверки чисел и многочленов на простоту, построения больших простых чисел, разложения чисел и многочленов на множители, дискретного логарифмирования в конечных циклических группах;	- корректно применять симметричные и асимметричные криптографические алгоритмы; - формулировать задачу по оцениванию безопасности криптографического протокола применительно к конкретным условиям;	- криптографической терминологией; - простейшими подходами к анализу безопасности криптографических протоколов; - навыками эффективного вычисления в кольцах вычетов и в кольцах многочленов.

Компьютерная безопасность 090301

Компетенции:

- способностью к самостоятельному построению алгоритма, проведению его анализа и реализации в современных программных комплексах (ПК-12);
- способностью проводить обоснование и выбор рационального решения по уровню защищенности компьютерной системы с учетом заданных требований (ПК-19);
- способностью участвовать в разработке системы защиты информации предприятия (организации) и подсистемы информационной безопасности компьютерной системы (ПК-24);
- способностью производить установку, тестирование программного обеспечения и программно-аппаратных средств по обеспечению информационной безопасности компьютерных систем (ПК-34);
- способностью принимать участие в эксплуатации программного обеспечения и программно-аппаратных средств обеспечения информационной безопасности компьютерных систем (ПК-35).

Компьютерная безопасность 090301 Математические методы ЗИ

Дисциплина: Методы алгебраической геометрии в криптографии

Знать	Уметь	Владеть
- принципы построения псевдослучайных генераторов и их свойства; - принципы применения эллиптических и гиперэллиптических кривых в криптографии.	- разрабатывать быстрые вычислительные алгоритмы для криптографических приложений.	- навыками использования систем компьютерной математики для решения профессиональных задач; - методами построения быстрых вычислительных алгоритмов алгебры и теории чисел.
способность разрабатывать вычислительные алгоритмы, реализующие современные математические методы защиты информации (ПСК-2.3); способность разрабатывать вычислительные алгоритмы, реализующие современные математические методы защиты информации (ПСК-2.3);		

Компьютерная безопасность 090301 Безопасность ПО мобильных систем

Дисциплина: Безопасность системно-программного обеспечения мобильных устройств

Знать	Уметь	Владеть
- быстрые алгебраические и теоретико-числовые алгоритмы;	- разрабатывать системное и прикладное программное обеспечение мобильных устройств; - создавать приложения для компьютерных сетей, взаимодействующих с мобильными устройствами;	- методами встраивания средств криптографической защиты информации в мобильные системы; - технологиями создания безопасного программного обеспечения мобильных устройств.

- способностью разрабатывать программные средства обеспечения защиты мобильных устройств и устройств беспроводной связи (ПСК-6.1);
- способностью реализовывать быстрые вычислительные алгоритмы средствами мобильных устройств (ПСК-6.2);
- способностью разрабатывать прикладное и системное программное обеспечение для мобильных устройств с учетом требований по безопасности (ПСК-6.5);

ИБ Телекоммуникационных систем (ИБ ТС 090302)

Объекты профессиональной деятельности:

- Методы, системы средства ИБ ТС.
- Управление ИБ ТС.
- Информационно-телекоммуникационные сети и системы, оборудование, принципы работы и построения.

Виды профессиональной деятельности:

- научно-исследовательская;
- проектная;
- контрольно-аналитическая;
- организационно-управленческая;
- эксплуатационная.

ИБ ТС 090302

Специализации:

1. Мониторинг в ТС;
2. Системы представительской связи;
3. Сети специальной связи;
4. Инструментальный контроль ИБ ТС;
5. Системы специальной связи и информации для органов государственной власти;
6. ИБ космических ТС;
7. Разработка защищенных ТС;
8. Системы подвижной цифровой защищенной связи;
9. ЗИ в радиосвязи и телерадиовещании;
10. ЗИ в системах связи и управления;
11. ИБ мультисервисных ТС и сетей на транспорте;
12. Безопасность ТС информационного взаимодействия.

