МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

ПЕНЗЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ЮРИДИЧЕСКИЙ ФАКУЛЬТЕТ

УТВЕРЖДАЮ
Декан факультета
_____ В.В.Гошуляк
«10» апреля 2017 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

С1.1.9 Основы информационной безопасности в деятельности правоохранительных органов

Специальность 40.05.02 Правоохранительная деятельность

Специализация Административная деятельность

Квалификация выпускника – юрист

Форма обучения очная, заочная

Пенза, 2016 г.

1. Цели освоения дисциплины

Целями освоения дисциплины «Основы информационной безопасности в деятельности правоохранительных органов» является формирование теоретических знаний о методах и средствах, применяемых для обеспечения безопасности информации, нормативных правовых документах в области информационной безопасности, особенностях расследований преступлений в сфере информационных технологий, а также навыков применения методов и средств защиты информации.

2. Место дисциплины в структуре ООП специалитета

Дисциплина относится к базовому блоку дисциплин, обеспечивающих подготовку специалистов по специальности 40.05.02 «Правоохранительная деятельность». Изучение дисциплины базируется на следующих дисциплинах, формирующих определенные знания, умения и навыки: Гражданское право, Налоговое право, Уголовное право, Уголовно-процессуальное право, Криминалистика, Правоохранительные органы, Военная подготовка (специальная подготовка), Административная деятельность правоохранительных органов, Государственная служба в правоохранительных органах, Преступления против личности, Преступления в сфере экономики, Семейное право, Трудовое право, Информатика и информационные технологии в профессиональной деятельности, Информационно-правовая статистика, Правовые системы «Гарант», «Консультант+».

Основные положения дисциплины «Основы информационной безопасности в деятельности правоохранительных органов» используются в следующих дисциплинах: Основы оперативно-розыскной деятельности, Теория доказательств, Актуальные проблемы уголовного права, Предупреждение преступлений и административных правонарушений правоохранительными органами.

Также основные положения дисциплины могут быть использованы при прохождении практики по получению профессиональных умений и опыта профессиональной деятельности, преддипломной практики, подготовке к государственному экзамену, подготовке и защите выпускной квалификационной работы.

3. Компетенции обучающегося, формируемые в результате освоения дисциплины «Основы информационной безопасности в деятельности правоохранительных органов» (С1.1.9)

Процесс изучения дисциплины «Основы информационной безопасности в деятельности правоохранительных органов» направлен на формирование элементов следующих компетенций в соответствии с ФГОС ВО по специальности 40.05.02 «Правоохранительная деятельность»:

Коды компетенции	Наименование компетенции	Структурные элементы компетенции (в результате освоения дисциплины обучающийся должен знать, уметь, владеть)
1	2	3
ПК-4	способность квалифицированно применять нормативные правовые акты в конкретных сферах юридической деятельности	Знать: основные методы и средства хранения, поиска, систематизации, обработки передачи и защиты компьютерной информации; нормативные правовые акты в области защиты информации и противодействия иностранным техническим разведкам; основные методы, способы и мероприятия по обеспечению информационной безопасности в профессиональной деятельности.
		Уметь: работать в локальной и глобальной компьютерных сетях; самообучаться в современных компьютерных средах; использовать методы и средства обеспечения информационной безопасности с целью предотвращения

		несанкционированного доступа, злоумышленной модификации или утраты информации, составляющей государственную тайну и иной служебной информации.
		Владеть: навыками компьютерной обработки служебной документации; навыками обеспечения защиты информации, составляющей государственную тайну и иной служебной информации, с использованием положений нормативных правовых актов в области защиты информации.
ПК-16	способность реализовывать мероприятия по получению юридически значимой информации, проверять, анализировать, оценивать ее и использовать в интересах предупреждения, пресечения, раскрытия и расследования преступлений	Знать: основные нормативные правовые документы в области защиты информации, устанавливающие квалификацию преступлений в сфере информационных технологий и ответственность за совершение преступлений; особенности расследования преступлений в сфере информационных технологий.
		Уметь: квалифицировать преступления в сфере информационных технологий; определять мероприятия, которые могут применяться для сбора юридически значимой информации, при расследовании преступлений в сфере информационных технологий.
		Владеть: терминологией, используемой в нормативных правовых документах в области защиты информации, устанавливающих квалификацию преступлений в сфере информационных технологий; навыками применения методов и средств, используемых для сбора информации, необходимой при расследовании преступлений в сфере информационных технологий.

4. Структура и содержание дисциплины Основы информационной безопасности в деятельности правоохранительных органов

4.1. Структура дисциплины, очники

Общая трудоемкость дисциплины составляет 3 зачетных единицы, 108 часов.

