

Федеральное государственное бюджетное образовательное учреждение
высшего образования
"Волжский государственный университет водного транспорта"

УТВЕРЖДАЮ


Подписано в АСУ
"Учебный процесс"

С.В. Крепак

(Ф.И.О.)

23 мая 2024 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Наименование образовательной программы	Безопасность автоматизированных систем на транспорте (по видам)
Наименование дисциплины	Б.1.О.Д15 Теоретические основы криптографии
Институт	Институт экономики, управления и права
Кафедра	едра систем информационной безопасности, управления и телекоммуникаций
Специальность	10.05.03 Информационная безопасность автоматизированных систем
Специализация	Безопасность автоматизированных систем на транспорте (по видам)

Распределение часов по семестрам (курсам)

Вид занятий	Очная форма обучения, часы*											Заочная форма обучения, часы*								Общая трудо- емкость, з.е.	
	№ семестра											№ курса									
	1	2	3	4	5	6	7	8	9	10	11	Σ	1	2	3	4	5	6	7		Σ
лекции					34							34									
практические занятия					17							17									
лабораторные занятия					17							17									
контактная самостоятельная работа																					
экзамен					36							36									
самостоятельная работа					40							40									
всего					144							144									4

* - здесь и далее указываются академические часы

Распределение форм контроля по семестрам (курсам)

Форма контроля	Очная форма обучения											Заочная форма обучения						
	№ семестра											№ курса						
	1	2	3	4	5	6	7	8	9	10	11	1	2	3	4	5	6	7
экзамен					ЭК													
зачет с оценкой																		
зачет																		
курсовая работа (проект)																		

г. Нижний Новгород

2024

Программа составлена в соответствии с Федеральным государственным образовательным стандартом высшего образования по специальности:

ФГОС 10.05.03 Информационная безопасность автоматизированных систем от 26.11.2020 № 1457

Разработчик(и) программы В.И. Логинов

(Ф.И.О.)

Программа одобрена на заседании кафедры

протокол № 8 от 11 апреля 2024 г.

Заведующий кафедрой

(должность)



(Подписано в АСУ "Учебный процесс")

Ю.С. Федосенко

(Ф.И.О.)

11 апреля 2024 г.

1. Место дисциплины в структуре ООП

Код дисциплины	Наименование блока	Трудоемкость дисциплины, з.е.
Б.1.О.Д15	Блок 1 Дисциплины (модули) (Обязательная часть)	4

2. Перечень планируемых результатов обучения, соотнесенных с планируемыми результатами освоения ООП

Процесс изучения дисциплины направлен на формирование и развитие у обучающегося следующих компетенций:

№ п/п	Компетенция	Индикатор достижения компетенции		
		Знать	Уметь	Владеть
1	ОПК-10.Способен использовать средства криптографической защиты информации при решении профессиональной деятельности	ОПК-10.3.1 Знать способы использования средств криптографической защиты информации при решении профессиональной деятельности	ОПК-10.У.1 Уметь использовать средства криптографической защиты информации при решении профессиональной деятельности	ОПК-10.В.1 Владеть способами использования средств криптографической защиты информации при решении профессиональной деятельности

