Аннотация к рабочей программе дисциплины «Организационное и правовое обеспечение информационной безопасности»

Цель преподавания дисциплины

Дисциплина «Организационное и правовое обеспечение информационной безопасности» изучается с целью формирования у студентов знаний в области организационного и правового обеспечения информационной безопасности.

Задачи изучения дисциплины

– изучение основ организационно-правового обеспечения информационной безопасности;

– изучение российского законодательства в области информационной безопасности;

– изучение организационных методов и мероприятий защиты информации.

Компетенции, формируемые в результате освоения дисциплины

Способен использовать основы правовых знаний в различных сферах деятельности (ОК-4);

Способен использовать нормативные правовые акты в профессиональной деятельности (ОПК-5);

Способен оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов (ПК-8);

Способен проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности (ПК-10);

Способен 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 (ПК-15).

Разделы дисциплины

Введение в дисциплину «Организационное и правовое обеспечение информационной безопасности». Понятие «организационная защита информации». Правовые основы организационной защиты информации. Концептуальные положения организационного обеспечения информационной безопасности объектов защиты. Организационные источники и каналы утечки информации. Порядок допуска к конфиденциальной информации. Технические средства защиты информации. Допуск и доступ к конфиденциальной информации и документам. Государственная тайна и порядок отнесения к ней информации. Организация засекречивания и рассекречивания сведений, документов и продукции. Защита персональных данных. Организация автоматизированной обработки информации, содержащей персональные данные. Разработка организационно-распорядительной документации для объекта информатизации. Анализ эффективности применения средств защиты информации на объекте информатизации. Коммерческая тайна и порядок её определения Организация работ с информацией, составляющей коммерческую тайну. Подбор персонала на должности, связанные с работой с информацией ограниченного доступа. Организация внутриобъектового режима. Требования, предъявляемые к помещениям и хранилищам, в которых ведутся закрытые работы, хранятся документы ограниченного доступа и изделия. Организация защиты информации при приеме в организации посетителей командированных лиц и иностранных представителей. Организация охраны объекта. Организация пропускного режима. Организация защиты информации при подготовке и проведении совещаний и переговоров. Организация защиты информации при осуществлении научно-публицистической и рекламной деятельности. Защита информации при представлении ее в средствах массовой информации. Организация аналитической работы по предупреждению утечки конфиденциальной информации. Методы, используемые аналитическими подразделениями служб безопасности, по

предупреждению утечки конфиденциальной информации. Методы работы с персоналом, обладающим конфиденциальной информацией. Подготовка лиц, ответственных за обеспечение безопасности информации. Модель угроз информационной безопасности. Модель нарушителя информационной безопасности.

МИНОБРНАУКИ РОССИИ
Юго-Западный государственный университет

УТВЕРЖДАЮ:
Декан факультета
фундаментальной и прикладной
(наименование ф-та полностью)
информатики

Т.А. Ширабакина
(подпись, инициалы, фамилия)
«01» 02 2017 г

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Организационное и правовое обеспечение информационной безопасности
(наименование дисциплины)

направление подготовки (специальность) 10.03.01
(шифр согласно ФГОС)

Информационная безопасность
и наименование направление подготовки (специальности)

Безопасность автоматизированных систем
наименование профиля, специализации или магистерской программы

форма обучения очная
(очная, очно-заочная, заочная)

Курск – 2017

Рабочая программа составлена в соответствии с Федеральным государственным образовательным стандартом высшего образования направления подготовки 10.03.01 Информационная безопасность и на основании учебного плана направления подготовки 10.03.01 Информационная безопасность (профиль Безопасность автоматизированных систем), одобренного Учёным советом университета, протокол № 5 «30» 01 2017г.

Рабочая программа обсуждена и рекомендована к применению в учебном процессе для обучения студентов по направлению подготовки 10.03.01 Информационная безопасность на заседании кафедры информационной безопасности № «9» 01.02 2017г.

Зав. кафедрой ИБ Таныгин М.О.
Разработчик программы
доцент кафедры ИБ Спеваков А.Г.

Директор научной библиотеки Макаровская В.Г.

Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки 10.03.01 Информационная безопасность, одобренного Ученым советом университета протокол № 1 «28» 08 2017г. на заседании кафедры

(наименование кафедры, дата, номер протокола)

Зав. кафедрой

Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки 10.03.01 Информационная безопасность, одобренного Ученым советом университета протокол № 5 «01» 30 2017г. на заседании кафедры ИБ 29.06.2018 №12

(наименование кафедры, дата, номер протокола)

Зав. кафедрой

Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки 10.03.01 Информационная безопасность, одобренного Ученым советом университета протокол № « » 20 г. на заседании кафедры информационной безопасности 27.06.2019, №11

(наименование кафедры, дата, номер протокола)

Зав. кафедрой к.т.н. доцент Таныгин М.О.

Программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки *10.03.01 – «Информационная безопасность»*, одобренного Ученым советом университета протокол №7 «25» 02 2020 г. на заседании кафедры информационной безопасности. Протокол №1 от «31» 08 2020г.

Зав. кафедрой _____

Программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки *10.03.01 – «Информационная безопасность»*, одобренного Ученым советом университета протокол №7 «25» 02 2020 г. на заседании кафедры информационной безопасности. Протокол №11 от «28» 06 2021 г.

Зав. кафедрой _____

Программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки *10.03.01 – «Информационная безопасность»*, одобренного Ученым советом университета протокол №7 «25» 02 2020 г. на заседании кафедры информационной безопасности. Протокол №11 от «30» 06 2022 г.

Зав. кафедрой _____

Программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки *10.03.01 – «Информационная безопасность»*, одобренного Ученым советом университета протокол №__ «___» _____ 20__ г. на заседании кафедры информационной безопасности. Протокол №__ от «__»_____20__г.

Зав. кафедрой _____

Программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки *10.03.01 – «Информационная безопасность»*, одобренного Ученым советом университета протокол №__ «___» _____ 20__ г. на заседании кафедры информационной безопасности. Протокол №__ от «__»_____20__г.

Зав. кафедрой _____

1. Цель и задачи дисциплины. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы

1.1. Цель дисциплины

Дисциплина «Организационное и правовое обеспечение информационной безопасности» изучается с целью формирования у студентов знаний в области организационного и правового обеспечения информационной безопасности.

