Федеральное государственное бюджетное образовательное учреждение
высшего образования
"Дальневосточный государственный университет путей сообщения"
(ДВГУПС)

УТВЕРЖДАЮ

Зав.кафедрой

(к202) Информационные технологии и системы

Попов М.А., канд. техн. наук, доцент

23.05.2025

РАБОЧАЯ ПРОГРАММА

дисциплины **Основы информационной безопасности**

10.05.03 Информационная безопасность автоматизированных систем

Составитель(и): к.т.н., доцент, Духовников В.К.

Обсуждена на заседании кафедры: (к202) Информационные технологии и системы

Протокол от 14.05.2025г. № 5

Обсуждена на заседании методической комиссии по родственным направлениям и специальностям: Протокол

г. Хабаровск
2025 г.

Визирование РПД для исполнения в очередном учебном году

Председатель МК РНС

__ _____ 2026 г.

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2026-2027 учебном году на заседании кафедры (к202) Информационные технологии и системы

Протокол от __ _____ 2026 г. № __
Зав. кафедрой Попов М.А., канд. техн. наук, доцент

Визирование РПД для исполнения в очередном учебном году

Председатель МК РНС

__ _____ 2027 г.

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2027-2028 учебном году на заседании кафедры (к202) Информационные технологии и системы

Протокол от __ _____ 2027 г. № __
Зав. кафедрой Попов М.А., канд. техн. наук, доцент

Визирование РПД для исполнения в очередном учебном году

Председатель МК РНС

__ _____ 2028 г.

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2028-2029 учебном году на заседании кафедры (к202) Информационные технологии и системы

Протокол от __ _____ 2028 г. № __
Зав. кафедрой Попов М.А., канд. техн. наук, доцент

Визирование РПД для исполнения в очередном учебном году

Председатель МК РНС

__ _____ 2029 г.

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2029-2030 учебном году на заседании кафедры (к202) Информационные технологии и системы

Протокол от __ _____ 2029 г. № __
Зав. кафедрой Попов М.А., канд. техн. наук, доцент

Рабочая программа дисциплины Основы информационной безопасности

разработана в соответствии с ФГОС, утвержденным приказом Министерства образования и науки Российской Федерации от 26.11.2020 № 1457

Квалификация **специалист по защите информации**

Форма обучения **очная**

ОБЪЕМ ДИСЦИПЛИНЫ (МОДУЛЯ) В ЗАЧЕТНЫХ ЕДИНИЦАХ С УКАЗАНИЕМ КОЛИЧЕСТВА АКАДЕМИЧЕСКИХ ЧАСОВ, ВЫДЕЛЕННЫХ НА КОНТАКТНУЮ РАБОТУ ОБУЧАЮЩИХСЯ С ПРЕПОДАВАТЕЛЕМ (ПО ВИДАМ УЧЕБНЫХ ЗАНЯТИЙ) И НА САМОСТОЯТЕЛЬНУЮ РАБОТУ ОБУЧАЮЩИХСЯ

Общая трудоемкость **3 ЗЕТ**

Часов по учебному плану 108
в том числе:
контактная работа 76
самостоятельная работа 32

Виды контроля в семестрах:
зачёты (семестр) 2

Распределение часов дисциплины по семестрам (курсам)

Семестр (<Курс>.<Семестр на курсе>)	**2 (1.2)**		Итого	
Недель	17			
Вид занятий	УП	РП	УП	РП
Лекции	32	32	32	32
Практические	32	32	32	32
Контроль самостоятельной работы	12	12	12	12
В том числе инт.	8	8	8	8
Итого ауд.	64	64	64	64
Контактная работа	76	76	76	76
Сам. работа	32	32	32	32
Итого	108	108	108	108

1. АННОТАЦИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
1.1	Модели нарушителя. Вредоносное программное обеспечение. Средства защиты информации. Вывод АС из эксплуатации. Компьютерно-техническая экспертиза. Информационное противоборство. Защита информации от утечки по техническим каналам.

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Код дисциплины:	Б1.О.09
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Физика
2.2	**Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	Организационное и правовое обеспечение информационной безопасности
2.2.2	Правоведение
2.2.3	Управление информационной безопасностью
2.2.4	Управление данными и их безопасность

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ), СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

УК-8: Способен создавать и поддерживать в повседневной жизни и в профессиональной деятельности безопасные условия жизнедеятельности для сохранения природной среды, обеспечения устойчивого развития общества, в том числе при угрозе и возникновении чрезвычайных ситуаций и военных конфликтов

Знать:

Классификацию и источники чрезвычайных ситуаций природного и техногенного происхождения; причины, признаки и последствия опасностей, способы защиты от чрезвычайных ситуаций; принципы организации безопасности труда на предприятии, технические средства защиты людей в условиях чрезвычайной ситуации.

