МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ
«БЕЛГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ им. В.Г.ШУХОВА»
(БГТУ им. В.Г. Шухова)

УТВЕРЖДАЮ
Директор института ЭИТУС

_____А.В. Белоусов

«_____» _____2017 г.

РАБОЧАЯ ПРОГРАММА
дисциплины

Криптографические интерфейсы

Направление подготовки:
10.05.03 Информационная безопасность автоматизированных систем

профиль подготовки:

Обеспечение информационной безопасности распределенных информационных систем

Квалификация (степень)
специалист

Форма обучения
очная

Институт энергетики, информационных технологий и управляющих систем

Кафедра программного обеспечения вычислительной техники и автоматизированных систем

Белгород – 2017

Рабочая программа составлена на основании требований:

- Федерального государственного образовательного стандарта высшего образования по специальности 10.05.03 «Информационная безопасность автоматизированных систем», утверждённого приказом Министерства образования и науки Российской Федерации от 01 декабря 2016 г. № 1509
- плана учебного процесса БГТУ им. В. Г. Шухова по специальности 10.05.03 «Информационная безопасность автоматизированных систем», специализация 10.05.03-07 «Обеспечение информационной безопасности распределённых информационных систем», введённого в действие в 2017 году

Составитель: _____ (А.В. Смакаев)
(ученая степень и звание, подпись) (инициалы, фамилия)

Рабочая программа согласована с выпускающей кафедрой
Программного обеспечения вычислительной техники и автоматизированных систем

Заведующий кафедрой: к.т.н., доцент _____ (В. М. Поляков)
(ученая степень и звание, подпись) (инициалы, фамилия)

« ____ » _____ 2017 г.

Рабочая программа обсуждена на заседании кафедры
Программного обеспечения вычислительной техники и автоматизированных систем

« ____ » _____ 2017 г., протокол № _____

Заведующий кафедрой: к.т.н., доцент _____ (В. М. Поляков)
(ученая степень и звание, подпись) (инициалы, фамилия)

Рабочая программа одобрена методической комиссией института
Энергетики, информационных технологий и управляющих систем

«____ » _____ 2017 г., протокол № _____

Председатель: к.т.н., доцент _____ (А.Н. Семернин)
(ученая степень и звание, подпись) (инициалы, фамилия)

1.ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Формируемые компетенции			Требования к результатам обучения
№	Код компетен-ции	Компетенция	
Профессиональные			
1	ПК-13	Способностью участвовать в проектировании средств защиты информации автоматизированной системы	В результате освоения дисциплины обучающийся должен **Знать:** – принципы работы криптографических интерфейсов в операционных системах семейства Windows; – основные технические характеристики и показатели быстродействия включённых в состав ЭВМ устройств; **Уметь:** – разрабатывать программное обеспечение с использованием криптографических интерфейсов для обеспечения защиты информационных ресурсов; – реализовывать криптографические алгоритмы в рамках криптопровайдеров Microsoft CNG; **Владеть:** – навыками работы с Microsoft CryptoAPI и CNG.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Содержание дисциплины основывается и является логическим продолжением следующих дисциплин:

№	Наименование дисциплины (модуля)
1	Математические основы криптографии
2	Криптографические методы защиты информации

Содержание дисциплины служит основой для изучения следующих дисциплин:

№	Наименование дисциплины (модуля)
1	Технология построения защищенных распределенных приложений

3. ОБЪЁМ ДИСЦИПЛИНЫ

Общая трудоёмкость дисциплины составляет 4 зачётных единицы, 144 часа

Вид учебной работы	Всего часов	Семестр № 7
Общая трудоёмкость дисциплины, час	144	144
Контактная работа (аудиторные занятия), в т.ч.:	54	54
лекции	18	18
лабораторные	36	36
практические	–	–
Самостоятельная работа студентов, в том числе:	90	90
Курсовой проект	–	–
Курсовая работа	27	27
Расчетно-графическое задание	–	–
Индивидуальное домашнее задание	–	–
Другие виды самостоятельной работы	63	63
Форма промежуточной аттестации (зачёт, экзамен)	*дифф. зачёт*	*дифф. зачёт*

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1. Наименование тем, их содержание и объём

Курс 3 Семестр №5

№ п/п	Наименование раздела (краткое содержание)	Объём на тематический раздел по видам учебной нагрузки, час			
		Лекции	Практические занятия	Лабораторные занятия	Самостоятельная работа
1.	Использование Microsoft CryptoAPI и CNG. Структура и интерфейсы CNG				
	Исторические этапы развития криптографических интерфейсов. Знакомство с общим устройством Microsoft CryptoAPI и CNG.	6	–	24	54
2.	Основы разработки криптопровайдеров средствами Microsoft Cryptographic Provider Development Kit				
	Знакомство с документацией Microsoft CryptoAPI и CNG. Изучение основных криптографических интерфейсов Microsoft CNG.	4	–	4	12
3.	Реализации криптографических алгоритмов в рамках криптопровайдера				
	Симметричное шифрование файлов с имитовставкой. Инфраструктура открытых ключей. Протокол обмена ключами Диффи-Хеллмана	4	–	4	12
4.	Знакомство с криптографическими библиотеками различных языков программирования				
	Основные криптографические интерфейсы популярных языков программирования. Java Crypto Interface. Pycrypto. C# Cryptography API	4	–	4	12
	ВСЕГО	18		36	90

