федеральное государственное бюджетное образовательное учреждение высшего образования «Мордовский государственный педагогический

университет имени М.Е. Евсевьева»

Физико-математический факультет

Кафедра информатики и вычислительной техники

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Организационное и правовое обеспечение информационной безопасности

Направление подготовки: 44.03.05 Педагогическое образование (с двумя профилями подготовки)
Профиль подготовки: Менеджмент в образовании. Информационная безопасность в образовании
Форма обучения: Очная

Разработчик: Голяев С.С., кандидат педагогических наук, доцент кафедры информатики и вычислительной техники

Программа рассмотрена и утверждена на заседании кафедры информатики и вычислительной техники, протокол № 3 от 21.10.2021 года

Зав. кафедрой_____Зубрилин А. А.

1. Цель и задачи изучения дисциплины

Цель изучения дисциплины - сформировать единый подход к вопросам применения норм права при защите информации ограниченного доступа, обеспечить углубленное изучение правовых и научных источников по данной тематике, рассмотреть наиболее проблемные вопросы теории и правоприменительной практики, касающиеся обеспечения информационной безопасности. Применять нормативные правовые акты, реализовывать нормы материального и процессуального права в профессиональной деятельности с использование ИТ.

Задачи дисциплины:

- изучение информационного законодательства РФ;
- изучение правил лицензирования и сертификации в области защиты
- информации;
- изучение международного законодательства в области защиты информации;
- умение построения систем организационной защиты образовательных объектов;

том числе воспитательные задачи:

- формирование мировоззрения и системы базовых ценностей личности;
- формирование основ профессиональной культуры обучающегося в условиях трансформации области профессиональной деятельности.

1. Место дисциплины в структуре ОПОП ВО

К.М.06.ДВ.01.01 «Организационное и правовое обеспечение информационной безопасности» относится к дисциплинам по выбору обязательной части учебного плана.

Изучению дисциплины «Защита персональных данных» предшествует освоение дисциплин (практик):

ИКТ и медиаинформационная грамотность;

Безопасность образовательных Интернет-систем;

Безопасность информационных систем и баз данных;

Программно-аппаратные средства защиты информации.

Область профессиональной деятельности,на которую ориентирует дисциплина «Защита персональных данных», включает: 01 Образование и наука (в сфере дошкольного, начального общего, основного общего, среднего общего образования, профессионального обучения, профессионального образования, дополнительного образования).

Типы задач и задачи профессиональной деятельности, к которым готовится обучающийся, определены учебным планом.

2. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

Компетенция в соответствии ФГОС ВО	
Индикаторы достижения компетенций	**Образовательные результаты**
ПК-11. Способен использовать теоретические и практические знания для постановки и решения исследовательских задач в предметной области (в соответствии с профилем и уровнем обучения) и в области образования.	
ПК-11.2 Проектирует и решает исследовательские задачи в предметной области в соответствии с профилем и уровнем обучения и в области образования.	знать: - базовые понятия и определения, используемые в области информационной безопасности; - Принципы и методы организации информационной безопасности; уметь: - использовать нормативно-правовую базу и информационные ресурсы в организации защиты информации; - разрабатывать документацию в области информационной безопасности; владеть: - навыками применения различного инструментария при решении задач по защите информации; - разработки и реализации методов защиты информации.

УК-2. Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений.	
УК-2.1. Определяет совокупность взаимосвязанных задач, обеспечивающих достижение поставленной цели, исходя из действующих правовых норм.	знать: - базовые понятия и определения, используемые в информационной безопасности; - основную нормативно-правовую базу в области информационной безопасности; уметь: - ориентироваться в дисциплинах, являющихся составными частями информационной безопасности; - пользоваться специальной документацией и литературой в изучаемой области; владеть: - навыками организации мероприятий по информационной безопасности; - разработки и реализации образовательных программ.

3. Объем дисциплины и виды учебной работы

Вид учебной работы	Всего часов	Седьмой семестр
Контактная работа (всего)	**52**	**52**
Лекции	**18**	18
Лабораторные	**34**	34
Самостоятельная работа (всего)	**92**	**92**
Виды промежуточной аттестации		
Экзамен		
Общая трудоемкость часы	**144**	**144**
Общая трудоемкость зачетные единицы	**4**	**4**

4. Содержание дисциплины

4.1. Содержание разделов дисциплины

Раздел 1. Информация как объект правового регулирования. Правовые режимы защиты конфиденциальной информации.