ИБ ТС 090302

Дисциплина: Криптографические методы ЗИ

Знать	Уметь	Владеть
- основные криптографические протоколы системы шифрования с открытыми ключами; - криптографические средства и СЗИ и их программно-аппаратную реализацию; - требования к шифрам и их основные характеристики;	- оценивать криптографическую стойкость шифров; - применять криптографические средства и системы ИБ;	- методами оценки криптографической стойкости алгоритмов шифрования; - криптографическими средствами и базовыми технологиями ИБ;
- способность участвовать в разработке компонентов ТС (ПК-18); - способность обеспечить эффективное применение средств защиты информационно-технологических ресурсов ТС (ПК-33);		

ИБ ТС 090302
Системы подвижной цифровой защищенной связи

Дисциплина: Беспроводные системы связи и их безопасность

Знать	Уметь	Владеть
- требования по обеспечению безопасности систем беспроводного доступа, современные протоколы шифрования		
- Способность понимать и использовать принципы работы и методы эксплуатации систем подвижной цифровой защищенной связи (ПСК-8.3)		

Информационно-аналитические системы безопасности (ИА СБ 090305)

Объекты профессиональной деятельности:

- специальные автоматизированные информационно-аналитические системы;

- модели, методы и методики информационно-аналитической деятельности в процессе организационного управления.

Виды профессиональной деятельности:

- информационно-аналитическая;
- научно-исследовательская;
- проектная;
- эксплуатационно-технологическая;
- организационно-управленческая;
- правоохранительная.

Информационно-аналитические системы безопасности (ИАБС 090305)

Специализации:

1. Автоматизация информационно-аналитической деятельности.
2. Информационная безопасность финансовых и экономических структур.
3. Технологии информационно-аналитического мониторинга.

ИА СБ 090305

Дисциплина: Криптографические методы ЗИ

Знать	Уметь	Владеть
- принципы построения и основные виды симметричных и асимметричных криптографических алгоритмов; - математические модели шифров; - криптографические стандарты; - базовые криптографические протоколы и основные требования к ним;		
- способностью разрабатывать защитные механизмы и средства обеспечения информационной безопасности (ПК-30);		

ИБ автоматизированных систем (ИБ АС) 090303

Объекты профессиональной деятельности:

- автоматизированные системы;

-информационные технологии;

- технологии обеспечения ИБ АС;

- системы управления ИБ АС.

Виды профессиональной деятельности:

- научно-исследовательская;

- проектно-конструкторская;

- контрольно-аналитическая;

- организационно-управленческая;

- эксплуатационная.

ИБ АС 090303

Специализации:

1. АИС специального назначения;
2. Высокопроизводительные вычислительные системы специального назначения;
3. ИБ АС критически важных объектов;
4. Безопасность открытых ИС;
5. ИБ автоматизированных банковских систем;
6. Защищенные автоматизированные системы управления;
7. Обеспечение ИБ распределенных ИС;
8. Анализ безопасности ИС;
9. Создание АС в защищенном исполнении.
10. ИБ АС на транспорте .

ИБ АС 090303

Дисциплина: Криптографические методы ЗИ

Знать	Уметь	Владеть
- основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения безопасности в компьютерных сетях;	- эффективно использовать криптографические методы и средства защиты информации в автоматизированных системах; - применять математические методы исследования моделей шифров;	- криптографической терминологией; - навыками использования типовых криптографических алгоритмов; - навыками использования ЭВМ в анализе простейших шифров; - навыками математического моделирования в криптографии;
- способность участвовать в разработке компонентов автоматизированных систем в сфере профессиональной деятельности (ПК-19); - способность проводить контрольные проверки работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации (ПК-23).		

ИБ АС 090303
Безопасность открытых информационных систем

Дисциплина: Криптографические стандарты и протоколы

Знать	Уметь	Владеть
- основные криптографические протоколы и стандарты; - основные стандарты построения и взаимодействия открытых систем;		
- способностью проводить анализ и исследовать модели защищенности открытых информационных систем (ПСК-4.1); - способностью участвовать в разработке компонентов открытых информационных систем (ПСК-4.2).		

ИБ АС 090303
ИБ автоматизированных банковских систем

Дисциплина: Криптография в банковском деле

Знать	Уметь	Владеть
- основные криптографические протоколы и стандарты, используемые в автоматизированных банковских системах;	- применять на практике стандарты, относящиеся к обеспечению информационной безопасности банковской организации;	
- способность на практике применять криптографические протоколы и стандарты при обеспечении информационной безопасности автоматизированных банковских систем (ПСК-5.3).		