3. Распределение разделов (тем) по семестрам (курсам) с указанием часов

№ п/п	Наименование раздела (темы)	Индикатор достижения компетенции	Очная форма обучения						Общее кол-во часов	Заочная форма обучения						Общее кол-во часов
			№ сем.	лекции	практические занятия	лабораторные занятия	КСР	самостоятельная работа		№ кур- са	лекции	практические занятия	лабораторные занятия	КСР	самостоятельная работа	
1	Введение	ОПК-10.3.1 ОПК-10.У.1 ОПК-10.В.1	5	1				2	3							
1.1	Предмет и задачи дисциплины.	ОПК-10.3.1	5	1					1							
1.2	Краткий обзор развития современной криптографии.	ОПК-10.3.1	5	1					1							
2	Используемые положения элементарной теории чисел и конечной математики	ОПК-10.3.1 ОПК-10.У.1 ОПК-10.В.1	5	1				2	3							
2.1	Основные типы алгебраических структур. Группы, кольца и поля.	ОПК-10.3.1	5	1					1							
2.2	Делимость целых чисел. Теория сравнений и основные операции модульной арифметики. Теоремы Ферма и Эйлера. Обобщенная теорема и функция Эйлера.	ОПК-10.3.1 ОПК-10.У.1 ОПК-10.В.1	5	1	1	2			4							
2.3	Китайская теорема об остатках. Алгоритм быстрого возведения в степень. Индексы и показатели. Основные свойства дискретных логарифмов.	ОПК-10.3.1 ОПК-10.У.1 ОПК-10.В.1	5	1	1				2							
2.4	Степенные сравнения и алгоритмы извлечения корней по модулю. Доказательства перечисленных теорем и утверждений.	ОПК-10.3.1 ОПК-10.У.1 ОПК-10.В.1	5	1	1	2			4							
3	Базовые вычислительные алгоритмы	ОПК-10.3.1 ОПК-10.У.1 ОПК-10.В.1	5	1				4	5							
3.1	Генерация простых чисел. Алгоритм быстрого возведения в большую степень.	ОПК-10.3.1 ОПК-10.У.1 ОПК-10.В.1	5	1	2	2			5							
3.2	Алгоритмы дискретного логарифмирования и факторизации.	ОПК-10.3.1 ОПК-10.У.1 ОПК-10.В.1	5	1	1				2							
3.3	Генерация примитивного элемента.	ОПК-10.3.1 ОПК-10.У.1 ОПК-10.В.1	5	1	1				2							
3.4	Генерация чисел заданного порядка. Доказательства корректности работы перечисленных алгоритмов	ОПК-10.3.1 ОПК-10.У.1 ОПК-10.В.1	5	1	1				2							
4	Специальные вычислительные алгоритмы	ОПК-10.3.1 ОПК-10.У.1 ОПК-10.В.1	5	1				6	7							
4.1	Случайные блуждания.	ОПК-10.3.1	5	1					1							
4.2	Алгоритм Флойда.	ОПК-10.3.1 ОПК-10.У.1 ОПК-10.В.1	5	1	1				2							
4.3	Извлечение корней по простому модулю.	ОПК-10.3.1 ОПК-10.У.1 ОПК-10.В.1	5	1	1	2			4							

4.4	Извлечение квадратных корней. Симметричные шифры	ОПК-10.3.1 ОПК-10.У.1 ОПК-10.В.1	5	1	1	2			4							
5	Симметричные шифры	ОПК-10.3.1 ОПК-10.У.1 ОПК-10.В.1														
5.1	Типы криптосистем с разделяемым секретным ключом.	ОПК-10.3.1 ОПК-10.У.1 ОПК-10.В.1	5	1	1				2							
5.2	Проблема распределения ключей.	ОПК-10.3.1	5	1					1							
5.3	Защищенный канал.	ОПК-10.3.1	5	1					1							
5.4	Коммутативные шифры. Доказательства корректности работы перечисленных алгоритмов	ОПК-10.3.1	5	1					1							
6	Базовые понятия и конструктивные схемы криптографии с открытым ключом	ОПК-10.3.1 ОПК-10.У.1 ОПК-10.В.1	5	1		2		8	11							
6.1	Открытое распределение ключей. Понятие открытого ключа.	ОПК-10.3.1	5	1					1							
6.2	Протокол Диффи-Хеллмана.	ОПК-10.3.1 ОПК-10.У.1 ОПК-10.В.1	5	1	2	2			5							
6.3	Понятие открытого шифрования.	ОПК-10.3.1	5	1					1							
6.4	Электронная цифровая подпись. Криптосистема RSA. Понятие стойкости. Доказуемая стойкость. Криптосхема Рабина.	ОПК-10.3.1 ОПК-10.У.1 ОПК-10.В.1	5	1	2	2			5							
7	Хэш-функции	ОПК-10.3.1 ОПК-10.У.1 ОПК-10.В.1	5	1				10	11							
7.1	Контроль целостности информации. Алгоритмы защитного контрольного суммирования.	ОПК-10.3.1	5	1					1							
7.2	Ключевые и бесключевые хэш-функции.	ОПК-10.3.1 ОПК-10.У.1 ОПК-10.В.1	5	1	1	1			3							
8	Протоколы аутентификации	ОПК-10.3.1 ОПК-10.У.1 ОПК-10.В.1	5	1				8	9							
8.1	Простая и строгая аутентификации субъектов. Протокол рукопожатия.	ОПК-10.3.1	5	1					1							
8.2	Протоколы с нулевым разглашением секрета.	ОПК-10.3.1	5	1					1							
8.3	Преобразование протоколов аутентификации с нулевым разглашением в протоколы цифровой подписи.	ОПК-10.3.1	5	1					1							