1.2. Задачи дисциплины

- изучение основ организационно-правового обеспечения информационной безопасности;
- изучение российского законодательства в области информационной безопасности;
- изучение организационных методов и мероприятий защиты информации.

1.3. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательный программы

Обучающиеся должны **знать:**

- нормативно-правовые основы информационной безопасности;
- основные положения важнейших законодательных актов РФ в области защиты информации;
-угрозы информационной безопасности объекта;
- ответственность за нарушения в сфере информационной безопасности.

уметь:

- разрабатывать организационно-распорядительную документацию по защите информации на объекте автоматизации;
- проводить мероприятия по учету и контролю средств защиты информации на объекте информатизации;
- производить оценку угроз информационной безопасности на объекте информатизации.

владеть:

- навыками критического анализа и оценки уровня защищенности информационной безопасности объекта;
- навыками реализации процессов управления информационной безопасностью, направленных на эффективное управление информационной безопасностью конкретной организации;

У обучающегося формируются следующие компетенции:

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

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

способностью оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов (ПК-8);

способностью проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности (ПК-10);

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 (ПК-15).

2. Указание места дисциплины в структуре образовательной программы

«Организационное и правовое обеспечение информационной безопасности» представляет дисциплину с индексом Б1.Б.Б17 базовой части учебного плана направления подготовки 10.03.01 Информационная безопасность, изучаемую на 3 курсе в 5 и 6 семестрах.

3. Объем дисциплины в зачетных единицах с указанием количества академических или астрономических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся

Общая трудоёмкость (объём) дисциплины составляет 6 зачётных единиц (з.е.), 216 академических часов.

Таблица 3 – Объём дисциплины

Виды учебной работы	Всего, часов
Общая трудоемкость дисциплины	216
Контактная работа обучающихся с преподавателем (по видам учебных занятий) (всего)	90
в том числе:	
лекции	54
лабораторные занятия	0
практические занятия	36
Самостоятельная работа обучающихся (всего)	88,75
Контроль (подготовка к экзамену)	36
Контактная работа по промежуточной аттестации (всего АттКР)	1,25
в том числе:	
зачет	0,1
зачет с оценкой	не предусмотрен
курсовая работа (проект)	не предусмотрена
экзамен (включая консультацию перед экзаменом)	1,15

4. Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

4.1 Содержание дисциплины

Таблица 4.1.1 – Содержание дисциплины, структурированное по темам (разделам)

№ п/п	Раздел (тема) дисциплины	Содержание
1	2	3
5 семестр		
1	Введение в дисциплину «Организационное и правовое обеспечение информационной безопасности»	Законодательство об информационной безопасности.
2	Понятие «организационная защита информации». Правовые основы организационной защиты информации	Состав нормативно-методических материалов по регламентации системы защиты информации.
3	Концептуальные положения организационного обеспечения информационной безопасности объектов защиты	Концептуальные положения организационного обеспечения информационной безопасности объектов защиты.
4	Организационные источники и каналы утечки информации.	Организационные источники и каналы утечки информации. Силы, средства и условия организационной защиты информации.
5	Порядок допуска к конфиденциальной информации.	Организация допуска к конфиденциальной информации
6	Технические средства защиты информации.	Программные и аппаратные средства защиты информации
7	Допуск и доступ к конфиденциальной информации и документам.	Организация допуска и доступа к конфиденциальной информации и документам.
8	Государственная тайна и порядок отнесения к ней информации	Порядок допуска к информации, составляющую государственную тайну
9 9	Организация засекречивания и рассекречивания сведений, документов и продукции.	Особенности системы организационной защиты информации, составляющей государственную тайну
10	Защита персональных данных	Порядок классификации персональных данных, перечень нормативно-правовых актов в области защиты персональных данных.
11	Организация автоматизированной обработки информации, содержащей персональные данные	Требования к защите информации, обрабатываемой в автоматизированных системах
12	Разработка организационно-распорядительной документации для объекта информатизации	Рассматриваются методы создания документации по организации системы защиты информации

13	Анализ эффективности применения средств защиты информации на объекте информатизации.	Рассматриваются методы анализа эффективности применения средств защиты информации
14	Коммерческая тайна и порядок её определения	Основные положения по работе с коммерческой тайной
6 семестр		
15	Организация работ с информацией, составляющей коммерческую тайну	Организационные мероприятия для организации обработки информации, составляющей коммерческую тайну
16	Подбор персонала на должности, связанные с работой с информацией ограниченного доступа	Порядок подбора персонала на должности, связанные с работой с информацией ограниченного доступа
17	Организация внутриобъектового режима.	Организация внутриобъектового режима Организация деятельности службы безопасности объекта
18	Требования, предъявляемые к помещениям и хранилищам, в которых ведутся закрытые работы, хранятся документы ограниченного доступа и изделия.	Требования, предъявляемые к помещениям и хранилищам, в которых ведутся закрытые работы, хранятся документы ограниченного доступа и изделия.
19	Организация защиты информации при приеме в организации посетителей командированных лиц и иностранных представителей.	Организация защиты информации при приеме в организации посетителей командированных лиц и иностранных представителей.
20	Организация охраны объекта. Организация пропускного режима.	Организация охраны объекта. Организация пропускного режима
21	Организация защиты информации при подготовке и проведении совещаний и переговоров.	Состав нормативно-методических материалов по регламентации системы защиты информации.
22	Организация защиты информации при осуществлении научно-публицистической и рекламной деятельности.	Методы защиты информации при осуществлении научно-публицистической и рекламной деятельности
23	Защита информации при представлении ее в средствах массовой информации.	Методы защиты информации при представлении ее в средствах массовой информации.
24	Организация аналитической работы по предупреждению утечки конфиденциальной информации.	Основные принципы организации аналитической работы служб безопасности по недопущению утечки конфиденциальной информации
25	Методы, используемые аналитическими подразделениями служб безопасности, по предупреждению утечки конфиденциальной информации	Содержание методов, используемых аналитическими подразделениями служб безопасности, по предупреждению утечки конфиденциальной информации
26	Методы работы с персоналом, обладающим конфиденциальной информацией.	Содержание основных методов и работы с персоналом, обладающим конфиденциальной информацией
27	Подготовка лиц, ответственных за обеспечение безопасности информации	Мероприятия по подготовке лиц, ответственных за обеспечение безопасности информации