№ п/п	Наименование разделов и тем дисциплины	Семестр	Недели семестра	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)						Формы текущего контроля успеваемости *(по неделям семестра)*		
				Аудиторная работа			Самостоятельная работа					
				Всего	Лекция	Практические занятия	Всего	Подготовка к тестированию по темам лекций, практических занятий	Подготовка отчетов о выполнении практических заданий	Тестирование по темам лекций	Тестирование по темам практических занятий	Проверка отчетов о выполнении практических занятий
1.	Раздел 1. Основные термины и определения в области ИБ	9	1-4	4	4		6	6		4		
1.1.	Тема 1.1 Общая проблема информационной безопасности информационных систем	9	1-2	2	2		3	3		4		
1.2.	Тема 1.2 Основные угрозы ИБ. Методы и способы реализации угроз	9	3-4	2	2		3	3		4		
2	Раздел 2. Организационно-правовые основы ИБ	9	5-8	10	4	6	12	6	6	8		
2.1	Тема 2.1 Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства	9	5-6	2	2		3	3		8		
2.2	Тема 2.2 Правовое обеспечение ИБ в РФ	9	7-8	8	2	6	9	3	6	8		
3	Раздел 3. Методы и средства защиты в вычислительных системах	9	9-14	34	6	28	40	9	28	14		
3.1	Тема 3.1 Идентификация и аутентификация. Управление доступом	9	9-10	4	2	2	5	3	2	14	9	9

3.2	Тема 3.2 Криптографические методы и средства защиты. Средства антивирусной защиты	9	11-12	14	2	12	15	3	12	14	9	
3.3	Тема 3.3 Защитные механизмы операционных систем. Методы и средства защиты в локальных и глобальных компьютерных сетях	9	13-14	16	2	14	17	3	14	14	15	15
4	Раздел 4. Расследование преступлений в сфере ИТ	9	15-18	3	3		2	2		18		
4.1	Тема 4.1. Преступления в сфере ИТ. Ответственность за преступления в сфере ИТ	9	15-16	1	1		1	1		18		
4.2	Тема 4.2. Особенности проведения расследования преступлений в сфере ИТ	9	17	2	2		1	1		18		
	Общая трудоемкость, в часах	9	1-17	51	17	34	57	23	34	Промежуточная аттестация		
										Форма	Семестр	
										Зачет	9	
										Экзамен	–	

4.2. Структура дисциплины, заочники

№ п/п	Наименование разделов и тем дисциплины	Семестр	Недели семестра	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)						Формы текущего контроля успеваемости (по неделям семестра)	
				Аудиторная работа			Самостоятельная работа				
				Всего	Лекция	Практические занятия	Всего	Подготовка к аудиторным занятиям	Контрольная работа	Проверка тестов	Проверка контрольных работ
1.	Тема 1. Общая проблема информационной безопасности информационных систем. Угрозы ИБ	9		2	2		32	16	16	16	16
1.1.	Тема 2. Организационно-правовые основы ИБ	9		2	2		32	16	16	16	16
1.2.	Тема 3. Методы и средства защиты в вычислительных системах	9		8	2	6	32	16	16	16	16
	Общая трудоемкость, в часах	9		12	6	6	96	48	48	Промежуточная аттестация	
										Форма	Семестр
										Зачет	9
										Экзамен	–

4.3. Содержание дисциплины Основы информационной безопасности в деятельности правоохранительных органов, очники

№ п/п	Наименование раздела дисциплины	Содержание раздела
1	Раздел 1. Основные термины и определения в области ИБ	
1.1	Тема 1.1 Общая проблема информационной безопасности информационных систем	Виды информации: правовое определение информации; защищаемая информация Понятие информационной безопасности применительно к информационным системам. Понятия угрозы, уязвимости, источника угрозы, нападения.
1.2	Тема 1.2 Классификация угроз ИБ. Методы и способы реализации угроз	Классификация угроз ИБ. Виды классификации. Классификация нарушителей ИБ. Виды классификации Модель нарушителя. Основные методы реализации угроз. Типовой сценарий реализации угроз
2	Раздел 2. Организационно-правовые основы ИБ	
2.1	Тема 2.1 Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства	Доктрина информационной безопасности РФ: основные положения; государственная политика обеспечения информационной безопасности Российской Федерации: основные принципы, функции государства. ФЗ О безопасности.
2.2	Тема 2.2 Правовое обеспечение ИБ в РФ	Нормативные правовые документы в области ИБ. Основные положения Федеральных законов РФ в области ИБ. ФЗ Об информации, информационных технологиях и защите информации. ФЗ О персональных данных. ФЗ Об электронной подписи. ФЗ О государственной тайне
3	Раздел 3. Методы и средства защиты в вычислительных системах	
3.1	Тема 3.1 Идентификация и аутентификация	Определение процедур идентификации и аутентификации. Виды идентификации и аутентификации. Методы и средства реализации. Способы управления доступом. Реализация способов управления доступом
3.2	Тема 3.2 Криптографические методы и средства защиты. Средства антивирусной защиты	Термины и определения. Симметричные и асимметричные криптографические системы. Основные характеристики используемых в настоящее время алгоритмов шифрования. Электронная подпись. Компьютерные вирусы: определение и классификация. Методы защиты от вирусов. Средства антивирусной защиты
3.3	Тема 3.3 Защитные механизмы операционных систем. Методы и средства защиты в локальных и глобальных компьютерных сетях	Модели безопасности операционных систем (ОС). Защитные механизмы, реализованные в ОС Windows. Особенности обеспечения ИБ при использовании сетей передачи данных общего пользования. Основные угрозы ИБ и защита информации в сетях.

