

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



11.06.2021

РАБОЧАЯ ПРОГРАММА

дисциплины **Управление информационной безопасностью**

10.04.01 Информационная безопасность

Составитель(и): доцент, Рак Е.В.; канд. техн. наук, доцент, Дунин В.С.

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

Протокол от 09.06.2021г. № 6

Обсуждена на заседании методической комиссии учебно-структурного подразделения: Протокол от
11.06.2021 г. № 6

г. Хабаровск
2022 г.

Визирование РПД для исполнения в очередном учебном году

Председатель МК РНС

__ _____ 2023 г.

Рабочая программа пересмотрена, обсуждена и одобрена для
исполнения в 2023-2024 учебном году на заседании кафедры
(к202) Информационные технологии и системы

Протокол от __ _____ 2023 г. № __
Зав. кафедрой Попов М.А., канд. техн. наук, доцент

Визирование РПД для исполнения в очередном учебном году

Председатель МК РНС

__ _____ 2024 г.

Рабочая программа пересмотрена, обсуждена и одобрена для
исполнения в 2024-2025 учебном году на заседании кафедры
(к202) Информационные технологии и системы

Протокол от __ _____ 2024 г. № __
Зав. кафедрой Попов М.А., канд. техн. наук, доцент

Визирование РПД для исполнения в очередном учебном году

Председатель МК РНС

__ _____ 2025 г.

Рабочая программа пересмотрена, обсуждена и одобрена для
исполнения в 2025-2026 учебном году на заседании кафедры
(к202) Информационные технологии и системы

Протокол от __ _____ 2025 г. № __
Зав. кафедрой Попов М.А., канд. техн. наук, доцент

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

Рабочая программа дисциплины Управление информационной безопасностью
разработана в соответствии с ФГОС, утвержденным приказом Министерства образования и науки Российской Федерации от 26.11.2020 № 1455

Квалификация **магистр**

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 **4 ЗЕТ**

Часов по учебному плану	144	Виды контроля в семестрах:
в том числе:		экзамены (семестр) 3
контактная работа	76	курсовые работы 3
самостоятельная работа	32	
часов на контроль	36	

Распределение часов дисциплины по семестрам (курсам)

Семестр (<Курс>.<Семестр на курсе>)	3 (2.1)		Итого	
	9 2/6			
Неделя				
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
Часы на контроль	36	36	36	36
Итого	144	144	144	144

1. АННОТАЦИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

1.1	Ключевые аспекты и вопросы формирования информационной безопасности современного предприятия. Защищенная информационная система. Уровни и структура ИБ. Модели и стандарты в сфере ИБ и управления рисками ИБ. Технологии и методы реализации ИБ. Ком-плексная защита информационной инфраструктуры.
-----	--

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Код дисциплины:	Б1.О.05
2.1	Требования к предварительной подготовке обучающегося:
2.1.1	Безопасность систем баз данных
2.1.2	Технологии обеспечения информационной безопасности
2.2	Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:
2.2.1	Обеспечение безопасности современных серверов баз данных
2.2.2	Интеллектуальные системы и технологии

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

ОПК-3: Способен разрабатывать проекты организационно-распорядительных документов по обеспечению информационной безопасности;

Знать:

знать основы отечественных и зарубежных стандартов в области сертификации и аттестации объектов информатизации, в области управления информационной безопасностью с целью разработки проектов организационно-распорядительных документов; перспективные направления развития средств и методов обеспечения кибербезопасности

Уметь:

выбирать и анализировать показатели качества и критерии оценки систем и методов и средств обеспечения кибербезопасности; уметь разрабатывать технические задания на создание подсистем обеспечения информационной безопасности

Владеть:

владеть навыками разработки политик безопасности различных уровней, владеть навыками расчета и управления рисками информационной безопасности, навыками разработки положения о применимости механизмов контроля в контексте управления рисками информационной безопасности; методами формальной постановки и решения задач обеспечения кибербезопасности