Понятие информации и ее основные положения. Подходы к определению понятия «информация». Двуединство документированной информации с правовой точки зрения. Структура информационной сферы. Виды информации, определенные законодательством РФ. Общедоступная информация и информация ограниченного доступа. Нормативная база, регулирующая область соответствующей информации ограниченного доступа. Конфиденциальная информация и ее виды. Правовые основы защиты служебной тайны. Нормативно-правовые акты и положения Гражданского кодекса РФ, регулирующие правовую защиту служебной тайны. Правовые основы защиты коммерческой тайны. Охрана коммерческой тайны в трудовых отношениях. Тайна следствия и судопроизводства. Процессуальные тайны. Тайна совещания судей. Следственная тайна.

Раздел 2. Лицензирование и сертификация в информационной сфере. Защита интеллектуальной собственности. Защита информации в компьютерных системах.

Понятие лицензирования по российскому законодательству и виды деятельности в информационной сфере, подлежащих лицензированию. Участники лицензионных отношений в сфере защиты информации. Специальные экспертизы и государственная аттестация

руководителей. Органы лицензирования и их полномочия. Государственный контроль за соблюдением лицензиатом условий ведения деятельности. Понятие сертификации по российскому законодательству. Правовая регламентация сертификационной деятельности в области защиты информации. Электронный документ как доказательство.

Понятие интеллектуальной собственности. Понятие авторского права. Объекты и субъекты авторского права. Смежные права. Интеллектуальная собственность в сети Интернет. Понятие патентного права. Объекты и субъекты патентного права. Понятия изобретения. Объекты изобретения, связанные с электронно-вычислительной техникой и информацией. Защита прав патентообладателей и авторов изобретений. Особенности договорных отношений в области информационной безопасности. Особенности трудовых отношений в сфере защиты информации.

Безопасность и целостность данных информационных систем и технологий. Угрозы информации в компьютерных системах. Обеспечение целостности информации в компьютерных системах. Защита персонального компьютера от несанкционированного доступа. Защита информации от копирования.

5.2 Содержание дисциплины: Лекции (18 ч.)

Раздел 1. Информация как объект правового регулирования. Правовые режимы защиты конфиденциальной информации. (8 ч.)

Тема1. Информация как объект правового регулирования. (2 ч.)

Понятие информации и ее основные положения. Подходы к определению понятия «информация». Двуединство документированной информации с правовой точки зрения. Структура информационной сферы. Понятие среды. Типы сред. Виды информации, определенные законодательством РФ. Общедоступная информация и информация ограниченного доступа. Нормативная база, регулирующая область соответствующей информации ограниченного доступа.

Тема 2. Законодательство в области информационной безопасности. (2 ч.)

Законодательство РФ в области информации и информационной безопасности: Конституция РФ, Законы РФ «О безопасности», «О правовой охране программ для электронных вычислительных машин и баз данных», «Об авторском праве и смежных правах», «О государственной тайне», Федеральные законы РФ «Об электронной цифровой подписи», «Об информации, информационных технологиях и защите информации», «О персональных данных», «О связи», «О коммерческой тайне», «Об оперативно-розыскной деятельности», «Об обязательном экземпляре документов».

Тема 3. Правовой режим защиты государственной тайны. (2 ч.)

Понятие правового режима защиты государственной тайны. Реквизиты носителей сведений, составляющих государственную тайну. Законодательные и иные нормативно-правовые акты РФ, регулирующие защиту государственной тайны. Обеспечение защиты государственной тайны, органы защиты. Государственные органы защиты государственной тайны и их компетенция.

Организация доступа должностного лица или гражданина к сведениям, составляющим государственную тайну. Допуск предприятий, учреждений и организаций к проведению работ, связанных с использованием сведений, составляющих государственную тайну. Меры по обеспечению сохранности сведений, составляющих государственную тайну.

Тема 4. Правовые режимы защиты конфиденциальной информации. (2 ч.)

Конфиденциальная информация и ее виды. Правовые основы защиты служебной тайны. Нормативно-правовые акты и положения Гражданского кодекса РФ, регулирующие правовую защиту служебной тайны. Правовые основы защиты коммерческой тайны. Охрана коммерческой тайны в трудовых отношениях. Тайна следствия и судопроизводства. Процессуальные тайны. Тайна совещания судей. Следственная тайна.

Раздел 2. Лицензирование и сертификация в информационной сфере. Защита интеллектуальной собственности. Защита информации в компьютерных системах. (10 ч.)

Тема 5. Лицензирование и сертификация в информационной сфере. (2 ч.)