Уметь:

Поддерживать безопасные условия жизнедеятельности; выявлять признаки, причины и условия возникновения чрезвычайных ситуаций; оценивать вероятность возникновения потенциальной опасности и принимать меры по ее предупреждению.

Владеть:

Методами прогнозирования возникновения опасных или чрезвычайных ситуаций; навыками по применению основных методов защиты в условиях чрезвычайных ситуаций.

ОПК-1: Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства;

Знать:

сущность и понятие информации, информационной безопасности, их роль в современном обществе значение для обеспечения объективных потребностей личности, общества и государства;
угрозы и источники угроз информационной безопасности современного общества;
основные методы обеспечения информационной безопасности.

Уметь:

применять основные методы обеспечения информационной безопасности.

Владеть:

базовой терминологией и гуманитарными аспектами в области информационной безопасности личности, общества и государства;
базовыми методами выявления и классификации угроз информационной безопасности современного общества, основными подходами к противодействию угрозам информационной безопасности.

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ), СТРУКТУРИРОВАННОЕ ПО ТЕМАМ (РАЗДЕЛАМ) С УКАЗАНИЕМ ОТВЕДЕННОГО НА НИХ КОЛИЧЕСТВА АКАДЕМИЧЕСКИХ ЧАСОВ И ВИДОВ УЧЕБНЫХ ЗАНЯТИЙ

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Компетен-ции	Литература	Инте ракт.	Примечание
	Раздел 1.						

1.1	1) Понятие национальной безопасности. 2) Виды безопасности и сферы жизнедеятельности личности, общества и государства. 3) Определение информационной безопасности 4) Место информационной безопасности в системе национальной безопасности /Лек/	2	4	ОПК-1 УК-8	Л1.1 Л1.2 Л1.3Л2.1 Э1 Э2 Э3 Э4 Э5	0	
1.2	1) Интересы личности в информационной сфере 2) Интересы общества в информационной сфере 3) Интересы государства в информационной сфере /Лек/	2	4	ОПК-1 УК-8	Л2.1 Э1 Э2	0	
1.3	. 1) Угрозы информационному обеспечению государственной политики Российской Федерации 2) Виды угроз информационной безопасности 3) Внешние источники угроз информационной безопасности 4) Внутренние источники угроз информационной безопасности государства /Лек/	2	4	ОПК-1 УК-8	Л1.2 Э3 Э4	0	
1.4	1) Информационное оружие, его классификация и возможности. 2) Доктрина информационной войны 3) Методы и средства ведения информационной войны 4) Понятие информационного противоборства . /Лек/	2	4	ОПК-1 УК-8	Л1.2 Л1.3 Э1 Э2 Э3 Э4 Э5	0	
1.5	1) Причины искажения информации, 2) Виды искажения информации 3) Каналы утечки информации 4) Естественные и искусственные каналы утечки информации /Лек/	2	4	ОПК-1 УК-8	Л1.1 Л1.2 Л1.3 Э1 Э2 Э3 Э4 Э5	2	лекция визуализация
1.6	1) Правовые, организационно-технические и экономические методы обеспечения информационной безопасности /Лек/	2	4	ОПК-1 УК-8	Л1.1 Л1.2 Э1 Э2 Э3 Э4 Э5	2	лекция визуализация
1.7	Основы комплексного обеспечения информационной безопасности. 1) Критерии и классы защищенности средств ВТ /Лек/	2	4	ОПК-1 УК-8	Л1.1 Л1.2 Э1 Э2 Э3 Э4 Э5	0	