28	Модель угроз информационной безопасности	Основные разделы модели угроз информационной безопасности

Таблица 4.1.2 – Содержание дисциплины и его методическое обеспечение

№ п/п	Раздел (тема) дисциплины	Виды деятельности			Учебно-методические материалы	Формы текущего контроля успеваемости *(по неделям семестра)*	Компетенции
		лек., час	№ лаб.	№ пр.			
1	2	3	4	5	6	7	8
5 семестр							
1	Введение в дисциплину «Организационное и правовое обеспечение информационной безопасности»	2			У – 1-7 МУ – 1-2	УО	ОК-4
2	Понятие «организационная защита информации». Правовые основы организационной защиты информации	2			У – 1-7 МУ – 1-2	УО	ОК-4, ОПК-5
3	Концептуальные положения организационного обеспечения информационной безопасности объектов защиты	2			У – 1-7 МУ – 1-2	УО	ОК-4, ОПК-5, ПК-10
4	Организационные источники и каналы утечки информации.	2		1	У – 1-7 МУ – 1-2	УО ЗПР	ПК-10
5	Порядок допуска к конфиденциальной информации	2			У – 1-7 МУ – 1-2	УО	ОК-4, ОПК-5
6	Технические средства защиты информации	2		2	У – 1-7 МУ – 1-2	УО ЗПР	ПК-15
7	Допуск и доступ к конфиденциальной информации и документам	2			У – 1-7 МУ – 1-2	УО	ОК-4, ОПК-5, ПК-8
8	Государственная тайна и порядок отнесения к ней информации	2			У – 1-7 МУ – 1-2	УО	ОК-4, ОПК-5, ПК-8
9	Организация засекречивания и рассекречивания сведений, документов и продукции	2			У – 1-7 МУ – 1-2	УО	ОК-4, ОПК-5, ПК-8, ПК-15

10	Защита персональных данных	2		3	У – 1-7 МУ – 1-2	УО ЗПР	ОК-4, ОПК-5, ПК-8
11	Организация автоматизированной обработки информации, содержащей персональные данные	2			У – 1-7 МУ – 1-2	УО	ПК-8, ПК-10, ПК-15
12	Разработка организационно-распорядительной документации для объекта информатизации	2		4	У – 1-7 МУ – 1-2	УО ЗПР	ОК-4, ОПК-5, ПК-8
13	Анализ эффективности применения средств защиты информации на объекте информатизации	2			У – 1-7 МУ – 1-2	УО	ОК-4, ОПК-5, ПК-8, ПК-10
14	Коммерческая тайна и порядок её определения	2			У – 1-7 МУ – 1-2	УО	ОК-4, ОПК-5
15	Организация работ с информацией, составляющей коммерческую тайну	2		5	У – 1-7 МУ – 1-2	УО ЗПР	ОК-4, ОПК-5, ПК-8, ПК-15
16	Подбор персонала на должности, связанные с работой с информацией ограниченного доступа	2			У – 1-7 МУ – 1-2	УО	ОК-4
17	Организация внутриобъектового режима.	2		6	У – 1-7 МУ – 1-2	УО ЗПР	ОК-4, ОПК-5, ПК-15
18	Требования, предъявляемые к помещениям и хранилищам, в которых ведутся закрытые работы, хранятся документы ограниченного доступа и изделия.	2			У – 1-7 МУ – 1-2	УО	ОК-4
19	Организация защиты информации при приеме в организации посетителей командированных лиц	2			У – 1-7 МУ – 1-2	УО	ОК-4, ОПК-5, ПК-15

	и иностранных представителей.						
20	Организация охраны объекта. Организация пропускного режима.	2		7	У – 1-7 МУ – 1-2	УО ЗПР	ОК-4, ПК-15
21	Организация защиты информации при подготовке и проведении совещаний и переговоров.	2			У – 1-7 МУ – 1-2	УО	ОК-4, ОПК-5, ПК-15
22	Организация защиты информации при осуществлении научно-публицистической и рекламной деятельности.	2			У – 1-7 МУ – 1-2	УО	ОК-4, ОПК-5, ПК-15
23	Защита информации при представлении ее в средствах массовой информации.	2			У – 1-7 МУ – 1-2	УО	ОК-4, ОПК-5, ПК-15
24	Организация аналитической работы по предупреждению утечки конфиденциальной информации.	2			У – 1-7 МУ – 1-2	УО	ОК-4, ОПК-5, ПК-10, ПК-15
25	Методы, используемые аналитическими подразделениями служб безопасности, по предупреждению утечки конфиденциальной информации	2			У – 1-7 МУ – 1-2	УО	ОК-4, ОПК-5
26	Методы работы с персоналом, обладающим конфиденциальной информацией.	1			У – 1-7 МУ – 1-2	УО	ОК-4, ОПК-5
27	Подготовка лиц, ответственных за обеспечение безопасности информации	1			У – 1-7 МУ – 1-2	УО	ОК-4, ОПК-5
28	Модель угроз информационной безопасности	1		8	У – 1-7 МУ – 1-2	УО ЗПР	ОК-4, ОПК-5, ПК-8, ПК-10

С – собеседование, ЗПР – защита практической работы.

4.2 Лабораторные работы и (или) практические занятия

4.2.1 Практические занятия

Таблица 4.2.1 – Практические занятия

№	Наименование практического занятия	Объем, час.
1	2	3
1	Организационные источники и каналы утечки информации	4
2	Технические средства защиты информации	4
3	Защита персональных данных	6
4	Разработка организационно-распорядительной документации для объекта информатизации	6
5	Анализ эффективности применения средств защиты информации на объекте информатизации	6
6	Организация внутриобъектового режима	4
7	Организация пропускного режима	4
8	Разработка модели угроз информационной безопасности	6
Итого		36

4.3 Самостоятельная работы студентов (СРС)

Таблица 4.3 – Самостоятельная работа студентов

№	Наименование раздела дисциплины	Срок выполнения	Время, затрачиваемое на выполнение СРС, час.
1	2	3	4
1	Принципы, силы, средства и условия организационной защиты информации.	4 неделя	9
2	Порядок засекречивания и рассекречивания сведений, документов и продукции.	8 неделя	9
3	Особенности системы организационной защиты информации, составляющей государственную тайну.	12 неделя	9
4	Допуск и доступ к конфиденциальной информации и документам.	18 неделя	9
5	Организация внутриобъектового и пропускного режимов на предприятиях	4 неделя	10,75
6	Организация подготовки и проведения совещаний и заседаний по конфиденциальным вопросам.	8 неделя	14
7	Организация аналитической работы по предупреждению утечки конфиденциальной информации.	12 неделя	14
8	Направления и методы работы с персоналом, обладающим конфиденциальной информацией.	18 неделя	14
Итого			88,75

5. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

Студенты могут при самостоятельном изучении отдельных тем и вопросов дисциплин пользоваться учебно-наглядными пособиями, учебным оборудованием и методическими разработками кафедры в рабочее время, установленное Правилами внутреннего распорядка работников.