Понятие лицензирования по российскому законодательству и виды деятельности в информационной сфере, подлежащих лицензированию. Участники лицензионных отношений в сфере защиты информации. Специальные экспертизы и государственная аттестация руководителей. Органы лицензирования и их полномочия. Государственный контроль за соблюдением лицензиатом условий ведения деятельности. Понятие сертификации по российскому законодательству. Правовая регламентация сертификационной деятельности в области защиты информации. Электронный документ как доказательство.

Тема 6. Защита интеллектуальной собственности. (2 ч.)

Понятие интеллектуальной собственности. Понятие авторского права. Объекты и субъекты авторского права. Смежные права. Интеллектуальная собственность в сети Интернет. Понятие патентного права. Объекты и субъекты патентного права. Понятия изобретения. Объекты изобретения, связанные с электронно-вычислительной техникой и информацией. Защита прав патентообладателей и авторов изобретений. Особенности договорных отношений в области информационной безопасности. Особенности трудовых отношений в сфере защиты информации.

Тема 7. Защита информации в компьютерных системах. (2 ч.)

Безопасность и целостность данных информационных систем и технологий. Угрозы информации в ПЭВМ. Обеспечение целостности информации в ПЭВМ. Защита ПЭВМ от несанкционированного доступа. Защита информации от копирования. Защита информации от вредоносных закладок.

Тема 8. Практические вопросы документа и документооборота в информационных технологиях. (2 ч.)

Конституционно-правовая основа формирования и использование информационных ресурсов.

Тема 9. Международное законодательство в области защиты информации. (2 ч.)

Законодательство РФ об участии в международном информационном обмене информации. Национальные законодательства о компьютерных правонарушениях и защите информации. Международное сотрудничество в области борьбы с компьютерной преступностью.

5.3 Содержание дисциплины: Практические занятия (34 ч.)

Раздел 1. Информация как объект правового регулирования. Правовые режимы защиты конфиденциальной информации. (16 ч.)

Тема1. Информация как объект правового регулирования. (4 ч.)

Понятие информации и ее основные положения. Подходы к определению понятия «информация». Двуединство документированной информации с правовой точки зрения. Структура информационной сферы. Понятие среды. Типы сред. Виды информации, определенные законодательством РФ. Общедоступная информация и информация ограниченного доступа. Нормативная база, регулирующая область соответствующей информации ограниченного доступа.

Тема 2. Законодательство в области информационной безопасности. (4 ч.)

Законодательство РФ в области информации и информационной безопасности: Конституция РФ, Законы РФ «О безопасности», «О правовой охране программ для электронных вычислительных машин и баз данных», «Об авторском праве и смежных правах», «О государственной тайне», Федеральные законы РФ «Об электронной цифровой подписи», «Об информации, информационных технологиях и защите информации», «О персональных данных», «О связи», «О коммерческой тайне», «Об оперативно-розыскной деятельности», «Об обязательном экземпляре документов».

Тема 3. Правовой режим защиты государственной тайны. (4 ч.)

Понятие правового режима защиты государственной тайны. Реквизиты носителей сведений, составляющих государственную тайну. Законодательные и иные нормативно-правовые акты РФ, регулирующие защиту государственной тайны. Обеспечение защиты государственной тайны, органы защиты. Государственные органы защиты государственной тайны и их компетенция.

Организация доступа должностного лица или гражданина к сведениям, составляющим государственную тайну. Допуск предприятий, учреждений и организаций к проведению работ, связанных с использованием сведений, составляющих государственную тайну. Меры по обеспечению сохранности сведений, составляющих государственную тайну.

Тема 4. Правовые режимы защиты конфиденциальной информации. (4 ч.)

Конфиденциальная информация и ее виды. Правовые основы защиты служебной тайны. Нормативно-правовые акты и положения Гражданского кодекса РФ, регулирующие правовую защиту служебной тайны. Правовые основы защиты коммерческой тайны. Охрана коммерческой тайны в трудовых отношениях. Тайна следствия и судопроизводства. Процессуальные тайны. Тайна совещания судей. Следственная тайна.

Раздел 2. Лицензирование и сертификация в информационной сфере. Защита интеллектуальной собственности. Защита информации в компьютерных системах. (18 ч.)

Тема 5. Лицензирование и сертификация в информационной сфере. (2 ч.)

Понятие лицензирования по российскому законодательству и виды деятельности в информационной сфере, подлежащих лицензированию. Участники лицензионных отношений в сфере защиты информации. Специальные экспертизы и государственная аттестация руководителей. Органы лицензирования и их полномочия. Государственный контроль за соблюдением лицензиатом условий ведения деятельности. Понятие сертификации по российскому законодательству. Правовая регламентация сертификационной деятельности в области защиты информации. Электронный документ как доказательство.

Тема 6. Защита интеллектуальной собственности. (4 ч.)

