Уп2015-2016

Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
**«Владимирский государственный университет
имени Александра Григорьевича и Николая Григорьевича Столетовых»
(ВлГУ)**

УТВЕРЖДАЮ
Проректор
по образовательной деятельности
_____ А.А.Панфилов
«29» 12 2016 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ОРГАНИЗАЦИОННОЕ И ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

(наименование дисциплины)

Направление подготовки 10.03.01 Информационная безопасность

Профиль / программа подготовки Комплексная защита объектов информатизации

Уровень высшего образования бакалавриат

Форма обучения очная

Семестр	Трудоемкость зач. ед,/ час.	Лекции, час.	Практич. занятия, час.	Лаборат. работы, час.	СРС, час.	Форма промежуточного контроля (экз./зачет)
6	2/72	18	36	-	18	Зачет
7	6/216	36	36	-	108	Экзамен (36ч)
Итого	8/288	54	72		126	Зачет, Экзамен (36ч)

Владимир 2016

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целями освоения дисциплины «Организационное и правовое обеспечение информационной безопасности» являются обеспечение подготовки бакалавров в соответствии с требованиями ФГОС ВО и учебного плана по направлению 10.03.01 «Информационная безопасность»; формирование у бакалавров знаний по современным проблемам организационного и правового обеспечения информационной безопасности. Курс предусматривает формирование и уяснение студентами значения норм права, регулирующих поиск, получение, производство и распространение информации по действующему законодательству Российской Федерации, изучение правовых средств, используемых наряду с техническими для обеспечения защиты информационных прав и свобод. В курсе раскрыты основные направления работы по организационной защите информации на предприятии, являющиеся наиболее актуальными. Определены последовательность и алгоритм решения задач организационной защиты информации с учетом положений нормативно-методических документов и специфики деятельности предприятия.

Задачей освоения дисциплины «Организационное и правовое обеспечение информационной безопасности» является изучение: - угроз утечки информации по организационному каналу; - организация и ведение секретного и конфиденциального делопроизводства; - организация службы безопасности объекта; - подбор и работа с кадрами в сфере информационной безопасности; - организация охраны объектов; - ознакомление с важнейшими источниками информационного права Российской Федерации; - усвоение основополагающих нормативно-правовых актов; - умение работать с ними и применять в конкретных практических ситуациях; - приобретение навыка составления основных документов (договоров, положений, локальных актов и др.), используемых в сфере информационной безопасности; - освоение предусмотренных законодательством способов защиты информационных прав и свобод.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО БАКАЛАВРИАТА

Данная дисциплина относится к базовой части блока Б1 (код Б1.Б.9). В учебном плане предусмотрены виды учебной деятельности, обеспечивающие синтез теоретических лекций и практических занятий. Курс тесно взаимосвязан с другими дисциплинами данного цикла.

Дисциплина изучается на третьем и четвертом курсе, требования к «входным» знаниям, умениям и готовностям (пререквизитам) обучающегося определяются требованиями к уровню подготовки по курсам «Основы информационной безопасности», «Информационные технологии», «Правоведение» по направлению подготовки 10.03.01 «Информационная безопасность», квалификации - бакалавр. Кроме того, для грамотного использования полученных знаний в профессиональной деятельности, требуется изучение курсов «Математика»; «Документоведение».

Курс тесно взаимосвязан с другими дисциплинами данного цикла. Он является полезным для изучения таких дисциплин как «Система защиты информации на предприятии», «Политики информационной безопасности в корпоративных ИС», «Сети и системы передачи информации» и др.

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ

В результате освоения дисциплины бакалавр должен обладать общекультурными компетенциями:

ОК-4- способностью использовать основы правовых знаний в различных сферах деятельности;

общекультурными компетенциями:

ОПК – 5 - способностью использовать нормативные правовые акты в профессиональной деятельности;

профессиональными компетенциями:

ПК-13- способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации;

ПК-15- способностью организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю.

В результате освоения дисциплины обучающийся должен демонстрировать следующие результаты образования:

1) Знать: основные понятия, законы, модели и структуры обеспечения организационной безопасности на предприятии; основные понятия, законы и модели прогнозирования принятия решений; определять виды и формы информации, подверженной угрозам, виды и возможные методы и пути реализации угроз на основе анализа структуры и содержания информационных процессов предприятия, целей и задач деятельности предприятия. Знать методологию анализа исходных данных для проектирования подсистем и средств обеспечения информационной безопасности (ОК – 4; ОПК-5; ПК-13; ПК-14).

2) Уметь: анализировать и формализовать задачи своей профессиональной деятельности (научно-исследовательские, экспертно-аналитические, организационно-управленческие и др.) и выбирать адекватные пути и методы для их решения; квалифицированно применять имеющийся математический аппарат; использовать математические методы и модели для решения прикладных задач; применять основные закономерности принятия управленческих решений и управления коллективом при решении прикладных задач обеспечения информационной безопасности. организовать проведение и сопровождать аттестацию объекта на соответствие требованиям государственных или корпоративных нормативных документов (ОК – 4; ОПК-5; ПК-13; ПК-14);

3) Владеть: знаниями в области правового обеспечения информационной безопасности и навыками правоприменения нормативного законодательства в данной сфере; навыками поиска нормативной и технической информации, необходимой для профессиональной деятельности, обоснования, выбора, реализации и контроля результатов работы (ОК – 4; ОПК-5; ПК-13; ПК-14).

У обучаемых в процессе изучения дисциплины должны вырабатываться дополнительные компетенции, с учетом требований работодателей:

- способность прогнозировать угрозы утечки информации по организационному каналу;
- способность оценивать состояние информационной безопасности объекта с учетом действующих нормативных и методических документов.

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины составляет 8 зачетных единиц, 2 часов.