Учебно-методическое обеспечение для самостоятельной работы обучающихся по данной дисциплине организуется:

библиотекой университета:

- библиотечный фонд укомплектован учебной, методической, научной, периодической, справочной и художественной литературой в соответствии с данной РПД;

- имеется доступ к основным информационным образовательным ресурсам, информационной базе данных, в том числе библиографической, возможность выхода в Интернет.

кафедрой:

- путем обеспечения доступности всего необходимого учебно- методического и справочного материала;

- путем предоставления сведений о наличии учебно-методической литературы современных программных средств;

- путем разработки вопросов к экзамену и зачету;

- методических указаний к выполнению практических работ.

типографией университета:

- путем помощи авторам в подготовке и издании научной, учебной, учебно методической литературы;

- путем удовлетворения потребностей в тиражировании научной, учебной, учебно-методической литературы.

6. Образовательные технологии

В соответствии с требованиями ФГОС и Приказа Министерства образования и науки РФ от 19 декабря 2013 г. № 1367 реализация компетентностного подхода предусматривает широкое использование в образовательном процессе активных и интерактивных форм проведения занятий в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков студентов. В рамках дисциплины предусмотрены встречи с экспертами и специалистами в области информационной безопасности. Удельный вес занятий, проводимых в интерактивных формах, составляет 28,6 процентов от аудиторных занятий согласно УП.

Таблица 6.1 – Интерактивные образовательные технологии, используемые при проведении аудиторных занятий

№	Наименование раздела (лекции, практического или лабораторного занятия)	Используемые интерактивные образовательные технологии	Объем в часах
1	2	3	4
5 семестр			
1	Организационные источники и каналы утечки информации	Разбор конкретных ситуаций	4
2	Технические средства защиты информации	Разбор конкретных ситуаций	2
3	Защита персональных данных	Разбор конкретных ситуаций	6
4	Разработка организационно-распорядительной документации для объекта информатизации	Разбор конкретных ситуаций	6
Всего			18
6 семестр			
1	Организация внутриобъектового и пропускного режимов на предприятиях	Разбор конкретных ситуаций	2
2	Организация подготовки и проведения совещаний и заседаний по конфиденциальным вопросам.	Разбор конкретных ситуаций	2
3	Организация аналитической работы по предупреждению утечки конфиденциальной информации.	Разбор конкретных ситуаций	2
4	Направления и методы работы с персоналом, обладающим конфиденциальной информацией.	Разбор конкретных ситуаций	2
Всего			8
Итого			26

7. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплины

7.1 Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

Код и содержание компетенции	Этапы* формирования компетенций и дисциплины (модуле), при изучении которых формируется данная компетенция		
	начальный	основной	завершающий
1	2	3	4
Способностью использовать основы правовых знаний в различных сферах деятельности(ОК-4)		Организационное и правовое обеспечение информационной безопасности	Организация и управление службой защиты информации; Работа с конфиденциальной информациией; Преддипломная практика;
Способностью использовать нормативные правовые акты в профессиональной деятельности(ОПК-5)	Правоведение; Патентоведение;	Организационное и правовое обеспечение; информационной безопасности;	Организация и управление службой защиты информации; Работа с конфиденциальной информацией; Преддипломная практика;
Способностью оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов(ПК-8)	Основы риверсинжениринга программных средств;	Организационное и правовое обеспечение информационной безопасности; Методы защиты программного обеспечения	Технологическая практика; Проектно-технологическая практика;
Способностью проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности(ПК-10);	Организационное и правовое обеспечение информационной безопасности; Учебно-исследовательская работа студентов; Проектно-технологическая практика		Организация и управление службой защиты информации; Работа с конфиденциальной информацией; Преддипломная практика
Способностью организовывать технологический процесс защиты информации	Организационное и правовое обеспечение информационной безопасности; Проектно-технологическая практика		Защита и обработка конфиденциальных документов;

ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю(ПК-15).		Организация и управление службой защиты информации; Работа с конфиденциальной информацией

7.2 Описание показателей и критериев оценивания компетенций на различных этапах формирования, описание шкал оценивания

Код компетенции/ этап *(указывается название этапа из п 7.1)*	Показатели оценивания компетенций	Критерии и шкала оценивания компетенций		
		Пороговый уровень («удовлетворительно»)	Продвинутый уровень («хорошо»)	Высокий уровень («отлично»)
1	2	3	4	5
ОК - 4/ основной	*1.Доля освоенных обучающимся знаний, умений навыков от общего объема ЗУН, установленных в п.1.ЗРПД* *2.Качество освоенных обучающимися знаний, умений, навыков*	Знать: -стандарты в области информационной безопасности; Уметь: - сопоставлять характеристики правового обеспечения действующим стандартам, Владеть: - комплексной оценкой защищённости систем документооборота	Знать: - методологические подходы применения нормативных документов при оценке защищённости правового обеспечения; Уметь: - выявлять не декларируемые угрозы; Владеть: - способностью к критическому анализу используемых методов аудита информационной безопасности	Знать: - принципы формирования комплексных отчётов по аудиту информационной безопасности ; Уметь: - вырабатывать методические рекомендации по формированию политик безопасности; Владеть: -организационными формами и методами проведения научных исследований