Понятие интеллектуальной собственности. Понятие авторского права. Объекты и субъекты авторского права. Смежные права. Интеллектуальная собственность в сети Интернет. Понятие патентного права. Объекты и субъекты патентного права. Понятия изобретения. Объекты изобретения, связанные с электронно-вычислительной техникой и информацией. Защита прав патентообладателей и авторов изобретений. Особенности договорных отношений в области информационной безопасности. Особенности трудовых отношений в сфере защиты информации.

Тема 7. Защита информации в компьютерных системах. (4 ч.)

Безопасность и целостность данных информационных систем и технологий. Угрозы информации в ПЭВМ. Обеспечение целостности информации в ПЭВМ. Защита ПЭВМ от несанкционированного доступа. Защита информации от копирования. Защита информации от вредоносных закладок.

Тема 8. Практические вопросы документа и документооборота в информационных технологиях. (4 ч.)

Конституционно-правовая основа формирования и использование информационных ресурсов.

Тема 9. Международное законодательство в области защиты информации. (4 ч.)

Законодательство РФ об участии в международном информационном обмене информации. Национальные законодательства о компьютерных правонарушениях и защите информации. Международное сотрудничество в области борьбы с компьютерной преступностью.

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

6.1 Вопросы и задания для самостоятельной работы

Седьмой семестр (92 ч.)

Раздел 1. Информация как объект правового регулирования. Правовые режимы защиты конфиденциальной информации. (46 ч.)

Вид СРС: *Подготовка к практическим занятиям Перечень контрольных вопросов по модулю " Информация как объект правового регулирования. Правовые режимы защиты конфиденциальной информации "

1. Нормативно-правовая база защиты информации в РФ
2. Основное содержание концепции информационной безопасности РФ
3. Основное содержание закона РФ "Об информации, информатизации и защите информации"
4. Понятие информации, форма представления (двоичная система) и единица измерения (бит)
5. Цели защиты информации, основные угрозы информации
6. Модель информационной безопасности
7. Классификация информации по уровню конфиденциальности
8. Основные направления и методы защиты информации
9. Источники и классификация угроз
10. Технические средства защиты информации
11. Основные этапы развития криптографических методов защиты
12. Шифр простой замены. Способы задания, основные свойства
13. Шифр гаммирования.

Вид СРС: *Работа с электронными ресурсами и информационными системами
Пройти дистанционное обучение по указанному курсу.
Основы информационной безопасности : учебник / В. Ю. Рогозин, И. Б. Галушкин, В. Новиков, С. Б. Вепрев ; Академия Следственного комитета Российской Федерации. – Москва : Юнити-Дана : Закон и право, 2018. – 287 с. : ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=562348. – Библиогр. в кн. – ISBN 978-5-238-02857-6. – Текст : электронный.

В основе изложения анализ и систематизация современного уровня развития нормативной правовой базы Российской Федерации в области информационной безопасности (защиты информации).

Рассматриваются основы государственной политики в области информационной безопасности, методы обеспечения информационной безопасности, методы и средства ведения информационной войны. Уделяется внимание организационной и технической защите информации, защите информационных процессов в компьютерных и телекоммуникационных системах.

Рассматривается юридическая ответственность за нарушение норм в области информационной безопасности.

Вид СРС: *Подготовка к контрольной работе. С использованием информационно- правочной системы «Гарант» решите и обоснуйте решение следующих задач.

Задача 1. При проведении проверки первичной документации по учёту труда и его оплаты было обнаружено, что в личном деле одного из референтов федерального агентства отсутствуют сведения из налоговой службы об имущественном положении, а также данные дактилоскопической регистрации. Инспектор труда потребовал предъявить указанные документы.

Правомерны ли требования инспектора труда?

Задача 2. Семенов обратился в ОАО «Решение» с просьбой принять его на работу в качестве ведущего специалиста отдела продаж. Начальник кадровой службы направил запрос в психоневрологический диспансер по месту жительства Семенова, в котором просил сообщить

сведения о состоянии психологического здоровья и о фактах обращения Семенова за психиатрической помощью, поскольку организации необходимо решить вопрос о пригодности Семенова для выполнения работы.

Законны ли действия начальника кадровой службы?

Задача 3. Начальник отдела кадров Дубовцева распространяла среди своих знакомых сведения об образовании и данные медицинского осмотра заведующего складом Мамонтова, которые, по её мнению, порочили его честь и достоинство. Мамонтов потребовал от директора организации защитить его персональные данные от неправомерного использования и привлечь Дубовцеву к административной ответственности. Директор оштрафовал Дубовцеву на сумму, равную трем минимальным размера оплаты труда.