№ п/п	Раздел (тема) дисциплины	Семестр	Неделя семестра	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)						Объем учебной работы, с применением интерактивных методов (в часах / %)	Формы текущего контроля успеваемости *(по неделям семестра)*, форма промежуточной аттестации *(по семестрам)*
				Лекции	Практические занятия	Лабораторные работы	Контрольные работы,	СРС	КП / КР		
1	Основы информационного законодательства РФ. Структура информационного законодательства	6	1-2	2	4			2		2(33%)	
2	ФЗ «Об информации, информационных технологиях и о защите информации»	6	3	1	2			1		1(33%)	
3	ФЗ «О государственной тайне»	6	4	1	2			1		1(33%)	
4	ФЗ «Об обязательном экземпляре документов»	6	5	1	2			1		1(33%)	Рейтинг - контроль №1
5	ФЗ «О связи»	6	6	1	2			1		1(33%)	
6	ФЗ «О персональных данных»	6	7	1	2			1		1(33%)	
7	ФЗ «Об цифровой подписи»	6	8	1	2			1		1(33%)	
8	ФЗ «О коммерческой тайне»	6	9	1	2			1		1(33%)	
9	ФЗ «О лицензировании отдельных видов деятельности	6	10	1	2			1		1(33%)	
10	ФЗ «Об оперативно-розыскной деятельности	6	11	1	2			1		1(33%)	
11	ФЗ «О безопасности	6	12	1	2			1		1(33%)	Рейтинг - контроль №2
12	ФЗ «О техническом регулировании»	6	13	1	2			1		1(33%)	
13	ФЗ «О частной детективной и охранной деятельности в РФ»	6	14	1	2			1		1(33%)	
14	ФЗ" Об оружии"	6	15	1	2			1		1(33%)	
15	Указы Президента РФ в области обеспечения ИБ	6	16	1	2			1		1(33%)	
16	Доктрина информационной безопасности РФ	6	17	1	2			1		1(33%)	
17	Постановления Правительства РФ в области обеспечения ИБ	6	18	1	2			1		1(33%)	Рейтинг - контроль №3
Всего по семестру 6:				18	36			18			ЗАЧЕТ
18	Информационная безопасность и ее обеспечение	7	1	2	2			6		2(50%)	
19	Анализ угроз объекту ИБ	7	2	2	2			6		2(50%)	
20	Организационные источники и каналы	7	3-4	4	4			12		2(25%)	

№ п/п	Раздел (тема) дисциплины	Семестр	Неделя семестра	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)						Объем учебной работы, с применением интерактивных методов (в часах / %)	Формы текущего контроля успеваемости *(по неделям семестра)*, форма промежуточной аттестации *(по семестрам)*
				Лекции	Практические занятия	Лабораторные работы	Контрольные работы,	СРС	КП / КР		
	утечки информации										
21	Организационные основы защиты КИ на предприятии	7	5-6	4	4			12		2(25%)	Рейтинг - контроль №1
22	Отнесение сведений к КИ Засекречивание и рассекречивание сведений	7	7-8	4	4			12		2(25%)	
23	Организация допуска и доступа персонала к КИ	7	9	2	2			6		2(50%)	
24	Основные направления рабо-ты с персоналом допущенным к КИ	7	10	2	2			6		2(50%)	
25	Организация КПиОР режимов на предприятии	7	11	2	2			6		2(50%)	
26	Планирование мероприятий по ЗИ на предприятии	7	12	2	2			6		2(50%)	Рейтинг - контроль №2
27	Организация ЗИ при проведении совещаний	7	13	2	2			6		2(50%)	
28	Организация ЗИ при рекламной и публикаторской деятельности	7	14	2	2			6		2(50%)	
29	ЗИ при осуществлении международного сотрудничества и выезде персонала предприятия за границу	7	15	2	2			6		2(50%)	
30	Организация допуска к проведению работ с ГТ	7	16	2	2			6		2(50%)	
31	Организация контроля над состоянием защиты КИ на предприятии	7	17	2	2			6		2(50%)	
32	Организация служебного расследования по фактам разглашения КИ или утраты носителей	7	18	2	2			6		2(50%)	Рейтинг - контроль №3
Всего по 7 семестру:				36	36			108			Экзамен(36 ч)
ИТОГО:		6-8		54	72			126		69(38%)	Зачет, экзамен (36 ч)

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Изучение дисциплины предполагает не только запоминание и понимание, но и анализ, синтез, рефлексию, формирует универсальные умения и навыки, являющиеся основой становления бакалавра по направлению «Информационная безопасность».

Для реализации компетентностного подхода предлагается интегрировать в учебный процесс интерактивные образовательные технологии, включая информационные и коммуникационные технологии (ИКТ), при осуществлении различных видов учебной работы:

разбор конкретных ситуаций;

учебную дискуссию;

электронные средства обучения (слайд-лекции).

Лекционные занятия проводятся в аудитории, оборудованной проектором, что позволяет сочетать активные и интерактивные формы проведения занятий.

Как традиционные, так и лекции инновационного характера могут сопровождаться компьютерными слайдами или слайд-лекциями. Основное требование к слайд-лекции – применение динамических эффектов (анимированных объектов), функциональным назначением которых является наглядно-образное представление информации, сложной для понимания и осмысления бакалаврами, а также интенсификация и диверсификация учебного процесса.

Удельный вес **занятий, проводимых в интерактивных формах**, определяется главной целью ООП бакалавриата по направлению 10.03.01, особенностью контингента обучающихся и содержанием конкретных дисциплин, и в целом, в учебном процессе, они должны составлять **не менее 20% аудиторных занятий**. Занятия лекционного типа для соответствующих групп студентов не могут составлять более 45 процентов аудиторных занятий. Программа дисциплины соответствует данным требованиям.