4. Материально-техническое и учебно-методическое обеспечение программы

4.1. Помещения и оборудование

№ п/п	Вид помещений	Оснащение помещений	№ помещений
1	Учебные аудитории для проведения учебных занятий	оборудование и технические средства обучения (Стул (24+24 ед.); Стол лабораторный (15 ед.); Стол компьютерный (21 ед.); Компьютер (14 ед.); Принтер (1 ед.); Интерактивный комплект (1 ед.); Мультимедийное оборудование (1 ед.) (363))	363
2	Помещения для самостоятельной работы обучающихся	компьютерная техника с возможностью подключения к сети "Интернет" и обеспечение доступа в электронную информационно-образовательную среду университета	361,363

4.2. Лицензионное и свободно распространяемое программное обеспечение, в том числе отечественного производства

№ п/п	Наименование
1	Microsoft Office Professional Plus 2016 (Договор №44/109-15 от 28.12.2015 (бессрочно))
2	Microsoft Office ProPlus 2013 (Договор №44/59-18 от 09.04.2018 (бессрочно))

4.3. Карта обеспеченности печатными и(или) электронными изданиями и электронными образовательными ресурсами

№ п/п	Наименование источника	Год издания	Ресурс	Количество экземпляров
1	Крайнова, В.В. Методические указания по организации и выполнению внеаудиторной (самостоятельной) работы [Электронный ресурс] : для преподавателей и студ.по направлениям подготовки (спец.) высш.и сред.проф.образования / В. В. Крайнова ; ВГУВТ. - Н.Новгород, 2018. - 1 текст/файл. - Авторский вариант. - Режим доступа: http://94.100.87.24:8080/MarcWeb/Tmp/fl15520.pdf	2018	ЭР	0
2	Васильева, И.Н.;Криптографические методы защиты информации;учебник и практикум для вузов;Васильева, И.Н.-Москва,Юрайт; URL: https://urait.ru/viewer/kriptograficheskie-metody-zaschity-informacii-489919#page/1 (дата обращения: 11.09.2022) ;	2022	ЭР	0
3	Фомичев, В.М.;Криптографические методы защиты информации;учебник для вузов;В 2 частях;Мельников, Д.А.Фомичев, В.М.-Москва,Юрайт; URL: https://urait.ru/viewer/kriptograficheskie-metody-zaschity-informacii-v-2-ch-chast-2-sistemnye-i-prikladnye-aspekty-490421#page/1 (дата обращения: 16.09.2022) ;	2022	ЭР	0
4	Дмитриев, В.Г.;Стеганографические и криптографические методы защиты информации;учебное пособие;Агишев, Т.Х.Богданов, М.Р.Горбунов, В.М.Дмитриев, В.Г.Жилко, Е.П.Захаров, А.В.Зиангирова, Л.Ф.Рамазанова, Р.Р.Титова, Л.Н.-Уфа; URL: https://e.lanbook.com/reader/book/90963/#1 (дата обращения: 18.02.2021). - Режим доступа: для авторизованных пользователей ;	2016	ЭР	0
5	Запечников, С.В.;Криптографические методы защиты информации;учебник для вузов;Запечников, С.В.Казарин, О.В.Тарасов, А.А.-Москва,Юрайт; URL: https://urait.ru/bcode/536453 (дата обращения: 12.04.2024) ;	2024	ЭР	0

