Федеральное государственное бюджетное образовательное учреждение инклюзивного высшего образования

«МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ ГУМАНИТАРНО-ЭКОНОМИЧЕСКИЙ УНИВЕРСИТЕТ»

Факультет Прикладной математики и информатики
Кафедра Информационных технологий и прикладной математики

УТВЕРЖДАЮ
И.о. проректора по УМР
_____
«30» августа 2021 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ

образовательная программа по специальности
45.05.01 «Перевод и переводоведение»

Блок Б1.О.09 «Дисциплины (модули)», обязательная часть

специализация "Лингвистическое обеспечение межгосударственных отношений"

Квалификация
Специалист

Форма обучения: очная

Курс: 5 семестр: 9

Москва
2021

Рабочая программа составлена на основании федерального государственного образовательного стандарта высшего профессионального образования направления специальности 45.05.01 «Перевод и переводоведение» (уровень специалитета), утвержденного Приказом Министерства науки и высшего образования Российской Федерации от 12 августа 2020 № 989 "Об утверждении федерального государственного образовательного стандарта высшего образования по специальности 45.05.01 «Перевод и переводоведение» (уровень специалитета). Зарегистрировано в Минюсте России 27 августа 2020 г. Регистрационный № 59501

Составители рабочей программы: МГГЭУ, доцент кафедры ИТиПМ
место работы, занимаемая должность

подпись Никольский А.Е. «20» августа 2021 г.
Ф.И.О. Дата

Рецензент: МГГЭУ, доцент кафедры ИТиПМ
место работы, занимаемая должность

подпись Белоглазов А.А. «20» августа 2021 г.
Ф.И.О. Дата

Рабочая программа утверждена на заседании кафедры Информационных технологий и прикладной математики (протокол № 1 от «23» августа 2021 г.)

Зав. кафедрой ИТиПМ подпись Митрофанов Е.П. «23» августа 2021 г.
Ф.И.О. Дата

СОГЛАСОВАНО
Начальник
Учебного отдела

«23» августа 2021 г. И.Г. Дмитриева
(дата) (подпись) (Ф.И.О.)

СОГЛАСОВАНО
Декан
факультета

«23» августа 2021 г. Петрунина Е.В.
(дата) подпись Ф.И.О.

СОГЛАСОВАНО
Заведующий
библиотекой

«23» августа 2021г. В.А. Ахтырская

РЕКОМЕНДОВАНО
ОДОБРЕНО НА
УЧЕБНО-МЕТОДИЧЕСКИМ
СОВЕТОМ МГГЭУ
Протокол № 01 от 31 августа 2021 г.

1. ОРГАНИЗАЦИОННО-МЕТОДИЧЕСКИЙ РАЗДЕЛ

1.1. Цель и задачи изучения учебной дисциплины (модуля)

Целью изучения дисциплины является подготовка студентов к освоению организационных, технических, алгоритмических и других методов и средств защиты компьютерной информации, ознакомление с законодательством и стандартами в этой области, с современными криптосистемами, изучение методов идентификации пользователей, борьбы с вирусами, изучение способов применения методов защиты информации при проектировании автоматизированных систем обработки информации и управления (АСОИУ).

Задачи:

- раскрытие специфики защиты компьютерных сетей как объекта научного исследования;
- определение основных этапов и базовых концептуальных подходов к созданию систем защиты компьютерных сетей в рамках исторического развития отечественной и зарубежной науки;
- знакомство со способами и особенностями создания систем защиты компьютерных сетей на различных уровнях взаимодействия с окружением;
- приобретение студентами навыков аналитического и эмпирического исследования систем компьютерной защиты сетей;
- выработка целостного представления о различных аспектах строения и функционирования систем компьютерной защиты сетей на всех ее уровнях;
- рост навыков в сфере создания систем компьютерной защиты сетей и умения применять полученные знания на практике.

1.2. Требования к результатам освоения дисциплины

Изучение данной дисциплины направлено на формирование следующих компетенций

Код и содержание компетенции	Планируемые результаты обучения по дисциплине (модулю), характеризующие этапы формирования компетенций
ОПК-4. Способен работать с электронными словарями, различными источниками информации, осуществлять поиск, хранение, обработку и анализ информации, представлять ее в требуемом формате с использованием информационных, компьютерных и сетевых технологий	ОПК-4.1. Знает методы и способы работы с различными источниками информации. ОПК-4.2. Умеет работать с электронными словарями, осуществлять поиск, хранение, обработку информации; представлять данные в требуемом формате с использованием информационных, компьютерных и сетевых технологий. ОПК-4.3. Владеет навыками анализа информации.