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

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Компетен-ции	Литература	Инте ракт.	Примечание
	Раздел 1. Лекции						
1.1	Документирование политики информа- ционной безопасности. Анализ полити- ки ИБЗ /Лек/	3	2	ОПК-3	Л1.1 Л1.2Л2.1Л3.1 Э1 Э2	0	
1.2	Координация вопросов обеспечения ИБ. Распределение обязанностей по обеспечению ИБ /Лек/	3	2	ОПК-3	Л1.1 Л1.2Л2.1Л3.1 Э1 Э2	0	
1.3	Обеспечение безопасности при нали- чии доступа сторонних организаций к информационным системам /Лек/	3	2	ОПК-3	Л1.1 Л1.2Л2.1Л3.1 Э1 Э2	0	
1.4	Ответственность за защиту активов организации. Классификация инфор- мации /Лек/	3	2	ОПК-3	Л1.1 Л1.2Л2.1Л3.1 Э1 Э2	0	
1.5	Правила безопасности, связанные с персоналом /Лек/	3	2	ОПК-3	Л1.1 Л1.2Л2.1Л3.1 Э1 Э2	0	

1.6	Физическая защита и защита от воздействия окружающей среды /Лек/	3	2	ОПК-3	Л1.1 Л1.2Л2.1Л3.1 Э1 Э2	0	
1.7	Эксплуатация средств и ответственность. Управление поставкой услуг лицами и/или сторонними организациями /Лек/	3	2	ОПК-3	Л1.1 Л1.2Л2.1Л3.1 Э1 Э2	0	
1.8	Защита от вредоносного кода и мобильного кода. Резервирование. Управление безопасностью сети /Лек/	3	2	ОПК-3	Л1.1 Л1.2Л2.1Л3.1 Э1 Э2	0	
1.9	Обращение с носителями информации. Обмен информацией. Мониторинг /Лек/	3	2	ОПК-3	Л1.1 Л1.2Л2.1Л3.1 Э1 Э2	0	
1.10	Бизнес-требования к контролю доступа. Управление доступом пользователей. Ответственность пользователей /Лек/	3	2	ОПК-3	Л1.1 Л1.2Л2.1Л3.1 Э1 Э2	0	
1.11	Контроль сетевого доступа. Контроль доступа к операционной системе. Контроль доступа к прикладным системам /Лек/	3	2	ОПК-3	Л1.1 Л1.2Л2.1Л3.1 Э1 Э2	0	
1.12	Менеджмент технических уязвимостей /Лек/	3	2	ОПК-3	Л1.1 Л1.2Л2.1Л3.1 Э1 Э2	0	
1.13	Оповещение о нарушениях и недостатках ИБ. Управление инцидентами ИБ и его усовершенствование /Лек/	3	2	ОПК-3	Л1.1 Л1.2Л2.1Л3.1 Э1 Э2	0	
1.14	Вопросы информационной безопасности управления непрерывностью бизнеса /Лек/	3	2	ОПК-3	Л1.1 Л1.2Л2.1Л3.1 Э1 Э2	0	
1.15	Соответствие правовым требованиям. Вопросы аудита информационных систем /Лек/	3	2	ОПК-3	Л1.1 Л1.2Л2.1Л3.1 Э1 Э2	0	
1.16	Соответствие политикам и стандартам безопасности и техническое соответствие требованиям безопасности /Лек/	3	2	ОПК-3	Л1.1 Л1.2Л2.1Л3.1 Э1 Э2	0	
Раздел 2. Практические работы							
2.1	Сбор данных об информационной системе с помощью средств администрирования Windows /Пр/	3	2	ОПК-3	Л1.1 Л1.2Л2.1Л3.1 Э1 Э2	2	Кейс-задание
2.2	Сбор данных о топологии сети с помощью средства администрирования сетей /Пр/	3	2	ОПК-3	Л1.1 Л1.2Л2.1Л3.1 Э1 Э2	0	Кейс-задание
2.3	Выявление уязвимостей. Настройка локальной политики паролей /Пр/	3	2	ОПК-3	Л1.1 Л1.2Л2.1Л3.1 Э1 Э2	2	Кейс-задание
2.4	Использование сканеров безопасности для получения информации о сети /Пр/	3	2	ОПК-3	Л1.1 Л1.2Л2.1Л3.1 Э1 Э2	0	Кейс-задание
2.5	Использование Microsoft Security Assessment Tool (MSAT) /Пр/	3	2	ОПК-3	Л1.1 Л1.2Л2.1Л3.1 Э1 Э2	1	Кейс-задание

