Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Кубанский государственный университет»
Факультет компьютерных технологий и прикладной математики



РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.Б.09 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ

Специальность **45.05.01 Перевод и переводоведение**

Специализация: Лингвистическое обеспечение межгосударственных отношений

Программа подготовки академическая

Форма обучения очная

Квалификация (степень) выпускника лингвист-переводчик

Краснодар 2019

Рабочая программа дисциплины «ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ» составлена в соответствии с Федеральным государственным образовательным стандартом высшего образования (ФГОС ВО) по специальности **45.05.01 Перевод и переводоведение**, утвержденным приказом Министерства науки и высшего образования Российской Федерации № 1290 от 17 октября 2016 г.

Программу составили:

Нестеренко А.Г., канд. физ.-мат. наук, доцент кафедры математического моделирования КубГУ

Еремин А.А, канд. физ.-мат. наук, старший научный сотрудник Института Математики, механики и информатики КубГУ

Рабочая программа дисциплины «Основы информационной безопасности в профессиональной деятельности» утверждена на заседании кафедры математического моделирования
протокол № 11 « 10 » апреля 2019 г.

Заведующий кафедрой математического моделирования акад. РАН, д-р физ.-мат. наук, проф. Бабешко В.А.

Рабочая программа дисциплины «Основы информационной безопасности в профессиональной деятельности» утверждена на заседании кафедры теории и практики перевода
протокол № 10 « 27» мая 2019 г.

Заведующий кафедрой теории и практики перевода д-р филол. наук, проф. Дармодехина А.Н.

Утверждена на заседании учебно-методической комиссии факультета компьютерных технологий и прикладной математики
протокол № 1 « 15» мая 2019 г.

Председатель УМК факультета
канд. эконом. наук, доцент Коваленко А.В.

Рецензенты:

Осипян В.О., д-р физ.-мат. наук, проф. кафедры информационных технологий КубГУ

Бегларян М.Е., канд. физ.-мат. наук, зав. кафедрой СГЕНД СКФ ФГБОУ ВО «РГУП»

1 Цели и задачи изучения дисциплины

1.1 Цель освоения дисциплины

Дисциплина «Основы информационной безопасности в профессиональной деятельности» ставит своей целью освоение основ информационной безопасности. Цели дисциплины соответствуют следующим формируемым компетенциям: ОПК-2, ОПК-5.

Защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера является залогом успешной деятельности при работе с информационными ресурсами. Информационная безопасность является составляющей компьютерной грамотности и основными задачами дисциплины являются: ознакомить студентов с базовыми понятиями информационной безопасности, сформировать представление о принципах защиты от несанкционированного доступа и навыки работы с защищенными программами.

1.2 Задачи дисциплины

Основные **задачи** дисциплины:

– ознакомить студентов с базовыми понятиями информационной безопасности;

– сформировать представление о принципах защиты от несанкционированного доступа и навыки работы с защищенными программами.

1.3 Место дисциплины в структуре образовательной программы

Дисциплина «Основы информационной безопасности в профессиональной деятельности» в базовую часть дисциплин Блока 1. для специальности 45.05.01 Перевод и переводоведение ФГОС ВО.

Данная дисциплина призвана обучить студентов соблюдать в профессиональной деятельности требования правовых актов в области защиты государственной тайны и информационной безопасности, при необходимости обеспечивать соблюдение режима секретности, понимать виды и назначение различных мер обеспечения информационной безопасности.

Необходимым требованием к «входным» знаниям, умениям и опыту деятельности обучающегося при освоении данной дисциплины является знакомство с основами и практикой использования средств информационно-коммуникационных технологий, а также сведения предшествующего курса «Информатика и информационные технологии в профессиональной деятельности».

1.4 Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Программа определяет общий объем знаний, позволяющий сформировать у студента знания по проблемам правового, административного, технического и программного обеспечения информационной безопасности. Кроме того, освоение дисциплины «Основы информационной безопасности в профессиональной деятельности» способствует повышению информационной культуры обучающихся.

В результате изучения дисциплины студент должен

-знать терминологию в области информационной безопасности, источники возникновения информационных угроз, методы и средства обеспечения информационной безопасности, средства защиты от нарушения конфиденциальности, целостности и доступности информации;

-уметь проводить анализ угроз информационной безопасности, применять на практике основные принципы теории информационной безопасности;

-владеть информацией о современных направлениях развития систем безопасности, об основных типах угроз информационной безопасности.

