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

27.05.2022

РАБОЧАЯ ПРОГРАММА

дисциплины **Информационная безопасность автоматизированных систем на транспорте**

10.05.03 Информационная безопасность автоматизированных систем

Составитель(и): канд. техн. наук, доцент, Пономарчук Ю.В.

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

Протокол от 18.05.2022г. № 5

Обсуждена на заседании методической комиссии учебно-структурного подразделения: Протокол от 27.05.2022 г. № 7

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 Информационная безопасность автоматизированных систем на транспорте

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 **6 ЗЕТ**

Часов по учебному плану 216
в том числе:
контактная работа 94
самостоятельная работа 86
часов на контроль 36

Виды контроля в семестрах:
экзамены (семестр) 9
РГР 9 сем. (1)

Распределение часов дисциплины по семестрам (курсам)

Семестр (<Курс>.<Семестр на курсе>)	**9 (5.1)**		Итого	
Недель	17 3/6			
Вид занятий	УП	РП	УП	РП
Лекции	16	16	16	16
Лабораторные	32	32	32	32
Практические	32	32	32	32
Контроль самостоятельной работы	14	14	14	14
В том числе инт.	8	8	8	8
Итого ауд.	80	80	80	80
Контактная работа	94	94	94	94
Сам. работа	86	86	86	86
Часы на контроль	36	36	36	36
Итого	216	216	216	216

1. АННОТАЦИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
1.1	Основные концептуальные положения системы защиты информации. Угрозы конфиденциальной информации. Правовая защита. Организационная защита. Инженерно-техническая защита. Требования, предъявляемые к обеспечению безопасности информационных технологий. Технические средства и методы защиты информации. Криптографические методы защиты информации. Программно-аппаратные средства обеспечения информационной безопасность. Оорганизация управления доступом и защиты ресурсов ОС; основные механизмы безопасности. Архитектура подсистемы безопасности, базовая настройка подсистемы безопасности. Корпоративных сетей Intranet, причины уязвимости в Intranet-сетях. Средства мониторинга безопасности сети и ОС, анализаторы протоколов, средства обнаружения вторжений, средства управления сетью. Архитектура ОС и области применения, архитектура и настройка сетевой подсистемы, архитектура подсистемы безопасности, базовая настройка подсистемы безопасности. Информационная безопасность при использовании вычислительной сети. Работа с ActiveDirectory. Решение вопросов безопасности при администрировании Windows 2000. Безопасность работы в сети, построенной на базе Windows. Информационная безопасность при использовании Internet.
1.2	

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Код дисциплины:	Б1.О.36.01
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Защита информации от утечки по техническим каналам
2.1.2	Организация ЭВМ и вычислительных систем
2.1.3	Виртуальные частные сети и их безопасность
2.1.4	Информационная безопасность киберфизических систем
2.2	**Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	Научно-исследовательская работа
2.2.2	Преддипломная практика

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ), СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ
ОПК-9.1.: Способен проектировать системы защиты информации автоматизированных, информационно-управляющих и информационно-логистических систем на транспорте (по видам) и сопровождать их разработку;
Знать:
особенности проектирования систем защиты информации автоматизированных систем на транспорте и информационно-управляющих и информационно-логистических систем на транспорте
Уметь:
проектировать систему защиты информации автоматизированных на транспорте и информационно-управляющих и информационно-логистических систем на транспорте, в том числе автоматизированных систем управления технологическими процессами
Владеть:
навыками применения методов и средств защиты информации при построении систем защиты информации автоматизированных на транспорте и информационно-управляющих и информационно-логистических систем на транспорте, в том числе автоматизированных систем управления технологическими процессами

ОПК-9.3.: Способен осуществлять контроль защищенности автоматизированных, информационно-управляющих и информационно-логистических систем на транспорте (по видам) с учетом установленных требований безопасности;
Знать:
основные угрозы и уязвимости, методы контроля защищенности автоматизированных систем на транспорте и методы контроля защищенности информационно-управляющих и информационно-логистических систем на транспорте
Уметь:
выявлять уязвимости в автоматизированных системах на транспорте и в информационно-управляющих и информационно-логистических системах на транспорте, в том числе в автоматизированных системах управления технологическими процессами; анализировать, прогнозировать и устранять угрозы информационной безопасности в течение всего времени их применения
Владеть:
навыками применения автоматизированных средств контроля защищенности автоматизированных систем на транспорте и контроля защищенности информационно-управляющих и информационно-логистических систем на транспорте