1.3. Место дисциплины (модуля) в структуре образовательной программы

Дисциплина «Основы информационной безопасности в профессиональной деятельности» представляет собой компонент обязательной части блока Б1. «Дисциплины (модули)» в соответствии с федеральным государственным образовательным стандартом высшего образования по специальности 45.05.01 «Перевод и переводоведение» (уровень специалитета).

Изучение дисциплины «Основы информационной безопасности в профессиональной деятельности» основывается на знаниях, полученных при прохождении дисциплины «Интернет-ресурсы».

Изучение дисциплины формирует знание и навыки в области информационных технологиях, что развивает способность работать с различными источниками информации, информационными ресурсами и технологиями, а также применять переводческие трансформации.

2. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

2.1.Объем дисциплины и виды учебной работы в соответствии с формами обучения

Объем дисциплины «Основы информационной безопасности в профессиональной деятельности» составляет 3 зачетные единицы/108 часов:

Вид учебной работы	Всего, часов	Курс, часов
	Очная форма	5 курс, 9 сем.
Аудиторная работа обучающихся с преподавателем (по видам учебных занятий), всего в том числе:	*44*	*44*
Лекции	12	12
Практические занятия	24	24
Лабораторные занятия	8	8
Самостоятельная работа обучающихся	28	28
Промежуточная аттестация (подготовка и сдача), всего:		
Контрольная работа		
Курсовая работа		
Зачет		
Экзамен	36	36
Итого: Общая трудоемкость учебной дисциплины (в часах, зачетных единицах)	**108/3**	**108/3**

2.2. Содержание дисциплины по темам (разделам)

Семестр - 9, вид отчетности – экзамен.

№ п/п	Наименование раздела дисциплины Содержание раздела	Формируемые компетенции (индекс)
Раздел 1. Основные понятия информационной безопасности и защиты информации.		
1.	Анализ угроз информационной безопасности. Анализ угроз корпоративных сетей. Характерные особенности сетевых атак. Угрозы и уязвимости беспроводных сетей. Тенденции развития ИТ-угроз. Криминализация атак на компьютерные сети и системы. Появление кибероружия для ведения технологических кибервойн. Обеспечение информационной безопасности компьютерных систем. Меры и средства обеспечения информационной безопасности. Пути решения проблем информационной безопасности.	ОПК-4
Раздел 2. Стандарты информационной безопасности.		
2.	Роль стандартов информационной безопасности. Международные стандарты информационной безопасности. Стандарты ISO/IEC 17799:2002 (BS 7799:2000). Германский стандарт BSI. Международный стандарт ISO 15408. «Общие критерии	ОПК-4

	безопасности информационных технологий». Стандарты для беспроводных сетей. Стандарты информационной безопасности для Интернета. Отечественные стандарты безопасности информационных технологий. Стандарт «Критерии оценки безопасности информацион0ных технологий» ГОСТ Р ИСО/МЭК 15408.	
Раздел 3 Криптографическая защита информации.		
3.	Основные понятия криптографической защиты информации. Симметричные криптосистемы шифрования. Алгоритмы шифрования DES и 3-DES. Стандарт шифрования ГОСТ 28147-89. Стандарт шифрования AES. Другие симметричные криптоалгоритмы. Основные режимы работы блочного симметричного алгоритма. Особенности применения алгоритмов симметричного шифрования. Асимметричные криптосистемы шифрования. Алгоритм шифрования RSA. Функции хэширования. Электронная цифровая подпись. Отечественный стандарт цифровой подписи ГОСТ Р 34.10-2001.	ОПК-4
Раздел 4 Принципы многоуровневой защиты корпоративной информации.		
4.	Корпоративная информационная система с традиционной структурой. Системы «облачных» вычислений. Многоуровневый подход к обеспечению информационной безопасности КИС. Безопасность «облачных» вычислений.	ОПК-4
Раздел 5. Защита информации в компьютерных сетях, антивирусная защита.		
5.	Концепция построения виртуальных защищенных сетей VPN. PN-решения для построения защищенных сетей. Современные VPN-продукты.	ОПК-4
Раздел 6. Защита удаленного доступа.		
6.	Особенности удаленного доступа. Средства и протоколы аутентификации удаленных пользователей. Централизованный контроль удаленного доступа. Протокол Kerberos.	ОПК-4

2.3. Разделы дисциплин и виды занятий

№ п/п	Наименование темы дисциплины	Лекционные занятия	Лабораторная работа	Практические занятия	Самостоятельная работа	Всего часов	Формы текущего контроля успеваемости
1.	Основные понятия информационной безопасности и защиты информации.	2	-	4	4	10	Устный опрос, проверка пр. и лб. работ
2.	Стандарты информационной безопасности.	2	-	4	4	10	Устный опрос, проверка пр. и лб. работ
3.	Криптографическая защита информации.	2	2	4	4	12	Устный опрос, проверка пр. и лб. работ
4.	Принципы многоуровневой защиты корпоративной информации.	2	2	4	4	12	Устный опрос, проверка пр. и лб. работ
5.	Защита информации в компьютерных сетях,	2	2	4	6	14	Устный опрос, проверка пр. и

