

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.Э.Д06 Технологии электронной подписи
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										20		20											
практические занятия																							
лабораторные занятия										40		40											
контактная самостоятельная работа																							
экзамен																							
самостоятельная работа										48		48											
всего										108		108										3	

* - 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																		
зачет с оценкой										зач								
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.Э.Д06	Блок 1 Дисциплины (модули) (Элективные дисциплины (модули))	3

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	ПК-2.способно сть выполнять работы по развертыванию , сопровождени ю, оптимизации функциониров ания баз данных (БД), являющихся частью различных информационн ых систем	ПК-2.3.1 Знать правила выполнения работ по развертыванию, сопровождению, оптимизации функционирования баз данных (БД), являющихся частью различных информационных систем	ПК-2.У.1 Уметь выполнять работы по развертыванию, сопровождению, оптимизации функционирования баз данных (БД), являющихся частью различных информационных систем	ПК-2.В.1 Владеть способами выполнения работ по развертыванию, сопровождению, оптимизации функционирования баз данных (БД), являющихся частью различных информационных систем
2	ПК-5.способно сть выполнять работы по установке, настройке и обслуживанию систем обнаружения, предупрежден ия и ликвидации последствий компьютерных атак на информационн ые системы и информационн о-телекоммуни кационные сети	ПК-5.3.1 Знать способы выполнения работ по установке, настройке и обслуживанию систем обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные системы и информационно-телекомм уникационные сети	ПК-5.У.1 Уметь выполнять работы по установке, настройке и обслуживанию систем обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные системы и информационно-телекомм уникационные сети	ПК-5.В.1 Уметь выполнять работы по установке, настройке и обслуживанию систем обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные системы и информационно-телекомм уникационные сети

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	Нормативно-правовая база электронной цифровой подписи	ПК-2.3.1 ПК-2.У.1 ПК-2.В.1 ПК-5.3.1 ПК-5.У.1 ПК-5.В.1	10	2				2	4							
1.1	Теоретических основ построения систем электронной цифровой подписи.		10	2				2	4							
1.2	Состав, структура и принцип работы программно-аппаратного комплекса электронной цифровой подписи.		10	2				4	6							
1.3	Однонаправленные функции. Алгоритм безопасного хэширования.		10	2				4	6							
2	Алгоритмы электронной цифровой подписи	ПК-2.3.1 ПК-2.У.1 ПК-2.В.1 ПК-5.3.1 ПК-5.У.1 ПК-5.В.1	10	2				2	4							
2.1	Алгоритм RSA	ПК-2.3.1 ПК-2.У.1 ПК-2.В.1 ПК-5.3.1 ПК-5.У.1 ПК-5.В.1	10	1		2		4	7							
2.1. 1	Алгоритм RSA часть 2	ПК-2.3.1 ПК-2.У.1 ПК-2.В.1 ПК-5.3.1 ПК-5.У.1 ПК-5.В.1	10	1		2		4	7							
2.1. 2	Алгоритм RSA часть 3	ПК-2.3.1 ПК-2.У.1 ПК-2.В.1 ПК-5.3.1 ПК-5.У.1 ПК-5.В.1	10			2			2							
2.2	Алгоритм Эль-Гамаля	ПК-2.3.1 ПК-2.У.1 ПК-2.В.1 ПК-5.3.1 ПК-5.У.1 ПК-5.В.1	10	1		2		4	7							
2.2. 1	Алгоритм Эль-Гамаля, Часть 2	ПК-2.3.1 ПК-2.У.1 ПК-2.В.1 ПК-5.3.1 ПК-5.У.1 ПК-5.В.1	10			2			2							
2.2. 2	Алгоритм Эль-Гамаля, Часть 3	ПК-2.3.1 ПК-2.У.1 ПК-2.В.1 ПК-5.3.1 ПК-5.У.1 ПК-5.В.1	10	1		2		4	7							

2.2. 2	Алгоритм Эль-Гамалля, Часть 4	ПК-2.3.1 ПК-2.У.1 ПК-2.В.1 ПК-5.3.1 ПК-5.У.1 ПК-5.В.1	10			2			2							
2.3	Алгоритм DSA	ПК-2.3.1 ПК-2.У.1 ПК-2.В.1 ПК-5.3.1 ПК-5.У.1 ПК-5.В.1	10	1		2		4	7							
2.3	Алгоритм DSA	ПК-2.3.1 ПК-2.У.1 ПК-2.В.1 ПК-5.3.1 ПК-5.У.1 ПК-5.В.1	10			2			2							
2.3. 1	Алгоритм DSA, часть 2	ПК-2.3.1 ПК-2.У.1 ПК-2.В.1 ПК-5.3.1 ПК-5.У.1 ПК-5.В.1	10	1		2		4	7							
2.3. 2	Алгоритм DSA, часть 3	ПК-2.3.1 ПК-2.У.1 ПК-2.В.1 ПК-5.3.1 ПК-5.У.1 ПК-5.В.1	10			2			2							
2.4	Алгоритм ГОСТ Р 34.10-2012	ПК-2.3.1 ПК-2.У.1 ПК-2.В.1 ПК-5.3.1 ПК-5.У.1 ПК-5.В.1	10	1		2		4	7							
2.4. 1	Алгоритм ГОСТ Р 34.10-2012, Часть 2	ПК-2.3.1 ПК-2.У.1 ПК-2.В.1 ПК-5.3.1 ПК-5.У.1 ПК-5.В.1	10			2			2							
2.4. 2	Алгоритм ГОСТ Р 34.10-2012. Часть 3	ПК-2.3.1 ПК-2.У.1 ПК-2.В.1 ПК-5.3.1 ПК-5.У.1 ПК-5.В.1	10	1		2		4	7							
2.4. 3	Алгоритм ГОСТ Р 34.10-2012. Часть 4	ПК-2.3.1 ПК-2.У.1 ПК-2.В.1 ПК-5.3.1 ПК-5.У.1 ПК-5.В.1	10			2			2							
3	Технология работы с программными комплексами "Крипто-АРМ", «Русский офис», «Сигнал-«Ком», «Крипто-Банк», «Крипто-PRO», «Криптон-Подпись», ПКЗИ «ШИПКА».	ПК-2.3.1 ПК-2.У.1 ПК-2.В.1 ПК-5.3.1 ПК-5.У.1 ПК-5.В.1	10	2		2		2	6							
3.1	Технология работы с программными комплексами "Крипто-АРМ", «Русский офис», «Сигнал-«Ком», «Крипто-Банк», «Крипто-PRO», «Криптон-Подпись», ПКЗИ «ШИПКА».	ПК-2.3.1 ПК-2.У.1 ПК-2.В.1 ПК-5.3.1 ПК-5.У.1 ПК-5.В.1	10			2			2							