4.2. Содержание лабораторных занятий

№ п/п	Наименование раздела дисциплины	Тема лабораторного занятия	Кол-во лаб. часов
семестр №7			
1	Знакомство с CNG. Симметричное шифрование	Ознакомление с криптографическим API операционных систем семейства Windows. Разработка консольного приложения, использующего CNG для генерации ключа и шифрования/расшифрования файлов. Исследование лавинного эффекта при разных режимах сцепления блоков.	6
2	Гибридное шифрование с использованием CNG	Ознакомление с принципами гибридного шифрования, изучение возможностей криптографического API операционных систем семейства Windows. Разработка консольного приложения с использованием CNG для симметричного и асимметричного шифрования,	6

		реализующего простейшую схему гибридного шифрования.	
3	Симметричное шифрование файлов с имитовставкой	Знакомство с принципами работы шифрования с имитовставкой. Разработка консольного приложения, использующего алгоритм HMAC для генерации имитовставки и осуществляющего шифрование и дешифрование файла с подтверждением целостности данных.	6
4	Протоколы обмена ключами	Знакомство с протоколами обмена ключами. Разработка консольного приложения, осуществляющего выработку общего ключа по протоколу Диффи-Хеллмана для симметричного шифрования и расшифрования с использованием алгоритма AES.	4
5	Объединение блочных шифров	Знакомство с принципами объединения блочных шифров и алгоритмом 3DES. Разработка консольного приложения, использующего для шифрования и расшифрования алгоритм 3DES.	6
6	Работа с инфраструктурой открытых ключей	Знакомство с принципами работы инфраструктуры открытых ключей, методами хранения ключей и форматом сертификатов X.509. Разработка консольного приложения, работающего со встроенным в операционную систему хранилищем сертификатов.	4
7	Цифровая подпись	Знакомство с принципами работы и алгоритмами, используемыми для создания электронно-цифровой подписи. Разработка консольного приложения, позволяющего сгенерировать и проверить цифровую подпись для файла.	4
		ИТОГО:	36

5. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ, ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ИТОГАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

5.1. Перечень контрольных вопросов (типовых заданий)

№ п/п	Наименование раздела дисциплины	Содержание вопросов (типовых заданий)
1	Использование Microsoft CryptoAPI и CNG. Структура и интерфейсы CNG	Криптографические интерфейсы. Назначение криптографических интерфейсов. Примеры криптографических АПИ. Структура CNG. Криптопровайдеры. Отличия от Crypto API. Гибридное шифрование. Принцип работы. Преимущества и недостатки. Примеры схем.
2	Основы разработки криптопровайдеров средствами Microsoft	Использование CNG. Порядок получения хэш-суммы. Порядок выполнения симметричного шифрования. Порядок выполнения асимметричного шифрования. Порядок создания ЭЦП. Обмен ключами.

	Cryptographic Provider Development Kit	
3	Реализации криптографических алгоритмов в рамках криптопровайдера	Имитовставки. Использование имитовставок при шифровании. Способы генерации модификатора ключа. Протоколы обмена ключами. Примеры. Протокол Диффи-Хэллмана. Алгоритмы распределения ключей с использованием третьей доверенной стороны. Инфраструткура открытых ключей. Принципы работы. Преимущества и недостатки. Возможные уязвимости. Цепочки сертификатов. Структура сертификата X.509. Форматы хранения сертификатов. Нотация ASN.1.
4	Знакомство с криптографическими библиотеками различных языков программирования	Объединение блочных шифров. Принцип работы. Преимущества и недостатки. Примеры схем. Цифровая подпись. Принцип работы. Подпись на основе алгоритма RSA. DSA.

5.2. Перечень тем курсовых проектов, курсовых работ, их краткое содержание и объём.

Учебным планом предусмотрена курсовая работа, на выполнение которой отведено 27 часов самостоятельной работы студента.

Тема курсовой работы: использование криптографических интерфейсов для обеспечения безопасности хранения и передачи информации.

Цель работы: закрепить практические навыки работы с криптографическими интерфейсами и теоретические знания о криптографических средствах защиты информации.

Типовые задания для курсовых работ:

1. Моделирование атаки "Человек посередине" (Man-in-the-middle).
2. Реализация протокола "Держась за руки" (Interlock protocol).
3. Обмен ключами с использованием цифровых подписей.
4. Реализация протокола Yahalom.
5. Реализация схемы разделения секрета Блэкли 3,m.
6. Честное подбрасывание монеты на основные цифровых подписей.
7. Реализация центра выдачи сертификатов.

5.3. Перечень индивидуальных домашних заданий, расчетно-графических заданий.