Законно ли действие работодателя? Какие виды юридической ответственности установлены законодательством России за нарушение норм, регулирующих сбор, обработку, хранение, распространение и защиту персональных данных работника.

Задача 4. Работник Падерин, ознакомившись со своими персональными данными, хранящимися в организации, потребовал от директора ООО «Аквамарин» исключить устаревшие и исправить неверные, а также известить всех лиц, которым они ранее были сообщены, обо всех исправлениях или дополнениях. Директор не выполнил требования работника.

Правомерен ли отказ директора? Какие права по защите своих персональных данных, хранящихся у работодателя, закон предоставляет работнику?

Раздел 2. Лицензирование и сертификация в информационной сфере. Защита интеллектуальной собственности. Защита информации в компьютерных системах. (46 ч.)

Вид СРС: *Подготовка к практическим занятиям Перечень контрольных вопросов по модулю " Лицензирование и сертификация в информационной сфере. Защита интеллектуальной собственности. Защита информации в компьютерных системах."

1. Классификация криптографических методов защиты по надежности.
2. Блоковые шифры.
3. Нормативно-правовые аспекты защиты информации.
4. Шифрование с открытым ключом
5. Электронная цифровая подпись (способы формирования проверки; нормативно-правовая база применения ЭЦП в РФ)
6. Кэш-функция
7. Классификация вирусов
8. Бот-неты
9. Классификация угроз
10. Классификация атак
11. Отличие программ-шпионов от троянских коней
12. Брандмауэры
13. Отличие аутентификации от идентификации.

Вид СРС: *Работа с электронными ресурсами и информационными системами

Пройти дистанционное обучение по указанному курсу.

Петренко, В. И. Защита персональных данных в информационных системах : учебное пособие / В. И. Петренко ; Северо-Кавказский федеральный университет. – Ставрополь : Северо-Кавказский Федеральный университет (СКФУ), 2016. – 201 с. : схем. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=459205. – Текст : электронный.

Пособие предоставляет собой курс лекций, способствующих приобретению необходимых знаний для обеспечения безопасности персональных данных, в нем рассмотрены основные термины и законодательство Российской Федерации в данной предметной области. Приведены этапы построения системы защиты персональных данных.

Вид СРС: *Подготовка к контрольной работе. С использованием информационно-справочной системы «Гарант» решите и обоснуйте решение следующих задач.

Задача 5. Перевалов обратился в центр занятости по месту жительства в целях поиска подходящей работы. Инспектор центра занятости потребовал от гражданина предоставить сведения о последнем месте работы, о составе его семьи, его религиозных убеждениях и принадлежности к политическим партиям. Считая такие требования незаконными, Перевалов обратился с жалобой к руководителю центра занятости.

Законны ли требования инспектора. Какое решение по жалобе должен принять руководитель центра занятости?

Задача 6. 20.01.2015 менеджер проектов ООО «Ответ» Фалалеева сделала запрос о предоставлении персональных данных юриста ЗАО «Квадратный метр» Оленевой, в связи с осуществлением совместного проекта. Директор ЗАО «Квадратный метр» без согласования с Оленевой предоставил запрашиваемые данные.

Правомерны ли действия директора ЗАО? Какие требования установлены для передачи персональных данных работника?

Задача 7. В ОАО «Решение» было разработано и утверждено приказом директора Положение о порядке обработки и хранения персональных данных работников. Директор поручил своему заместителю ознакомить с положением всех работников под расписку.

Правомерно ли действие директора ОАО? Кто по законодательству имеет право вырабатывать меры защиты персональных данных работников, порядок их сбора, хранения и использования?

Задача 8. Администрация МУП г. Ижевска «Банно-прачечный комбинат» обратилась в органы ФСБ России с просьбой предоставить необходимые персональные данные на работника МУП Шатунова.

Законно ли обращение администрации? Какой порядок получения персональных данных работника установлен ТК РФ?

6. Тематика курсовых работ(проектов)

Курсовые работы (проекты) по дисциплине не предусмотрены.

7. Оценочные средства

8.1 Компетенции и этапы формирования

№ п/п	Оценочные средства	Компетенции, этапы их формирования
	Социально-гуманитарный модуль	УК-2
1	Предметно-методический модуль	УК-2, ПК-11.
3	Учебно-исследовательский модуль	ПК-11.