№ п/п	Наименование раздела дисциплины	Содержание раздела
4	Раздел 4. Расследование преступлений в сфере ИТ	
4.1	Тема 4.1. Преступления в сфере ИТ. Ответственность за преступления в сфере ИТ	Определение компьютерных преступлений. Структура компьютерных преступлений. Виды компьютерных преступлений. Виды ответственности за преступления в сфере ИТ. Нормативные правовые документы, устанавливающие ответственность за преступления в сфере ИТ
4.2	Тема 4.2. Особенности проведения расследования преступлений в сфере ИТ	Стадии совершения умышленного компьютерного преступления. Этапы расследования компьютерных преступлений. Лица, осуществляющие расследование. Действия лиц, осуществляющих расследование, на каждом этапе. Обнаружение компьютерных преступлений.

4.3. Содержание дисциплины Основы информационной безопасности в деятельности правоохранительных органов, заочники

№ п/п	Наименование раздела дисциплины	Содержание раздела
1.	Тема 1. Общая проблема информационной безопасности информационных систем. Угрозы ИБ	Виды информации: правовое определение информации; защищаемая информация Понятие информационной безопасности применительно к информационным системам. Понятия угрозы, уязвимости, источника угрозы, нападения. Классификация угроз ИБ. Виды классификации. Классификация нарушителей ИБ. Виды классификации Модель нарушителя. Основные методы реализации угроз. Типовой сценарий реализации угроз
1.2	Тема 2 Организационно-правовые основы ИБ.	Доктрина информационной безопасности РФ: основные положения; государственная политика обеспечения информационной безопасности Российской Федерации: основные принципы, функции государства. ФЗ О безопасности. Нормативные правовые документы в области ИБ. Основные положения Федеральных законов РФ в области ИБ. ФЗ Об информации, информационных технологиях и защите информации. ФЗ О персональных данных. ФЗ Об электронной подписи. ФЗ О государственной тайне
3	Тема 3. Методы и средства защиты в вычислительных системах	Определение процедур идентификации и аутентификации. Виды идентификации и аутентификации. Методы и средства реализации. Способы управления доступом. Реализация способов управления доступом. Термины и определения. Симметричные и асимметричные криптографические системы. Основные характеристики используемых в настоящее время алгоритмов шифрования. Электронная подпись. Компьютерные вирусы: определение и классификация. Методы защиты от вирусов. Средства антивирусной защиты. Модели безопасности операционных систем (ОС). Защитные механизмы, реализованные в ОС Windows. Особенности обеспечения ИБ при использовании сетей передачи данных общего пользования. Основные угрозы ИБ и защита информации в сетях.

Перечень практических занятий, очники

№ п/п	Наименование темы	Раздел дисциплины	Количество часов
1	Реализация методов идентификации и аутентификации в компьютерных сетях	3	2
2	Реализация методов криптографической защиты информации при ее передаче	3	4
3	Применение электронной подписи для обеспечения целостности передаваемой информации	3	2
4	Применение электронной подписи для обеспечения неотказуемости при передаче информации	3	4
5	Реализация криптографических протоколов для идентификации и аутентификации в компьютерных сетях	3	2
6	Реализация методов идентификации и аутентификации в ОС Windows	3	4
7	Реализация методов управления доступом к защищаемым ресурсам в ОС Windows	3	4
8	Применение механизма аудита событий безопасности ОС Windows для выявления нарушений	3	2
9	Реализация процедур идентификации и аутентификации ОС Windows для удаленного доступа к ресурсам локальной сети	3	2
10	Методы и средства антивирусной защиты	3	2
11	Организационно-правовые основы ИБ	2	6

Перечень практических занятий, заочники

№ п/п	Наименование темы	Раздел дисциплины	Количество часов
1	Реализация методов идентификации и аутентификации в компьютерных сетях	3	2
2	Реализация методов криптографической защиты информации при ее передаче	3	4

5. Образовательные технологии

В соответствии с требованиями ФГОС ВО по специальности 40.05.02 «Правоохранительная деятельность» и для реализации компетентностного подхода при изучении дисциплины предусматривается использование в учебном процессе активных и интерактивных форм проведения занятий.

Основными образовательными технологиями при освоении дисциплины являются лекции и практические занятия. Данные виды образовательных технологий относятся к аудиторной работе.

При изучении дисциплины предусматривается использование интерактивных методов и технологий формирования компетенций у студентов:

- лекций с применением мультимедийных технологий (очники – 18 часов, заочники - – 6 часов);

- использование на практических занятиях работу индивидуально и в малых группах (очники – 18 часов, заочники - – 6 часов).

В целях реализации индивидуального подхода к обучению студентов, осуществляющих учебный процесс по собственной траектории в рамках индивидуального

рабочего плана, изучение данной дисциплины базируется на следующих возможностях: обеспечение внеаудиторной работы со студентами, в том числе в электронной образовательной среде с использованием соответствующего программного оборудования, дистанционных форм обучения, возможностей интернет-ресурсов, индивидуальных консультаций и т.д.

6. Учебно-методическое обеспечение самостоятельной работы студентов. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины.

