

Минобрнауки России

Бузулукский гуманитарно-технологический институт (филиал)  
федерального государственного бюджетного образовательного учреждения  
высшего образования  
«Оренбургский государственный университет»

Кафедра педагогического образования

## **РАБОЧАЯ ПРОГРАММА**

**ДИСЦИПЛИНЫ**

*«Б1.Д.В.Э.2.2 Методы и средства защиты информации»*

Уровень высшего образования

**БАКАЛАВРИАТ**

Направление подготовки

*44.03.01 Педагогическое образование*

(код и наименование направления подготовки)

*Информатика*

(наименование направленности (профиля) образовательной программы)

Квалификация

*Бакалавр*

Форма обучения

*Заочная*

Год набора 2020

Рабочая программа рассмотрена и утверждена на заседании кафедры

педагогического образования

\_\_\_\_\_ наименование кафедры  
протокол № 6 от "10" 01 2020г. :

Декан \_\_\_\_\_ подпись О.Н. Григорьева \_\_\_\_\_ расшифровка подписи

Исполнители:  
ст. преподаватель \_\_\_\_\_ должность \_\_\_\_\_ подпись С.А. Литвинова \_\_\_\_\_ расшифровка подписи  
\_\_\_\_\_ должность \_\_\_\_\_ подпись \_\_\_\_\_ расшифровка подписи

СОГЛАСОВАНО:

Председатель методической комиссии по направлению подготовки  
44.03.01 Педагогическое образование \_\_\_\_\_ код наименование \_\_\_\_\_ личная подпись Л.А. Омеляненко \_\_\_\_\_ расшифровка подписи

Заведующий библиотекой \_\_\_\_\_ личная подпись \_\_\_\_\_ расшифровка подписи Т.А. Лопатина \_\_\_\_\_ расшифровка подписи

## 1 Цели и задачи освоения дисциплины

**Цель (цели)** освоения дисциплины: изучение комплекса проблем информационной безопасности, построения, функционирования и совершенствования правовых, организационных, технических и технологических процессов, обеспечивающих информационную безопасность и формирующих структуру системы защиты ценной и конфиденциальной информации.

### **Задачи:**

- получить знания о методах и средствах защиты информации при реализации информационных процессов (ввод, вывод, передача, обработка, накопление, хранение);
- получить знания о правовых нормах в образовательной деятельности;
- получить навыки применения технологии криптографической защиты информации и аутентификации;
- овладеть основными способами, алгоритмами, технологиями в области безопасности компьютерных систем.

## 2 Место дисциплины в структуре образовательной программы

Дисциплина относится к дисциплинам (модулям) по выбору вариативной части блока Д «Дисциплины (модули)»

Пререквизиты дисциплины: *Б1.Д.Б.20 Математика, Б1.Д.В.2 Базы данных и системы управления базами данных, Б1.Д.В.8 Программное обеспечение компьютера*

Постреквизиты дисциплины: *Отсутствуют*

## 3 Требования к результатам обучения по дисциплине

Процесс изучения дисциплины направлен на формирование следующих результатов обучения

Код и наименование формируемых компетенций	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций
ПК*-1 Способен применять в профессиональной деятельности современные языки программирования и языки баз данных, электронные библиотеки, пакеты программ, сетевые технологии	ПК*-1-В-3 Способен применять теоретические основы и общие принципы использования технологии вычислительных систем	<b><u>Знать:</u></b> – принципы функционирования основных программно-аппаратных средств обеспечения информационной безопасности, методы и средства защиты информации в процессе хранения и передачи по компьютерным сетям: классификация, функции; – технологии криптографической защиты информации, технологии аутентификации, модели безопасности операционных систем; – способы обеспечения информационной безопасности компьютерных систем <b><u>Уметь:</u></b> – выбирать инструментальные средства и методы управления средствами сетевой безопасности, решать профессиональные задачи по конфигурированию основных средств защиты информации; – применять технологии криптографической защиты информации, технологии аутентификации для защиты информации в

Код и наименование формируемых компетенций	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций
		компьютерных системах. <b>Владеть:</b> – основными способами, алгоритмами, технологиями в области безопасности компьютерных систем.