Индивидуальных домашних заданий и расчетно-графических заданий по дисциплине «Криптографические интерфейсы» учебным планом не предусмотрено.

5.4. Перечень контрольных работ

Контрольные работы по дисциплине «Криптографические интерфейсы» учебным планом не предусмотрены.

6. ОСНОВНАЯ И ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА

6.1. Перечень основной литературы

1. Рябко Б.Я. Криптографические методы защиты информации [Электронный ресурс]: учебное пособие/ Рябко Б.Я., Фионов А.Н. - Электрон. текстовые данные. - М.: Горячая линия - Телеком, 2012. - 229 с. - Режим доступа: http://www.iprbookshop.ru/11994. - ЭБС «IPRbooks», по паролю

2. Прикладная криптография. Использование и синтез криптографических интерфейсов / А. Ю. Щербаков, А. В. Домашев. - М. : Русская редакция, 2003. - 404 с. - ISBN 5-7502-0215-1

3. Криптографические методы защиты информации / С. Б. Гашков, С. Б. Применко, М. А. Черепнев. - М. : Академия, 2010. - 298 с. - ISBN 978-5-7695-4962-5

4. Криптографические протоколы. Основные свойства уязвимости / А. В. Черемушкин. - М. : Академия, 2009. - 272 с. - ISBN 978-5-7695-5748-4

5. Варенков С.С. Криптографические интерфейсы: методические указания к выполнению лабораторных работ для студентов специальности 100503 – Информационная безопасность автоматизированных систем / сост.: С.С. Варенков. – Белгород: Изд-во БГТУ, 2015. – 26 с.

6.2. Перечень дополнительной литературы

1. Криптографические интерфейсы и их использование / П. Б. Хорев. - М. : Горячая линия - Телеком, 2007. - 278 с. - ISBN 978-5-93517-331-9

6.3. Перечень интернет ресурсов

1. Cryptography Reference - https://msdn.microsoft.com/en-us/library/aa380256.aspx

2. Cryptography API: Next Generation - https://msdn.microsoft.com/ru-ru/library/windows/desktop/aa376210(v=vs.85).aspx

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ

Для проведения лекционных занятий требуется аудитория с доской (ГК426, ГК 430), комплектом пишущих маркеров для досок, компьютером и проектором.

Для проведения лабораторных занятий необходим компьютерный зал, в котором имеется следующее программное обеспечение:

1. Microsoft Visual Studio версии не ниже 2010,
2. Microsoft Cryptographic Provider Development Kit

7.УТВЕРЖДЕНИЕ РАБОЧЕЙ ПРОГРАММЫ

8.1. Утверждение рабочей программы без изменений

Рабочая программа и ГРС без изменений утверждена на 201_/201_ учебный год.

Протокол № _____ заседания кафедры от «___»_____ 201_г.

Заведующий кафедрой_____

подпись, ФИО

Директор института _____

подпись, ФИО

(или)

8.2. Утверждение рабочей программы и ГРС с изменениями, дополнениями

Рабочая программа и ГРС с изменениями, дополнениями утверждена на 201_/201_ учебный год.

Протокол № _____ заседания кафедры от «___»_____ 201_ г.

Заведующий кафедрой_____

подпись, ФИО

Директор института _____

подпись, ФИО

ПРИЛОЖЕНИЯ

Приложение №1. Методические указания для обучающегося по освоению дисциплины.

Дисциплина «Криптографические интерфейсы» входит в базовый блок учебного плана специальности 10.05.03 «Информационная безопасность автоматизированных систем». Для успешного освоения курса требуются знания математики криптографии и криптографичских средств защиты информации.

Целью курса является изучение криптографических интерфейсов операционных систем семейства Microsoft Windows. На лекционных занятиях детально рассматривается устройство и использование криптографического интерфейса Microsoft CNG. На лабораторных занятиях обучающиеся реализуют консольные приложения для шифрования с использованием симметричных и ассиметричных алгоритмов, обмена ключами, работы с PKI. Также рассматриваются вопросы использования криптографических интерфейсов популярных языков программирования (Java, Python, C#).

Методические указания к выполнению лабораторных работ даны в пособии:

Варенков С.С. Криптографические интерфейсы: методические указания к выполнению лабораторных работ для студентов специальности 100503 – Информационная безопасность автоматизированных систем / сост.: С.С. Варенков. – Белгород: Изд-во БГТУ, 2015. – 26 с.

Для выполнения лабораторных и самостоятельных работ обучающийся использует лекционный материал, а также литературу, перечисленную в списке основной литературы пункта 6.1.

Учебный план предусматривает проведение лабораторных и лекционных занятий, выполнение курсовой работы. Защита лабораторных работ проходит в виде проверки правильности выполнения задания и беседы с преподавателем. Итоговый контроль знаний осуществляется в форме зачёта с оценкой.

Основной целью курса является выработка у обучающихся навыков работы с различными криптографическими интерфейсами для проектирования и реализации средств защиты информации автоматизированных систем.