Основным оценочным средством промежуточной аттестации по итогам освоения дисциплины является зачет.

Зачетные вопросы и задания ежегодно обновляются ведущим преподавателем, обсуждаются на методических семинарах (заседаниях кафедры) и утверждаются зав. кафедрой.

Контроль усвоения знаний, формирования умений и навыков студентов осуществляется при письменном и компьютерном тестировании в процессе текущей аттестации в форме двух контрольных точек.

6.1. План самостоятельной работы студентов, очники

№ нед.	Тема	Вид самостоятельной работы	Задание	Рекомендуемая литература	Количество часов
1-4	Раздел 1. Основные термины и определения в области ИБ	Подготовка к тестированию по темам лекций	Изучение материала лекции и изучение основной и дополнительной литературы, а также материалов, размещенных на указанных Интернет-ресурсах	См. раздел 7 РПУД	8
5-8	Раздел 2. Организационно-правовые основы ИБ	Подготовка к тестированию по темам лекций, практических занятий, подготовка отчетов о выполнении практических заданий	Изучение материала лекции и изучение основной и дополнительной литературы, а также материалов, размещенных на указанных Интернет-ресурсах	См. раздел 7 РПУД	8
9-14	Раздел 3. Методы и средства защиты	Подготовка к тестированию по темам	Изучение материала лекции и изучение основной	См. раздел 7 РПУД	48

	в вычислительных системах	лекций, практических занятий, подготовка отчетов о выполнении практических заданий	и дополнительной литературы, а также материалов, размещенных на указанных Интернет-ресурсах		
15-18	Раздел 4. Расследование преступлений в сфере ИТ	Подготовка к тестированию по темам лекций	Изучение материала лекции и изучение основной и дополнительной литературы, а также материалов, размещенных на указанных Интернет-ресурсах	См. раздел 7 РПУД	8

6.2. План самостоятельной работы студентов, заочники

№ нед.	Тема	Вид самостоятельной работы	Задание	Рекомендуемая литература	Количество часов
16	Общая проблема информационной безопасности информационных систем. Угрозы ИБ	Подготовка к аудиторным занятиям, контрольная работа	Изучение материала лекции и изучение основной и дополнительной литературы, а также материалов, размещенных на указанных Интернет-ресурсах	См. раздел 7 РПУД	32
16	Организационно-правовые основы ИБ	Подготовка к аудиторным занятиям, контрольная работа	Изучение материала лекции и изучение основной и дополнительной литературы, а также материалов, размещенных на указанных Интернет-ресурсах	См. раздел 7 РПУД	32
16	Методы и	Подготовка к	Изучение материала	См. раздел 7	32

	средства защиты в вычислительных системах	аудиторным занятиям, контрольная работа	лекции и изучение основной и дополнительной литературы, а также материалов, размещенных на указанных Интернет-ресурсах	РПУД	

6.3. Методические указания по организации самостоятельной работы студентов

Основными видами самостоятельной работы студентов при освоении данной дисциплины являются: проработка учебного материала по дисциплине (конспектов лекций, учебников, методических пособий и др.) с целью подготовки к лекциям и практическим занятиям и подготовки к контрольному тестированию.

Подготовка к аудиторным занятиям проводится с целью более углубленного изучения материала, тщательной проработки материала, подготовки к контрольному тестированию, а также с целью изучения теоретического материала для подготовки к выполнению заданий на практических занятиях. При подготовке к аудиторным занятиям используется основная и дополнительная литература, а также материалы, размещенные на Интернет-ресурсах, приведенных в разделе 7.

При подготовке к зачету используется материал лекционных занятий, а также используется основная и дополнительная литература, материалы, размещенные на Интернет-ресурсах, приведенных в разделе 7.

Студенты выполняют отчеты о выполнении заданий, указанных в методических указаниях к практическим занятиям и присылают их для проверки по электронной почте преподавателю.

При недоборе минимума баллов по этапу рейтинговой системы студенты очной формы обучения выбирают из РПД тему презентации, разрабатывают презентацию, контрольные вопросы в виде контрольного теста и присылают их для проверки преподавателем по электронной почте. Студенты готовят презентации по выбранным темам, отображая основные их содержательные моменты в виде графических образов. Аналогично организуется работа по формированию тестовых заданий по пройденным темам. Студенты разрабатывают не менее четырех тестовых заданий по каждой теме с тремя-четырьмя вариантами ответов, предварительно ознакомившись с правилами корректного формирования тестов.

При выполнении контрольной работы студенты заочной формы обучения выбирают из РПД тему контрольной работы. По выбранной теме студенты разрабатывают презентацию, а также контрольные вопросы в виде контрольного теста по материалам презентации, и присылают их для проверки преподавателем по электронной почте. Студенты готовят презентации по выбранным темам, отображая основные их содержательные моменты в виде графических образов. Аналогично организуется работа по формированию тестовых заданий по пройденным темам. Студенты разрабатывают не менее четырех тестовых заданий по каждой теме с тремя-четырьмя вариантами ответов, предварительно ознакомившись с правилами корректного формирования тестов.