6	Лось, А.Б.;Криптографические методы защиты информации для изучающих компьютерную безопасность;учебник для вузов;Лось, А.Б.Нестеренко, А.Ю.Рожков, М.И.-Москва,Юрайт; URL: https://urait.ru/viewer/kriptograficheskie-metody-zaschity-informacii-dlya-izuchayuschih-kompyuternuyu-bezopasnost-469133#page/1 (дата обращения: 21.12.2021). - Режим доступа: для авторизированных пользователей ;	2021	ЭР	0
7	Попов, А.М.;Информатика и математика;учебник и практикум для вузов;Зайцев, М.А.Нагаева, Е.И.Попов, А.М.Сотников, В.Н.-Москва,Юрайт; URL: https://urait.ru/viewer/informatika-i-matematika-468496#page/1 (дата обращения: 18.02.2021). - Режим доступа: для авторизированных пользователей ;	2021	ЭР	0
8	Беляева, Т.М.;Информатика и математика;учебник и практикум для вузов;Беляева, Т.М.Кудинов, А.Т.Одинцов, А.Т.Пальянова, Н.В.Чубукова, С.Г.Швоев, М.И.Элькин, В.Д.-Москва,Юрайт; URL: https://urait.ru/viewer/informatika-i-matematika-469942#page/1 (дата обращения: 12.11.2021). - Режим доступа: для авторизированных пользователей ;	2021	ЭР	0

Программа предусматривает возможность применения электронного обучения, дистанционных образовательных технологий.

Электронная информационно-образовательная среда университета с возможностью доступа к информационно-телекоммуникационной сети "Интернет" - Режим доступа: <http://www.eios.vsuwt.ru/>.

4.4. Современные профессиональные базы данных

№ п/п	Наименование
1	Статистический сборник: Транспорт в России- Режим доступа: http://www.gks.ru/wps/wcm/connect/rosstat_main/rosstat/ru/statistics/publications/catalog/doc_1136983505312
2	Центральная база статистических данных - Режим доступа: http://cbsd.gks.ru/

4.5. Информационные справочные системы

№ п/п	Наименование
1	Справочная правовая система «КонсультантПлюс» - Режим доступа: http://www.consultant.ru (договор от 02.02.2015 г.)
2	Справочная правовая система «Гарант» - Режим доступа: http://www.garant.ru (договор 62/16 от 01.09.2016 г. - бессрочный)

5. Оценочные и методические материалы

Оценочные и методические материалы, определяющие процедуры оценивания индикаторов, характеризующих этапы формирования компетенций, являются приложением 1 программе.

№ п/п	Код контроли- руемой компетен- ции	Индикато р достиже- ния компе- тенций	Контроли- руемые разделы (темы)	Формы и методы контроля и оценки результатов обучения		Процедура оценивания	Критерии оценивания результата обучения и шкала оценивания			
							2	3	4	5
							не зачтено	зачтено		
1	ОПК-10.	ОПК-10.3. 1	1 2 3 4 5 6 7 8	промежуточная аттестация	Экзамен	Экзамен теоретический	Незнание или непонимание обучающимся основного материала; на большую часть и вопросов по содержанию экзамена затрудняется дать ответ или не дает верных ответов	Знания имеют фрагментарный характер, отличаются поверхностностью и малой содержательностью; раскрыто содержание билета раскрыто слабо, имеются неточности при ответе на основные вопросы билета; нарушена логика изложения, отсутствует осмысленность представляемого материала	Знания имеют достаточный содержательный уровень, однако отличаются слабой структурированно стью; раскрыто содержание билета, имеются неточности при ответе на дополнительные вопросы; недостаточно раскрыта проблема по одному из вопросов билета	Знания отличаются глубиной и содержательностью, дается полный исчерпывающий ответ, как на основные вопросы билета, так и на дополнительные; обучающийся свободно владеет научными понятиями; логично и доказательно раскрывает проблему, предложенную в билете; обучающийся демонстрирует умение вести диалог и вступать в научную дискуссию