3.2	Технология работы с программными комплексами "Крипто-АРМ", «Русский офис», «Сигнал-«Ком», «Крипто-Банк», «Крипто-PRO», «Криптон-Подпись», ПКЗИ «ШИПКА».	ПК-2.3.1 ПК-2.У.1 ПК-2.В.1 ПК-5.3.1 ПК-5.У.1 ПК-5.В.1	10			2			2							
3.3	Технология работы с программными комплексами "Крипто-АРМ", «Русский офис», «Сигнал-«Ком», «Крипто-Банк», «Крипто-PRO», «Криптон-Подпись», ПКЗИ «ШИПКА».	ПК-2.3.1 ПК-2.У.1 ПК-2.В.1 ПК-5.3.1 ПК-5.У.1 ПК-5.В.1	10			2			2							
3.4	Технология работы с программными комплексами "Крипто-АРМ", «Русский офис», «Сигнал-«Ком», «Крипто-Банк», «Крипто-PRO», «Криптон-Подпись», ПКЗИ «ШИПКА».	ПК-2.3.1 ПК-2.У.1 ПК-2.В.1 ПК-5.3.1 ПК-5.У.1 ПК-5.В.1	10			2			2							

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	360,361,363

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/fl5520.pdf	2018	ЭР	0
2	Шаньгин, В.Ф.;Защита информации в компьютерных системах и сетях;учеб.пособие;Шаньгин, В.Ф.-М.,ДМК Пресс; URL: https://e.lanbook.com/book/3032 ;	2012	ЭР	0
3	Никифоров, С.Н.;Методы защиты информации.Шифрование данных;учеб.пособие;Никифоров, С.Н.-Санкт-Петербург,Лань; URL: https://reader.lanbook.com/book/206285#1 (дата обращения: 24.05.2022) ;	2022	ЭР	0
4	Прохорова, О.В.;Информационная безопасность и защита информации;учебник;Прохорова, О.В.-Санкт-Петербург,Лань; URL: https://e.lanbook.com/reader/book/169817/#2 (дата обращения: 22.09.2021). - Режим доступа: для авторизованных пользователей ;	2021	ЭР	0
5	Вотинов, М.В.;Хранение и защита компьютерной информации;учебное пособие;Вотинов, М.В.-Мурманск,МГТУ; URL: https://reader.lanbook.com/book/142646#2 (дата обращения:13.10.2021) ;	2017	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	ПК-2. ПК-5.	ПК-2.3.1 ПК-2.У.1 ПК-2.В.1 ПК-5.3.1 ПК-5.У.1 ПК-5.В.1	1 2 3	промежуточная аттестация	Зачет с оценкой	Собеседование	Обучающийся показывает незнания основного учебного материала, допускает принципиальные ошибки в выполнении предусмотренных программой заданий, не знаком с рекомендованной литературой, не может исправить допущенные ошибки	Обучающийся показывает знания основного учебного материала в минимальном объеме; справляется с выполнением заданий, предусмотренных программой, допуская при этом большое количество не принципиальных ошибок; знаком с литературой, рекомендованной программой	Обучающийся показывает достаточный уровень знаний в пределах основного учебного материала, без существенных ошибок выполняет предусмотренные в программе задания; усвоил литературу, рекомендованную в программе; способен объяснить взаимосвязь основных понятий при дополнительных вопросах преподавателя	Обучающийся показывает всестороннее, систематическое и глубокое знание учебного материала, умеет свободно выполнять задания, предусмотренные программой; проявляет творческие способности в понимании и использовании учебного материала; усвоил рекомендованную литературу; может объяснить взаимосвязь основных понятий в их значении для последующей профессиональной деятельности

2	ПК-2. ПК-5.	ПК-2.У.1 ПК-2.В.1 ПК-5.У.1 ПК-5.В.1	1 2	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	ПК-2. ПК-5.	ПК-2.У.1 ПК-2.В.1 ПК-5.У.1 ПК-5.В.1	1 2	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	ПК-2. ПК-5.	ПК-2.У.1 ПК-2.В.1 ПК-5.У.1 ПК-5.В.1	1 2	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
---	----------------	--	--------	------------------	------------------------	---------------------------------	----	--	---	---	--