

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.Д47 Методы и средства криптографической защиты
информации

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 | | | | | | | | 36 | | | | 36 | | | | | | | | | | | |
| практические занятия | | | | | | | | 36 | | | | 36 | | | | | | | | | | | |
| лабораторные занятия | | | | | | | | 36 | | | | 36 | | | | | | | | | | | |
| контактная самостоятельная работа | | | | | | | | | | | | | | | | | | | | | | | |
| экзамен | | | | | | | | 36 | | | | 36 | | | | | | | | | | | |
| самостоятельная работа | | | | | | | | 72 | | | | 72 | | | | | | | | | | | |
| всего | | | | | | | | 216 | | | | 216 | | | | | | | | | 6 | | |

* - 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.Д47 | Блок 1 Дисциплины (модули) (Обязательная часть) | 6 |

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-11.Способен разрабатывать компоненты систем защиты информации автоматизированных систем | ОПК-11.З.1 Знать способы разработки компонент систем защиты информации автоматизированных систем | ОПК-11.У.1 Уметь разрабатывать компоненты систем защиты информации автоматизированных систем | ОПК-11.В.1 Владеть способами разработки компонент систем защиты информации автоматизированных систем |
| 2 | ОПК-9.1.Способен проектировать системы защиты информации автоматизированных, информационно-управляющих и информационно-логистических систем на водном транспорте и сопровождать их разработку | ОПК-9.1.З.1 Знать методы проектирования систем защиты информации автоматизированных, информационно-управляющих и информационно-логистических систем на водном транспорте и сопровождать их разработку | ОПК-9.1.У.1 Уметь проектировать системы защиты информации автоматизированных, информационно-управляющих и информационно-логистических систем на водном транспорте и сопровождать их разработку | ОПК-9.1.В.1 Владеть способами проектирования систем защиты информации автоматизированных, информационно-управляющих и информационно-логистических систем на водном транспорте и сопровождать их разработку |

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 | Краткий обзор проблематики и методов современной криптографии | | 8 | 1 | 1 | | | 2 | 4 | | | | | | | |
| 1.1 | Предмет и задачи дисциплины. Рекомендуемая литература. | | 8 | 2 | 2 | | | 4 | 8 | | | | | | | |
| 2 | Основы криптографических методов | ОПК-11.3.1 ОПК-11.У.1 ОПК-11.В.1 ОПК-9.1.3.1 ОПК-9.1.У.1 ОПК-9.1.В.1 | 8 | 1 | 1 | | | 2 | 4 | | | | | | | |
| 2.1 | Основные используемые результаты теории чисел. Модель криптосистемы. | | 8 | 2 | 2 | 2 | | 4 | 10 | | | | | | | |
| 2.2 | Основные используемые результаты теории чисел. Модель криптосистемы. Часть 2. | | 8 | | | 2 | | | 2 | | | | | | | |
| 2.2 | Задачи и фундаментальные проблемы криптографии. Криптографический протокол как распределенный вычислительный алгоритм. | | 8 | 2 | 2 | 2 | | 4 | 10 | | | | | | | |
| 3 | Методы и применение двухключевой криптографии | ОПК-11.3.1 ОПК-11.У.1 ОПК-11.В.1 ОПК-9.1.3.1 ОПК-9.1.У.1 ОПК-9.1.В.1 | 8 | 2 | 2 | 2 | | 4 | 10 | | | | | | | |
| 3.2 | Методы и применение двухключевой криптографии. Часть 2. | ОПК-11.3.1 ОПК-11.У.1 ОПК-11.В.1 ОПК-9.1.3.1 ОПК-9.1.У.1 ОПК-9.1.В.1 | 8 | | | 2 | | | 2 | | | | | | | |
| 3.3 | Проблема неотказуемости от электронных сообщений и документов. | | 8 | 2 | 2 | 2 | | 4 | 10 | | | | | | | |
| 3.4 | Электронная цифровая подпись (ЭЦП) на основе сложности задачи дискретного логарифмирования по простому модулю. Криптосистемы RSA, Рабина, Шнорра, Эль-Гамала. | | 8 | 2 | 2 | 2 | | 4 | 10 | | | | | | | |
| 3.5 | Стандарты ЭЦП. Проблема анонимности пользователей. Схемы слепой подписи. | | 8 | 2 | 2 | 2 | | 4 | 10 | | | | | | | |
| 4 | Симметричные шифры | ОПК-11.3.1 ОПК-11.У.1 ОПК-11.В.1 ОПК-9.1.3.1 ОПК-9.1.У.1 ОПК-9.1.В.1 | 8 | 2 | 2 | 2 | | 4 | 10 | | | | | | | |