Таким образом, применение интерактивных образовательных технологий придает инновационный характер практически всем видам учебных занятий, включая лекционные. При этом делается акцент на развитие самостоятельного, продуктивного мышления, основанного на диалогических дидактических приемах, субъектной позиции обучающегося в образовательном процессе. Тем самым создаются условия для реализации компетентностного подхода при изучении данной дисциплины.

6. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ, ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ИТОГАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ И УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ

Для текущего контроля успеваемости предлагается использование рейтинговой системы оценки, которая носит интегрированный характер и учитывает успешность бакалавра в различных видах учебной деятельности, степень сформированности у бакалавра общекультурных и профессиональных компетенций.

Примерный перечень заданий для текущих контрольных мероприятий:

Вопросы рейтинг-контроля №1 семестр 6:

- Какие существуют типы мер по защите информации по закону «Об информации, информационных технологиях и о защите информации»?
- -На достижение каких целей направлены правовые аспекты организационно-правового обеспечения защиты информации по закону «Об информации, информационных технологиях и о защите информации»?
- -Назовите основные принципы правового регулирования отношений, возникающих в телекоммуникационной сфере по закону «Об информации, информационных технологиях и о защите информации».
- -Какие существуют типы информации в зависимости от порядка ее предоставления или распространения по закону «Об информации, информационных технологиях и о защите информации»?

- -Как осуществляется допуск предприятий, учреждений и организаций к проведению работ, вязанных с использованием сведений, составляющий государственную тайну?
- -Что включает в себя правовой режим информации по закону «Об информации, информационных технологиях и о защите информации»?
- -Какие существуют основания для прекращения допуска гражданам и должностным лицам в доступе к государственной тайне?
- -На что имеет право обладатель информации, если иное не предусмотрено федеральными законами, согласно закону «Об информации, информационных технологиях и о защите информации»?
- -Какие существуют основания для отказа гражданам и должностным лицам в доступе к государственной тайне?
- -Какие существуют виды информационных систем согласно закону «Об информации, информационных технологиях и о защите информации»?
- -Какие государственные структуры относятся к органам защиты государственной тайны?
- -На что направлены меры по защите информации согласно закону «Об информации, информационных технологиях и о защите информации»?
- -В каких случаях сведения, содержащие государственную тайну подлежат рассекречиванию?
- -Что обязан обеспечить обладатель информации и оператор информационной системы (в случаях, установленных законодательством Российской Федерации) согласно закону «Об информации, информационных технологиях и о защите информации»?
- -Какую информацию должны содержать реквизиты носители сведений, содержащих государственную тайну?
- -Какие существуют грифы секретности и формы допуска к государственной тайне?
- -Дайте краткий перечень сведений, которые могут составлять государственную тайну.
- Назовите цели ФЗ «О связи».
- Дайте определение понятию «сети связи общего пользования».
- Дайте определение понятию «выделенные сети связи».

Вопросы рейтинг-контроля №2 семестр 6:

- На обработку каких персональных данных распространяется действие закона «О персональных данных»?
- Назовите основные принципы обработки персональных данных.
- В каких случаях не требуется согласие субъекта персональных данных на обработку его персональных данных?
- В каких случаях допускается обработка специальных категорий персональных данных?
- Какие сведения должно включать в себя письменное согласие субъекта персональных данных на обработку его персональных данных?
- Какими правами обладает субъект персональных данных по доступу к своим персональным данным и какую информацию субъект персональных данных имеет право получить?
- В каких случаях субъект персональных данных не может быть ознакомлен со своими персональными данными?
- Какие обязанности несет оператор персональных данных при их сборе и обработке?
- В каких случаях оператор персональных данных имеет право на их обработку без уведомления уполномоченного органа по защите прав субъектов персональных данных?
- Какими правами обладает уполномоченный орган по защите прав субъектов персональных данных?
- Какими обязанностями обладает уполномоченный орган по защите прав субъектов персональных данных?
- Дайте определение закрытого и открытого ключа электронной цифровой подписи.
- В каких условиях ЭЦП признается юридически равносильной собственноручной подписи на бумажном носителе?

- Дайте определение понятию владельца сертификата ключа ЭЦП.
- Какую основную информацию должен содержать сертификат ЭЦП?
- Какую основную деятельность осуществляет удостоверяющий центр (по вопросам обеспечения функционирования ЭЦП)?
- Назовите основные обязательства удостоверяющего центра по отношению к владельцу сертификата ключа ЭЦП.
- Назовите основные обязательства владельца сертификата ключа ЭЦП.
- Что включает в себя понятие «лицензирование деятельности»?
- Назовите, какие основные базовые направления деятельности лицензируются в особом порядке и не регулируются законом «О лицензировании отдельных видов деятельности».
- Назовите основные принципы осуществления лицензирования отдельных видов деятельности.

Вопросы рейтинг-контроля №3 семестр 6:

- Назовите основные обязательства владельца сертификата ключа ЭЦП.
- Что включает в себя понятие «лицензирование деятельности»?
- Назовите, какие основные базовые направления деятельности лицензируются в особом порядке и не регулируются законом «О лицензировании отдельных видов деятельности».
- Назовите основные принципы осуществления лицензирования отдельных видов деятельности.
- Что ФЗ «Об оперативно-розыскной деятельности» запрещается органам (должностным лицам), осуществляющим ОРД?
- Перечислите основные виды оперативно-розыскных мероприятий.
- Что является основанием для проведения ОРМ и для каких нужд вправе собирать информацию органы, осуществляющие ОРМ?
- Перечислите органы, имеющие право осуществления ОРД согласно ФЗ «Об оперативно-розыскной деятельности».
- Какие обязанности возлагаются на органы, осуществляющие ОРД?
- Какова основная цель создания ФЗ «О коммерческой тайне»?
- Перечислите основные изменения, внесенные в ГК РФ, вступлением в силу 4 части ГК РФ
- Назовите основные источники технических требований, устанавливаемых в рамках технического регулирования.
- Что понимается под техническим регламентом?
- В каких целях принимаются технические регламенты?
- В каких формах проводится оценка соответствия по ФЗ «О техническом регулировании»?
- Что понимается под стандартом?
- В каких целях осуществляется стандартизация?
- Перечислите основные принципы стандартизации.
- Назовите известные Вам указы президента РФ в области обеспечения информационной безопасности.
- Назовите основные составляющие национальных интересов Российской Федерации в информационной сфере, согласно «Доктрине информационной безопасности РФ».
- Какие угрозы информационной безопасности Российской Федерации можно выделить, опираясь на Доктрину информационной безопасности РФ?
- Перечислите известные Вам постановления Правительства в области обеспечения информационной безопасности.