8.2 Показатели и критерии оценивания компетенций, шкалы оценивания

Шкала, критерии оценивания и уровень сформированности компетенции			
2 (не зачтено) ниже порогового	3 (зачтено) пороговый	4 (зачтено) базовый	5 (зачтено) повышенный
ПК-11 Способен использовать теоретические и практические знания для постановки и решения исследовательских задач в предметной области (в соответствии с профилем и уровнем обучения) и в области образования			
ПК-11.1 Использует теоретические и практические знания для постановки и решения исследовательских задач в предметной области в соответствии с профилем и уровнем обучения и в области образования.			
Не способен использовать теоретические и практические знания для постановки и решения исследовательских задач в предметной области в	В целом успешно, но бессистемно Использует теоретические и практические знания для постановки и решения исследовательских задач в предметной	В целом успешно, но с отдельными недочетами Использует теоретические и практические знания для постановки и решения исследовательских	Способен в полном объеме использовать теоретические и практические знания для постановки и решения исследовательских задач в предметной области в соответствии

соответствии с профилем и уровнем обучения и в области образования.	области в соответствии с профилем и уровнем обучения и в области образования.	задач в предметной области в соответствии с профилем и уровнем обучения и в области образования.	с профилем и уровнем обучения и в области образования.
УК-2. Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений.			
УК-2.1. Определяет совокупность взаимосвязанных задач, обеспечивающих достижение поставленной цели, исходя из действующих правовых норм.			
Не способен определять совокупность взаимосвязанных задач, обеспечивающих достижение поставленной цели, исходя из действующих правовых норм.	В целом успешно, но бессистемно определяет совокупность взаимосвязанных задач, обеспечивающих достижение поставленной цели, исходя из действующих правовых	В целом успешно, но с отдельными недочетами определяет совокупность взаимосвязанных задач, обеспечивающих достижение поставленной цели, исходя из действующих правовых норм.	Способен в полном объеме определять совокупность взаимосвязанных задач, обеспечивающих достижение поставленной цели, исходя из действующих правовых норм.

Уровень сформированности компетенции	Шкала оценивания для промежуточной аттестации	Шкала оценивания по БРС
	Экзамен (дифференцированный зачет)	
Повышенный	5 (отлично)	90 – 100%
Базовый	4 (хорошо)	76 – 89%
Пороговый	3 (удовлетворительно)	60 – 75%
Ниже порогового	2 (неудовлетворительно)	Ниже 60%

8.2.1 Вопросы промежуточной аттестации Седьмой семестр (Зачет, ПК-11.1, УК-2.1)

14. Нормативно-правовая база защиты информации в РФ.
15. Основное содержание концепции информационной безопасности РФ.
16. Основное содержание закона РФ "Об информации, информатизации и защите информации".
17. Понятие информации, форма представления (двоичная система) и единица измерения (бит).
18. Цели защиты информации, основные угрозы информации.
19. Модель информационной безопасности.
20. Классификация информации по уровню конфиденциальности.
21. Основные направления и методы защиты информации.
22. Источники и классификация угроз.
23. Технические средства защиты информации.
24. Основные этапы развития криптографических методов защиты.
25. Шифр простой замены. Способы задания, основные свойства.
26. Шифр гаммирования.
14. Классификация криптографических методов защиты по надежности.

15. Блоковые шифры.
16. Нормативно-правовые аспекты защиты информации.
17. Шифрование с открытым ключом.
18. Электронная цифровая подпись (способы формирования проверки; нормативно-правовая база применения ЭЦП в РФ).
19. Кэш-функция.
20. Классификация вирусов.
21. Бот-неты.
22. Классификация угроз.
23. Классификация атак.
24. Отличие программ-шпионов от троянских коней.
25. Брандмауэры.
26. Отличие аутентификации от индентификации.

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

Промежуточная аттестация проводится в форме зачета.
Зачет по дисциплине или ее части имеет цель оценить сформированность компетенций, теоретическую и практическую подготовку студента, его способность к творческому мышлению, приобретенные им навыки самостоятельной работы, умение синтезировать полученные знания и применять их при решении практических задач.

Устный ответ на зачете
При определении уровня достижений студентов на зачете необходимо обращать особое внимание на следующее:
– дан полный, развернутый ответ на поставленный вопрос;
– показана совокупность осознанных знаний об объекте, проявляющаяся в свободном оперировании понятиями, умении выделить существенные и несущественные его признаки, причинно-следственные связи;
– знание об объекте демонстрируется на фоне понимания его в системе данной науки и междисциплинарных связей;
– ответ формулируется в терминах науки, изложен грамотным литературным языком, логичен, доказателен, демонстрирует авторскую позицию студента;
– теоретические постулаты подтверждаются примерами из практики.