## 4 Структура и содержание дисциплины

### 4.1 Структура дисциплины

Общая трудоемкость дисциплины составляет 3 зачетных единиц (108 академических часов).

Вид работы	Трудоемкость, академических часов	
	6 семестр	всего
<b>Общая трудоёмкость</b>	<b>108</b>	<b>108</b>
<b>Контактная работа:</b>	<b>10,5</b>	<b>10,5</b>
Лекции (Л)	4	4
Лабораторные работы (ЛР)	6	6
Промежуточная аттестация (зачет, экзамен)	0,5	0,5
<b>Самостоятельная работа:</b> - выполнение контрольной работы (КонтрР); - самоподготовка (проработка и повторение лекционного материала и материала учебников и учебных пособий); - подготовка к лабораторным занятиям;	<b>97,5</b> +	<b>97,5</b>
<b>Вид итогового контроля (зачет, экзамен, дифференцированный зачет)</b>	<b>зачет</b>	

Разделы дисциплины, изучаемые в 6 семестре

№ раздела	Наименование разделов	Количество часов				
		всего	аудиторная работа			внеауд. работа
			Л	ПЗ	ЛР	
1	Проблемы безопасности информации. Теоретические основы компьютерной безопасности.	20	2			18
2	Криптографические методы защиты информации	25	1		2	22
3	Методы идентификации и аутентификации пользователей компьютерных систем	24	1		1	22
4	Защита информации в сетях.	17			1	16
5	Комплексная защита процесса обработки информации в компьютерных системах	20			2	18
	Итого:	108	4		6	98
	Всего:	108	4		6	98

### 4.2 Содержание разделов дисциплины

**№ 1 Проблемы безопасности информации. Теоретические основы компьютерной безопасности**

Модели безопасности. Политика безопасности. Критерии и классы защищенности средств вычислительной техники и автоматизированных информационных систем. Стандарты безопасности. Исследование корректности систем защиты. Методология обследования и проектирования защиты. Модель политики контроля целостности. Модели безопасности основных ОС. Концепция защищенного ядра. Защищенные домены. Применение иерархического метода для построения защищенной операционной системы

## **№ 2 Криптографические методы защиты информации**

Краткая история развития криптологии. Основные понятия и определения. Криптографические модели. Алгоритмы шифрования. Подстановочные и перестановочные шифры. Шифры Цезаря, Виженера, Вернома. Симметричные системы шифрования (системы с секретным ключом): поточные шифры, блочные шифры. Аддитивные поточные шифры. Методы генерации криптографически качественных псевдослучайных последовательностей. Американский стандарт шифрования DES: алгоритм, скорость работы на различных платформах, режимы пользования, основные результаты по анализу стойкости. Отечественный стандарт шифрования данных ГОСТ 28147-89: алгоритм, скорость работы на различных платформах, режимы пользования. Асимметричные системы шифрования (системы с открытым ключом). Понятия однонаправленной функции и однонаправленной функции с лазейкой. Схема RSA: алгоритм шифрования, его обратимость, вопросы стойкости. Сравнение криптографических методов.

## **№ 3 Методы идентификации и аутентификации пользователей компьютерных систем**

Основные понятия и концепции. Идентификация и механизмы подтверждения подлинности пользователя. Взаимная проверка подлинности пользователя. Упрощенная схема идентификации с нулевой передачей знаний. Проблема аутентификации данных и электронная цифровая подпись. Алгоритмы аутентификации пользователей.

## **№ 4 Защита информации в сетях**

Режим функционирования межсетевых экранов и их основные компоненты. Маршрутизаторы. Шлюзы сетевого уровня. Усиленная аутентификация. Основные схемы сетевой защиты на базе межсетевых экранов. Применение межсетевых экранов для организации виртуальных корпоративных сетей. Многоуровневая защита корпоративных сетей. Программно-аппаратные средства защиты сетей. Методы средства ограничения доступа к компонентам сети. Администрирование сетей.