6.4. Материалы для проведения текущего и промежуточного контроля знаний студентов

Контроль освоения компетенций, очники

№ п\п	Вид контроля	Контролируемые темы (разделы)	Компетенции, компоненты которых контролируются
1	Текущий (тестирование по темам лекций, тестирование по темам практических занятий, проверка отчетов о выполнении практических занятий)	Разделы 1-4	ПК-4, ПК-16
2	Промежуточный (зачет)	Разделы 1-4	ПК-4, ПК-16

Контроль освоения компетенций, заочники

№ п\п	Вид контроля	Контролируемые темы (разделы)	Компетенции, компоненты которых контролируются
1	Текущий (проверка тестов, проверка контрольных работ)	Темы 1-3	ПК-4, ПК-16
2	Промежуточный (зачет)	Темы 1-3	ПК-4, ПК-16

Текущий (рейтинговый) контроль проводится с использованием контрольного тестирования периодически во время лекционный занятий и практических занятий в соответствии с расписанием. Контроль должен охватывать всех студентов. Студенты, не явившиеся на контрольное занятие, проходят текущий контроль во внеурочное время.

Результаты текущего контроля должны оцениваться лектором дифференцированно и учитываться при проведении рубежного рейтингового контроля (контрольных точек) и промежуточной аттестации студентов.

При контрольном тестировании используются один тип вопросов – с единственным правильным ответом из множества вариантов.

Пример тестового вопроса для текущего контроля:

Как называются действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц, в соответствии с ФЗ № 149?

а) рассылка информации

б) разглашение информации

в) передача информации

г) распространение информации

Промежуточный контроль по окончании девятого семестра проводится в виде зачета. На зачет выносится два теоретических вопроса и задание.

Примерный перечень вопросов и заданий к зачету

Формулировка вопроса для проверки уровня обученности ЗНАТЬ

1 Правовое определение информации. Виды информации, определенные нормативными правовыми документами и национальными стандартами

2 Понятие информационной безопасности применительно к информационным системам

3 Термины и определения: угрозы ИБ, уязвимость, источник угрозы, нападение

4 Свойства информации

5 Классификация угроз ИБ

6 Модель угроз ИБ. Причины существования угроз. Уязвимости

7 Классификация нарушителей ИБ

8 Основные методы реализации угроз. Атаки, направленные на реализацию угроз

9 Типовой сценарий реализации угроз

10 Структура и состав законодательства в области ИБ

11 Основные понятия, используемые в Федеральном законе N 149-ФЗ Об информации, информационных технологиях и о защите информации

12 Принципы правового регулирования отношений в сфере информации, информационных технологий и защиты информации

13 Права и обязанности обладателя информации в соответствии с N 149-ФЗ

14 Доступ к информации: права на доступ, ограничение на доступ, распространение информации в соответствии с N 149-ФЗ

15 Информация как объект правовых отношений. Виды информации в соответствии с N 149-ФЗ

16 Основные положения по защите информации в соответствии с N 149-ФЗ

17 Основные понятия, используемые в Федеральном законе N 63-ФЗ Об электронной подписи

18 Принципы использования электронной подписи

19 Виды электронных подписей

20 Условия признания электронных документов, подписанных электронной подписью, равнозначными документам на бумажном носителе, подписанным собственноручной подписью

21 Федеральные органы исполнительной власти в сфере использования электронной подписи и их полномочия

22 Использование простой и усиленных электронных подписей электронной подписи

23 Средства электронной подписи, применяемые для создания и проверки ЭП

24 Положения ФЗ N 63-ФЗ Об электронной подписи, регулирующие работу удостоверяющего центра

25 Основные понятия, используемые в Законе РФ от 21.07.1993№ 5485-1 О государственной тайне

26 Принципы отнесения сведений к государственной тайне в соответствии с Законом РФ от 21.07.1993№ 5485-1 О государственной тайне

27 Сведения, не подлежащие отнесению к государственной тайне и засекречиванию, в соответствии с Законом РФ от 21.07.1993№ 5485-1 О государственной тайне

28 Ограничение прав собственности предприятий, учреждений, организаций и граждан РФ на информацию в связи с ее засекречиванием

29 Система защиты государственной тайны, в соответствии с Законом РФ от 21.07.1993№ 5485-1 О государственной тайне

30 Основные понятия, используемые в Федеральном законе N 152-ФЗ «О персональных данных»

31 Принципы обработки персональных данных в соответствии с Федеральным законом N 152-ФЗ «О персональных данных»
32 Условия обработки персональных данных в соответствии с Федеральным законом N 152-ФЗ «О персональных данных»
33 Согласие субъекта персональных данных на обработку его персональных данных в соответствии с Федеральным законом N 152-ФЗ «О персональных данных»
34 Виды и категории персональных данных в соответствии с Федеральным законом N 152-ФЗ «О персональных данных»
35 Права субъекта персональных данных и обязанности оператора персональных данных в соответствии с Федеральным законом N 152-ФЗ «О персональных данных»
36 Обеспечение безопасности персональных данных в соответствии с Федеральным законом N 152-ФЗ «О персональных данных»