	антивирусная защита.						лб. работ
6.	Защита удаленного доступа.	2	2	4	6	14	Устный опрос, проверка пр. и лб. работ
Экзамен						36	
Итого:		12	8	24	28	108	

2.4. Планы теоретических (лекционных) занятий

№ п/п	Наименование тем лекций	Кол-во часов в 9 семестре
Раздел 1. Основные понятия информационной безопасности и защиты информации		
1.	Анализ угроз информационной безопасности. Характерные особенности сетевых атак. Угрозы и уязвимости беспроводных сетей. Тенденции развития ИТ-угроз. Криминализация атак на компьютерные сети и системы. Появление кибероружия для ведения технологических кибервойн. Обеспечение информационной безопасности компьютерных систем. Меры и средства обеспечения информационной безопасности.	2
Раздел 2. Стандарты информационной безопасности		
2.	Роль стандартов информационной безопасности. Международные стандарты информационной безопасности. Стандарты ISO/IEC 17799:2002 (BS 7799:2000).	2
Раздел 3. Криптографическая защита информации		
3.	Основные понятия криптографической защиты информации. Симметричные криптосистемы шифрования. Алгоритмы шифрования DES и 3-DES. Стандарт шифрования ГОСТ 28147-89. Стандарт шифрования AES. Другие симметричные криптоалгоритмы. Основные режимы работы блочного симметричного алгоритма. Особенности применения алгоритмов симметричного шифрования. Асимметричные криптосистемы шифрования. Алгоритм шифрования RSA. Функции хэширования. Электронная цифровая подпись. Отечественный стандарт цифровой подписи ГОСТ Р 34.10-2001.	2
Раздел 4. Принципы многоуровневой защиты корпоративной информации		
4.	Корпоративная информационная система с традиционной структурой. Системы «облачных» вычислений. Многоуровневый подход к обеспечению информационной безопасности КИС. Безопасность «облачных» вычислений	2
Раздел 5. Защита информации в компьютерных сетях, антивирусная защита защиты корпоративной информации		
5.	Защита информации в компьютерных сетях. Антивирусная защита.	2
Раздел 6. Защита удаленного доступа		
6.	Особенности удаленного доступа. Средства и протоколы аутентификации удаленных пользователей. Централизованный контроль удаленного доступа. Протокол Kerberos.	2

2.5. Планы практических (семинарских) занятий

№ п/п	Наименование тем практических занятий	Кол-во часов в 9 семестре
Раздел 1. Основные понятия информационной безопасности и защиты информации		

1.	Анализ угроз информационной безопасности. Характерные особенности сетевых атак. Угрозы и уязвимости беспроводных сетей. Тенденции развития ИТ-угроз. Криминализация атак на компьютерные сети и системы.	2
	Появление кибероружия для ведения технологических кибервойн. Обеспечение информационной безопасности компьютерных систем. Меры и средства обеспечения информационной безопасности. Пути решения проблем информационной безопасности.	2
Раздел 2. Стандарты информационной безопасности		
2.	Германский стандарт BSI. Международный стандарт ISO 15408. «Общие критерии безопасности информационных технологий»	2
	Стандарты для беспроводных сетей. Стандарты информационной безопасности для Интернета.	2
Раздел 3. Криптографическая защита информации		
3.	Стандарт шифрования AES. Другие симметричные криптоалгоритмы. Основные режимы работы блочного симметричного алгоритма. Особенности применения алгоритмов симметричного шифрования.	2
	Асимметричные криптосистемы шифрования. Алгоритм шифрования RSA. Электронная цифровая подпись. Отечественный стандарт цифровой подписи ГОСТ Р 34.10-2001.	2
Раздел 4. Принципы многоуровневой защиты корпоративной информации		
4.	Корпоративная информационная система с традиционной структурой. Системы «облачных» вычислений.	2
	Многоуровневый подход к обеспечению информационной безопасности КИС. Безопасность «облачных» вычислений	2
Раздел 5. Защита информации в компьютерных сетях, антивирусная защита защиты корпоративной информации		
5.	Защита информации в компьютерных сетях	2
	Антивирусная защита.	2
Раздел 6. Защита удаленного доступа		
6.	Особенности удаленного доступа. Средства и протоколы аутентификации удаленных пользователей.	2
	Централизованный контроль удаленного доступа. Протокол Kerberos.	2