	3. Умение применять знания, умения, навыки в типовых и нестандартных ситуациях			
ОПК-5/ основной	*1.Доля освоенных обучающимся знаний, умений навыков от общего объема ЗУН, установленных в п.1.ЗРПД* *2.Качество освоенных обучающимися знаний, умений, навыков* *3. Умение применять знания, умения, навыки в типовых и нестандартных ситуациях*	Знать: - основные нормативные правовые документы. Уметь: - ориентироваться в системе законодательства и нормативных правовых актов в области защиты информации. Владеть: - навыками поиска необходимых нормативных и законодательных документов и навыками работы с ними в профессиональной деятельности	Знать: - нормативно правовые документы. Уметь: - использовать нормативно правовые акты в задачах защиты информации Владеть: - навыками поиска необходимых нормативных и законодательных документов и навыками анализа результатов их применения.	Знать: - Российские и международные нормативно правовые документы в области защиты информации. Уметь: - разрабатывать рекомендации по применению нормативно правовых документов в области защиты информации. Владеть: - навыками разработки организационно-распорядительной документации на объекте информатизации
ПК - 8/ основной	*1.Доля освоенных обучающимся знаний, умений навыков от общего объема ЗУН, установленных в п.1.ЗРПД*	Знать: - структуру системы документационного обеспечения; Уметь: - работать с документами, содержащими конфиденциальную информацию;	Знать: - нормативно-методические документы в области информационной безопасности; -методы оформления и основные разделы технической документации в области защиты информации; Уметь:	Знать: - отечественные и международные стандарты разработки и оформления технической документации; -методы и средства подготовки технической документации в области защиты информации; Уметь:

	2.Качество освоенных обучающимися знаний, умений, навыков *3. Умение применять знания, умения, навыки в типовых и нестандартных ситуациях*	Владеть: - навыками оформления рабочей технической документации	- использовать и применять теоретические знания при разработке технической документации в области защиты информации; Владеть: - навыками разработки технической документации по защите информации	- использовать и применять теоретические знания при разработке технической документации в области защиты информации; - проводить аудит технической документации в области защиты информации. Владеть: - навыками разработки и анализа технической документации по защите информации
ПК - 10/ основной	*1.Доля освоенных обучающимся знаний, умений навыков от общего объема ЗУН, установленных в п.1.ЗРПД* *2.Качество освоенных обучающимися знаний, умений, навыков* *3. Умение применять знания, умения, навыки в типовых и нестандартных ситуациях*	Знать: -стандарты в отношении технических и аппаратно-программных средств защиты информации ; Уметь: - сопоставлять характеристики аппаратно-программных средств защиты информации действующим стандартам, Владеть: - навыками анализа информационной безопасности объектов и систем на соответствие требованиям стандартов	Знать: - стандарты информационной безопасности и методологические подходы анализа защищенности объектов и систем. Уметь: - определять угрозы информационной безопасности и выявлять уязвимости объектов и систем и подбирать для них адекватные технические и организационные меры защиты информации. Владеть: - способностью к критическому анализу используемых методов аудита информационной безопасности	Знать: - принципы формирования комплексных отчётов по аудиту технических и аппаратно-программных средств защиты информации. Уметь: - разрабатывать методические рекомендации по формированию политик безопасности; Владеть: - методикой выявления несоответствий на объекте информатизации требованиям стандартов в области информационной безопасности.
ПК - 15/ основной	*1.Доля освоенных обучающимся знаний, умений*	Знать: -методологию организации технологического процесса	Знать: - методы и средства организации технологического процесса в	Знать: - методы и средства организации технологического процесса в соответствии с

	навыков от общего объема ЗУН, установленных в п.1.ЗРПД *2.Качество освоенных обучающимися знаний, умений, навыков* *3. Умение применять знания, умения, навыки в типовых и нестандартных ситуациях*	защиты информации ограниченного доступа. Уметь: - организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и типовыми методическими рекомендациями; Владеть: - навыками подбора средств защиты информации, в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	соответствии с требования организаций, уполномоченных в сфере защиты информации; Уметь: - организовывать технологический процесс защиты информации ограниченного доступа; - осуществлять поиск уязвимостей в технологическом процессе и своевременно устранять их. Владеть: - навыками модернизации существующих систем защиты информации и приведения их к состоянию в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	требования организаций, уполномоченных в сфере защиты информации, и Уметь: - использовать теоретический материал в педагогической, научно-исследовательской, творческой, управленческой деятельностях Владеть: - углубленными навыками организации технологического процесса защиты информации; - навыками разработки новых методик, технологических процессов в области защиты информации.

7.3 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Таблица 7.3 – Паспорт комплекта оценочных средств для текущего контроля

№ п/п	Раздел (тема) дисциплины	Код контролируемой компетенции (или её части)	Технология формирования	Оценочные средства		Описание шкал оценивания
				наименование	№ заданий	
1	2	3	4	5	6	7
5 семестр						
1	Введение в дисциплину «Организационное и правовое обеспечение информационной безопасности»	ОК-4	Лекция, СРС	ВУО	1-10	Согласно табл. 7.2
2	Понятие «организационная защита информации». Правовые основы организационной защиты информации	ОК-4; ОПК-5	Лекция, СРС	ВУО	11-20	Согласно табл. 7.2
3	Концептуальные положения организационного обеспечения информационной безопасности объектов защиты	ОК-4; ОПК-5; ПК-10	Лекция, СРС	ВУО	21-30	Согласно табл. 7.2
4	Организационные источники и каналы утечки информации	ПК-10	Лекция; практическое занятие	ВУО КВЗПР	31-40 1-10	Согласно табл. 7.2
5	Порядок допуска к конфиденциальной информации	ОК-4, ОПК-5	Лекция, СРС	ВУО	41-50	Согласно табл. 7.2
6	Технические средства защиты информации	ПК-15	Лекция; практическое занятие	ВУО КВЗПР	51-60 1-10	Согласно табл. 7.2
7	Допуск и доступ к конфиденциальной информации и документам	ОК-4, ОПК-5, ПК-8	Лекция, СРС	ВУО	61-70	Согласно табл. 7.2
8	Государственная тайна и порядок отнесения к ней информации	ОК-4, ОПК-5, ПК-8	Лекция, СРС	ВУО	61-70	Согласно табл. 7.2
9	Организация засекречивания и рассекречивания сведений, документов и продукции	ОК-4, ОПК-5, ПК-8, ПК-15	Лекция, СРС	ВУО	71-80	Согласно табл. 7.2
10	Защита персональных данных	ОК-4, ОПК-5, ПК-8	Лекция; практическое занятие	ВУО КВЗПР	81-90 1-10	Согласно табл. 7.2