Изучение данной учебной дисциплины направлено на формирование у обучающихся общепрофессиональных и профессиональных компетенций:

- ОПК-2 – способность соблюдать в профессиональной деятельности требования правовых актов в области защиты государственной тайны и информационной безопасности, обеспечивать соблюдение режима секретности;
- ОПК-5 – способность самостоятельно осуществлять поиск профессиональной информации в печатных и электронных источниках, включая электронные базы данных.

Процесс освоения дисциплины «Основы информационной безопасности в профессиональной деятельности» направлен на получения необходимого объема знаний, отвечающих требованиями ФГОС и обеспечивающих успешное ведение специалистом производственной и научно-исследовательской деятельности, владение навыками работы с электронными ресурсами для решения лингвистических задач, овладение следующими компетенциями:

Индекс компетенции	Содержание компетенции (или её части)	В результате изучения учебной дисциплины обучающиеся должны		
		знать	**уметь**	**владеть**
ОПК-2	способностью соблюдать в профессиональной деятельности требования правовых актов в области защиты государственной тайны и информационной безопасности, обеспечивать соблюдение режима секретности	– терминологию в области информационной безопасности; – источники возникновения информационных угроз; – методы и средства обеспечения информационной безопасности; – средства защиты от нарушения конфиденциальности, целостности и доступности информации; – нормативные акты об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи; – тематические электронные	– проводить анализ угроз информационной безопасности; – компетентно довести до окружающих информацию об обеспечении безопасности хранения, обработки и передачи информации; – применять на практике основные принципы теории информационной безопасности	– информацией о современных направлениях развития систем безопасности; – информацией об основных типах угроз информационной безопасности; – навыками безопасного сбора и обработки информации

Индекс компетенции	Содержание компетенции (или её части)	В результате изучения учебной дисциплины обучающиеся должны		
		знать	**уметь**	**владеть**
		ресурсы		
ОПК-5	способностью самостоятельно осуществлять поиск профессиональной информации в печатных и электронных источниках, включая электронные базы данных	– способы и средства получения, переработки и представления информации с помощью информационно-коммуникационных технологий	– организовывать процессы поиска информации на основе IT-технологий; – использовать базы данных и знаний и тематические информационные ресурсы; – использовать электронные тематические ресурсы для углубления знаний о предметной области.	– коммуникационными сетевыми навыками; – навыками тематического поиска анализа информации

Процесс освоения дисциплины «Основы информационной безопасности в профессиональной деятельности» направлен на получения необходимого объема знаний, отвечающих требованиями ФГОС и обеспечивающих успешное ведение специалистом производственной и научно-исследовательской деятельности, владение навыками обеспечения информационной безопасности, средствами защиты от нарушения конфиденциальности, целостности и доступности информации.

2. Структура и содержание дисциплины

2.1 Распределение трудоёмкости дисциплины по видам работ

Общая трудоемкость дисциплины составляет 4 зачетных единиц, 144 академических часа. Курс «Основы информационной безопасности в профессиональной деятельности» состоит из лекционных и лабораторных занятий, сопровождаемых регулярной индивидуальной работой преподавателя со студентами в процессе самостоятельной работы. В конце семестра проводится зачет. Программой дисциплины предусмотрены 18 часов лекционных, 18 часов лабораторных занятий.

Вид учебной работы	Всего часов	Семестр (часы)
Контактная работа (всего)	**42,3**	**6**
В том числе:		
Занятия лекционного типа	18	18
Занятия семинарского типа (семинары, практические занятия)	–	–
Лабораторные занятия	18	18

Вид учебной работы		Всего часов	Семестр (часы)
Иная контактная работа:			
Контроль самостоятельной работы (КСР)		6	6
Промежуточная аттестация (ИКР)		0,3	0,3
Самостоятельная работа (всего)		**66**	**66**
В том числе:			
Проработка учебного (теоретического) материала		36	36
Подготовка к текущему контролю		30	30
Контроль:			
Подготовка к экзамену		35,7	35,7
Общая трудоемкость	**час.**	**144**	**144**
	в том числе контактная работа	**42,3**	**42,3**
	зач. ед	**4**	**4**

2.2 Структура дисциплины:

Распределение видов учебной работы и их трудоемкости по разделам дисциплины. Разделы дисциплины, изучаемые в 6 семестре

№	Наименование разделов	Количество часов				
		Всего	Аудиторная работа		Внеаудиторная работа	
			Л	ЛР	СРС	контроль
1	Введение в информационную безопасность	28	4		12	12
2	Способы обработки информации	56	6	12	26	12
3	Основные направления защиты информации	53,7	8	6	28	11,7
Контроль самостоятельной работы (КСР)		6	–	–	–	–
Промежуточная аттестация (ИКР)		0,3	–	–	–	–
Итого		**144**	**18**	**18**	**66**	**35,7**

Примечание: Л – лекции, ЛР – лабораторные занятия, СРС – самостоятельная работа студента.

2.3 Содержание разделов дисциплины:

№	Наименование раздела	Содержание раздела	Форма текущего контроля
1	2	3	4
1.	Введение в информационную безопасность	Основные понятия: задачи, объект, предмет, методы информационной безопасности. Официальные органы, обеспечивающие	Опрос по результатам лабораторного задания

№	Наименование раздела	Содержание раздела	Форма текущего контроля
1	2	3	4
		информационную безопасность в Российской Федерации. Обзор российского законодательства в сфере информационных технологий. Федеральный закон «Об информации, информационных технологиях и о защите информации», законодательство РФ в сфере СМИ. Правовое обеспечение информационной безопасности. Доктрина информационной безопасности РФ и Стратегия национальной безопасности Российской Федерации до 2020 года. Предмет и задачи информационной безопасности. Эволюция подходов к обеспечению информационной безопасности. Составляющие концептуальной модели информационной безопасности. Понятие угроз безопасности. Современная концепция информационной безопасности. Цели защиты информации. Носители защищаемой информации	
2.	Способы обработки информации	Понятие информации. Понятие конфиденциальной информации. Понятие государственной тайны. Степени грифа секретности. Виды сведений составляющих государственную тайну. Перечень информации, не подлежащей к засекречиванию. Классификация видов профессиональной тайны и объекты их приложения. Федеральный закон «О государственной тайне». Федеральный закон «О персональных данных». Федеральный закон «Об электронной подписи». Основные понятия безопасности: конфиденциальность, целостность, доступность. Объекты, цели и задачи защиты информации. Угрозы информационной безопасности: классификация, источники возникновения и пути реализации. Определение требований к уровню обеспечения информационной безопасности. Офисные технологии. Текстовые процессоры. Электронные таблицы. Обработка результатов экспериментов в электронных таблицах. Основные структуры данных. Базы и банки данных. Системы управления базами данных. Способы защиты персональных данных. Электронный документ. Электронный документооборот. Электронная подпись. Информационное облако. Понятие, структура, предназначение, перспективы применения	Опрос по результатам лабораторного задания
3.	Основные	Понятие, методы защиты информации. Уровни	Опрос по

№	Наименование раздела	Содержание раздела	Форма текущего контроля
1	2	3	4
	направления защиты информации	защиты информации. Угрозы информационным системам и их виды. Виды мер обеспечения информационной безопасности: законодательные, морально-этические, организационные, технические, программно-математические. Система защиты информации. Техническое и программное обеспечение информационной безопасности. Основные защитные механизмы: идентификация и аутентификация. Разграничение доступа. Контроль целостности. Защита информации при работе в сети Интернет. Признаки незаконного проникновения в компьютерную систему. Дальнейшие действия в случае обнаружения незаконного проникновения в компьютерную систему. Компьютерные вирусы: понятие, пути распространения, проявление действия вируса. Модели поведения вирусов, деструктивные действия вируса, разрушение программы защиты, изменение состояния программной среды; воздействия на программно-аппаратные средства защиты информации. Программы-шпионы. Взлом парольной защиты. Защита от воздействия вирусов. Использование антивирусных программы. Программы-детекторы, программы-доктора, программы-ревизоры, программы-фильтры. Профилактика заражения вирусом. Информационные войны. Компьютерные преступления. Киберпреследование. Переговорный процесс и обеспечение информационной безопасности. Переговорный процесс как способ разрешения конфликтных ситуаций. Виды переговоров. Стратегии переговоров. Роль переводчика в переговорном процессе.	результатам лабораторного задания

2.3.1 Занятия лекционного типа

Раздел 1. Основные понятия: задачи, объект, предмет, методы информационной безопасности. Официальные органы, обеспечивающие информационную безопасность в Российской Федерации. Обзор российского законодательства в сфере информационных технологий. Федеральный закон «Об информации, информационных технологиях и о защите информации», законодательство РФ в сфере СМИ. Правовое обеспечение информационной безопасности. Доктрина информационной безопасности РФ и Стратегия национальной безопасности Российской Федерации до 2020 года (**2** ч.)