1.8	1) Компьютерная система как объект информационной безопасности. 2) Информационные процессы как объект информационной безопасности 3) Влияние человеческого фактора на обеспечение информационной безопасности 4) Программно-аппаратные средства обеспечения информационной безопасности. 5) Классификация программно-аппаратных средств обеспечения информационной безопасности 6) Защита от несанкционированного доступа 7) Антивирусная защита /Лек/	2	4	ОПК-1 УК-8	Л1.1 Л1.2 Э1 Э2 Э3 Э4 Э5	0	
1.9	ПЗ №1.Введение в дисциплину. Терминологические основы информационной безопасности. Основные понятия и определения. /Пр/	2	6	ОПК-1 УК-8	Л1.1 Л1.2Л3.1	2	метод-проекта
1.10	ПЗ № 2. Понятие национальной безопасности, виды безопасности. Информационная безопасность РФ. /Пр/	2	4	ОПК-1 УК-8	Л1.1 Л1.2 Л1.3Л3.1 Э1	2	метод-проекта
1.11	ПЗ №3. Общеметодологические принципы теории информационной безопасности. Комплексность. /Пр/	2	4	ОПК-1 УК-8	Л1.1 Л1.2 Л1.3Л3.1 Э1 Э2 Э3 Э4	0	метод-проекта
1.12	ПЗ №4. Угрозы. Классификация и анализ угроз информационной безопасности. /Пр/	2	4	ОПК-1 УК-8	Л1.1 Л1.2Л3.1 Э1 Э3 Э4	0	метод-проекта
1.13	ПЗ №5. Угрозы. Классификация и анализ угроз информационной безопасности. (продолжение) /Пр/	2	4	ОПК-1 УК-8	Л1.2 Л1.3Л3.1 Э1 Э2 Э3	0	метод-проекта
1.14	ПЗ №6. Методы нарушения конфиден-циальности, целостности и доступности информации. /Пр/	2	4	ОПК-1 УК-8	Л1.2 Л1.3Л3.1 Э1 Э2 Э3	0	метод-проекта
1.15	ПЗ №7. Причины, виды, каналы утечки и искажения информации. /Пр/	2	4	ОПК-1 УК-8	Л1.2 Л1.3Л3.1 Э1 Э2 Э3 Э4 Э5	0	метод-проекта
1.16	ПЗ №8. Причины, виды, каналы утечки и искажения информации (продолжение). /Пр/	2	2	ОПК-1 УК-8	Л1.1 Л1.2 Э1 Э2	0	метод-проекта
	Раздел 2. самостоятельная работа						
2.1	подготовка к лекциям /Ср/	2	12	ОПК-1 УК-8	Л1.1 Л1.2 Л1.3 Э1 Э2 Э3 Э4 Э5	0	
2.2	подготовка к практическим занятиям /Ср/	2	12	ОПК-1 УК-8	Л1.1 Л1.2 Л1.3 Э1 Э2 Э3 Э4 Э5	0	
	Раздел 3. зачет						
3.1	/Зачёт/	2	8	ОПК-1 УК-8	Л1.1 Л1.2 Л1.3Л2.1 Э1 Э2 Э3 Э4 Э5	0	

5. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

Размещены в приложении

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

6.1. Рекомендуемая литература

6.1.1. Перечень основной литературы, необходимой для освоения дисциплины (модуля)

	Авторы, составители	Заглавие	Издательство, год
Л1.1	Бабаш А. В., Баранова Е. К.	Информационная безопасность. Лабораторный практикум: учеб. пособие	Москва: КноРус, 2016,
Л1.2	Загинайлов Ю. Н.	Основы информационной безопасности: курс визуальных лекций	М.|Берлин: Директ-Медиа, 2015, http://biblioclub.ru/index.php?page=book&id=362895
Л1.3	Нестеров С. А.	Основы информационной безопасности	Санкт-Петербург: Издательство Политехнического университета, 2014, http://biblioclub.ru/index.php?page=book&id=363040

6.1.2. Перечень дополнительной литературы, необходимой для освоения дисциплины (модуля)

	Авторы, составители	Заглавие	Издательство, год
Л2.1	Долгов В.А., Анисимов В.В.	Криптографические методы защиты информации: учеб. пособие	Хабаровск: Изд-во ДВГУПС, 2008,

6.1.3. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю)

	Авторы, составители	Заглавие	Издательство, год
Л3.1	Березюк Л.П.	Организационное обеспечение информационной безопасности: учеб. пособие	Хабаровск: Изд-во ДВГУПС, 2008,

6.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет", необходимых для освоения дисциплины (модуля)

Э1	основы информационной безопасности	http://www.intuit.ru/studies/courses/697/553/lecture/12442
Э2	Электронно-библиотечная система «Университетская библиотека ONLINE»	biblioclub.ru
Э3	Галатенко, В.А. Основы информационной безопасности.	www.intuit.ru
Э4	Галатенко, В.А. Информационная безопасность: основные стандарты и спецификации.	www.intuit.ru
Э5	ЦИК РФ	cikrf.ru

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

6.3.1 Перечень программного обеспечения

Windows 7 Pro - Операционная система, лиц. 60618367
Office Pro Plus 2007 - Пакет офисных программ, лиц.45525415
АСТ тест - Комплекс программ для создания банков тестовых заданий, организации и проведения сеансов тестирования, лиц.АСТ.РМ.А096.Л08018.04, дог.372
Free Conference Call (свободная лицензия)
Zoom (свободная лицензия)

6.3.2 Перечень информационных справочных систем

Профессиональная база данных, информационно-справочная система КонсультантПлюс - http://www.consultant.ru
Профессиональная база данных, информационно-справочная система Техэксперт - https://cntd.ru/

7. ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

Аудитория	Назначение	Оснащение
201	Компьютерный класс для практических и лабораторных занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также для самостоятельной работы.	Технические средства обучения: компьютерная техника с возможностью подключения к сети Интернет, свободному доступу в ЭБС и ЭИОС, проектор. Лицензионное программное обеспечение: Windows 10 Pro - MS DreamSpark 700594875, 7-Zip 16.02 (x64) - Свободное ПО, Autodesk 3ds Max 2021, Autodesk AutoCAD 2021, Autodesk AutoCAD Architecture 2021, Autodesk Inventor 2021, Autodesk Revit 2021- Для учебных заведений предоставляется бесплатно, Foxit Reader-Свободное ПО, MATLAB R2013b - Контракт 410 от 10.08.2015,