2.6	Использование цифровых сертификатов /Пр/	3	2	ОПК-3	Л1.1 Л1.2Л2.1Л3.1 Э1 Э2	1	Кейс-задание
2.7	Создание центра сертификации (удостоверяющего центра) в Windows Server /Пр/	3	4	ОПК-3	Л1.1 Л1.2Л2.1Л3.1 Э1 Э2	0	Кейс-задание
2.8	Шифрование данных при хранении /Пр/	3	4	ОПК-3	Л1.1 Л1.2Л2.1Л3.1 Э1 Э2	0	Кейс-задание
2.9	Управление разрешениями на файлы и папки /Пр/	3	2	ОПК-3	Л1.1 Л1.2Л2.1Л3.1 Э1 Э2	0	Кейс-задание
2.10	Резервное копирование в Windows Server /Пр/	3	2	ОПК-3	Л1.1 Л1.2Л2.1Л3.1 Э1 Э2	0	Кейс-задание
2.11	Встроенный межсетевой экран (firewall) Windows Server /Пр/	3	4	ОПК-3	Л1.1 Л1.2Л2.1Л3.1 Э1 Э2	1	Кейс-задание
2.12	Настройка протокола IPSec /Пр/	3	4	ОПК-3	Л1.1 Л1.2Л2.1Л3.1 Э1 Э2	1	Кейс-задание
Раздел 3. Самостоятельная работа							
3.1	Выполнение КР /Ср/	3	24	ОПК-3	Л1.1 Л1.2Л2.1Л3.1 Э1 Э2	0	
3.2	Изучение теоретического материала, подготовка к экзамену /Ср/	3	8	ОПК-3	Л1.1 Л1.2Л2.1Л3.1 Э1 Э2	0	
Раздел 4. Контроль							
4.1	подготовка к экзамену /Экзамен/	3	36	ОПК-3	Л1.1 Л1.2Л2.1Л3.1 Э1 Э2	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	Никитин И. А., Цулая М. Т.	Процессы анализа и управления рисками в области ИТ	Москва: Национальный Открытый Университет «ИНТУИТ», 2016, http://biblioclub.ru/index.php?page=book&id=429089
Л1.2	Н.Д. Эриашвили	Информационный менеджмент	Москва: Юнити-Дана, 2015, http://biblioclub.ru/index.php?page=book&id=426579

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

	Авторы, составители	Заглавие	Издательство, год
--	---------------------	----------	-------------------