Предмет и задачи информационной безопасности. Эволюция подходов к обеспечению информационной безопасности. Составляющие концептуальной модели информационной

безопасности. Понятие угроз безопасности. Современная концепция информационной безопасности. Цели защиты информации. Носители защищаемой информации (**2** ч.).

Раздел 2. Понятие информации. Понятие конфиденциальной информации. Понятие государственной тайны. Степени грифа секретности. Виды сведений составляющих государственную тайну. Перечень информации, не подлежащей к засекречиванию. Классификация видов профессиональной тайны и объекты их приложения. Федеральный закон «О государственной тайне». Федеральный закон «О персональных данных». Федеральный закон «Об электронной подписи» (**2** ч.).

Основные понятия безопасности: конфиденциальность, целостность, доступность. Объекты, цели и задачи защиты информации. Угрозы информационной безопасности: классификация, источники возникновения и пути реализации**.** Определение требований к уровню обеспечения информационной безопасности (**2** ч.).

Офисные технологии. Текстовые процессоры. Электронные таблицы. Обработка результатов экспериментов в электронных таблицах. Основные структуры данных. Базы и банки данных. Системы управления базами данных. Способы защиты персональных данных. Электронный документ. Электронный документооборот. Электронная подпись. Информационное облако. Понятие, структура, предназначение, перспективы применения (**2** ч.).

Раздел 3. Понятие, методы защиты информации. Уровни защиты информации. Угрозы информационным системам и их виды. Виды мер обеспечения информационной безопасности: законодательные, морально-этические, организационные, технические, программно-математические. Система защиты информации. Техническое и программное обеспечение информационной безопасности. Основные защитные механизмы: идентификация и аутентификация. Разграничение доступа. Контроль целостности. (**2** ч.).

Защита информации при работе в сети Интернет. Признаки незаконного проникновения в компьютерную систему. Дальнейшие действия в случае обнаружения незаконного проникновения в компьютерную систему. Компьютерные вирусы: понятие, пути распространения, проявление действия вируса. Модели поведения вирусов, деструктивные действия вируса, разрушение программы защиты, изменение состояния программной среды; воздействия на программно-аппаратные средства защиты информации. Программы-шпионы. Взлом парольной защиты (**2** ч.).

Защита от воздействия вирусов. Использование антивирусных программы. Программы-детекторы, программы-доктора, программы-ревизоры, программы-фильтры. Профилактика заражения вирусом. Информационные войны. Компьютерные преступления. Киберпреследование (**2** ч.).

Переговорный процесс и обеспечение информационной безопасности. Переговорный процесс как способ разрешения конфликтных ситуаций. Виды переговоров. Стратегии переговоров. Роль переводчика в переговорном процессе. (**2** ч.).

2.3.2 Занятия семинарского типа

Учебный план не предусматривает занятий семинарского типа по дисциплине «основы информационной безопасности в профессиональной деятельности».

2.3.3 Лабораторные занятия

1 Офисные пакеты. Пакет программ Microsoft Office. Редактор Word. Шаблоны и стили. Форматирование документа. Стили. Формы и макросы. Настройка среды Word. Возможности антивирусной защиты, защита доступа и редактирования (**2** ч.).

2, 3 Электронные таблицы: назначение и принцип работы программы Excel. Форматы данных. Возможности обработка экспериментальных данных. Настройка табличного процессора Excel. Макросы. Совместное использование приложений MS Office. Возможности антивирусной защиты, защита доступа и редактирования. (**4**.ч.)

4 Программа Power Point. Настройка и демонстрация презентаций. Защита доступа и редактирования (**2**.ч.).

5 Работа с базами данных. СУБД Microsoft Access. Создание структуры базы данных. Таблицы. Формы. Запросы по образцу (Query By Example). Отчеты. Макросы. Создание и обработка базы данных персональной информации (**4**.ч.).