Аудитория	Назначение	Оснащение
		Microsoft Office Профессиональный плюс 2007 - 43107380, Microsoft Visio профессиональный 2013 - MS DreamSpark 700594875, Microsoft Visual Studio Enterprise 2017- MS DreamSpark 700594875, Mozilla Firefox 99.0.1 - Свободное ПО, Opera Stable 38.0.2220.41 - Свободное ПО, PTC Mathcad Prime 3.0 - Контракт 410 от 10.08.2015 лиц. 3A1874498, КОМПАС-3D V19 - КАД-19-0909, АСТ-Тест лиц. АСТ.РМ.А096.Л08018.04, Договор № Л-128/21 от 01.06.2021 с 01 июля 2021 по 30 июня 2022. ПЭВМ с возможностью выхода в интернет по расписанию Windows 10 Pro Контракт №235 ДВГУПС от 24.08.2021; Office Pro Plus 2019 Контракт №235 от 24.08.2021; Kaspersky Endpoint Security Контракт № 0322100012923000077 от 06.06.2023; КОМПАС-3D V19 Контракт № 995 от 09.10.2019; nanoCAD Номер лицензии: NC230P-81412 Срок действия: с 01.08.2023 по 31.07.2024;
424	Учебная аудитория для проведения лекционных, лабораторных и практических занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации. "Основы информационной безопасности".	комплект учебной мебели, доска маркерная, проектор Windows 7 Pro Номер лицензии: 60618367 Контракт 208 ДВГУПС от 09.07.2012 бессрочная Office Pro Plus 2007 Номера лицензий: 45525415 (ГК 111 от 22.04.2009, бессрочная), 46107380 (Счет 00000000002802 от 14.11.07, бессрочная)
101	Компьютерный класс для практических, лабораторных занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также для самостоятельной работы. Кабинет информатики (компьютерные классы) *.	комплект учебной мебели. Технические средства обучения: компьютерная техника с возможностью подключения к сети Интернет, свободному доступу в ЭБС и ЭИОС (Intel(R) Core(TM) i5-3570K CPU @ 3.40GHz, 4Gb, int Video, 1 Tb, DVD+RW, ЖК 19). Лицензионное программное обеспечение: Windows 10 Pro - MS DreamSpark 700594875, 7-Zip 16.02 (x64) (свободно распространяемое ПО), Autodesk 3ds Max 2019, Autodesk AutoCAD 2021, Autodesk AutoCAD Architecture 2021, Autodesk Inventor 2021, Autodesk Revit 2021- Для учебных заведений предоставляется бесплатно, Foxit Reader (свободно распространяемое ПО), MATLAB R2013b - Контракт 410 от 10.08.2015, Microsoft Office Профессиональный плюс 2007 - 43107380, Microsoft Visio профессиональный 2013 - MS DreamSpark 700594875, Microsoft Visual Studio Enterprise 2017- MS DreamSpark 700594875, Mozilla Firefox 99.0.1 (свободно распространяемое ПО), Opera Stable 38.0.2220.41 (свободно распространяемое ПО), PTC Mathcad Prime 3.0 - Контракт 410 от 10.08.2015, лиц. 3A1874498, КОМПАС-3D V19 - КАД-19-0909.ПЭВМ с возможностью выхода в интернет по расписанию Windows 10 Pro Контракт №235 ДВГУПС от 24.08.2021; Office Pro Plus 2019 Контракт №235 от 24.08.2021; Kaspersky Endpoint Security Контракт № 0322100012923000077 от 06.06.2023; КОМПАС-3D V19 Контракт № 995 от 09.10.2019; nanoCAD Номер лицензии: NC230P-81412 Срок действия: с 01.08.2023 по 31.07.2024;
109	Компьютерный класс для практических и лабораторных занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также для самостоятельной работы. Зал инклюзивного образования.	Технические средства обучения: компьютерная техника с возможностью подключения к сети Интернет, свободному доступу в ЭБС и ЭИОС (Core i3- 8100 (3.60GHz), 8 Gb, int Video, 931GB, ЖК 24", ЖК панель 55"), 1 специализированный ПК для инклюзивного образования. Лицензионное программное обеспечение: Windows 10 Pro - MS DreamSpark 700594875, 7-Zip 16.02 (x64) - Свободное ПО, Autodesk 3ds Max 2021, Autodesk AutoCAD 2021, Autodesk AutoCAD Architecture 2021, Autodesk Inventor 2021, Autodesk Revit 2021- Для учебных заведений предоставляется бесплатно, Foxit Reader- Свободное ПО, MATLAB R2013b - Контракт 410 от 10.08.2015, Microsoft Office Профессиональный плюс 2007 - 43107380, Microsoft Visio профессиональный 2013 - MS DreamSpark 700594875, Microsoft Visual Studio Enterprise 2017- MS DreamSpark 700594875, Mozilla Firefox 99.0.1 - Свободное ПО, Opera Stable 38.0.2220.41 - Свободное ПО, PTC Mathcad Prime 3.0 - Контракт 410 от 10.08.2015 лиц. 3A1874498, КОМПАС-3D V19 - КАД-19-0909, АСТ-Тест лиц. АСТ.РМ.А096.Л08018.04, Договор № Л-128/21 от 01.06.2021 с 01 июля 2021 по 30 июня 2022.ПЭВМ с возможностью выхода в интернет по расписанию Windows 10 Pro Контракт №235 ДВГУПС