Вопросы и задания для устного опроса
При определении уровня достижений студентов при устном ответе необходимо обращать особое внимание на следующее:
– дан полный, развернутый ответ на поставленный вопрос;
– показана совокупность осознанных знаний об объекте, проявляющаяся в свободном оперировании понятиями, умении выделить существенные и несущественные его признаки, причинно-следственные связи;
– знание об объекте демонстрируется на фоне понимания его в системе данной науки и междисциплинарных связей;
– ответ формулируется в терминах науки, изложен литературным языком, логичен, доказателен, демонстрирует авторскую позицию студента;
– теоретические постулаты подтверждаются примерами из практики.
Оценка за опрос определяется простым суммированием баллов:
Критерии оценки ответа
Правильность ответа – 1 балл.
Всесторонность и глубина (полнота) ответа – 1 балл.
Наличие выводов – 1 балл.
Соблюдение норм литературной речи – 1 балл.
Владение профессиональной лексикой – 1 балл.

Итого: 5 баллов.

Практические задания
При определении уровня достижений студентов при выполнении практического задания необходимо обращать особое внимание на следующее:
– задание выполнено правильно;
– показана совокупность осознанных знаний об объекте, проявляющаяся в свободном оперировании понятиями, умении выделить существенные и несущественные его признаки, причинно-следственные связи;
– умение работать с объектом задания демонстрируется на фоне понимания его в системе данной науки и междисциплинарных связей;
– ответ формулируется в терминах науки, изложен литературным языком, логичен, доказателен, демонстрирует авторскую позицию студента;
– выполнение задания теоретически обосновано.
Оценка за опрос определяется простым суммированием баллов:
Критерии оценки ответа
Правильность выполнения задания – 1 балл.
Всесторонность и глубина (полнота) выполнения – 1 балл.
Наличие выводов – 1 балл.
Соблюдение норм литературной речи – 1 балл.
Владение профессиональной лексикой – 1 балл.
Итого: 5 баллов.

Контрольная работа
Виды контрольных работ: аудиторные, домашние, текущие, экзаменационные, письменные, графические, практические, фронтальные, индивидуальные. Система заданий письменных контрольных работ должна:
– выявлять знания студентов по определенной дисциплине (разделу дисциплины);
– выявлять понимание сущности изучаемых предметов и явлений, их закономерностей;
– выявлять умение самостоятельно делать выводы и обобщения;
– творчески использовать знания и навыки.
Требования к контрольной работе по тематическому содержанию соответствуют устному ответу.
Также контрольные работы могут включать перечень практических заданий.
Критерии оценки ответа
Правильность ответа – 1 балл.
Всесторонность и глубина (полнота) ответа – 1 балл.
Наличие выводов – 1 балл.
Соблюдение норм литературной письменной речи – 1 балл.
Владение профессиональной лексикой – 1 балл.
Итого: 5 баллов.

9. Перечень основной и дополнительной учебной литературы

Основная литература

1. Основы информационной безопасности : учебник / В. Ю. Рогозин, И. Б. Галушкин, В. Новиков, С. Б. Вепрев ; Академия Следственного комитета Российской Федерации. – Москва : Юнити-Дана : Закон и право, 2018. – 287 с. : ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=562348. – Библиогр. в кн. – ISBN 978-5-238-02857-6. – Текст : электронный.

Дополнительная литература

1. Петренко, В. И. Защита персональных данных в информационных системах : учебное пособие / В. И. Петренко ; Северо-Кавказский федеральный университет. – Ставрополь : Северо-Кавказский Федеральный университет (СКФУ), 2016. – 201 с. : схем. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=459205. – Текст : электронный.

10. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

1. https://www.garant.ru – Информационно-правовая система «Гарант [Электронный ресурс] / Режим доступа: https://www.garant.ru.

2. http://www.intuit.ru - Интернет-Университет Информационных Технологий [Электронный ресурс] / Бесплатные учебные курсы по информационным технологиям. – М. : НОУ «ИНТУИТ». - URL: http://www.intuit.ru

11. Методические указания обучающимся по освоению дисциплины (модуля)

При освоении материала дисциплины необходимо:
– спланировать и распределить время, необходимое для изучения дисциплины;
– конкретизировать для себя план изучения материала;
– ознакомиться с объемом и характером внеаудиторной самостоятельной работы для полноценного освоения каждой из тем дисциплины.

Сценарий изучения курса:
– проработайте каждую тему по предлагаемому ниже алгоритму действий;
– регулярно выполняйте задания для самостоятельной работы, своевременно отчитывайтесь преподавателю об их выполнении;
– изучив весь материал, проверьте свой уровень усвоения содержания дисциплины и готовность к сдаче зачета/экзамена, выполнив задания и ответив самостоятельно на примерные вопросы для промежуточной аттестации.