Формулировка вопроса для проверки уровня обученности УМЕТЬ
1 Определить тайну связи в соответствии действующим законодательством РФ
2 Определить виды ответственности за нарушение законодательства РФ в области связи
3 Определить режим служебной тайны и требования к его обеспечению
4 Определить виды ответственности за нарушение режима служебной тайны
5 Определить виды тайн – нотариальную, адвокатскую тайну и тайну страхования, в соответствии действующим законодательством РФ
6 Определить виды тайн – банковскую и налоговую тайны, в соответствии действующим законодательством РФ
7 Определить виды тайн – врачебную и медицинскую тайна, таможенную тайну, коммерческую тайну, в соответствии действующим законодательством РФ
8 Определить виды ответственности за нарушение режима доступа к информации ограниченного доступа (различным видам тайн) в соответствии действующим законодательством РФ
9 Определить преступления, относящиеся к сфере ИТ и ИБ, и структуру преступлений
10 Определить классификацию преступлений, относящихся к сфере ИТ и ИБ
11 Определить преступления в сфере компьютерной информации в соответствии с УК РФ (глава 28)
12 Определить процедуры идентификации, аутентификации и авторизации пользователя, реализуемые ОС Windows
13 Определить процедуру локальной аутентификации ОС Windows
14 Определить протоколы сетевой аутентификации ОС Windows
15 Определить основные типы прав доступа (разрешений и запретов) ОС Windows
16 Определить порядок регистрации событий безопасности ОС Windows: журналы ОС Windows, основные события, типы событий, содержание записей о событии
17 Определить основные угрозы для парольных систем и способы их реализации
18 Определить основные правила выбора стойких паролей
19 Определить основные виды криптографических систем, алгоритмов и используемых преобразований
20 Определить основные нарушения безопасности для систем электронной подписи и атаки, применяемые для их реализации

Формулировка задания/задачи для проверки уровня обученности ВЛАДЕТЬ
1 Обеспечение защиты от перехвата паролей при удаленной аутентификации
2 Управление асимметричной ключевой системой: создание пары ключей, экспорт открытого ключа, проверка свойств ключей.
3 Управление асимметричной ключевой системой: обмен ключами, импорт и подписание ключей, управление технологическими файлами
4 Обеспечение безопасности информации с помощью асимметричных ключевых систем

(шифрование сообщений)
5 Обеспечение целостности информации с помощью асимметричных ключевых систем (формирование электронной подписи)
6 Проверка электронной подписи с помощью асимметричных ключевых систем
7 Взаимодействие с удостоверяющим центром для публикации ключей и обмена ключами
8 Взаимодействие с удостоверяющим центром для проверки подлинности сообщений при обеспечении неотказуемости
9 Настройка парольной подсистемы ОС Windows
10 Настройка применения сложных паролей
11 Настройка управления доступом пользователей к файлам и каталогам
12 Создание учетных записей пользователей и управление учетными записями
13 Создание групп пользователей и объединение пользователей в группы
14 Настройка подсистемы аудита ОС Windows
15 Анализ записей журналов регистрации событий для обнаружения нарушений безопасности
16 Настройка механизма наследования разрешений на доступ к файлам и каталогам в ОС Windows
17 Настройка доступа к журналам регистрации событий и управлению журналами
18 Настройка блокировки компьютера при вводе пользователем неправильного имени и пароля, а также при неактивности пользователя

Темы презентаций для индивидуальных заданий для очников и темы контрольных работ для заочников

1. Доктрина информационной безопасности Российской Федерации: современное состояние и перспективы развития
2. Концепция обеспечения национальной безопасности Российской Федерации
3. Правовое регулирование деятельности средств массовой информации
4. Правовые основы защиты государственной тайны
5. Правовые основы защиты коммерческой тайны
6. Правовое регулирование защиты персональных данных в Российской Федерации
7. Правовая защита авторских и смежных прав в Российской Федерации
8. Информационное право в Российской Федерации: основные нормативно-правовые документы
9. Правовое регулирование защиты банковской и другой финансовой информации
10. Правовой режим служебной тайны
11. Правовой режим адвокатской и нотариальной тайны
12. Правовой режим тайны связи
13. Система правоохранительных органов Российской Федерации
14. Конституционное право в области информации и информационных технологий
15. Основные нормативно-правовые документы, регулирующие деятельность правоохранительных органов
16. Подразделение МВД РФ, осуществляющее деятельность по противодействию компьютерным преступлениям
17. Лицензирование деятельности в области защиты информации
18. Национальные стандарты в области защиты информации
19. Нормативные и методические документы ФСТЭК в области технической защиты информации
20. Правовое регулирование использования электронной подписи
21. Разрушающие программные воздействия. Компьютерные вирусы: определение, классификация, применение