Перечень вопросов к зачету (промежуточной аттестации по итогам освоения дисциплины) 6 семестр:

1. Какие существуют типы мер по защите информации по закону «Об информации, информационных технологиях и о защите информации»?

2. -На достижение каких целей направлены правовые аспекты организационно-правового обеспечения защиты информации по закону «Об информации, информационных технологиях и о защите информации»?

3. -Назовите основные принципы правового регулирования отношений, возникающих в телекоммуникационной сфере по закону «Об информации, информационных технологиях и о защите информации».

4. -Какие существуют типы информации в зависимости от порядка ее предоставления или распространения по закону «Об информации, информационных технологиях и о защите информации»?

5. -Как осуществляется допуск предприятий, учреждений и организаций к проведению работ, вязанных с использованием сведений, составляющий государственную тайну?

6. -Что включает в себя правовой режим информации по закону «Об информации, информационных технологиях и о защите информации»?

7. -Какие существуют основания для прекращения допуска гражданам и должностным лицам в доступе к государственной тайне?

8. -На что имеет право обладатель информации, если иное не предусмотрено федеральными законами, согласно закону «Об информации, информационных технологиях и о защите информации»?

9. -Какие существуют основания для отказа гражданам и должностным лицам в доступе к государственной тайне?

10. -Какие существуют виды информационных систем согласно закону «Об информации, информационных технологиях и о защите информации»?

11. -Какие государственные структуры относятся к органам защиты государственной тайны?

12. -На что направлены меры по защите информации согласно закону «Об информации, информационных технологиях и о защите информации»?

13. -В каких случаях сведения, содержащие государственную тайну подлежат рассекречиванию?

14. -Что обязан обеспечить обладатель информации и оператор информационной системы (в случаях, установленных законодательством Российской Федерации) согласно закону «Об информации, информационных технологиях и о защите информации»?

15. -Какую информацию должны содержать реквизиты носители сведений, содержащих государственную тайну?

16. -Какие существуют грифы секретности и формы допуска к государственной тайне?

17. -Дайте краткий перечень сведений, которые могут составлять государственную тайну.

18. Назовите цели ФЗ «О связи».

19. Дайте определение понятию «сети связи общего пользования».

20. Дайте определение понятию «выделенные сети связи».

21. Что является предметом правового регулирования ФЗ «О связи»?

22. На обработку каких персональных данных распространяется действие закона «О персональных данных»?

23. Назовите основные принципы обработки персональных данных.

24. В каких случаях не требуется согласие субъекта персональных данных на обработку его персональных данных?

25. В каких случаях допускается обработка специальных категорий персональных данных?

26. Какие сведения должно включать в себя письменное согласие субъекта персональных данных на обработку его персональных данных?

27. Какими правами обладает субъект персональных данных по доступу к своим персональным данным и какую информацию субъект персональных данных имеет право получить?

28. В каких случаях субъект персональных данных не может быть ознакомлен со своими персональными данными?

29. Какие обязанности несет оператор персональных данных при их сборе и обработке?

30. В каких случаях оператор персональных данных имеет право на их обработку без уведомления уполномоченного органа по защите прав субъектов персональных данных?

31. Какими правами обладает уполномоченный орган по защите прав субъектов персональных данных?

32. Какими обязанностями обладает уполномоченный орган по защите прав субъектов персональных данных?

33. Дайте определение закрытого и открытого ключа электронной цифровой подписи.

34. В каких условиях ЭЦП признается юридически равносильной собственноручной подписи на бумажном носителе?

35. Дайте определение понятию владельца сертификата ключа ЭЦП.

36. Какую основную информацию должен содержать сертификат ЭЦП?

37. Какую основную деятельность осуществляет удостоверяющий центр (по вопросам обеспечения функционирования ЭЦП)?

38. Назовите основные обязательства удостоверяющего центра по отношению к владельцу сертификата ключа ЭЦП.

39. Назовите основные обязательства владельца сертификата ключа ЭЦП.

40. Что включает в себя понятие «лицензирование деятельности»?

41. Назовите, какие основные базовые направления деятельности лицензируются в особом порядке и не регулируются законом «О лицензировании отдельных видов деятельности».

42. Назовите основные принципы осуществления лицензирования отдельных видов деятельности.

43. Что ФЗ «Об оперативно-розыскной деятельности» запрещается органам (должностным лицам), осуществляющим ОРД?

44. Перечислите основные виды оперативно-розыскных мероприятий.

45. Что является основанием для проведения ОРМ и для каких нужд вправе собирать информацию органы, осуществляющие ОРМ?

46. Перечислите органы, имеющие право осуществления ОРД согласно ФЗ «Об оперативно-розыскной деятельности».

47. Какие обязанности возлагаются на органы, осуществляющие ОРД?

48. Какова основная цель создания ФЗ «О коммерческой тайне»?

49. Перечислите основные изменения, внесенные в ГК РФ, вступлением в силу 4 части ГК РФ

50. Назовите основные источники технических требований, устанавливаемых в рамках технического регулирования.