6 Сетевые сервисы и механизмы безопасности. Основные типы браузеров и их особенности. Структура адресов. Поиск информации в Интернет. Поисковые системы. Электронная почта. Механизмы управления доступом. Средства аутентификации. (**4** ч.).

7 Создание архивов. Архивирование с паролем. Вирусы и антивирусы. Защита от вирусных атак. Работа с антивирусными программами (**2**.ч.).

2.3.4 Примерная тематика курсовых работ (проектов)

Учебный план не предусматривает курсовых работ по дисциплине «основы информационной безопасности в профессиональной деятельности».

2.4 Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплин

№	Вид СРС	Перечень учебно-методического обеспечения дисциплины по выполнению самостоятельной работы
1	2	3
1	Подготовка к текущему контролю	1. Артемов, А.В. Информационная безопасность. Орел : МАБИВ, 2014. 257 с. [Электронный ресурс]. - Режим доступа: http://biblioclub.ru/index.php?page=book&id=428605. 2. Основы информационной безопасности / Е.Б. Белов [и др.]. М.: Горячая линия-Телеком, 2006. .544 с. [Электронный ресурс]. - Режим доступа: https://e.lanbook.com/book/5121. 3. Мельников В.П., Клейменов С.А., Петраков А.М. Информационная безопасность и защита информации. М.: Академия, 2011. 331 с. 4. Чубукова С.Г., Элькин В.Д. Основы правовой информатики (юридические и математические вопросы информатики). М.: ИНФРА-М: КОНТРАКТ, 2010. 276 с.

Учебно-методические материалы для самостоятельной работы обучающихся из числа инвалидов и лиц с ограниченными возможностями здоровья (ОВЗ) предоставляются в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:

– в печатной форме увеличенным шрифтом,

– в форме электронного документа.

Для лиц с нарушениями слуха:

– в печатной форме,

– в форме электронного документа.

Для лиц с нарушениями опорно-двигательного аппарата:

– в печатной форме,

– в форме электронного документа.

Данный перечень может быть конкретизирован в зависимости от контингента обучающихся.

2.5 Самостоятельное изучение разделов дисциплины

Целью самостоятельной работы является углубление знаний, полученных в результате аудиторных занятий, выработка навыков индивидуальной работы, закрепление навыков, сформированных во время лабораторных занятий.

Темы для самостоятельной работы

1. Опыт законодательного регулирования информатизации в России и за рубежом.
2. Международные правовые акты по защите информации.
3. Объекты, цели и задачи защиты информации.
4. Модели безопасности и их применение.
5. Пакеты антивирусных программ.
6. Криптографические методы защиты информации.
7. Информационная безопасность при подключении к Internet. Межсетевые экраны.
8. Информационная безопасность при подключении к Internet. Сетевые фильтры.
9. Классификация угроз информационной безопасности. Угрозы, не зависящие от человека.
10. Атака. Локальная и удаленная атака. Хакер. Кракер. Фрикер.
11. Атаки на средства аутентификации. Биометрические средства аутентификации.
12. Компьютерные преступления. Киберпреследование. Способы защиты от киберпреследования.

3. Образовательные технологии

В соответствии с требованиями ФГОС ВО по направлению подготовки специалистов программа по дисциплине «Основы информационной безопасности в профессиональной деятельности» предусматривает использование в учебном процессе следующих образовательных технологий и методов формирования компетенций: применение технических и аудиовизуальных средств обучения, выполнение конкретных технических упражнений, поисковых задач, знакомство с конкретными программными продуктами.

Интерактивные формы лабораторных занятий: использование специализированных и прикладных программ; решение конкретных профессиональных ситуаций, используя методы и подходы информационной безопасности; компьютерное моделирование ситуаций; моделирование переговорного процесса, используя технологии информационной безопасности; групповая дискуссия.

Семестр 6	Вид занятия	Используемые интерактивные образовательные технологии	Общее количество часов
	ЛР	Выполнение групповых и индивидуальных заданий в компьютерном классе: решение конкретных профессиональных ситуаций, используя методы и подходы информационной безопасности; компьютерное моделирование ситуаций; моделирование переговорного процесса, используя технологии информационной безопасности; групповая дискуссия	18
Итого:			18

Для лиц с ограниченными возможностями здоровья предусмотрена организация консультаций с использованием электронной почты.