2.6. Планы лабораторных работ

№ п/п	Наименование тем лабораторных работ	Кол-во часов в 9 семестре
Раздел 1. Основные понятия информационной безопасности и защиты информации		
1.		-
Раздел 2. Стандарты информационной безопасности		
2.		-
Раздел 3. Криптографическая защита информации		
3.	Шифрование и расшифровка текста различными алгоритмами	2
Раздел 4. Принципы многоуровневой защиты корпоративной информации		
4.	Облачные технологии защиты информации	2
Раздел 5. Защита информации в компьютерных сетях, антивирусная защита защиты корпоративной информации		
5.	Виды компьютерных вирусов и защита от них	2
Раздел 6. Защита удаленного доступа		

6.	Защита информации в компьютерных сетях	2

2.7. Планы самостоятельной работы обучающегося по дисциплине (модулю)

№	Название разделов и тем	Виды самостоятельной работы	Трудоемкость	Формируемые компетенции	Формы контроля
1.	Информатика, информационные технологии, информационные системы, информационные ресурсы	Информационный поиск и самоподготовка по изучаемым темам	8	ОПК-4	Устный опрос
2.	Технологии обработки документов	Информационный поиск и самоподготовка по изучаемым темам	8	ОПК-4	Устный опрос
3.	Мультимедийные технологии	Информационный поиск и самоподготовка по изучаемым темам	8	ОПК-4	Устный опрос
4.	Информационные кросс - технологии	Информационный поиск и самоподготовка по изучаемым темам	8	ОПК-4	Устный опрос
5.	Технологии доступа к данным файловые системы и базы данных	Информационный поиск и самоподготовка по изучаемым темам	10	ОПК-4	Устный опрос
6.	Сетевые информационные технологии. Internet	Информационный поиск и самоподготовка по изучаемым темам	10	ОПК-4	Устный опрос
7.	Автоматизированные информационные технологии работа в программе SPSS	Информационный поиск и самоподготовка по изучаемым темам	10	ОПК-4	Устный опрос

3. ОСОБЕННОСТИ ОБУЧЕНИЯ ЛИЦ С ОВЗ (ПОДА)

При организации обучения студентов с инвалидностью и ОВЗ (ПОДА) обеспечиваются следующие необходимые условия:

- учебные занятия организуются исходя из психофизического развития и состояния здоровья лиц с ОВЗ совместно с другими обучающимися в общих группах, а также индивидуально, в соответствии с графиком индивидуальных занятий;

- при организации учебных занятий в общих группах используются социально-активные и рефлексивные методы обучения, технологии социокультурной реабилитации с целью оказания помощи в установлении полноценных межличностных отношений, создания комфортного психологического климата в группе;

- в процессе образовательной деятельности применяются материально-техническое оснащение, специализированные технические средства приема-передачи учебной информации в доступных формах для студентов с различными нарушениями, электронные образовательные ресурсы в адаптированных формах.

- подбор и разработка учебных материалов преподавателями производится с учетом психофизического развития и состояния здоровья лиц с ОВЗ;

- использование элементов дистанционного обучения при работе со студентами, имеющими затруднения с моторикой;

- обеспечение студентов текстами конспектов (при затруднении с конспектированием);

- использование при проверке усвоения материала методик, не требующих выполнения рукописных работ или изложения вслух (при затруднениях с письмом и речью) – например, тестовых бланков.

При проведении процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья по дисциплине обеспечивается выполнение следующих дополнительных требований в зависимости от индивидуальных особенностей обучающихся:

1. Инструкция по порядку проведения процедуры оценивания предоставляется в доступной форме (устно, в письменной форме, на электронном носителе, в печатной форме увеличенным шрифтом и т.п.);

2. Доступная форма предоставления заданий оценочных средств (в печатной форме, в печатной форме увеличенным шрифтом, в форме электронного документа);

3. Доступная форма предоставления ответов на задания (письменно на бумаге, набор ответов на компьютере, устно, др.).

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

В освоении дисциплины инвалидами и лицами с ограниченными возможностями здоровья большое значение имеет индивидуальная работа. Под индивидуальной работой подразумевается две формы взаимодействия с преподавателем: индивидуальная учебная работа (консультации), т.е. дополнительное разъяснение учебного материала и углубленное изучение материала с теми обучающимися, которые в этом заинтересованы, и индивидуальная воспитательная работа. Индивидуальные консультации по предмету являются важным фактором, способствующим индивидуализации обучения и установлению воспитательного контакта между преподавателем и обучающимся инвалидом или обучающимся с ограниченными возможностями здоровья.

4. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

Самостоятельная работа, наряду с аудиторными занятиями, является неотъемлемой частью изучения дисциплины. Приступая к изучению дисциплины, студенты должны ознакомиться с учебной программой, учебной, научной и методической литературой, имеющейся в библиотеке, получить в библиотеке рекомендованные учебники и учебно-методические пособия, завести тетради для конспектирования лекций и практических занятий.

К видам самостоятельной работы в рамках обучения относятся:

- самостоятельный поиск и изучение научных материалов в рамках курса, в том числе при подготовке к практическим занятиям;

- анализ изученных материалов и подготовка устных докладов и контрольной работы в соответствии с выбранной для этого вида работы темой;

- самостоятельное изучение определенных разделов и тем дисциплины;

- подготовка к аудиторным занятиям;

- подготовка к промежуточному, текущему контролю знаний и навыков (в т.ч. к контрольным работам, тестированию и т.п.);

- подготовка к зачету или экзамену.

При этом учесть рекомендации преподавателя и требования учебной программы. При подготовке к зачету повторять пройденный материал в соответствии с учебной программой, примерным перечнем учебных вопросов, выносящихся на зачет и содержащихся в данной программе. Использовать конспект лекций и литературу, рекомендованную преподавателем.

Обратить особое внимание на темы учебных занятий, пропущенных студентом по разным причинам. При необходимости обратиться за консультацией и методической помощью к преподавателю. Самостоятельная работа может осуществляться индивидуально или группами студентов в зависимости от цели, объема, конкретной тематики самостоятельной работы, уровня сложности, уровня умений студентов.

Контроль результатов внеаудиторной самостоятельной работы студентов может осуществляться в пределах времени, отведенного на обязательные учебные занятия по дисциплине и внеаудиторную самостоятельную работу студентов по дисциплине, может проходить в письменной, устной или смешанной форме.

5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ (МОДУЛЯ)

5.1 Перечень основной литературы

1. Сычев, Ю. Н. Защита информации и информационная безопасность : учебное пособие / Ю.Н. Сычев. — Москва : ИНФРА-М, 2021. — 201 с. — (Высшее образование: Бакалавриат). — DOI 10.12737/1013711. - ISBN 978-5-16-014976-9. - Текст : электронный. - URL: https://znanium.com/catalog/product/1013711. Режим доступа: по подписке.

2. Баранова, Е. К. Информационная безопасность и защита информации : учебное пособие / Е.К. Баранова, А.В. Бабаш. — 4-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2021. — 336 с. — (Высшее образование). — DOI: https://doi.org/10.29039/1761-6. - ISBN 978-5-369-01761-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1189326. Режим доступа: по подписке.

5.2 Перечень дополнительной литературы

1. Бойко, Г. М. Информационные технологии. Практикум для обучающихся по направлению подготовки 20.03.01 Техносферная безопасность : учебное пособие / Г. М. Бойко. - Железногорск : ФГБОУ ВО СПСА ГПС МЧС России. - 2020. - 109 с. : ил. - Текст : электронный. - URL: https://znanium.com/catalog/product/1202001

2. Котенко, В. В. Технологии информационного анализа пользовательского уровня телекоммуникационных систем : учебное пособие / В. В. Котенко ; Южный федеральный университет. - Ростов-на-Дону ; Таганрог : Издательство Южного федерального университета, 2019. - 194 с. - ISBN 978-5-9275-3176-9. - Текст : электронный. - URL: https://znanium.com/catalog/product/1088143.

Информационная безопасность и зашита информации : учебное пособие для направления подготовки 40.03.01 - Юриспруденция, специальности 40.05.02 - Правоохранительная деятельность, специальности 37.05.02 - Психология служебной деятельности, очной и заочной форм обучения / О. А. Панфилова, Д. Ю. Крюкова, А. Н. Наимов, В. В. Мухин ; Федер. служба исполн. наказаний, Вологод. ин-т права и экономики. - Вологда : ВИПЭ ФСИН России, 2018. - 59 с. - ISBN 978-5-94991-428-1. - Текст : электронный. - URL: https://znanium.com/catalog/product/1229037. Режим доступа: по подписке.

5.3 Программное обеспечение

1. VMware Player (свободно распространяемое ПО).
2. Java (свободно распространяемое ПО);
3. JavaNetSim (свободно распространяемое ПО).

5.4 Электронные ресурсы

1. Открытый ПП SiLab.
2. Национальный открытый Университет «ИНТУИТ» www.intuit.ru
3. Энциклопедия Кругосвет. Универсальная научно-популярная онлайн-энциклопедия. www.krugosvet.ru
4. Национальный открытый университет ИНТУИТ [Электронный ресурс]. URL: http://www.intuit.ru (дата обращения: 01.07.2014).
5. Хабрахабр [Электронный ресурс]. URL: http://habrahabr.ru/.
6. http://www.lessons-tva.info/ - На сайте представлены различные учебные материалы, в том числе онлайн учебники (авторские курсы) по дисциплинам: информатика, компьютерные сети и телекоммуникации, информатика и компьютерная техника.
7. Электронная библиотека https://znanium.com/
8. Электронная библиотека https://biblio-online.ru/

В распоряжении преподавателей и обучающихся имеется основное необходимое материально-техническое оборудование, Интернет-ресурсы, доступ к полнотекстовым электронным базам, книжный фонд библиотеки Московского государственного гуманитарно-экономического университета.