11	Организация автоматизированной обработки информации, содержащей персональные данные	ПК-8, ПК-10, ПК-15	Лекция, СРС	ВУО	91-100	Согласно табл. 7.2
12	Разработка организационно-распорядительной документации для объекта информатизации	ОК-4, ОПК-5, ПК-8	Лекция; практическое занятие	ВУО КВЗПР	101-110 1-10	Согласно табл. 7.2
13	Анализ эффективности применения средств защиты информации на объекте информатизации	ОК-4, ОПК-5, ПК-8, ПК-10	Лекция; СРС	ВУО	111-120	Согласно табл. 7.2
14	Коммерческая тайна и порядок её определения	ОК-4, ОПК-5	Лекция, СРС	ВУО	121-130	Согласно табл. 7.2
6 семестр						
15	Организация работ с информацией, составляющей коммерческую тайну	ОК-4, ОПК-5, ПК-8, ПК-15	Лекция; практическое занятие	ВУО КВЗПР	121-130 1-10	Согласно табл. 7.2
16	Подбор персонала на должности, связанные с работой с информацией ограниченного доступа	ОК-4	Лекция, СРС	ВУО	131-140	Согласно табл. 7.2
17	Организация внутриобъектового режима	ОК-4, ОПК-5, ПК-15	Лекция; практическое занятие	ВУО КВЗПР	141-150 1-10	Согласно табл. 7.2
18	Требования, предъявляемые к помещениям и хранилищам, в которых ведутся закрытые работы, хранятся документы ограниченного доступа и изделия	ОК-4	Лекция, СРС	ВУО	151-160	Согласно табл. 7.2
19	Организация защиты информации при приеме в организации посетителей командированных лиц и иностранных представителей	ОК-4, ОПК-5, ПК-15	Лекция, СРС	ВУО	161-170	Согласно табл. 7.2
20	Организация охраны объекта. Организация пропускного режима	ОК-4, ПК-15	Лекция; практическое занятие	ВУО КВЗПР	171-180 1-10	Согласно табл. 7.2

21	Организация защиты информации при подготовке и проведении совещаний и переговоров	ОК-4, ОПК-5, ПК-15	Лекция, СРС	ВУО	171-180	Согласно табл. 7.2
22	Организация защиты информации при осуществлении научно-публицистической и рекламной деятельности	ОК-4, ОПК-5, ПК-15	Лекция, СРС	ВУО	181-190	Согласно табл. 7.2
23	Защита информации при представлении ее в средствах массовой информации	ОК-4, ОПК-5, ПК-15	Лекция, СРС	ВУО	191-200	Согласно табл. 7.2
24	Организация аналитической работы по предупреждению утечки конфиденциальной информации	ОК-4, ОПК-5, ПК-10, ПК-15	Лекция, СРС	ВУО	201-210	Согласно табл. 7.2
25	Методы, используемые аналитическими подразделениями служб безопасности, по предупреждению утечки конфиденциальной информации	ОК-4, ОПК-5	Лекция, СРС	ВУО	211-220	Согласно табл. 7.2
26	Методы работы с персоналом, обладающим конфиденциальной информацией	ОК-4, ОПК-5	Лекция, СРС	ВУО	221-230	Согласно табл. 7.2
27	Подготовка лиц, ответственных за обеспечение безопасности информации	ОК-4, ОПК-5	Лекция, СРС	ВУО	231-240	Согласно табл. 7.2
28	Модель угроз информационной безопасности	ОК-4, ОПК-5, ПК-8, ПК-10	Лекция; практическое занятие	ВУО КВЗПР	241-250 1-10	Согласно табл. 7.2

ВУО – вопросы для устного опроса, КВЗПР – контрольные вопросы для защиты практических работ

Примеры типовых контрольных заданий для текущего контроля

Вопросы для устного опроса по теме 1 Введение в дисциплину «Организационное и правовое обеспечение информационной безопасности»

1. Задачи дисциплины "Организационная защита информации".
2. Что понимается под угрозой информационной безопасности.
3. Виды угроз информационной безопасности РФ.
4. Источники угроз информационной безопасности.

Контрольные вопросы для защиты практической работы №1 «Организационные источники и каналы утечки информации».

1. Что включают в себя каналы распространения информации?
2. Как вы понимаете термин «канал несанкционированного получения информации»?
3. В чем отличие третьего лица от злоумышленника?
4. Какие каналы несанкционированного доступа вы знаете?
5. Основные угрозы безопасности информации в компьютерных системах.

Полностью оценочные средства представлены в учебно-методическом комплексе дисциплины.

Типовые задания для промежуточной аттестации

Промежуточная аттестация по дисциплине проводится в форме зачета и экзамена. Экзамен и зачет проводится в форме тестирования (компьютерного).

Для тестирования используются контрольно-измерительные материалы (КИМ) – задания в тестовой форме, составляющие банк тестовых заданий (БТЗ) по дисциплине, утвержденный в установленном в университете порядке.

Проверяемыми на промежуточной аттестации элементами содержания являются темы дисциплины, указанные в разделе 4 настоящей программы. Все темы дисциплины отражены в КИМ в равных долях (%).

Для проверки *знаний* используются вопросы и задания в закрытой форме (с выбором одного или нескольких правильных ответов).

Умения, навыки и компетенции проверяются с помощью задач (ситуационных, производственных или кейсового характера) и различного вида конструкторов. Все задачи являются многоходовыми. Некоторые задачи, проверяющие уровень сформированности компетенций, являются многовариантными. Часть умений, навыков и компетенций прямо не отражена в формулировках задач, но они могут быть проявлены обучающимися при их решении.

В каждый вариант КИМ включаются задания по каждому проверяемому элементу содержания во всех перечисленных выше формах и разного уровня сложности. Такой формат КИМ позволяет объективно определить качество освоения обучающимися основных элементов содержания дисциплины и уровень сформированности компетенций.

7.4 Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций, регулируются следующими нормативными актами университета:

– положение П 02.016 «О балльно-рейтинговой системе оценивания результатов обучения по дисциплинам (модулям) и практикам при освоении обучающимися образовательных программ»;

– методические указания, используемые в образовательном процессе, указанные в списке литературы.