4. Оценочные средства для текущего контроля успеваемости и промежуточной аттестации

Учебная деятельность проходит в соответствии с графиком учебного процесса. Процесс самостоятельной работы контролируется во время аудиторных занятий и индивидуальных консультаций. Самостоятельная работа студентов проводится в форме изучения отдельных теоретических вопросов по предлагаемой литературе.

Фонд оценочных средств дисциплины состоит из средств текущего контроля (см. темы лабораторных работ, рефератов, вопросов), рубежного контроля и итоговой аттестации (экзамена). В рамках курса используются следующие виды контроля: опросы, проверка выполнения индивидуальных заданий во время и т.д. (текущий контроль).

Тему реферата выбирает студент. Подготовка и защита реферата является обязательным учебным заданием, которые студенты должны выполнить.

Соответствие компетенций, формируемых при изучении дисциплины, и видов занятий

Перечень компетенций	Виды занятий			Формы контроля
	Л.	Лаб.	СРС	
ОПК-2		+	+	– лабораторное задание; – представление реферата
ОПК-5	+	+	+	– лабораторное задание; – представление реферата

4.1 Фонд оценочных средств для проведения текущего контроля

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

Примерные темы рефератов

1. Информационное общество как новый этап развития цивилизации.

2. Информационная война как угроза национальной безопасности.
3. Информационная безопасность в лингвистических информационных системах.
4. Угрозы в области информационной деятельности.
5. Противодействие преступлениям в информационной сфере.

4.2 Фонд оценочных средств для проведения промежуточной аттестации

Основные требования к результатам освоения дисциплины представлены в таблице в виде признаков сформированности компетенций. Требования формулируются по двум уровням: пороговый и повышенный и в соответствии со структурой, принятой в ФГОС ВО: знать, уметь, владеть.

Примерный перечень вопросов, выносимых на экзамен

1. Понятие информации. Признаки информации.
2. Информация по структуре и по уровню доступа.
3. Объекты, цели и задачи защиты информации.
4. Нормативно-правовые, морально-этические, организационные и физические (технические) механизмы защиты.
5. Угрозы информационной безопасности: классификация, источники возникновения и пути реализации.
6. Конфиденциальная информация и ее разновидности.
7. Понятие электронного документа и электронного документооборота. Электронная подпись.
8. Понятие защиты информации. Уровни защиты информации.
9. Угрозы информационным системам и их виды. Программы-шпионы. Методы защиты информации.
10. Техническое и программное обеспечение информационной безопасности.
11. Система защиты информации. Информационное оружие.
12. Компьютерные вирусы.
13. Компьютерная система как объект информационной безопасности.
14. Информационные процессы как объект информационной безопасности
15. Влияние человеческого фактора на обеспечение информационной безопасности
16. Виды и назначение различных мер обеспечения информационной безопасности
17. Программно-аппаратные средства обеспечения информационной безопасности
18. Классификация программно-аппаратных средств обеспечения информационной безопасности
19. Защита от несанкционированного доступа
20. Антивирусная защита.
21. Защита информации при работе в сети Интернет.
22. Признаки незаконного проникновения в компьютерную систему.

Оценочные средства для инвалидов и лиц с ограниченными возможностями здоровья выбираются с учетом их индивидуальных психофизических особенностей.

– при необходимости инвалидам и лицам с ограниченными возможностями здоровья предоставляется дополнительное время для подготовки ответа;

– при проведении процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья предусматривается использование технических средств, необходимых им в связи с их индивидуальными особенностями;

– при необходимости для обучающихся с ограниченными возможностями здоровья и инвалидов процедура оценивания результатов обучения по дисциплине может проводиться в несколько этапов.

Процедура оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья по дисциплине предусматривает предоставление информации в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:

– в печатной форме увеличенным шрифтом,

– в форме электронного документа.

Для лиц с нарушениями слуха:

– в печатной форме,

– в форме электронного документа.

Для лиц с нарушениями опорно-двигательного аппарата:

– в печатной форме,

– в форме электронного документа.

Данный перечень может быть конкретизирован в зависимости от контингента обучающихся.

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

5.1 Основная литература:

5. Артемов, А.В. Информационная безопасность. Орел : МАБИВ, 2014. 257 с. [Электронный ресурс]. - Режим доступа: http://biblioclub.ru/index.php?page=book&id=428605.