2	ОПК-10.	ОПК-10.У. 1 ОПК-10.В. 1	1 2 3 4 5 6 7 8	текущий контроль	Лабораторная работа	Отчет лабораторной работе	по	Работа выполнена не полностью и объем выполненной части работы не позволяет сделать правильных выводов: если опыты, измерения, вычисления, наблюдения производились неправильно	Работа выполнена не полностью, но объем выполненной части позволяет получить правильные результаты и выводы, если в ходе проведения опыта, измерений, вычислений и наблюдений были допущены ошибки	Работа выполнена в полном объеме с соблюдением необходимой последовательности и проведения опытов, измерений, вычислений и наблюдений; все опыты проводит в условиях и режимах, обеспечивающих получение правильных результатов и выводов; в отчете правильно и аккуратно выполняет все записи, таблицы, рисунки, чертежи, графики, вычисления; правильно выполняет анализ погрешностей, но допускает несколько недочетов	Работа выполнена в полном объеме с соблюдением необходимой последовательности и проведения опытов, измерений, вычислений и наблюдений; все опыты проводит в условиях и режимах, обеспечивающих получение правильных результатов и выводов; в отчете правильно и аккуратно выполняет все записи, таблицы, рисунки, чертежи, графики, вычисления; правильно выполняет анализ погрешностей
---	---------	----------------------------------	--------------------------------------	------------------	------------------------	---------------------------------	----	---	---	---	--

3	ОПК-10.	ОПК-10.У. 1 ОПК-10.В. 1	1 2 3 4 5 6 7 8	текущий контроль	Лабораторная работа	Отчет лабораторной работе	по	Работа выполнена не полностью и объем выполненной части работы не позволяет сделать правильных выводов: если опыты, измерения, вычисления, наблюдения производились неправильно	Работа выполнена не полностью, но объем выполненной части позволяет получить правильные результаты и выводы, если в ходе проведения опыта, измерений, вычислений и наблюдений были допущены ошибки	Работа выполнена в полном объеме с соблюдением необходимой последовательности и проведения опытов, измерений, вычислений и наблюдений; все опыты проводит в условиях и режимах, обеспечивающих получение правильных результатов и выводов; в отчете правильно и аккуратно выполняет все записи, таблицы, рисунки, чертежи, графики, вычисления; правильно выполняет анализ погрешностей, но допускает несколько недочетов	Работа выполнена в полном объеме с соблюдением необходимой последовательности и проведения опытов, измерений, вычислений и наблюдений; все опыты проводит в условиях и режимах, обеспечивающих получение правильных результатов и выводов; в отчете правильно и аккуратно выполняет все записи, таблицы, рисунки, чертежи, графики, вычисления; правильно выполняет анализ погрешностей
---	---------	----------------------------------	--------------------------------------	------------------	------------------------	---------------------------------	----	---	---	---	--

4	ОПК-10.	ОПК-10.У. 1 ОПК-10.В. 1	1 2 3 4 5 6 7 8	текущий контроль	Лабораторная работа	Отчет лабораторной работе	по	Работа выполнена не полностью и объем выполненной части работы не позволяет сделать правильных выводов: если опыты, измерения, вычисления, наблюдения производились неправильно	Работа выполнена не полностью, но объем выполненной части позволяет получить правильные результаты и выводы, если в ходе проведения опыта, измерений, вычислений и наблюдений были допущены ошибки	Работа выполнена в полном объеме с соблюдением необходимой последовательности и проведения опытов, измерений, вычислений и наблюдений; все опыты проводит в условиях и режимах, обеспечивающих получение правильных результатов и выводов; в отчете правильно и аккуратно выполняет все записи, таблицы, рисунки, чертежи, графики, вычисления; правильно выполняет анализ погрешностей, но допускает несколько недочетов	Работа выполнена в полном объеме с соблюдением необходимой последовательности и проведения опытов, измерений, вычислений и наблюдений; все опыты проводит в условиях и режимах, обеспечивающих получение правильных результатов и выводов; в отчете правильно и аккуратно выполняет все записи, таблицы, рисунки, чертежи, графики, вычисления; правильно выполняет анализ погрешностей
---	---------	----------------------------------	--------------------------------------	------------------	------------------------	---------------------------------	----	---	---	---	--