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ (МОДУЛЯ)

№ п/п	Наименование оборудованных учебных кабинетов, лабораторий	Перечень оборудования и технических средств обучения
1	Аудитория №511	Системный блок: Процессор Intel Pentium 2160, 1.8 GHz 2048 ОЗУ HDD: 250 ГБ Акустическая система Sven Монитор Samsung SyncMaster 920NW
2	Аудитория №402	Аудитория 402 11 компьютеров Системный блок 1: Процессор Intel(R) Core(TM) i5-4570 CPU @ 3.20GHz 8192 ОЗУ HDD Объем: 500 ГБ Монитор Benq G922HDA- 22 дюйма Системный блок 2: Процессор Intel(R) Core(TM) i5-4170 CPU @ 3.70GHz 4096 МБ ОЗУ HDD Объем: 500 ГБ Монитор DELL 178FP

		Системный блок 3: Процессор Intel(R) Core(TM) i3-6100 CPU @ 3.70GHz 4096 МБ ОЗУ SSD Объем: 120 ГБ Монитор Samsung 940NW Акустическая система 2.0 Интерактивная доска Smart Board Проектор Epson EH-TW535W
3	Аудитория №403	Системный блок: Процессор Intel® Pentium®Dual-Core E2180 2048 ОЗУ 320 HDD Монитор AOC 2470W Проектор Epson EH-TW5300 с акустической системой
4	Аудитория №404 (учебный зал судебных заседаний)	Системный блок: Процессор Intel® Pentium®Dual-Core E2180 2048 ОЗУ 320 HDD Монитор Samsung SyncMaster 920NW Акустическая система Sven Проектор Nec M260W **Материально-техническое оснащение:** Герб 1 Флаг 1 Трибуна для выступлений участников процесса 1 Молоток 1 Стол судейский 3 Стул судейский 3 Столы ученические 14 Стулья ученические 28 Доска трехстворчатая 1 Стол прокурора 1 Стол адвоката 1 Микрофон 1 Скамья подсудимых 1 Ограждение скамьи подсудимых 1 **Табличка** «Список дел, назначенных к слушанию» 1 **Плакаты** Судебное следствие (гл.37 УПК РФ (извлечение) 12 Технологии в зале судебных заседаний 5 ФЗ «О статусе судей в РФ» (извлечение) 3
5	Аудитория №405	Системный блок: Процессор Intel® Pentium®Dual-Core E5200 2048 ОЗУ 320 HDD Монитор Samsung SyncMaster 940NW Акустическая система Sven Проектор Nec M260W
6	Аудитория №409	Системный блок:

		Процессор Intel(R) Core(TM) i5-6400 CPU @ 2.70GHz 8192 ОЗУ SSD Объем: 128 ГБ Монитор AOC 2470W Проектор Epson EH-TW5300 с акустической системой
7	Аудитории № 410	1 моноблок Модель: HP 24 - 10145UR Процессор Intel(R) Core(TM) i7-9700T CPU @ 2GHz 16384 ОЗУ SSD Объем:500 ГБ Встроенные колонки, микрофон, вебкамера. Диагональ экрана - 24 дюйма
8	Аудитории № 411	1 моноблок Модель: HP 24 - 10145UR Процессор Intel(R) Core(TM) i7-9700T CPU @ 2GHz 16384 ОЗУ SSD Объем:500 ГБ Встроенные колонки, микрофон, вебкамера. Диагональ экрана - 24 дюйма
9	Аудитории № 412	1 моноблок Модель: HP 24 - 10145UR Процессор Intel(R) Core(TM) i7-9700T CPU @ 2GHz 16384 ОЗУ SSD Объем:500 ГБ Встроенные колонки, микрофон, вебкамера. Диагональ экрана - 24 дюйма
10	Аудитория №302	11 компьютеров Системный блок: Процессор Intel(R) Core(TM) i3-2100 CPU @ 3.10GHz 4096 МБ ОЗУ HDD Объем: 320 ГБ Монитор Acer P206HL - 20 дюймов Акустическая система Sven Интерактивная доска Smart Board Проектор Epson EH-TW535W
11	Аудитория №303	Системный блок: Процессор Intel® Pentium®Dual-Core E5200 2048 ОЗУ 320 HDD Монитор Samsung SyncMaster 940NW Акустическая система Sven Проектор Nec M260W
12	Аудитория №304	Системный блок: Процессор Intel® Core i3-2100 3,1 GHz 4096 ОЗУ 250 HDD Монитор Samsung SyncMaster 940NW Акустическая система Sven Проектор Nec NP410
13	Аудитория №305	Системный блок: Процессор Intel® Core™2 Duo E8500