6. Мельников В.П., Клейменов С.А., Петраков А.М. Информационная безопасность и защита информации. М.: Академия, 2011. 331 с.

7. Чубукова С.Г., Элькин В.Д. Основы правовой информатики (юридические и математические вопросы информатики). М.: ИНФРА-М: КОНТРАКТ, 2010. 276 с.

Для освоения дисциплины инвалидами и лицами с ограниченными возможностями здоровья имеются издания в электронном виде в электронно-библиотечных системах.

Нормативные источники

1. Конституция РФ.
2. Федеральный конституционный закон от 28.04.1995 № 1-ФКЗ «Об арбитражных судах в Российской Федерации».
3. Закон РФ от 05.03.1992 № 2446-1 «О безопасности».
4. Федеральный закон от 12.08.1995 № 144-ФЗ «Об оперативно-розыскной деятельности».
5. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
6. Закон от 27.12.1991 № 2124-1 «О средствах массовой информации».
7. Федеральный закон от 13.01.1995 № 7-ФЗ «О порядке освещения деятельности органов государственной власти в государственных средствах массовой информации».
8. Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи».
9. Закон РФ от 21.07.1993 № 5485-1 «О государственной тайне».
10. Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне».
11. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».
12. Федеральный закон от 22.12.2008 № 262-ФЗ «Об обеспечении доступа к информации о деятельности судов в Российской Федерации».

13. Федеральный закон от 09.02.2009 № 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления».

14. Федеральный закон от 10.01.2003 № 20-ФЗ «О Государственной автоматизированной системе Российской Федерации «Выборы».

15. Федеральный закон от 25.07.1998 № 128-ФЗ «О государственной дактилоскопической регистрации в Российской Федерации».

16. Доктрина информационной безопасности Российской Федерации.

17. Указ Президента РФ от 12.05.2009 № 537 «О Стратегии национальной безопасности Российской Федерации до 2020 года».

18. Указ Президента РФ от 17.03.2008 № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».

19. Указ Президента РФ от 01.09.2004 № 1135 «Об утверждении Положения об Управлении информационного и документационного обеспечения Президента Российской Федерации».

20. Указ Президента РФ от 27.07.1992 № 802 «О научном и информационном обеспечении проблем инвалидности и инвалидов».

21. Указ Президента РФ от 28.06.1993 № 966 «О Концепции правовой информатизации России».

22. Указ Президента РФ от 20.01.1994 № 170 «Об основах государственной политики в сфере информатизации».

23. Указ Президента РФ от 19.10.2005 № 1222 «Об основных документах, удостоверяющих личность гражданина Российской Федерации за пределами территории Российской Федерации, содержащих электронные носители информации».

24. Постановление Правительства РФ от 22.10.2007 № 689 «Об утверждении Положения о лицензировании деятельности по выявлению электронных устройств, предназначенных для негласного получения информации, в помещениях и технических средствах (за исключением случая, если указанная деятельность осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)».

25. Постановление Правительства РФ от 24.11.2009 № 953 «Об обеспечении доступа к информации о деятельности Правительства Российской Федерации и федеральных органов исполнительной власти» (вместе с «Требованиями к технологическим, программным и лингвистическим средствам обеспечения пользования официальным сайтом Правительства Российской Федерации в сети Интернет»).

26. Постановление Правительства РФ от 17.11.2007 № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных».

27. Постановление Правительства РФ от 28.01.2002 № 65 «О федеральной целевой программе «Электронная Россия (2002 - 2010 годы)».

28. Приказ ФСБ РФ от 09.02.2005 № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)».

29. Приказ ФАПСИ от 13.06.2001 № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну».

5.2 Дополнительная литература:

1. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам / А.А. Афанасьев [и др.]. М.: Горячая линия-Телеком, 2012. 550 с. [Электронный ресурс]. - Режим доступа: https://e.lanbook.com/book/5114.
2. Загинайлов Ю.Н. Основы информационной безопасности: курс визуальных лекций. М.; Берлин: Директ-Медиа, 2015. 105 с. [Электронный ресурс]. - Режим доступа: http://biblioclub.ru/index.php?page=book&id=362895.
8. Основы информационной безопасности / Е.Б. Белов [и др.]. М.: Горячая линия-Телеком, 2006. .544 с. [Электронный ресурс]. - Режим доступа: https://e.lanbook.com/book/5121.