Аудитория	Назначение	Оснащение
		от 24.08.2021; Office Pro Plus 2019 Контракт №235 от 24.08.2021; Kaspersky Endpoint Security Контракт № 0322100012923000077 от 06.06.2023; КОМПАС-3D V19 Контракт № 995 от 09.10.2019; nanoCAD Номер лицензии: NC230P-81412 Срок действия: с 01.08.2023 по 31.07.2024;
108	Компьютерный класс для практических и лабораторных занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также для самостоятельной работы.	Технические средства обучения: компьютерная техника с возможностью подключения к сети Интернет, свободному доступу в ЭБС и ЭИОС (Intel(R) Core(TM) i5-4670 CPU @ 3.40GHz, 8 Gb, 1Tb, DVD+RW, ЖК 23"), проектор, экран для проектора. Лицензионное программное обеспечение: Windows 10 Pro - MS DreamSpark 700594875, 7-Zip 16.02 (x64) - Свободное ПО, Autodesk 3ds Max 2021, Autodesk AutoCAD 2021, Autodesk AutoCAD Architecture 2021, Autodesk Inventor 2021, Autodesk Revit 2021- Для учебных заведений предоставляется бесплатно, Foxit Reader- Свободное ПО, MATLAB R2013b - Контракт 410 от 10.08.2015, Microsoft Office Профессиональный плюс 2007 - 43107380, Microsoft Visio профессиональный 2013 - MS DreamSpark 700594875, Microsoft Visual Studio Enterprise 2017- MS DreamSpark 700594875, Mozilla Firefox 99.0.1 - Свободное ПО, Opera Stable 38.0.2220.41 - Свободное ПО, PTC Mathcad Prime 3.0 - Контракт 410 от 10.08.2015 лиц. 3A1874498, КОМПАС-3D V19 - КАД-19-0909, АСТ-Тест лиц. АСТ.РМ.А096.Л08018.04, Договор № Л-128/21 от 01.06.2021 с 01 июля 2021 по 30 июня 2022. ПЭВМ с возможностью выхода в интернет по расписанию Windows 10 Pro Контракт №235 ДВГУПС от 24.08.2021; Office Pro Plus 2019 Контракт №235 от 24.08.2021; Kaspersky Endpoint Security Контракт № 0322100012923000077 от 06.06.2023; КОМПАС-3D V19 Контракт № 995 от 09.10.2019; nanoCAD Номер лицензии: NC230P-81412 Срок действия: с 01.08.2023 по 31.07.2024;

8. МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

С целью эффективной организации учебного процесса студентам в начале семестра представляется учебно-методическое и информационное обеспечение, приведенное в данной рабочей программе. В процессе обучения студенты должны, в соответствии с планом выполнения самостоятельных работ (табл. 1 приложения), изучать теоретические материалы по предстоящему занятию и формулировать вопросы, вызывающие у них затруднения для рассмотрения на практических занятиях. При выполнении самостоятельной работы необходимо руководствоваться литературой, предусмотренной рабочей программой и указанной преподавателем.
Курс имеет одинаковую ценность практических и лекционных занятий. Изучение теоретического материала не менее важно чем практические навыки, получаемые на практических и индивидуальных занятиях, при самостоятельной подготовке. Лекционные занятия должны проходить в аудиториях, предназначенных для проведения лекций. Расстояние от лектора до первых рядов аудитории не менее 2,5 метров. Угол обзора с последних рядов аудитории должен обеспечивать полный обзор досок, экранов и лектора. Слышимость на последних рядах должна быть достаточной.
Желательно использование маркерных досок, т.к. они более контрастны, позволяют использовать различные цвета и способствуют лучшему усвоению материала. Желательно использование стационарного проектора (с компьютером) для показа наглядного материала. Проведение практических занятий: практические занятия обязательно проводить в компьютерных классах, оборудованных проектором и экраном. Проектор должен быть подключен либо к стационарному компьютеру, либо должен быть ноутбук, с которого будут вестись презентации. Компьютеры должны быть объединены в локальную сеть и иметь легко доступные USB-разъмы на передней панели, либо с помощью USB-удлинителей. В целях сохранения результатов работы желательно, чтобы студенты имели при себе компактные USB-носители информации.