51. Что понимается под техническим регламентом?

52. В каких целях принимаются технические регламенты?

53. В каких формах проводится оценка соответствия по ФЗ «О техническом регулировании»?

54. Что понимается под стандартом?

55. В каких целях осуществляется стандартизация?

56. Перечислите основные принципы стандартизации.

57. Назовите известные Вам указы президента РФ в области обеспечения информационной безопасности.

58. Назовите основные составляющие национальных интересов Российской Федерации в информационной сфере, согласно «Доктрине информационной безопасности РФ».

59. Какие угрозы информационной безопасности Российской Федерации можно выделить, опираясь на Доктрину информационной безопасности РФ?

60. Перечислите известные Вам постановления Правительства в области обеспечения информационной безопасности.

Вопросы рейтинг-контроля №1 семестр 7:

- Перечислите основные источники конфиденциальной информации на предприятии.

- Назовите основные организационные каналы передачи и обмена информацией на предприятии.
- Каким образом подразделяются (классифицируются) организационные каналы утечки информации.
- Назовите основные направления деятельности руководства предприятия в области организации защиты информации.
- Что называют организационной защитой информации на предприятии, какие у нее основные задачи.
- Назовите основные принципы организационной защиты информации на предприятии.
- Назовите основные условия организационной защиты информации на предприятии.
- Какие типовые структурные подразделения входят в службу безопасности (занимаются ЗИ на предприятии), какие основные функции они выполняют?
- Какие основные функции выполняет режимно-секретное подразделение?
- Какие основные функции выполняет подразделение по технической защите информации и противодействию иностранным техническим разведкам?
- Какие основные функции выполняет подразделение по обеспечению охраны и контрольно-пропускного режима?
- Какие основные функции выполняет подразделение криптографической защиты информации?
- Какие существуют средства и системы для защиты конфиденциальной информации?
- Какие существуют методы защиты информации?
- Что включают в себя правовые методы защиты информации?
- Что включают в себя технические методы защиты информации?
- Что включают в себя организационные методы защиты информации?
- Назовите типы информации с ограниченным доступом, которая может обрабатываться на предприятии.
- Какими ФЗ и другими законодательными документами регламентируется конфиденциальная информация на предприятии?
- Какие существуют государственные конфиденциальные информационные ресурсы и информационные ресурсы, защищаемые государством?
- Какие информационные ресурсы предприятия относятся к коммерческой тайне и чем это регламентировано?

Вопросы рейтинг-контроля №2 семестр 7:

- Какими ФЗ и другими законодательными документами регламентируется конфиденциальная информация на предприятии?
- Какие существуют государственные конфиденциальные информационные ресурсы и информационные ресурсы, защищаемые государством?
- Какие информационные ресурсы предприятия относятся к коммерческой тайне и чем это регламентировано?
- Какие информационные ресурсы предприятия не могут быть отнесены к коммерческой тайне?
- Назовите грифы секретности и реквизиты носителей сведений, составляющих государственную тайну.
- Какие сведения могут и не могут быть отнесены к государственной тайне?
- Основания и порядок рассекречивания сведений составляющих государственную тайну и их носителей.
- Основания для отказа гражданину или должностному лицу в допуске к сведениям, составляющим государственную тайну.
- Какие мероприятия включают в себя условия правомерного доступа персонала предприятия к сведениям, составляющим коммерческую тайну?
- Какие основные разделы включает в себя «Положение о разрешительной системе доступа к сведениям, составляющим коммерческую тайну»?

- Порядок доступа к конфиденциальной информации командированных лиц.
- Назовите основные причины разглашения конфиденциальной информации персоналом предприятия.
- Обязанности работодателя по отношению к сотруднику в связи с действием на предприятии режима охраны коммерческой тайны.
- Назовите основные этапы работы с персоналом предприятия.
- Назовите основные направления работы с сотрудниками предприятия, допущенным к конфиденциальной информации.
- Назовите основные методы проверки и оценки соответствия кандидата при приеме на работу предъявляемым требованиям.
- Какие существуют основные требования к морально-деловым и личным качествам кандидата при приеме на работу?
- Методы мотивации деятельности персонала. Группы методов мотивации, методы стимулирования труда.

Вопросы рейтинг-контроля №3 семестр 7:

- Назовите основные направления работы с сотрудниками предприятия, допущенным к конфиденциальной информации.
- Назовите основные методы проверки и оценки соответствия кандидата при приеме на работу предъявляемым требованиям.
- Какие существуют основные требования к морально-деловым и личным качествам кандидата при приеме на работу?
- Методы мотивации деятельности персонала. Группы методов мотивации, методы стимулирования труда.
- Основные задачи контрольно-пропускного режима на предприятии.
- Основные принципы организации контрольно-пропускного режима на предприятии.
- Основные элементы организации контрольно-пропускного режима на предприятии.
- Что обязаны знать сотрудники, допущенные к конфиденциальной информации.
- Что запрещается сотрудникам, допущенным к конфиденциальной информации.
- Требования к помещениям, в которых проводятся работы с конфиденциальной информации.
- Основные задачи бюро пропусков.
- Основные функции и оборудование КПП при организации контрольно-пропускного режима.
- Виды пропусков при контрольно-пропускном режиме.
- Основные цели планирования мероприятий по защите информации.
- Что является основой для планирования мероприятий по защите информации.
- Основные типы планов подразделений службы безопасности по защите информации.
- Основные разделы плана мероприятий по защите информации.
- Основные мероприятия плана по защите информации при чрезвычайных ситуациях.
- Планирование защиты информации при проведении различных совещаний.
- Техническая подготовка помещений к проведению совещаний.
- Защита информации при осуществлении публикаторской деятельности.