		2048 ОЗУ 250 HDD Монитор Samsung SyncMaster 940NW Акустическая система Sven Проектор Nec M260W
14	Аудитория №306	12 компьютеров Системный блок: Процессор Intel(R) Core(TM) i5-2400 CPU @ 3.10GHz 8192 ОЗУ HDD Объем: 500 ГБ Монитор DELL EX231W - 24 дюйма Интерактивная доска Elite Panaboard UB-T880W с акустической системой Проектор Epson EB-440W
15	Аудитория №308	11 компьютеров Системный блок: Процессор Intel(R) Core(TM) i5-2400 CPU @ 3.10GHz 8192 ОЗУ HDD Объем: 500 ГБ Монитор DELL EX231W - 24 дюйма Интерактивная доска Elite Panaboard UB-T880W с акустической системой Проектор Epson EB-440W
16	Аудитория №2-120	11 компьютеров Системный блок: Процессор Intel(R) Core(TM) i5-6400 CPU @ 2.70GHz 8192 ОЗУ SSD Объем: 128 ГБ Монитор AOC 2470W - 24 дюйма Акустическая система Defender Интерактивная доска Smart Board Проектор Epson EH-TW535W
17	Аудитория №109	11 компьютеров Системный блок: Процессор Intel(R) Core(TM) i5-6400 CPU @ 2.70GHz 4096 МБ ОЗУ SSD Объем: 120 ГБ Монитор Philips PHL 243V5 - 24 дюйма Акустическая система Sven Интерактивная доска Smart Board Проектор Epson EH-TW535W
18	Аудитории № 309	1 моноблок Модель: Lenovo V530-24ICB Процессор Intel(R) Core(TM) i5-8400T CPU @ 1,7GHz 8192 ОЗУ SSD Объем:240 ГБ Встроенные колонки, микрофон, вебкамера. Диагональ экрана - 24 дюйма
19	Аудитории № 310	1 моноблок Модель: Lenovo V530-24ICB Процессор Intel(R) Core(TM) i5-8400T CPU @ 1,7GHz

		8192 ОЗУ SSD Объем:240 ГБ Встроенные колонки, микрофон, вебкамера. Диагональ экрана - 24 дюйма
20	Аудитории № 311	1 моноблок Модель: Lenovo V530-24ICB Процессор Intel(R) Core(TM) i5-8400T CPU @ 1,7GHz 8192 ОЗУ SSD Объем:240 ГБ Встроенные колонки, микрофон, вебкамера. Диагональ экрана - 24 дюйма

7. ОЦЕНКА КОМПЕТЕНЦИЙ ПО ИЗУЧАЕМОЙ ДИСЦИПЛИНЕ

№	Критерии оценки			
	«неудовлетворительно»	**«удовлетворительно»**	**«хорошо»**	**«отлично»**
	ЗНАТЬ			
1	Студент не способен самостоятельно выделять главные положения в изученном материале дисциплины. Не знает основных принципов информационной безопасности.	Студент усвоил основное содержание материала дисциплины, но имеет пробелы в усвоении материала. Имеет несистематизированные знания о принципах информационной безопасности.	Студент способен самостоятельно выделять главные положения в изученном материале. Знает основные методы и способы работы с различными источниками информации, принципы информационной безопасности.	Студент знает, понимает, выделяет главные положения в изученном материале и способен дать краткую характеристику основным идеям проработанного материала дисциплины. Знает основные методы и способы работы с различными источниками информации, принципы информационной безопасности. Показывает глубокое знание и понимание изучаемой дисциплины.
	УМЕТЬ			
2	Студент не умеет работать с электронными словарями, осуществлять поиск, хранение, обработку информации; представлять данные в требуемом формате с использованием информационных, компьютерных и сетевых технологий.	Студент затрудняется работать с электронными словарями, осуществлять поиск, хранение, обработку информации; представлять данные в требуемом формате с использованием информационных, компьютерных и сетевых технологий.	Студент умеет самостоятельно работать с электронными словарями, осуществлять поиск, хранение, обработку информации; представлять данные в требуемом формате с использованием информационных, компьютерных и сетевых технологий.	Студент умеет анализировать элементы, устанавливать связи между ними. Умеет самостоятельно работать с электронными словарями, осуществлять поиск, хранение, обработку информации; представлять данные в требуемом формате с использованием информационных, компьютерных и сетевых технологий. Способен работать с электронными словарями, различными источниками информации
	ВЛАДЕТЬ			
3	Студент не владеет методами,	Студент владеет основными	Студент владеет методами,	Студент владеет концептуально-