Алгоритм работы над каждой темой:
– изучите содержание темы вначале по лекционному материалу, а затем по другим источникам;
– прочитайте дополнительную литературу из списка, предложенного преподавателем;
– выпишите в тетрадь основные понятия и категории по теме, используя лекционный материал или словари, что поможет быстро повторить материал при подготовке к промежуточной аттестации;
– составьте краткий план ответа по каждому вопросу, выносимому на обсуждение на аудиторном занятии;
– повторите определения терминов, относящихся к теме;
– продумайте примеры и иллюстрации к обсуждению вопросов по изучаемой теме;
– подберите цитаты ученых, общественных деятелей, публицистов, уместные с точки зрения обсуждаемой проблемы;
– продумывайте высказывания по темам, предложенным к аудиторным занятиям.

Рекомендации по работе с литературой:
– ознакомьтесь с аннотациями к рекомендованной литературе и определите основной метод изложения материала того или иного источника;
– составьте собственные аннотации к другим источникам, что поможет при подготовке рефератов, текстов речей, при подготовке к промежуточной аттестации;
– выберите те источники, которые наиболее подходят для изучения конкретной темы;
– проработайте содержание источника, сформулируйте собственную точку зрения на проблему с опорой на полученную информацию.

12. Перечень информационных технологий

Реализация учебной программы обеспечивается доступом каждого студента к информационным ресурсам – электронной библиотеке и сетевым ресурсам Интернет. Для использования ИКТ в учебном процессе используется программное обеспечение, позволяющее осуществлять поиск, хранение, систематизацию, анализ и презентацию информации, экспорт информации на цифровые носители, организацию взаимодействия в реальной и виртуальной образовательной среде.
Индивидуальные результаты освоения дисциплины студентами фиксируются в электронной информационно-образовательной среде университета.

12.1 Перечень программного обеспечения (обновление производится по мере появления новых версий программы)

1. 1С: Университет ПРОФ
2. Microsoft Windows 7 Pro
3. Microsoft Office Professional Plus 2010

12.2 Перечень информационных справочных систем (обновление выполняется еженедельно)

1. Справочная правовая система «КонсультантПлюс» (http://www.consultant.ru)
2. Информационно-правовая система "ГАРАНТ" (http://www.garant.ru)

12.3 Перечень современных профессиональных баз данных

1. Электронная библиотечная система Znanium. com (http://znanium.com/)
2. Единое окно доступа к образовательным ресурсам (http://window.edu.ru)
3. Профессиональная база данных «Открытые данные Министерства образования и науки РФ» (http://xn--- 8sblcdzzacvuc0jbg.xn--80abucjiibhv9a.xn--p1ai/ope

13. Материально-техническое обеспечение дисциплины(модуля)

Для проведения аудиторных занятий необходим стандартный набор специализированной учебной мебели и учебного оборудования, а также мультимедийное оборудование для демонстрации презентаций на лекциях. Для проведения практических занятий, а также организации самостоятельной работы студентов необходим компьютерный класс с рабочими местами, обеспечивающими выход в Интернет.

Индивидуальные результаты освоения дисциплины фиксируются в электронной информационно-образовательной среде университета.

Реализация учебной программы обеспечивается доступом каждого студента к информационным ресурсам – электронной библиотеке и сетевым ресурсам Интернет.

Для использования ИКТ в учебном процессе необходимо наличие программного обеспечения, позволяющего осуществлять поиск информации в сети Интернет, систематизацию, анализ и презентацию информации, экспорт информации на цифровые носители.

Учебная аудитория для проведения учебных занятий.

Учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.

Лаборатория вычислительной техники.

Помещение оснащено оборудованием и техническими средствами обучения.

Основное оборудование:

Автоматизированное рабочее место в составе (системный блок, монитор, клавиатура, мышь, гарнитура, проектор, интерактивная доска), магнитно-маркерная доска.

Лабораторное оборудование: автоматизированное рабочее место (компьютеры – 24 шт.).

Помещение для самостоятельной работы.

Помещение оснащено оборудованием и техническими средствами обучения.

Основное оборудование:

Компьютерная техника с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду университета (персональный компьютер 10 шт.).

Учебно-наглядные пособия:

Презентации.

Помещение для самостоятельной работы.

Читальный зал.

Основное оборудование:

Компьютерная техника с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета (компьютер 10 шт., проектор с экраном 1 шт., многофункциональное устройство 1 шт., принтер 1 шт.)

Учебно-наглядные пособия:

Учебники и учебно-методические пособия, периодические издания, справочная литература.

Стенды с тематическими выставками.