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. Лекции						
1.1	Концептуальная модель информационной безопасности /Лек/	9	2	ОПК-9.3. ОПК-9.1.	Л1.4Л3.1 Л3.2 Э1 Э2 Э3	2	Диалог
1.2	Исследование причин нарушений безопасности /Лек/	9	2	ОПК-9.3. ОПК-9.1.	Л1.1 Л1.2 Л1.4Л3.1 Л3.2 Э2 Э3	2	Диалог
1.3	Понятие политики безопасности. Реализация и гарантирование политики безопасности /Лек/	9	2	ОПК-9.3. ОПК-9.1.	Л1.2 Л1.3Л2.2Л3.1 Л3.2 Э2 Э3	0	
1.4	Особенности современных автоматизированных систем. Требования к системам и средствам защиты информации от несанкционированного доступа.	9	2	ОПК-9.3. ОПК-9.1.	Л1.1 Л1.3 Л1.4Л3.1 Л3.2 Э2 Э3	0	
1.5	Классификация автоматизированных систем и требования по защите информации. /Лек/	9	2	ОПК-9.3. ОПК-9.1.	Л1.3Л2.3Л3.1 Л3.2 Э2 Э3	0	
1.6	Принципы построения системы защиты информации. Определение уязвимостей автоматизированных транспортных систем и выбор средств защиты. /Лек/	9	2	ОПК-9.3. ОПК-9.1.	Л1.1 Л1.4Л2.2Л3.1 Л3.2 Э2 Э3	0	
1.7	Формирование требований к построению систем защиты. Создание автоматизированных транспортных систем в защищенном исполнении. /Лек/	9	2	ОПК-9.3. ОПК-9.1.	Л1.1Л2.3Л3.1 Л3.2 Э2 Э3	0	
1.8	Формальные модели безопасности. Дискреционная модель Харрисона-Руззо-Ульмана. /Лек/	9	2	ОПК-9.3. ОПК-9.1.	Л1.5Л2.1 Л2.3Л3.1 Л3.2 Э2 Э3	0	
	Раздел 2. Лабораторные занятия						
2.1	Сущность и задачи комплексной системы защиты информации /Лаб/	9	6	ОПК-9.3. ОПК-9.1.	Л1.1Л3.1 Л3.2 Э2 Э3	0	
2.2	Современные симметричные криптосистемы /Лаб/	9	4			0	
2.3	Современные ассиметричные криптосистемы /Лаб/	9	8	ОПК-9.3. ОПК-9.1.	Л1.1Л3.1 Л3.2 Э2 Э3	0	
2.4	Определение состава носителей защищаемой информации /Лаб/	9	6	ОПК-9.3. ОПК-9.1.	Л1.1Л3.1 Л3.2 Э2 Э3 Э4	0	
2.5	Выявление способов воздействия на информацию Контроль доступа к ресурсам операционной системы, отслеживание событий ОС и анализ системных журналов /Лаб/	9	8	ОПК-9.3. ОПК-9.1.	Л1.5Л2.2Л3.1 Л3.2 Э2 Э3	0	
2.6	Хеширование и электронная цифровая подпись /Пр/	9	8	ОПК-9.3. ОПК-9.1.	Л1.1Л3.1 Л3.2 Э2 Э3	1	Работа в малых группах
2.7	Перехват и анализ сетевых пакетов /Пр/	9	8	ОПК-9.3. ОПК-9.1.	Л1.1Л2.1Л3.1 Л3.2 Э2 Э3 Э4	1	Работа в малых группах

2.8	Разработка программного обеспечения блочных симметричных шифров /Пр/	9	8	ОПК-9.3. ОПК-9.1.	Л1.3Л3.1 Л3.2 Э2 Э3	1	Работа в малых группах
2.9	Разработка программного обеспечения асимметричных шифров /Пр/	9	8	ОПК-9.3. ОПК-9.1.	Л1.1Л2.1Л3.1 Л3.2 Э2 Э3	1	Работа в малых группах
	Раздел 3. Самостоятельная работа						
3.1	Изучение литературы теоретического курса /Ср/	9	26	ОПК-9.3. ОПК-9.1.	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э2 Э3	0	
3.2	Оформление и подготовка отчетов по ЛР /Ср/	9	22	ОПК-9.3. ОПК-9.1.	Л1.1 Л1.2Л3.1 Л3.2 Э2 Э3	0	
3.3	Оформление и подготовка отчетов по практическим работам /Ср/	9	22			0	
3.4	выполнение РГР /Ср/	9	16	ОПК-9.3. ОПК-9.1.	Л3.1 Л3.2 Э2 Э3	0	
	Раздел 4. Контроль						
4.1	подготовка к экзамену /Экзамен/	9	36	ОПК-9.3. ОПК-9.1.	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э2 Э3	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		Информационная безопасность и защита информации	Москва: Студенческая наука, 2012, http://biblioclub.ru/index.php?page=book&id=227774
Л1.2		Информационная безопасность	Москва: ГРОТЕК, 2014, http://biblioclub.ru/index.php?page=book&id=238445
Л1.3	Прохорова О. В.	Информационная безопасность и защита информации: Учебник	Самара: Самарский государственный архитектурно-строительный университет, 2014, http://biblioclub.ru/index.php?page=book&id=438331
Л1.4	Громов Ю.Ю.	Информационная безопасность и защита информации: учеб. пособие для вузов	Старый Оскол: ТНТ, 2016,
Л1.5	Трофимов В. Б., Кулаков С. М.	Интеллектуальные автоматизированные системы управления технологическими объектами	Москва-Вологда: Инфра-Инженерия, 2016, http://biblioclub.ru/index.php?page=book&id=444175