	способами и средствами получения, и переработки информации.	методами, способами и средствами получения, и переработки информации.	способами и средствами получения, и переработки информации, но допускает незначительные ошибки.	понятийным аппаратом, научным языком и терминологией изучаемой дисциплины. Владеет методами, способами и средствами получения, и переработки информации.
	Компетенция или ее часть не сформирована	Компетенция или ее часть сформирована на базовом уровне	Компетенция или ее часть сформирована на среднем уровне	Компетенция или ее часть сформирована на высоком уровне

8. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Интерактивные образовательные технологии, используемые в аудиторных занятиях и самостоятельной работе обучающихся

Семестр	Вид занятия (Л, ПР, ЛР)	Используемые интерактивные образовательные технологии	Количество часов
	Л	Лекция-беседа	10
	ПР	Практикум на ЭВМ, проблемный метод, взаимообучение.	6
	ЛР	Компьютерное тестирование	14
Итого:			30

9. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

9.1. Организация входного, текущего и промежуточного контроля обучения

Входное тестирование – не предусмотрены.

Текущий контроль – устный опрос, проверка практических и лабораторных работ.

Промежуточная аттестация – экзамен.

9.2. Тематика рефератов, проектов, творческих заданий, эссе и т.п.

Не предусмотрены

9.3. Курсовая работа

Не предусмотрена

9.4. Вопросы к зачету

Не предусмотрены

9.5. Вопросы к экзамену

1. Уточнение задач информационной безопасности организации. Изучение источников, рисков и форм атак на информацию в АСОИУ.
2. Изучение источников, рисков и форм атак на информацию в АСОИУ. Классификация рисков и основные задачи обеспечения безопасности информации в АСОИУ.
3. Изучение Российского законодательства по защите информационных технологий. Изучение нормативно-правовой информации, определяющей функционирование систем защиты. Разработка политики информационной безопасности организации.
4. Изучение международных и Государственных стандартов информационной безопасности.
5. Изучение симметричных и ассиметричных криптосистем для защиты компьютерной информации в АСОИУ.
6. Изучение стандартных алгоритмов шифрования. Безопасность и быстродействие криптосистем.
7. Изучение принципов идентификации и механизмов подтверждения подлинности пользователя. Правила формирования электронной цифровой подписи.

8. Изучение средств защиты локальных сетей от несанкционированного доступа. Анализ функционирования маршрутизаторов, шлюзов сетевого уровня и межсетевых экранов.

9. Анализ способов защиты информации в компьютерных сетях от разрушающего программного воздействия. Изучение методов борьбы с компьютерными вирусами и средств защиты информации в Internet. Угрозы исходящие от использования «электронной почты».

10. Изучение требований по обеспечению информационной безопасности к аппаратным средствам и программному обеспечению АСОИ. Порядок и правила организации аудита информационной безопасности АСОИУ и предприятия в целом.

11. Понятие информационной безопасности. Характеристики информации с позиции безопасности.

12. Классификация угроз безопасности информации.

13. Классификация угроз безопасности распределенных вычислительных систем

14. Модель OSI.

15. Объясните понятие «политика безопасности организации».

16. Какие разделы должна содержать документально оформленная политика безопасности?

17. Какие проблемы решает верхний уровень политики безопасности?

18. Какие задачи решает средний уровень политики безопасности?

19. Каковы особенности нижнего уровня политики безопасности?

20. Сформулируйте главную задачу стандартов информационной безопасности с позиций производителей и потребителей продуктов информационных технологий, а также специалистов по сертификации этих продуктов.

21. Назовите основные международные стандарты информационной безопасности.

22. Дайте краткую характеристику международного стандарта 17799 (BS 7799).

23. Каковы основные особенности германского стандарта BSI «Руководство по защите информационных технологий для базового уровня защищенности».

24. Перечислите стандарты для беспроводных сетей и дайте их краткую характеристику.

25. Назовите стандарты информационной безопасности для Internet.

9.6. Контроль освоения компетенций

Вид контроля	**Контролируемые темы (разделы)**	**Компетенции, компоненты которых контролируются**
Устный опрос	*1,2,3,4,5,6*	*ОПК-4*
Проверка практических и лабораторных работ	*1,2,3,4,5,6*	*ОПК-4*

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

№ п/п	Номер и дата протокола заседания кафедры	Перечень измененных пунктов	Подпись заведующего кафедрой