| | | | | | | | | | | | | | | | | |
|-----|---|---|---|---|---|---|--|---|----|--|--|--|--|--|--|--|
| 4.1 | Основные типы симметричных шифров и поточные шифры. Основные схемы построения блочных шифров, режимы использования и требования к ним. Стандарты симметричного шифрования AES и ГОСТ. | | 8 | 2 | 2 | 2 | | 4 | 10 | | | | | | | |
| 4.2 | Технология многоуровневого шифрования. Скоростные программные шифры. | | 8 | 2 | 2 | 2 | | 4 | 10 | | | | | | | |
| 4.3 | Схемы построения хэш-функций на основе блочных шифров | | 8 | 2 | 2 | 2 | | 4 | 10 | | | | | | | |
| 5 | Управление криптографическими ключами. | ОПК-11.3.1 ОПК-11.У.1 ОПК-11.В.1 ОПК-9.1.3.1 ОПК-9.1.У.1 ОПК-9.1.В.1 | 8 | 2 | 2 | 2 | | 4 | 10 | | | | | | | |
| 5.1 | Основные задачи и функции управления ключами. Иерархия ключевой системы. Инфраструктура открытых ключей. | | 8 | 2 | 2 | 2 | | 4 | 10 | | | | | | | |
| 5.2 | Цифровые сертификаты. Схемы разделения секрета, на основе китайской теоремы об остатках и на основе восстановления многочленов. | | 8 | 2 | 2 | 2 | | 4 | 10 | | | | | | | |
| 6 | Специальные криптографические методы. | ОПК-11.3.1 ОПК-11.У.1 ОПК-11.В.1 ОПК-9.1.3.1 ОПК-9.1.У.1 ОПК-9.1.В.1 | 8 | 2 | 2 | 2 | | 4 | 10 | | | | | | | |
| 6.1 | Отрицаемое шифрование как метод защиты от атак с принуждением. Отрицаемое шифрование по открытому и разделяемому секретному ключу. Криптографические обманные ловушки. | | 8 | 2 | 2 | 2 | | 4 | 10 | | | | | | | |
| 6.2 | Методы обеспечения заданного уровня стойкости протокола криптографической защиты информации при использовании секретных ключей малого размера. | | 8 | 2 | 2 | 2 | | 4 | 10 | | | | | | | |

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 | 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 | Советов, Б.Я.;Информационные технологии: теоретические основы;учебное пособие;Советов, Б.Я.Цехановский, В.В.-Санкт-Петербург,Лань; URL: https://reader.lanbook.com/book/209876#3 (дата обрщения 24.05.2022) ; | 2022 | ЭР | 0 |
| 4 | 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 |
| 5 | Никифоров, С.Н.;Методы защиты информации.Защита от внешних вторжений;учебное пособие;Никифоров, С.Н.-Санкт-Петербург,Лань; URL: https://reader.lanbook.com/book/200480#1 (дата обращения 24.05.2022) ; | 2022 | ЭР | 0 |
| 6 | Марасанов, А.М.;Распределенные базы и хранилища данных;учеб.пособие;Аносова, Н.П.Бородин, О.О.Гаврилов, Е.С.Марасанов, А.М.-СПб.,Лань; URL: https://e.lanbook.com/book/100445 ; | 2016 | ЭР | 0 |
| 7 | Жердев, А.А.;Администрирование информационных систем;учеб.пособие;Жердев, А.А.-СПб.,Лань; URL: https://e.lanbook.com/book/108078 ; | 2017 | ЭР | 0 |

| | | | | |
|----|---|------|----|---|
| 8 | Зверева, Е.Н.;Сборник примеров и задач по основам теории информации и кодирования сообщений;учебно-метод.пособие;Зверева, Е.Н.Лебедев, Е.Г.-СПб.,Лань; URL: https://e.lanbook.com/book/71068 ; | 2014 | ЭР | 0 |
| 9 | Жуматий, С.А.;Администрирование суперкомпьютеров и кластерных систем;;Дацок, О.В.Жуматий, С.А.-СПб.,Лань; URL: https://e.lanbook.com/book/96160 ; | 2014 | ЭР | 0 |
| 10 | 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 авторизированных пользователей ; | 2016 | ЭР | 0 |
| 11 | 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 |
| 12 | 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 |
| 13 | Гаврилов, М.В.;Информатика и информационные технологии;учебник для вузов;Гаврилов, М.В.Климов, В.А.-Москва,Юрайт; URL: https://urait.ru/viewer/informatika-i-informacionnye-tehnologii-468473#page/1 (дата обращения: 27.09.2021). - 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://cbstd.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-11. ОПК-9.1. | ОПК-11.3. 1 ОПК-11.У. 1 ОПК-11.В. 1 ОПК-9.1.3. 1 ОПК-9.1.У .1 ОПК-9.1.В. 1 | 1 2 3 4 5 6 | промежуточная аттестация | Экзамен | Экзамен теоретический | Незнание или непонимание обучающимся основного материала; на большую часть вопросов по содержанию экзамена затрудняется дать ответ или не дает верных ответов | Знания имеют фрагментарный характер, отличаются поверхностностью и малой содержательностью; 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; 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-11. ОПК-9.1. | ОПК-11.У. 1 ОПК-11.В. 1 ОПК-9.1.У .1 ОПК-9.1.В. 1 | 1 2 3 4 5 6 | текущий контроль | Комплект типовых задач | Опрос | Ответ на задачи дан неправильный. Объяснение хода их решения дано неполное, непоследовательно е, с грубыми ошибками | Ответ на задачи дан правильный. Объяснение хода их решения недостаточно полное, непоследовательно е, с ошибками | Ответ на задачи дан правильный. Объяснение хода их решения подробное, но недостаточно логичное, с единичными ошибками в деталях | Ответ на задачи дан правильный. Объяснение хода их решения подробное, последовательное, грамотное |
| 3 | ОПК-11. ОПК-9.1. | ОПК-11.У. 1 ОПК-11.В. 1 ОПК-9.1.У .1 ОПК-9.1.В. 1 | 1 2 3 4 5 6 | текущий контроль | Лабораторная работа | Отчет по лабораторной работе | 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-11. ОПК-9.1. | ОПК-11.У. 1 ОПК-11.В. 1 ОПК-9.1.У .1 ОПК-9.1.В. 1 | 1 2 3 4 5 6 | 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 |
|---|---------------------|--|----------------------------|------------------|------------------------|---------------------------------|----|--|---|---|--|