	Авторы, составители	Заглавие	Издательство, год
Л2.1	Анисимов А. А.	Менеджмент в сфере информационной безопасности	Москва: Интернет-Университет Информационных Технологий, 2009, http://biblioclub.ru/index.php?page=book&id=232981
6.1.3. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю)			
	Авторы, составители	Заглавие	Издательство, год
Л3.1	Долгов В.А., Анисимов В.В.	Криптографические методы защиты информации: учеб. пособие	Хабаровск: Изд-во ДВГУПС, 2008,
6.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет", необходимых для освоения дисциплины (модуля)			
Э1	Научная электронная библиотека eLIBRARY.RU		
Э2	Электронный каталог НТБ		
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			
Free Conference Call (свободная лицензия)			
Zoom (свободная лицензия)			
6.3.2 Перечень информационных справочных систем			
Профессиональная база данных, информационно-справочная система Гарант - http://www.garant.ru			
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
424	Учебная аудитория для проведения лабораторных и практических занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации. Лаборатория электронных устройств регистрации и передачи информации	комплект учебной мебели, мультимедийный проектор, экран, компьютер преподавателя
324	Учебная аудитория для проведения практических и лабораторных занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации. Лаборатория «Защита информации от утечки за счет несанкционированного доступа в локальных вычислительных сетях»	Комплект учебной мебели, экран, автоматизированное рабочее место IZEC «Студент» в сборе 16 шт, Автоматизированное рабочее место IZEC «Преподаватель» в сборе, автоматизированное рабочее место IZEC «Диспетчер АСУ ТП» в сборе, сервер IZEC на платформе WOLF PASS 2U в сборе, сервер IZEC на платформе SILVER PASS 1U в сборе, Ноутбук HP 250 G6 15.6, МФУ XEROX WC 6515DNI, электронный идентификатор ruToken S 64 КБ, электронный идентификатор JaCarta-2 PRO/ГОСТ, средство доверенной загрузки Dallas Lock PCI-E Full Size, средство доверенной загрузки "Соболь" версия 4 PCI-E 5 шт, рупор измерительный широкополосный Пб-124 зав. № 150718305 в комплекте с диэлектрическим штативом, кабель КИ-18-5м-SMAM-SMAM, индуктор магнитный ИРМ-500М Зав. № 015, пробник напряжения Я6-122/1М Зав. № 024, токосъемник измерительный ТК-400М Зав. № 87, антенна измерительная липольная активная АИ5-0 Зав. № 1742, мультимедийный проектор, столы, стулья, компьютерная техника с возможностью подключения к сети Интернет, свободному доступу в ЭБС и ЭИОС, проектор
201	Компьютерный класс для практических и лабораторных занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также для самостоятельной работы	
304	Учебная аудитория для проведения занятий лекционного типа	комплект учебной мебели: столы, стулья, интерактивная доска, мультимедийный проектор, компьютер, система акустическая

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, изучать теоретические материалы по предстоящему занятию и формулировать вопросы, вызывающие у них затруднения для рассмотрения на лекционных или лабораторных занятиях. При выполнении самостоятельной работы необходимо руководствоваться литературой, предусмотренной рабочей программой и указанной преподавателем.

Преподавание дисциплины предусматривает следующие формы организации учебного процесса: лекции, практические занятия, самостоятельная работа.

Самостоятельная работа – изучение студентами теоретического материала, подготовка к лекциям, практическим занятиям, оформление конспектов лекций, выполнение КР, написание отчетов, работа в электронной образовательной среде и др. для приобретения новых теоретических и фактических знаний, теоретических и практических умений.

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 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.

Тема курсовой работы: Проведение аудита состояния информационной безопасности на предприятии.

Вопросы к курсовой "Проведение аудита состояния информационной безопасности на предприятии":

- 1) Этапы аудита.
- 2) Порядок проведения аудита.
- 3) Анализ действующей на предприятии политики безопасности.
- 4) Какие процедуры исследуются во время аудита?
- 5) Что должен содержать отчет по аудиту?

КР должна соответствовать следующим требованиям:

1. Пояснительная записка оформляется в текстовом редакторе MS Word на листах формата А4 (297x210).

2. Отчет должен быть отпечатан на компьютере через 1-1,5 интервала, номер шрифта – 12-14 пт Times New Roman.

Расположение текста должно обеспечивать соблюдение следующих полей:

- левое 20 мм.
- правое 15 мм.
- верхнее 20 мм.
- нижнее 25 мм.

3. Все страницы отчета, включая иллюстрации и приложения, имеют сквозную нумерацию без пропусков, повторений, литературных добавлений. Первой страницей считается титульный лист, на которой номер страницы не ставится.

4. Таблицы и диаграммы, созданные в MS Excel, вставляются в текст в виде динамической ссылки на источник через специальную вставку.

5. Основной текст делится на главы и параграфы. Главы нумеруются арабскими цифрами в пределах всей работы и начинаются с новой страницы.

6. Подчеркивать, переносить слова в заголовках и тексте нельзя. Если заголовок состоит из двух предложений, их разделяют точкой. В конце заголовка точку не ставят.

7. Ссылки на литературный источник в тексте сопровождаются порядковым номером, под которым этот источник включен в список используемой литературы. Перекрестная ссылка заключается в квадратные скобки. Допускаются постраничные сноски с фиксированием источника в нижнем поле листа.

8. Составление библиографического списка используемой литературы осуществляется в соответствии с ГОСТ.

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»