Преподавание дисциплины предусматривает следующие формы организации учебного процесса: лекции,практические занятия, самостоятельная работа.
Самостоятельная работа – изучение студентами теоретического материала, подготовка к лекциям, лабораторным работам и практическим занятиям, оформление конспектов лекций, написание рефератов, отчетов, работа в электронной образовательной среде и др. для приобретения новых теоретических и фактических знаний, теоретических и практических умений.
При подготовке к практическим работам необходимо изучить рекомендованную учебную литературу, изучить указания к практической работе, составленные преподавателем.
Практические работы проводятся в компьютерных классах, на компьютерах которых установлено соответствующее программное обеспечение, позволяющее решать поставленные задачи обработки информации.

Технология организации самостоятельной работы обучающихся включает использование информационных и материально-

технических ресурсов университета: библиотеку с читальным залом, укомплектованную в соответствии с существующими нормами; учебно-методическую базу учебных кабинетов, лабораторий и зала кодификации; компьютерные классы с возможностью работы в Интернет; аудитории для консультационной деятельности; учебную и учебно-методическую литературу, разработанную с учетом увеличения доли самостоятельной работы студентов, и иные методические материалы.

При подготовке к зачету необходимо ориентироваться на конспекты лекций, рабочую программу дисциплины, нормативную, учебную и рекомендуемую литературу. Основное в подготовке к сдаче зачета - это повторение всего материала дисциплины, по которому необходимо сдавать зачет. При подготовке к сдаче зачета студент весь объем работы должен распределять равномерно по дням, отведенным для подготовки к зачету, контролировать каждый день выполнение намеченной работы. В период подготовки к зачету студент вновь обращается к уже изученному (пройденному) учебному материалу.

Оформление и защита производится в соответствии со стандартом ДВГУПС СТ 02-11-17 «Учебные студенческие работы. Общие положения»
Оценка знаний по дисциплине производится в соответствии со стандартом ДВГУПС СТ 02-28-14 «Формы, периодичность и порядок текущего контроля успеваемости и промежуточной аттестации»

Оценочные материалы при формировании рабочих программ дисциплин (модулей)

Специальность 10.05.03 Информационная безопасность автоматизированных систем

Специализация: специализация N 9 "Безопасность автоматизированных систем на транспорте" (по видам)

Дисциплина: Основы информационной безопасности

Формируемые компетенции:

1. Описание показателей, критериев и шкал оценивания компетенций.

Показатели и критерии оценивания компетенций

Объект оценки	Уровни сформированности компетенций	Критерий оценивания результатов обучения
Обучающийся	Низкий уровень Пороговый уровень Повышенный уровень Высокий уровень	Уровень результатов обучения не ниже порогового

Шкалы оценивания компетенций при сдаче зачета

Достигнутый уровень результата обучения	Характеристика уровня сформированности компетенций	Шкала оценивания
Пороговый уровень	Обучающийся: - обнаружил на зачете всесторонние, систематические и глубокие знания учебно-программного материала; - допустил небольшие упущения в ответах на вопросы, существенным образом не снижающие их качество; - допустил существенное упущение в ответе на один из вопросов, которое за тем было устранено студентом с помощью уточняющих вопросов; - допустил существенное упущение в ответах на вопросы, часть из которых была устранена студентом с помощью уточняющих вопросов	Зачтено
Низкий уровень	Обучающийся: - допустил существенные упущения при ответах на все вопросы преподавателя; - обнаружил пробелы более чем 50% в знаниях основного учебно-программного материала	Не зачтено

Описание шкал оценивания

Компетенции обучающегося оценивается следующим образом:

Планируемый уровень результатов освоения	Содержание шкалы оценивания достигнутого уровня результата обучения			
	Неудовлетворительн	Удовлетворительно	Хорошо	Отлично
	Не зачтено	Зачтено	Зачтено	Зачтено