5.3. Периодические издания:

Не используются

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

1. http://www.kremlin.ru
2. http://www.government.ru
3. http://www.council.gov.ru
4. http://www.duma.gov.ru
5. http://siberia-expert.com
6. http://elibrary.ru

7. Методические указания для обучающихся по освоению дисциплины

В ходе проводимых занятий предлагаемые студентам задания, упражнения и т.п. должны быть ориентированы на расширение спектра функциональных возможностей, используемых в образовательных учреждениях информационных технологий.

Для приобщения обучаемых к поиску, к исследовательской работе, для развития их творческого потенциала следует по возможности избегать прямого руководства работой обучающихся при выполнении ими тех или иных заданий, чаще выступать в роли консультанта, эксперта.

Важнейшим этапом курса является самостоятельная работа по дисциплине. Поиск информации для ответов на вопросы для самостоятельной работы и выполнения заданий в некоторых случаях предполагает не только изучение основной учебной литературы, но и привлечение дополнительной литературы, а также использование ресурсов сети Интернет.

Примерные варианты тем для самостоятельных работ и индивидуальных заданий

1. Современные стратегии доступа к информации.
2. Безопасный сетевой поиск информации.
3. Программный инструментарий, применяемый для защиты информации.
4. Новейшие компьютерные технологии в защите информации.
5. Наиболее распространенные угрозы информационной безопасности.
6. Стандарты и спецификации в области информационной безопасности.
7. Идентификация и аутентификация, управление доступом к информации.
8. Протоколирование и аудит, шифрование, контроль целостности.
9. Обеспечение высокой доступности.

10. Обеспечение высокой защищенности.

Индивидуальные консультации по предмету являются важным фактором, способствующим индивидуализации обучения и установлению воспитательного контакта между преподавателем и обучающимся инвалидом или лицом с ограниченными возможностями здоровья.

8. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине

8.1 Перечень информационных технологий

– Консультирование посредством электронной почты.
– Использование электронных презентаций при проведении лекционных и лабораторных занятий.
– Использование офисных пакетов при проведении лабораторных занятий.

8.2 Перечень необходимого программного обеспечения

1. Операционная система MS Windows.
2. Интегрированное офисное приложение MS Office.
3. Программное обеспечение для организации управляемого коллективного и безопасного доступа в Интернет.

8.3 Перечень информационных справочных систем:

1. Справочно-правовая система «Консультант Плюс» (http://www.consultant.ru)
2. Электронная библиотечная система "Юрайт" (http://www.biblio-online.ru).
3. Электронная библиотечная система "Университетская библиотека ONLINE" (http://www.biblioclub.ru).
4. Электронная библиотечная система издательства "Лань" (http://e.lanbook.com).
5. Электронная библиотечная система eLIBRARY.RU (http://www.elibrary.ru).

9. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине

Настоящий курс предполагает значительный объём самостоятельной работы студентов. В частности, для выполнения заданий лабораторного практикума, подготовки рефератов предполагается систематическая, целенаправленная работа студентов в сети Интернет, связанная с поиском материалов, соответствующих выбранной тематике. Кроме того, реализация курса предполагает наличие необходимого материально-технического обеспечения: аудитория, оснащенная видеопроектором в качестве средства поддержки лекционных занятий; интерактивная доска в качестве средства поддержки лекционных занятий.

№	Вид работ	Материально-техническое обеспечение дисциплины и оснащенность
1.	Лекционные занятия	Лекционная аудитория, оснащенная презентационной техникой (проектор, экран, компьютер/ноутбук) и соответствующим программным обеспечением. (аудитории 305, 312, 324)
2.	Лабораторные	Кабинет оснащенный компьютерными рабочими местами

	занятия	с возможностью подключения к сети «Интернет», лицензионным программным обеспечением. (компьютерные залы 105, 107)
3.	Текущий контроль, промежуточная аттестация	Кабинет оснащенный компьютерными рабочими местами с возможностью подключения к сети «Интернет», установленным интегрированным офисным приложением MS Office. (компьютерные залы 105, 107).
4.	Самостоятельная работа	Кабинет для самостоятельной работы, оснащенный компьютерной техникой с возможностью подключения к сети «Интернет», программой экранного увеличения и обеспеченный доступом в электронную информационно-образовательную среду университета. (аудитория 102а, читальный зал)