Для *текущего контроля успеваемости* по дисциплине в рамках действующей в университете балльно-рейтинговой системы применяется следующий порядок начисления баллов:

Таблица 7.4 – Порядок начисления баллов в рамках БРС

Форма контроля	Минимальный балл		Максимальный балл	
	балл	примечание	балл	примечание
1	2	3	4	5
5 семестр				
Практическая работа №1 (Организационные источники и каналы утечки информации)	2	Выполнил, доля правильных ответов от 50% до 90%	4	Выполнил, доля правильных ответов от 50% до 90%
Практическая работа №2 (Технические средства защиты информации)	2	Выполнил, доля правильных ответов от 50% до 90%	4	Выполнил, доля правильных ответов от 50% до 90%
Практическая работа №3 (Защита персональных данных)	2	Выполнил, доля правильных ответов от 50% до 90%	4	Выполнил, доля правильных ответов от 50% до 90%
Практическая работа №4 (Разработка организационно-распорядительной документации для объекта информатизации)	2	Выполнил, доля правильных ответов от 50% до 90%	4	Выполнил, доля правильных ответов от 50% до 90%
Устный опрос	16		32	
Итого	24		48	
Посещаемость	0		16	
Экзамен	0		36	
Итого	24		100	
6 семестр				
Практическая работа №5 (Анализ эффективности применения средств защиты информации на объекте информатизации)	2	Выполнил, доля правильных ответов от 50% до 90%	4	Выполнил, доля правильных ответов от 50% до 90%
Практическая работа №6 Организация внутриобъектового режима	2	Выполнил, доля правильных ответов от 50% до 90%	4	Выполнил, доля правильных ответов от 50% до 90%
Практическая работа №7 Организация пропускного режима	2	Выполнил, доля правильных ответов от 50% до 90%	4	Выполнил, доля правильных ответов от 50% до 90%

Практическая работа №8 Разработка модели угроз информационной безопасности	2	Выполнил, доля правильных ответов от 50% до 90%	4	Выполнил, доля правильных ответов от 50% до 90%
Устный опрос	16		32	
Итого	24		48	
Посещаемость	0		16	
Экзамен	0		36	
Итого	24		100	

Для промежуточной аттестации обучающихся, проводимой в виде тестирования, используется следующая методика оценивания знаний, умений, навыков и (или) опыта деятельности. В каждом варианте КИМ - 16 заданий (15 вопросов и одна задача).

Каждый верный ответ оценивается следующим образом:

- задание в закрытой форме –2балла,
- задание в открытой форме – 2 балла,
- задание на установление правильной последовательности – 2 балла,
- задание на установление соответствия – 2 балла,
- решение компетентностно-ориентированной задачи – 6 баллов.

Максимальное количество баллов за тестирование - 36 баллов.

8. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

8.1 Основная учебная литература

1. Корнилова, А. А. Защита персональных данных : учебное пособие : [16+] / А. А. Корнилова, Д. С. Юнусова, А. С. Исмагилова ; Башкирский государственный университет. – Уфа : Башкирский государственный университет, 2020. – 119 с. : ил., табл. – Режим доступа:– URL: https://biblioclub.ru/index.php?page=book&id=611314 . – Библиогр. в кн. – Текст : электронный.

2. Информационная безопасность в цифровом обществе : учебное пособие : [16+] / А. С. Исмагилова, И. В. Салов, И. А. Шагапов, А. А. Корнилова ; Башкирский государственный университет. – Уфа : Башкирский государственный университет, 2019. – 128 с. : табл., ил. – Режим доступа: – URL: https://biblioclub.ru/index.php?page=book&id=611084. – Библиогр. в кн. – Текст : электронный.

3. Моргунов, А. В. Информационная безопасность : учебно-методическое пособие : [16+] / А. В. Моргунов ; Новосибирский государственный технический университет. – Новосибирск : Новосибирский государственный технический университет, 2019. – 83 с. : ил., табл. – Режим доступа: – URL: https://biblioclub.ru/index.php?page=book&id=576726. – Библиогр.: с. 64. – ISBN 978-5-7782-3918-0. – Текст : электронный.

4. Арзуманян, А. Б. Международные стандарты правовой защиты информации и информационных технологий : учебное пособие : [16+] / А. Б. Арзуманян ; Южный федеральный университет. – Ростов-на-Дону ; Таганрог : Южный федеральный университет, 2020. – 140 с. – Режим доступа:– URL: https://biblioclub.ru/index.php?page=book&id=612162. – Библиогр.: с. 129-133. – ISBN 978-5-9275-3546-0. – Текст : электронный.

5. Информационная безопасность в цифровом обществе : учебное пособие : [16+] / А. С. Исмагилова, И. В. Салов, И. А. Шагапов, А. А. Корнилова ; Башкирский государственный университет. – Уфа : Башкирский государственный университет, 2019. – 128 с. : табл., ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=611084 (дата обращения: 17.09.2021). – Библиогр. в кн. – Текст : электронный.

8.2 Дополнительная учебная литература

6. Спеваков А. Г. Основы правового обеспечения информационной безопасности [Текст] : учебное пособие / А. Г. Спеваков, А. П. Фисун ; Юго-Зап. гос. ун-т. - Курск : ЮЗГУ, 2013. - Текст : непосредственный. Ч. 1. - 150 с. : ил., табл. - Имеется электрон. аналог. - Библиогр.: с. 137-149. - ISBN 978-5-7681-08 57-1

7. Спеваков А. Г. Основы правового обеспечения информационной безопасности [Текст] : учебное пособие / А. Г. Спеваков, А. П. Фисун ; Юго-Зап. гос. ун-т. - Курск : ЮЗГУ, 2013. - Текст : непосредственный.

Ч. 2. - 303 с. : ил., табл. - Библиогр.: с. 290-302. - Имеется электрон. аналог. - ISBN 978-5-7681-08 58-8

8.3 Перечень методических указаний

1. Организационно-правовое обеспечение информации [Текст] : методические рекомендации по выполнению практических работ/ Юго-Зап. гос. ун-т; сост.: А.Л. Марухленко. – Курск, 2022. – 14 с. – Библиогр.: с.13.