Знать	Неспособность обучающегося самостоятельно продемонстрировать наличие знаний при решении заданий, которые были представлены преподавателем вместе с образцом их решения.	Обучающийся способен самостоятельно продемонстриро-вать наличие знаний при решении заданий, которые были представлены преподавателем вместе с образцом их решения.	Обучающийся демонстрирует способность к самостоятельному применению знаний при решении заданий, аналогичных тем, которые представлял преподаватель, и при его консультативной	Обучающийся демонстрирует способность к самостоятельно-му применению знаний в выборе способа решения неизвестных или нестандартных заданий и при консультативной поддержке в части междисциплинарных
Уметь	Отсутствие у обучающегося самостоятельности в применении умений по использованию методов освоения учебной дисциплины.	Обучающийся демонстрирует самостоятельность в применении умений решения учебных заданий в полном соответствии с образцом, данным преподавателем.	Обучающийся продемонстрирует самостоятельное применение умений решения заданий, аналогичных тем, которые представлял преподаватель, и при его консультативной поддержке в части современных проблем.	Обучающийся демонстрирует самостоятельное применение умений решения неизвестных или нестандартных заданий и при консультативной поддержке преподавателя в части междисциплинарных связей.
Владеть	Неспособность самостоятельно проявить навык решения поставленной задачи по стандартному образцу повторно.	Обучающийся демонстрирует самостоятельность в применении навыка по заданиям, решение которых было показано преподавателем.	Обучающийся демонстрирует самостоятельное применение навыка решения заданий, аналогичных тем, которые представлял преподаватель, и при его консультативной поддержке в части современных проблем.	Обучающийся демонстрирует самостоятельное применение навыка решения неизвестных или нестандартных заданий и при консультативной поддержке преподавателя в части междисциплинарных связей.

2. Перечень вопросов и задач к экзаменам, зачетам, курсовому проектированию, лабораторным занятиям. Образец экзаменационного билета

1. Сущность и основные отличия информационных войн.
2. Формы психологического воздействия. Убеждение и внушение.
3. Классификация и виды информационно-психологического оружия.
4. Классификация и виды информационно-технологического оружия.
5. Защита от неинформированности как вид информационной защиты. Право на доступ к информации.
6. Виды опасных для человека информационных воздействий. Избыточная информация. Реакции человека на информационную перегрузку.
7. Защита от опасной информации в формах клеветы, угроз, обмана, вредоносной пропаганды и агитации.
8. Ценность информации, чем она определяется.
9. Информация и эмоции.
10. Копирование как уникальное свойство информации.
11. Носители информации и их характеристика. Информация и сообщение.
12. Представление информации на физическом уровне. Свойства вещественных и энергетических носителей информации.
13. Формы и особенности представления компьютерной информации.
14. Особенности представления и защиты информации на уровне средств взаимодействия с носителем.
15. Логический уровень представления компьютерной информации. Уязвимость и особенности

реализации защиты информации на логическом уровне.

16. Синтаксический уровень представления информации.
17. Виды и характеристика способов информационной защиты на синтаксическом уровне.
18. Признаковая информация и формы ее защиты.
19. Виды кодирования информации.
20. Способы сжатия и декомпрессии компьютерной информации.
21. Характеристика информации как объекта собственности.
22. Общая характеристика информационных угроз.
23. Угрозы конфиденциальности, целостности и доступности.
24. Субъекты (источники и носители) информационных угроз.
25. Информационные нарушители и их классификация
26. Угрозы информации, связанные с человеческим фактором.
27. Пользователи как источники информационных угроз
28. «Внешние» нарушители информационной безопасности
29. Характеристика информационных нарушителей с точки зрения их осведомленности, оснащенности и подготовленности
30. Демаскирующие признаки человека-нарушителя: геометрическая и биомеханическая модель
31. Демаскирующие признаки человека-нарушителя: физико-химическая и социальная модель
32. Демаскирующие признаки вредоносной программы
33. Демаскирующие признаки специальных технических средств
34. Модель абсолютной защиты для сложной информационной системы.
35. Стратегии информационной защиты.
36. Активные и пассивные способы обнаружения информационных угроз.
37. Стратегия пассивной защиты
38. Стратегия маскировки, имитации и дезинформации
39. Стратегия ликвидации источников и носителей информационных угроз
40. Сущность энергетического скрытия информации
41. Информационное скрытие на логическом и синтаксическом уровнях
42. Модель канала связи.
43. Угрозы информации в каналах связи
44. Методы защиты информации в каналах связи.
45. Виды и способы сокрытия источников и получателей сообщений в открытых информационных сетях.
46. Характеристика, этапы и демаскирующие признаки удаленного доступа к сетевой ЭВМ.
47. Модель комплексной защиты информации и ее элементы.
48. Общая характеристика нормативно-правовой защиты информации.
49. Защищаемая законом информация. Особенности правовой защиты информации ограниченного доступа.
50. Основные принципы защиты сведений, составляющих государственную тайну.
51. Основные положения о защите коммерческой тайны
52. Сущность и основные принципы организационно-распорядительной защиты информации.
53. Инженерно-техническая защита информации: постулаты, тактические требования, основные элементы защиты.
54. Объекты информатизации и их классификация.
55. Защита от утечки информации по техническим каналам. Термины и определения. Каналы утечки.
56. Основные способы защиты информации от утечки по техническим каналам.
57. Основные принципы защиты информации от электронных средств негласного подслушивания.
58. Общие принципы защиты компьютерной информации и ЭВМ от вредоносных программ.
59. Общая характеристика систем управления доступом.
60. Системы управления физическим доступом. Специальные режимы работы СУФД.
61. Особенности систем управления логическим доступом. Виды удаленного доступа.
62. Защита объектов информатизации, технических средств обработки информации и машинных носителей от дестабилизирующих факторов окружающей среды. Классификация дестабилизирующих воздействий и способов защиты от них.
63. Понятия об информационных и компьютерных преступлениях.
64. Основные причины и особенности компьютерных преступлений.
65. Уголовно наказуемые формы распространения и разглашения информации
66. Уголовно наказуемые формы фальсификации информации
67. Формы законного и незаконного собирания информации.
68. Незаконное хранение, передача, предоставление и использование информации.