Перечень вопросов к экзамену (промежуточной аттестации по итогам освоения дисциплины) 7 семестр:

1. Перечислите основные источники конфиденциальной информации на предприятии.
2. Назовите основные организационные каналы передачи и обмена информацией на предприятии.
3. Каким образом подразделяются (классифицируются) организационные каналы утечки информации.
4. Назовите основные направления деятельности руководства предприятия в области организации защиты информации.

5. Что называют организационной защитой информации на предприятии, какие у нее основные задачи.
6. Назовите основные принципы организационной защиты информации на предприятии.
7. Назовите основные условия организационной защиты информации на предприятии.
8. Какие типовые структурные подразделения входят в службу безопасности (занимаются ЗИ на предприятии), какие основные функции они выполняют?
9. Какие основные функции выполняет режимно-секретное подразделение?
10. Какие основные функции выполняет подразделение по технической защите информации и противодействию иностранным техническим разведкам?
11. Какие основные функции выполняет подразделение по обеспечению охраны и контрольно-пропускного режима?
12. Какие основные функции выполняет подразделение криптографической защиты информации?
13. Какие существуют средства и системы для защиты конфиденциальной информации?
14. Какие существуют методы защиты информации?
15. Что включают в себя правовые методы защиты информации?
16. Что включают в себя технические методы защиты информации?
17. Что включают в себя организационные методы защиты информации?
18. Назовите типы информации с ограниченным доступом, которая может обрабатываться на предприятии.
19. Какими ФЗ и другими законодательными документами регламентируется конфиденциальная информация на предприятии?
20. Какие существуют государственные конфиденциальные информационные ресурсы и информационные ресурсы, защищаемые государством?
21. Какие информационные ресурсы предприятия относятся к коммерческой тайне и чем это регламентировано?
22. Какие информационные ресурсы предприятия не могут быть отнесены к коммерческой тайне?
23. Назовите грифы секретности и реквизиты носителей сведений, составляющих государственную тайну.
24. Какие сведения могут и не могут быть отнесены к государственной тайне?
25. Основания и порядок рассекречивания сведений составляющих государственную тайну и их носителей.
26. Основания для отказа гражданину или должностному лицу в допуске к сведениям, составляющим государственную тайну.
27. Какие мероприятия включают в себя условия правомерного доступа персонала предприятия к сведениям, составляющим коммерческую тайну?
28. Какие основные разделы включает в себя «Положение о разрешительной системе доступа к сведениям, составляющим коммерческую тайну»?
29. Порядок доступа к конфиденциальной информации командированных лиц.
30. Назовите основные причины разглашения конфиденциальной информации персоналом предприятия.
31. Обязанности работодателя по отношению к сотруднику в связи с действием на предприятии режима охраны коммерческой тайны.
32. Назовите основные этапы работы с персоналом предприятия.
33. Назовите основные направления работы с сотрудниками предприятия, допущенным к конфиденциальной информации.
34. Назовите основные методы проверки и оценки соответствия кандидата при приеме на работу предъявляемым требованиям.
35. Какие существуют основные требования к морально-деловым и личным качествам кандидата при приеме на работу?
36. Методы мотивации деятельности персонала. Группы методов мотивации, методы стимулирования труда.
37. Основные задачи контрольно-пропускного режима на предприятии.

38. Основные принципы организации контрольно-пропускного режима на предприятии.
39. Основные элементы организации контрольно-пропускного режима на предприятии.
40. Что обязаны знать сотрудники, допущенные к конфиденциальной информации.
41. Что запрещается сотрудникам, допущенным к конфиденциальной информации.
42. Требования к помещениям, в которых проводятся работы с конфиденциальной информации.
43. Основные задачи бюро пропусков.
44. Основные функции и оборудование КПП при организации контрольно-пропускного режима.
45. Виды пропусков при контрольно-пропускном режиме.
46. Основные цели планирования мероприятий по защите информации.
47. Что является основой для планирования мероприятий по защите информации.
48. Основные типы планов подразделений службы безопасности по защите информации.
49. Основные разделы плана мероприятий по защите информации.
50. Основные мероприятия плана по защите информации при чрезвычайных ситуациях.
51. Планирование защиты информации при проведении различных совещаний.
52. Техническая подготовка помещений к проведению совещаний.
53. Защита информации при осуществлении публикаторской деятельности.

Темы практических занятия 6 семестр:
Тема 1. Правовое обеспечение защиты государственной тайны;
Тема 2. Правовое обеспечение защиты коммерческой тайны;
Тема 3. Правовое обеспечение защиты служебной тайны;
Тема 4. Правовое обеспечение защиты персональных данных;
Тема 5. Правовое обеспечение защиты профессиональной тайны;
Тема 6. Практика правоприменения и вводные задачи при правовом обеспечении защиты результатов интеллектуальной деятельности;
Тема 7. Практика правоприменения и вводные задачи при правовом регулировании отношений в сфере патентного права;
Тема 8. Практика правоприменения и вводные задачи при обеспечении права на секрет производства;
Тема 9. Практика правоприменения и вводные задачи при обеспечении прав на средства индивидуализации юридических лиц, товаров, работ, услуг и предприятий;
Тема 10. Практика правоприменения и вводные задачи при лицензировании деятельности в области обеспечения ИБ;
Тема 11. Практика правоприменения и вводные задачи при прохождении сертификации при обеспечении информационной безопасности;
Тема 12. Вводные задачи при определении мер ответственности за нарушения в области лицензирования и сертификации при обеспечении информационной безопасности;
Тема 13. Порядок аттестации объектов информатизации.