ИБ АС 090303
ИБ автоматизированных банковских систем

Дисциплина: Защита электронного документооборота, Безопасность систем пластиковых карт

Знать	Уметь	Владеть
- методы электронного документооборота в автоматизированных банковских системах; - основные методы обеспечения безопасности пластиковых карт;		
способностью на практике применять криптографические протоколы и стандарты при обеспечении информационной безопасности автоматизированных банковских систем (ПСК-5.3)		

Обеспечение ИБ распределенных ИС

Дисциплина: Организационно-техническое и программное обеспечение удостоверяющего центра

Актуальность:

Развитие PKI-технологий в России по времени совпадает с развитием образования в области обеспечение ИБ. Но вузы выпускают меньшее количество специалистов которые требуются сфере, поэтому ее обеспечением и развитием занимаются специалисты из смежных областей (например IT-специалисты).

Содержание дисциплины

- **Тема 1. Основы обеспечения информационной безопасности с использованием средств криптографической защиты информации (СКЗИ) в удостоверяющем центре (16 часов)**

Информация ограниченного доступа, классификация информации по уровням конфиденциальности (государственная тайна, конфиденциальная информация, персональные данные, общедоступные данные).

Нормативно-правовые документы в области защиты информации (в том числе с использованием СКЗИ), особенности легитимной работы удостоверяющего центра.

Лицензионные требования и условия осуществления деятельности, связанной с СКЗИ для удостоверяющих центров.

Содержание дисциплины

- **Тема 2. Основы криптографической защиты информации. Основные криптографические алгоритмы. (16 часов)**

Основные понятия и определения в области криптографии. Основные современные криптографические методы защиты информации.

Симметричные криптографические алгоритмы (DES, AES, ГОСТ 28147-89). Ассиметричные криптографические алгоритмы, цифровая подпись, хеширование (RSA, DSA, ГОСТ Р 34.10-2001, MD5, SHA1, ГОСТ Р 34.11-94). Сертификат открытого ключа. Программно-аппаратные комплексы удостоверяющих комплексов.

Содержание дисциплины

- **Тема 3. Управление ключами. Инфраструктура открытых ключей. (16 часов)**

Жизненный цикл ключевой информации: создание, передача, проверка, использование, хранение ключей. Компрометация ключей. Время жизни ключей. Управление открытыми ключами. Протоколы X509.

Список отозванных сертификатов, компоненты инфраструктуры открытых ключей, модели инфраструктуры открытых ключей, кросс-сертификат. Примеры инфраструктур, функционирующих в РФ (ФНС, ПФР, ФСС, Росстат, ОГИЦ, электронные торги). Работа с ПО удостоверяющих центров, зарубежными и российскими СКЗИ.

Содержание дисциплины

- **Тема 4. Организационные меры защиты информации с использованием СКЗИ. (12 часов)**

Основные положения (ПКЗ, приказы). Выполнение необходимых требований. Регламентация действий сотрудников. Регламентация работы с ключевыми носителями. Система организационно-распорядительных документов при работе с СКЗИ в удостоверяющем центре.

Содержание дисциплины

- **Тема 5. Практические аспекты безопасного функционирования удостоверяющего центра (12 часов)**

Материально-техническая база удостоверяющего центра. Штат сотрудников удостоверяющего центра. Риски, возникающие при работе удостоверяющего центра, ответственность работников удостоверяющего центра. Меры и особенности проверки клиентов удостоверяющего центра. Организация архивохранилища и резервного копирования информации в удостоверяющем центре.

Материально-техническое обеспечение

Обеспеченность:

1. Квалифицированные кадры;
2. Учебно-методические материалы;
3. Программно-аппаратные комплексы;
4. Возможность проведения дистанционных курсов.

УЦ СИБИРИ

Спасибо за внимание!

Шелупанов
Александр
Александрович
Тел. (3822) 900111
saa@udcs.ru
www.udcs.ru
г. Томск, пр.Ленина 40, оф. 301мк