69. Компьютерная система как орудие преступления.
70. Компьютерная система как средство совершения преступления и хранилище информации о преступной деятельности.
71. Государственные органы власти, обеспечивающие защиту информации в России.
72. Основные федеральные законы в области защиты информации.
73. Технология двухфакторной аутентификации.
74. Идентификация в вычислительной системе.
75. Циклические коды.
76. Недостатки систем хеширования.
77. Способы защиты информации.
78. Стратегии защиты информации.
79. Периметр охраняемой территории.
80. «Абсолютная» система защиты.

3. Тестовые задания. Оценка по результатам тестирования.

1. В каком правовом документе дается определение термина «информационная безопасность»?
а) Федеральный закон «О безопасности».
б) Стратегия национальной безопасности Российской Федерации до 2020 года.
в) Доктрина информационной безопасности Российской Федерации.
г) Конституция.
д) Федеральный закон «Об информации, информационных технологиях и о защите информации».

2. Основными аспектами деятельности (задачами) информационной безопасности выступают –
а) Конфиденциальность.
б) Доступность.
в) Системность.
г) Целостность.
д) Защита информации.

Полный комплект тестовых заданий в корпоративной тестовой оболочке АСТ размещен на сервере УИТ ДВГУПС, а также на сайте Университета в разделе СДО ДВГУПС (образовательная среда в личном кабинете преподавателя).

Соответствие между бальной системой и системой оценивания по результатам тестирования устанавливается посредством следующей таблицы:

Объект оценки	Показатели оценивания результатов обучения	Оценка	Уровень результатов обучения
Обучающийся	60 баллов и менее	«Неудовлетворительно»	Низкий уровень
	74 – 61 баллов	«Удовлетворительно»	Пороговый уровень
	84 – 75 баллов	«Хорошо»	Повышенный уровень
	100 – 85 баллов	«Отлично»	Высокий уровень

4. Оценка ответа обучающегося на вопросы, задачу (задание) экзаменационного билета, зачета, курсового проектирования.

Оценка ответа обучающегося на вопросы, задачу (задание) экзаменационного билета, зачета

Элементы оценивания	Содержание шкалы оценивания			
	Неудовлетворительн	Удовлетворитель	Хорошо	Отлично
	Не зачтено	Зачтено	Зачтено	Зачтено
Соответствие ответов формулировкам вопросов (заданий)	Полное несоответствие по всем вопросам.	Значительные погрешности.	Незначительные погрешности.	Полное соответствие.

Структура, последовательность и логика ответа. Умение четко, понятно, грамотно и свободно излагать свои мысли	Полное несоответствие критерию.	Значительное несоответствие критерию.	Незначительное несоответствие критерию.	Соответствие критерию при ответе на все вопросы.
Знание нормативных, правовых документов и специальной литературы	Полное незнание нормативной и правовой базы и специальной литературы	Имеют место существенные упущения (незнание большей части из документов и специальной литературы по названию, содержанию и т.д.).	Имеют место несущественные упущения и незнание отдельных (единичных) работ из числа обязательной литературы.	Полное соответствие данному критерию ответов на все вопросы.
Умение увязывать теорию с практикой, в том числе в области профессиональной работы	Умение связать теорию с практикой работы не проявляется.	Умение связать вопросы теории и практики проявляется редко.	Умение связать вопросы теории и практики в основном проявляется.	Полное соответствие данному критерию. Способность интегрировать знания и привлекать сведения из различных научных сфер.
Качество ответов на дополнительные вопросы	На все дополнительные вопросы преподавателя даны неверные ответы.	Ответы на большую часть дополнительных вопросов преподавателя даны неверно.	. Даны неполные ответы на дополнительные вопросы преподавателя. 2. Дан один неверный ответ на дополнительные вопросы преподавателя.	Даны верные ответы на все дополнительные вопросы преподавателя.

Примечание: итоговая оценка формируется как средняя арифметическая результатов элементов оценивания.