Темы практических занятий 7 семестр:
1. Изучение «Инструкции о порядке допуска должностных лиц и граждан Российской Федерации к государственной тайне» (утверждена постановлением правительства РФ от 06.02.2010 №63);
2. Изучение требований типовых инструкций по обеспечению сохранности конфиденциальной информации на предприятии;
3. Изучение требований типовых инструкций по обеспечению сохранности конфиденциальной информации при ее обработке на средствах вычислительной техники;
4. Изучение порядка аттестации объектов информатизации;
5. Изучение форм и порядка заполнения документации по результатам аттестации объектов информатизации;
6. Изучение порядка проведения организационных и технических мероприятий по ТЗИ на ОИ;

7. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К) -2001;
8. Изучение документа ФСТЭК РФ Р_1994.11.25. Положение по аттестации объектов информатизации по требованиям безопасности информации;
9. Изучение документа ФСТЭК РФ Р_2010.08.31_489. Об утверждении требований о защите информации, содержащейся в информационных системах общего пользования;
10. Изучение документа ФСТЭК РФ приказ №17 от 11.02.2013 об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах;
11. Изучение документа ФСТЭК РФ RD_1992.03.30_1. Руководящий документ автоматизированные системы. Защита от несанкционированного доступа к информации классификация автоматизированных систем и требования по защите информации;
12. Изучение документа ФСТЭК РФ RD_1992.03.30_3. Руководящий документ защита от несанкционированного доступа к информации .термины и определения;
13. Изучение документа ФСТЭК РФ RD_1992.03.30_4. Руководящий документ концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации.

Вопросы и задания для самостоятельной работы студентов 6 семестр

- Изучение ФЗ «Об информации, информационных технологиях и о защите информации»
- Изучение законодательства о государственной тайне
- Изучение ФЗ «О связи».
- Изучение ФЗ «О персональных данных»?
- Изучение ФЗ «Об электронной подписи»
- Изучение постановлений правительства
- Изучение административного регламента ФСТЭК России «По исполнению государственной функции по контролю за соблюдением лицензионных требований при осуществлении деятельности по технической защите конфиденциальной информации»
- Изучение административного регламента ФСТЭК России «По исполнению государственной функции по контролю за соблюдением лицензионных требований при осуществлении деятельности по разработке и производству средств защиты конфиденциальной информации»
- Изучение административного регламента ФСТЭК России «По предоставлению государственной услуги по лицензированию деятельности по технической защите конфиденциальной информации»
- Изучение административного регламента ФСТЭК России «По предоставлению государственной услуги по лицензированию деятельности по разработке и производству средств защиты конфиденциальной информации»
- Изучение совместного приказа ФСТЭК России, ФСБ России и Минкомсвязи России от 31 декабря 2013 г. №151/786/461 «О признании утратившим силу приказа Федеральной службы по техническому и экспортному контролю, Федеральной службы безопасности Российской Федерации и Министерства информационных технологий и связи Российской Федерации от 13 февраля 2008 г. N 55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных»»
- Изучение ФЗ «О лицензировании отдельных видов деятельности».
- Изучение ФЗ «Об оперативно-розыскной деятельности».
- Изучение ФЗ «О коммерческой тайне»
- Изучение 4 части ГК РФ
- Изучение ФЗ «О техническом регулировании»

Вопросы и задания для самостоятельной работы студентов 7 семестр

1. Требования типовых инструкций по обеспечению сохранности конфиденциальной информации на предприятии;

2. Требования типовых инструкций по обеспечению сохранности конфиденциальной информации при ее обработке на средствах вычислительной техники;
3. Порядок аттестации объектов информатизации;
4. Порядок заполнения документации по результатам аттестации объектов информатизации;
5. Проведение организационных и технических мероприятий по ТЗИ на ОИ;
6. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К) -2001;
7. Положение по аттестации объектов информатизации по требованиям безопасности информации;
8. Требования к защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах;

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

а) Основная литература:

1. Защита информации: Учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - 2-е изд. - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2015. - 392 с. ISBN 978-5-369-01378-6, Режим доступа: http://znanium.com/catalog.php?bookinfo=474838

2. Информационная безопасность: защита и нападение / Бирюков А.А. - М. : ДМК Пресс, 2012. - http://www.studentlibrary.ru/book/ISBN9785940746478.html. 474 с.

3. Региональная и национальная безопасность: Учебное пособие / А.Б. Логунов. - 3-е изд., перераб. и доп. - М.: Вузовский учебник: НИЦ ИНФРА-М, 2014. - 457 с.: ISBN 978-5-9558-0310-4, Режим доступа: http://znanium.com/catalog.php?bookinfo=406872

б) Дополнительная литература:

1. Моделирование системы защиты информации: Практикум: Учебное пособие / Е.К.Баранова, А.В.Бабаш - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2015 - 120 с.: Режим доступа: http://znanium.com/catalog.php?bookinfo=476047

2. Файман, О.И. Правовое обеспечение информационной безопасности : учебное пособие / О. И. Файман, В. А. Граник, М. Ю. Монахов ; Владимирский государственный университет (ВлГУ) .— Владимир : 2010 .— 86 с. : Имеется электронная версия (экземпл)

3. Петров С.В. Информационная безопасность [Электронный ресурс]: учебное пособие/ Петров С.В., Кисляков П.А.— Электрон. текстовые данные.— Саратов: Ай Пи Ар Букс, 2015.— 326 с.— Режим доступа: http://www.iprbookshop.ru/33857

в) Периодические издания:

1. Журнал "Алгоритм безопасности» – Режим доступа: http://www.algoritm.org/index.php;
2. Электронный научный журнал «Проблемы безопасности» – Режим доступа: http://www.pb.littera-n.ru/

г) Программное обеспечение и Интернет-ресурсы:

1. Образовательный сервер кафедры ИЗИ.– Режим доступа: http://edu.izi.vlsu.ru
3. Информационная образовательная сеть.- Режим доступа: http://ien.izi.vlsu.ru
4. Внутривузовские издания ВлГУ.– Режим доступа: http://e.lib.vlsu.ru/
5. ИНТУИТ. Национальный открытый университет.– Режим доступа: http://www.intuit.ru/