2. Организационно-правовое обеспечение информационной безопасности [Текст] : методические рекомендации по выполнению самостоятельных работ/ Юго-Зап. гос. ун-т; сост.: А.Л. Марухленко. – Курск, 2022. – 19 с. – Библиогр.: с.19.

9 Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. Федеральная служба безопасности [официальный сайт]. Режим доступа: http://www.fsb.ru/
2. Федеральная служба по техническому и экспортному контролю [официальный сайт]. Режим доступа: http://fstec.ru/

10 Методические указания для обучающихся по освоению дисциплины

Основными видами аудиторной работы студента при изучении дисциплины «Организационное и правовое обеспечение информационной безопасности» являются лекции и практические занятия. Студент не имеет права пропускать занятия без уважительных причин.

На лекциях излагаются и разъясняются основные понятия темы, связанные с ней теоретические и практические проблемы, даются рекомендации для самостоятельной работы. В ходе лекции студент должен внимательно слушать и конспектировать материал.

Изучение наиболее важных тем или разделов дисциплины завершают практические занятия, которые обеспечивают: контроль подготовленности студента; закрепление учебного материала; приобретение опыта устных публичных выступлений, ведения дискуссии, в том числе аргументации и защиты выдвигаемых положений и тезисов.

Практическому занятию предшествует самостоятельная работа студента, связанная с освоением материала, полученного на лекциях, и материалов, изложенных в учебниках и учебных пособиях, а также литературе, рекомендованной преподавателем.

Качество учебной работы студентов преподаватель оценивает по результатам тестирования, собеседования и результатам докладов.

Преподаватель уже на первых занятиях объясняет студентам, какие формы обучения следует использовать при самостоятельном изучении дисциплины «Организационное и правовое обеспечение информационной безопасности»: конспектирование учебной литературы и лекции, составление словарей понятий и терминов и т. п.

В процессе обучения преподаватели используют активные формы работы со студентами: чтение лекций, привлечение студентов к творческому процессу на лекциях, промежуточный контроль путем отработки студентами пропущенных лекции, участие в групповых и индивидуальных консультациях (собеседовании). Эти формы способствуют выработке у студентов умения работать с учебником и литературой. Изучение литературы составляет значительную часть самостоятельной работы студента. Это большой труд, требующий усилий и желания студента. В самом начале работы над книгой важно определить цель и направление этой работы. Прочитанное следует закрепить в памяти. Одним из приемов закрепление освоенного материала является конспектирование, без которого немыслима серьезная работа над литературой. Систематическое конспектирование помогает научиться правильно, кратко и четко излагать своими словами прочитанный материал.

Самостоятельную работу следует начинать с первых занятий. От занятия к занятию нужно регулярно прочитывать конспект лекций, знакомиться с соответствующими разделами учебника, читать и конспектировать литературу по каждой теме дисциплины. Самостоятельная работа дает студентам возможность равномерно распределить нагрузку, способствует более глубокому и качественному усвоению учебного материала. В случае необходимости студенты обращаются за консультацией к преподавателю по вопросам дисциплины «Организационное и правовое обеспечение информационной безопасности» с целью усвоения и закрепления компетенций.

Основная цель самостоятельной работы студента при изучении дисциплины «Организационное и правовое обеспечение информационной безопасности» - закрепить теоретические знания, полученные в процессе лекционных занятий, а также сформировать практические навыки самостоятельного анализа особенностей дисциплины.

11 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем (при необходимости)

Microsoft Office 2016.Лицензионный договор №S0000000722 от 21.12.2015 г. с ООО «АйТи46», лицензионный договор №K0000000117 от 21.12.2015 г. с ООО «СМСКанал»,

Kaspersky Endpoint Security Russian Edition, лицензия 156A-140624-192234,

Windows 7, договор IT000012385

12 Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Учебная аудитория для проведения занятий лекционного типа и лаборатории кафедры информационной безопасности, оснащенные учебной мебелью: столы, стулья для обучающихся; стол, стул для преподавателя; доска. Проекционный экран на штативе; Мультимедиацентр: ноут-букASUSX50VLPMD-T2330/14"/1024Mb/ 160Gb/сумка/проектор inFocusIN24+

13 Особенности реализации дисциплины для инвалидов и лиц с ограниченными возможностями здоровья

При обучении лиц с ограниченными возможностями здоровья учитываются их индивидуальные психофизические особенности. Обучение инвалидов осуществляется также в соответствии с индивидуальной программой реабилитации инвалида (при наличии).

Для лиц с нарушением слуха возможно предоставление учебной информации в визуальной форме (краткий конспект лекций; тексты заданий, напечатанные увеличенным шрифтом), на аудиторных занятиях допускается присутствие ассистента, а также сурдопереводчиков и тифлосурдопереводчиков. Текущий контроль успеваемости осуществляется в письменной форме: обучающийся письменно отвечает на вопросы, письменно выполняет практические задания. Промежуточная аттестация для лиц с нарушениями слуха проводится в письменной форме, при этом используются общие критерии оценивания. При необходимости время подготовки к ответу может быть увеличено.

Для лиц с нарушением зрения допускается аудиальное предоставление информации, а также использование на аудиторных занятиях звукозаписывающих устройств (диктофонов и т.д.). Допускается присутствие на занятиях ассистента (помощника), оказывающего обучающимся необходимую техническую помощь. Текущий контроль успеваемости осуществляется в устной форме. При проведении промежуточной аттестации для лиц с нарушением зрения тестирование может быть заменено на устное собеседование по вопросам.

Для лиц с ограниченными возможностями здоровья, имеющих нарушения опорно-двигательного аппарата, на аудиторных занятиях, а также при проведении процедур текущего контроля успеваемости и промежуточной аттестации могут быть предоставлены необходимые технические средства (персональный компьютер, ноутбук или другой гаджет); допускается присутствие ассистента (ассистентов), оказывающего обучающимся необходимую техническую помощь (занять рабочее место, передвигаться по аудитории, прочитать задание, оформить ответ, общаться с преподавателем).

14. Лист дополнений и изменений, внесенных в рабочую программу дисциплины

Номер изменения	Номера страниц				Всего страниц	Дата	Основание для изменения и подпись лица, проводившего
	изменённых	заменённых	аннулированных	новых			