22. Разрушающие программные воздействия. Методы и средства защиты
23. Разрушающие программные воздействия, применяемые в компьютерных сетях общего пользования
24. Виды преступлений с использованием банковских карт. Кардинг
25. Преступления с использованием сети интернет. Фишинг
26. Преступления, совершаемые с использованием мобильной и беспроводной связи
27. Виды ответственности за преступления в сфере информационных технологий
28. Особенности расследования преступлений в сфере информационных технологий
29. Основные технические каналы утечки информации
30. Методы и средства защиты от утечки по техническим каналам
31. Стеганография как метод защиты информации
32. Методы и средства физической защиты. Организация пропускного режима
33. Судебная практика по делам о преступлениях в сфере информационных технологий
34. Правовые основы оперативно-розыскной деятельности
35. Система сертификации средств защиты информации
36. Лицензирование и сертификация при разработке и эксплуатации средств криптографической защиты информации
37. Промышленный шпионаж: методы и средства защиты
38. Организация работы службы безопасности предприятий и организаций
39. Методы и средства обеспечения безопасного межсетевого взаимодействия
40. Управление персоналом и обеспечение информационной безопасности
41. Программно-аппаратные средства защиты информации от несанкционированного доступа
42. Программно-аппаратные средства криптографической защиты информации
43. Криптографическая защита информации. Асимметричные системы
44. Криптографическая защита информации. Симметричные системы
45. Криптографическая защита информации. Электронная подпись и хэш-функция
46. Защищенный электронный документооборот
47. Ответственность за преступления в сфере информационных технологий
48. Объекты информатизации: определение, основные угрозы и методы и средства защиты
49. Методы и средства защиты ПО от неправомерного копирования
50. Методы и средства защиты от рассылки нежелательных сообщений (спама)
51. Основные положения ФЗ «О безопасности». Применение Федерального закона
52. Теория конфликта: основные положения и применение основных положений в информационной безопасности
53. Цензура и ее применение как метода информационного противоборства
54. Агитация как метод воздействия: формы и используемые средства
55. Теория игр и теория принятия решений, их применение в информационной безопасности
56. Судебная система РФ, проблемы обеспечения информационной безопасности в деятельности судов
57. Модели угроз и нарушителей информационной безопасности: виды моделей, построение и применение
58. Механизмы безопасности, реализованные в ОС на основе Linux
59. Биометрическая аутентификация: виды аутентификации, биометрические характеристики личности
60. Использование отпечатков пальцев для идентификации личности. Дактилоскопия

61. Криптографические протоколы, используемые в сети Интернет
62. Международные правовые документы, регулирующие обеспечение информационной безопасности
63. Правовые основы защиты врачебной и медицинской тайны
64. Виды тайн, относящихся к деятельности судов (тайна совещания судей, совещания присяжных заседателей и др.)
65. Виды тайн, относящихся к деятельности правоохранительных органов (тайна предварительного следствия, дактилоскопическая тайна др.)

7. Учебно-методическое и информационное обеспечение дисциплины Основы информационной безопасности в деятельности правоохранительных органов

а) основная литература:

1. Шаньгин, В.Ф. Информационная безопасность [Электронный ресурс] : учеб. пособие — Электрон. дан. — Москва : ДМК Пресс, 2014. — 702 с. — Режим доступа: https://e.lanbook.com/book/50578. — Загл. с экрана.
2. Семь безопасных информационных технологий [Электронный ресурс] : учеб. / А.В. Барабанов [и др.]. — Электрон. дан. — Москва : ДМК Пресс, 2017. — 224 с. — Режим доступа: https://e.lanbook.com/book/97352. — Загл. с экрана.
3. Калмыков И.А. Компьютерная криминалистика [Электронный ресурс]: Лабораторный практикум/ Калмыков И.А., Пелешенко В.С.— Электрон. текстовые данные.— Ставрополь: Северо-Кавказский федеральный университет, 2017.— 84 с.— Режим доступа: http://www.bibliocomplectator.ru/book/?id=69392, – «БИБЛИОКОМПЛЕКТАТОР», по паролю.

б)дополнительная литература:

4. Боер В. М., Павельева О. Г. Информационное право [Электронный ресурс]: учеб. пособие. Ч. 1 / В. М. Боер, О. Г. Павельева; ГУАП. — Электрон. дан. — СПб., 2006. — 116 с. Режим доступа: http://window.edu.ru/catalog/pdf2txt/004/45004/21782. — Загл. с экрана.
5. Шаньгин, В.Ф. Защита компьютерной информации [Электронный ресурс] : учеб. пособие — Электрон. дан. — Москва : ДМК Пресс, 2010. — 544 с. — Режим доступа: https://e.lanbook.com/book/1122. — Загл. с экрана.
6. Климентьев, К.Е. Компьютерные вирусы и антивирусы: взгляд программиста [Электронный ресурс] — Электрон. дан. — Москва : ДМК Пресс, 2013. — 656 с. — Режим доступа: https://e.lanbook.com/book/63192. — Загл. с экрана.
7. Конституция Российской Федерации. - 1993 г.
8. Концепция национальной безопасности Российской Федерации (в редакции Указа Президента РФ от 10 января 2000 года № 24).
9. Доктрина информационной безопасности Российской Федерации (утв. Президентом РФ 9 сентября 2000 г. № Пр-1895).
10. Закон РФ от 5 мая 1992 года № 2446-1 «О безопасности».
11. Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
12. Федеральный закон от 12.08.1995 N 144-ФЗ (ред. от 06.07.2016) «Об оперативно-розыскной деятельности».
13. Закон РФ от 21 июля 1993 года №5485-1 «О государственной тайне».
14. Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных».
15. Федеральный закон от 10 января 2002 года № 1-ФЗ «Об электронной цифровой подписи».
16. Федеральный закон № 126-ФЗ от 07.07.2003 «О связи»
17. Федеральный закон «О почтовой связи» от 17.07.1999 № 176-ФЗ
18. Федеральный закон от 27.07.2004 № 79-ФЗ «О государственной гражданской

службе Российской Федерации»

19. Федеральный закон от 07.02.2011 № 3-ФЗ «О полиции»

20. Федерального закона от 31.05.2002 № 63-ФЗ «Об адвокатской деятельности и адвокатуре в Российской Федерации».