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

	Авторы, составители	Заглавие	Издательство, год
Л2.1	Иванов М.А., Михайлов Д.М.	Защита информации в электронных платежных системах: электрон. учеб. для вузов	Москва: Кнорус, 2011,

	Авторы, составители	Заглавие	Издательство, год
Л2.2	Сергеева Ю. С.	Защита информации: Конспект лекций	Москва: А-Приор, 2011, http://biblioclub.ru/index.php?page=book&id=72670
Л2.3	Ханипова Л. Ю., Кутлова Г. Р.	Информационная безопасность и защита информации: Учебное пособие	Уфа: БГПУ, 2010, http://biblioclub.ru/index.php?page=book&id=438523

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

	Авторы, составители	Заглавие	Издательство, год
Л3.1	Кузнецова В.Д., Никитин В.Н.	Разработка методических рекомендаций администратору безопасности информации по обеспечению защиты информации в ходе эксплуатации аттестованной информационной системы	, ,
Л3.2	Никитин В.Н.	Проведение анализа защищённости информации в информационной системе: учеб. пособие	Хабаровск: Изд-во ДВГУПС, 2020,

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

Э1	Единая коллекция Цифровых Образовательных Ресурсов	http://school-collection.edu.ru/
Э2	Национальный открытый университет ИНТУИТ	http://www.intuit.ru
Э3	Компьютерная безопасность	www.bugtraq.ru
Э4	Каталог по безопасности	www.sec.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

ПО DreamSpark Premium Electronic Software Delivery - Подписка на программное обеспечение компании Microsoft. В подписку входят все продукты Microsoft за исключением Office, контракт 203

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

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
201	Компьютерный класс для практических и лабораторных занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также для самостоятельной работы	столы, стулья, компьютерная техника с возможностью подключения к сети Интернет, свободному доступу в ЭБС и ЭИОС, проектор
249	Помещения для самостоятельной работы обучающихся. Читальный зал НТБ	Тематические плакаты, столы, стулья, стеллажи Компьютерная техника с возможностью подключения к сети Интернет, свободному доступу в ЭБС и ЭИОС.
328	Учебная аудитория для проведения занятий лекционного типа	проектор, звуковая система, интерактивная доска, компьютер с монитором, комплект учебной мебели, доска меловая и маркерная

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, лабораторные работы, практические занятия, самостоятельная работа.
Самостоятельная работа – изучение студентами теоретического материала, подготовка к лекциям, лабораторным работам, оформление конспектов лекций, выполнение РГР, написание рефератов, 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.
Лабораторная работа является средством связи теоретического и практического обучения. Дидактической целью лабораторной работы является выработка умений решать практические задачи по обработке информации. Одновременно формируются профессиональные навыки владения методами и средствами обработки информации, в том числе графической.
При подготовке к лабораторным работам необходимо изучить рекомендованную учебную литературу, изучить указания к практическим работам, составленные преподавателем.
Лабораторные работы проводятся в компьютерных классах, на компьютерах которых установлено соответствующее программное обеспечение, позволяющее решать поставленные задачи обработки мультимедийной информации.

При подготовке к экзамену необходимо ориентироваться на конспекты лекций, рекомендуемую литературу, образовательные Интернет- ресурсы. Студенту рекомендуется также в начале учебного курса познакомиться со следующей учебно-методической документацией:
- программой дисциплины;
- перечнем знаний и умений, которыми студент должен владеть;
- тематическими планами практических занятий;
- учебниками, пособиями по дисциплине, а также электронными ресурсами;
- перечнем вопросов к экзамену.
После этого у студента должно сформироваться четкое представление об объеме и характере знаний и умений, которыми надо будет овладеть в процессе освоения дисциплины. Систематическое выполнение учебной работы на практических занятиях позволит успешно освоить дисциплину и создать хорошую базу для сдачи экзамена.

Тема РГР: Реализация ролевой модели доступа для информационной системы
Вопросы:
1) Модели доступа
2) Особенности ролевой модели доступа.
3) Виды атак. Сетевые атаки.
4) Хэш-функции. Основные требования и примеры построения.
5) Система отслеживания вторжений в автоматизированных транспортных системах.

Отчет должен соответствовать следующим требованиям:
1. Отчет результатов РГР оформляется в текстовом редакторе MS Word на листах формата А4 (297х210).
2. Изложение материала в отчете должно быть последовательным и логичным. Отчет состоит из задания на РГР, содержания, разделов, выводов и списка литературных источников. В структуру отчета может входить Приложение.
3. Объем РГР работы должен быть – 10-15 страниц.
4. 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.
5. 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.
6. Таблицы и диаграммы, созданные в MS Excel, вставляются в текст в виде динамической ссылки на источник через специальную вставку.
7. Основной текст делится на главы и параграфы. Главы нумеруются арабскими цифрами в пределах всей работы и начинаются с новой страницы.
8. Подчеркивать, переносить слова в заголовках и тексте нельзя. Если заголовок состоит из двух предложений, их разделяют точкой. В конце заголовка точку не ставят.
9. 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.
10. Составление библиографического списка используемой литературы осуществляется в соответствии с ГОСТ.

Оформление и защита работ 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».