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

ауд. 408-2, Лекционная аудитория, количество студенческих мест – 50, площадь 60 м2, оснащение: мультимедийное оборудование (интерактивная доска Hitachi FX-77WD, проектор BenQ MX 503 DLP 2700ANSI XGA), ноутбук Lenovo Idea Pad B5045

ауд. 427а-2, лаборатория сетевых технологий, количество студенческих мест – 14, площадь 36 м2, оснащение: компьютерный класс с 8 рабочими станциями Core 2 Duo E8400 с выходом в Internet, 3 маршрутизатора Cisco 2800 Series, 6 маршрутизаторов Cisco 2621, 6 коммутаторов Cisco Catalyst 2960 Series, 3 коммутатора Cisco Catalyst 2950 Series, коммутатор Cisco Catalyst Express 500 Series, проектор BenQ MP 620 P, экран настенный рулонный. Лицензионное программное обеспечение: операционная система Windows 7 Профессиональная, офисный пакет приложений Microsoft Office Профессиональный плюс 2007, бесплатно распространяемое программное обеспечение: линейка интегрированных сред разработки Visual Studio Express 2012, программный продукт виртуализации Oracle VM VirtualBox 5.0.4, симулятор сети передачи данных Cisco Packet Tracer 7.0, интегрированная среда разработки программного обеспечения IntelliJ IDEA Community Edition 15.0.3.

ауд. 427б-2, УНЦ «Комплексная защита объектов информатизации», количество студенческих мест – 15, площадь 52 м2, оснащение: компьютерный класс с 7 рабочими станциями Alliance Optima P4 с выходом в Internet, коммутатор D-Link DGS-1100-16 мультимедийный комплект (проектор Toshiba TLP X200, экран настенный рулонный), прибор ST-031P «Пиранья-Р» многофункциональный поисковый, прибор «Улан-2» поисковый, виброакустический генератор шума «Соната АВ 1М», имитатор работы средств нелегального съема информации, работающих по радиоканалу «Шиповник», анализатор спектра «GoodWill GSP-827», индикатор поля «SEL SP-75 Black Hunter», устройство блокирования работы систем мобильной связи «Мозайка-3», устройство защиты телефонных переговоров от прослушивания «Прокруст 2000», диктофон Edic MINI Hunter, локатор «Родник-2К» нелинейный, комплекс проведения акустических и виброакустических измерений «Спрут мини-А», видеорегистратор цифровой Best DVR-405, генератор Шума «Гном-3»,учебно-исследовательский комплекс «Сверхширокополосные беспроводные сенсорные сети» (Nano Xaos), сканирующий приемник «Icom IC-R1500», анализатор сетей Wi-Fi Fluke AirCheck с активной антенной. Лицензионное программное обеспечение: Windows 8 Профессиональная, офисный пакет приложений Microsoft Office Профессиональный плюс 2010, бесплатно распространяемое программное обеспечение: линейка интегрированных сред разработки Visual Studio Express 2012, инструмент имитационного моделирования AnyLogic 7.2.0 Personal Learning Edition, интегрированная среда разработки программного обеспечения IntelliJ IDEA Community Edition 14.1.4.

Рабочая программа дисциплины составлена в соответствии с требованиями ФГОС ВО по направлению 10.03.01 «Информационная безопасность» профиль «Комплексная защита объектов информатизации»

Рабочую программу составил доцент кафедры ИЗИ к.т.н. Тельный А.В.
(ФИО, подпись)

Рецензент
(представитель работодателя) Заместитель руководителя РАЦ ООО «ИнфоЦентр»

к.т.н. Вертилевский Н.В.
(место работы, должность, ФИО, подпись)

Программа рассмотрена и одобрена на заседании кафедры ИЗИ
Протокол № 7 от 28.12.16 года
Заведующий кафедрой д.т.н., профессор /М.Ю. Монахов/
(ФИО, подпись)

Рабочая программа рассмотрена и одобрена на заседании учебно-методической комиссии направления 10.03.01 «Информационная безопасность» профиль «Комплексная защита объектов информатизации»
Протокол № 4 от 28.12.16 года
Председатель комиссии д.т.н., профессор /М.Ю. Монахов/
(ФИО, подпись)

ЛИСТ ПЕРЕУТВЕРЖДЕНИЯ
РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ (МОДУЛЯ)

Рабочая программа одобрена на 2017/18 учебный год
Протокол заседания кафедры № 1 от 28.08.17 года
Заведующий кафедрой д.т.н., профессор /М.Ю. Монахов/
(ФИО, подпись)

ЛИСТ ПЕРЕУТВЕРЖДЕНИЯ
РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ (МОДУЛЯ)

Рабочая программа одобрена на _____ учебный год
Протокол заседания кафедры № _____ от _____ года
Заведующий кафедрой д.т.н., профессор /М.Ю. Монахов/
(ФИО, подпись)

Приложение

Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
**«Владимирский государственный университет
имени Александра Григорьевича и Николая Григорьевича Столетовых»
(ВлГУ)**

Институт _____

Кафедра _____

Актуализированная
рабочая программа
рассмотрена и одобрена
на заседании кафедры
протокол № ____ от ____ 20__г.

Заведующий кафедрой

_____
(подпись, ФИО)

Актуализация рабочей программы дисциплины

_____
(наименование дисциплины)

Направление подготовки

Профиль/программа подготовки

Уровень высшего образования

Форма обучения

Владимир 20__

Рабочая программа учебной дисциплины актуализирована в части рекомендуемой литературы.

Актуализация выполнена: _____
(подпись, должность, ФИО)

а) основная литература:_____

б) дополнительная литература: _____

в) периодические издания: _____

в) интернет-ресурсы: _____