21. Закон РФ от 02.12.1990 № 395-1 «О банках и банковской деятельности».

22. Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне».

23. Федеральный закон от 15.12.2001 № 167-ФЗ «Об обязательном пенсионном страховании в Российской Федерации».

24. Федеральный закон от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации».

25. Закон РФ от 27.12.1991 № 2124-1 (ред. от 03.07.2016) «О средствах массовой информации».

26. Перечень сведений, отнесенных к государственной тайне ("Утв. Указом Президента РФ от 30 ноября 1995 года № 1203).

27. Перечень сведений конфиденциального характера (утв. Указом Президента РФ от 6 марта 1997 года № 188 (в ред. Указа Президента РФ от 23 сентября 2005 года №1111)).

28. Приложение к Приказу ФСБ России от 9 февраля 2005 года № 66 «Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)».

29. Гражданский кодекс Российской Федерации. Части 1-4.

30. Уголовный кодекс Российской Федерации.

31. Налоговый кодекс Российской Федерации.

32. Трудовой кодекс.

33. Кодекс Российской Федерации об административных правонарушениях.

34. ГОСТ Р 50922-96. Защита информации. Основные термины и определения.

35. ГОСТ 28388-89. Системы обработки информации. Документы на магнитных носителях данных. Порядок выполнения и обращения.

36. ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения

37. ГОСТ Р 51275-99. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения.

38. ГОСТ Р ИСО/МЭК 27001-2006 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования

39. ГОСТ Р ИСО/МЭК 15408-1-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель

40. Р 50.1.053-2005 Техническая защита информации. Основные термины и определения

41. Руководящие документы Федеральной службы по техническом и экспортному контролю (Государственной технической комиссии при Президенте РФ).

в) программное обеспечение и Интернет-ресурсы:

Сайт: www.fstec.ru – официальный сайт Федеральной службы по техническому и экспортному контролю.

8. Материально-техническое обеспечение дисциплины Основы информационной безопасности в деятельности правоохранительных органов

Учебная аудитория для проведения лекционных занятий, групповых и индивидуальных консультаций, текущей и промежуточной аттестации.

Оснащение аудитории:

- комплект учебной мебели: парты, стол преподавательский, стулья, доска;

- мультимедийная система: проектор, экран настенный, ноутбук.

Программное обеспечение:

- лицензионное программное обеспечение - ОС Microsoft Windows;
- свободно распространяемое программное обеспечение:
    - офисный пакет LibreOffice;
    - программа просмотра pdf-документов Sumatra PDF Reader.

Компьютерная лаборатория для проведения практических занятий, текущей и промежуточной аттестации, самостоятельной работы студентов, консультаций.

Оснащение лаборатории:

- комплект учебной мебели: стол преподавательский, столы компьютерные, стулья;
- персональные компьютеры, сетевой коммутатор, сетевая кабельная система.

Программное обеспечение:

- лицензионное программное обеспечение:
    - ОС Microsoft Windows;
    - антивирус Касперского;
- свободно распространяемое программное обеспечение:
    - программа просмотра pdf-документов Sumatra PDF Reader;
    - офисный пакет LibreOffice;
    - средство виртуализации Oracle Virtual Box;
    - браузер Mozilla Firefox.

Рабочая программа дисциплины «Основы информационной безопасности в деятельности правоохранительных органов» составлена в соответствии с требованиями ФГОС ВО по специальности 40.05.02 «Правоохранительная деятельность».

Программу составил: к.т.н., доцент кафедры ИБСТ Фатеев А.Г.
(Ф.И.О., должность, подпись)

Настоящая программа не может быть воспроизведена ни в какой форме без предварительного письменного разрешения кафедры-разработчика программы.

Программа одобрена на заседании кафедры ИБСТ

Протокол № 5 от « 28 » декабря 2016 года

Зав. кафедрой ИБСТ С.Л. Зефиров
(подпись) (Ф.И.О.)

Программа согласована с заведующим выпускающей кафедры
«Правоохранительная деятельность» Свечников Н.И.
(название кафедры) (подпись, Ф.И.О., дата)

Программа одобрена методической комиссией юридического факультета

Протокол № 5 от «10» января 2017 года

Председатель методической комиссии юридического факультета:
(подпись) Романовский Г.Б.
(Ф.И.О.)

Сведения о переутверждении программы на очередной учебный год и регистрации изменений

Учебный год	Решение кафедры (№ протокола, дата, подпись зав. кафедрой)	Внесенные изменения	Номера листов (страниц)		
			заменен-ных	новых	аннулиро-ванных