## **№ 5 Комплексная защита процесса обработки информации в компьютерных системах**

Требования к системам защиты информации. Концепция комплексной защиты информации. Анализ схемы функций защиты и результатов защиты информации. Постановка задач оптимизации систем защиты информации. Методология создания, организации и обеспечения функционирования систем комплексной защиты информации (КЗИ). Пути и проблемы практической реализации концепции КЗИ. Перспективы КЗИ: защищенные информационные технологии.

### **4.3 Лабораторные работы**

№ ЛР	№ раздела	Наименование лабораторных работ	Кол-во часов
1	2	Шифры замены и перестановки. Симметричные шифры. Ассиметричные шифры.	2
2	3	Параметры цифровой подписи. Формирование цифровой подписи.	1
2	4	Системы открытого распределения ключей и открытого шифрования. Математические основы. Системы Диффи-Хеллмана и RSA.	1
3	5	Анализ схемы функций защиты и результатов защиты информации.	2
		Итого:	6

### **4.4 Контрольная работа (6 семестр)**

1) *Расшифровать фразу, зашифрованную столбцевой перестановкой и двойной перестановкой.*

## Часть I Шифрование методом перестановки

Столбцовая перестановка:

1. ОКЕСНВРП\_ЫРЕАДЕЫН\_В\_РСИКО
2. ДСЛИЕЗТЕА\_Д\_ЛЬЮДМИ\_АОЧХК
3. НМВИАИ\_НЕВЕ\_СМСТУОРДИАНКМ
4. ЕДСЗЫНДЕ\_МУБД\_УЭ\_КТЗЕМНАЫ
5. СОНРЧОУО\_ХДТ\_ИЕЙ\_ВЗКАТРРИ
6. \_ОНКА\_БНЬЕЦВЛЕ\_К\_ТГОАНЕИР
7. НЗМАЕЕАА\_Г\_НОТВОССОТЬЯАЛС
8. РППОЕААДТВЛ\_ЕБЬЛНЫЕ\_ПА\_ВР
9. ОПЗДЕП\_ИХРДОТ\_И\_ВРИТЧ\_САА
10. ВКЫОСИРЙУ\_ОБВНЕ\_СОАПНИОТС

Двойная перестановка

1. ВР\_ЕСДЕИ\_ТПХРОИ\_ЗБУАДНУА\_
2. КЭЕ\_ТДУМБ\_БСЗЕДНЕЗМАОР\_ТУ
3. ЕСДНОГТЕАНН\_НЕОВМР\_ЕУНПТЕ
4. ЕШИАНИРЛПГЕЧАВРВ\_СЕЫНА\_ЛО
5. МДООИТЕБ\_СМТ\_НАДТЕСУБЕХНО
6. НДИАЕОЫЛПНЕ\_НВЕАНГТ\_ИЗЛА
7. П\_БИРДЛЬНЕВ\_ОП\_ОПЗДЕВЫТЕА
8. АИНАЛЖНОЛЕШФ\_ЗИ\_УАРОБСНЕ\_
9. СЯСЕ\_ЛУНЫИАККННОГЯДУЧАТН
10. ДОПК\_СОПАЛЕЧНЛ\_ГИНЙОИЖЕ\_Т

2 Расшифровать фразу (система Плейфейра)

- 1) ЙЦЦГЕБЪЦЦКХЗЖЛХНИПОЙИДЪЦ
- 2) ЛФАФЦЛБТЖДЕБТРБРУККА
- 3) ЙРЦНЕВПМЭЩНРЕЖПУБРЦКАБАКРЙЦКФКГНПЦБН
- 4) БТЖДПИПОДНОПВОРГАКЦКДЖОЙХЗЖЛ
- 5) ЪХКЦНЙХИИРУЫРЯЙК
- 6) УЙКЖБРНГГФВХХНТРКРВРЩДГАГЖАРГБФЪ
- 7) ТРБРУККАТЪПНЦОВХИПОЙИДФЪИЧПРЙОБГБЭБН
- 8) БТНХАНАГБХХКНЖИВЗЖУТЫЗШИМЕЙПЕПЬЛ
- 9) ШИЕКЦЛИЕАФБГЛЭКДИГТУЙОАННДВХ
- 10) ТЪПИРАВХЕГБЗГЪРПРВВХ

## Часть II Кодирование информации

1. Мальчик заменил каждую букву своего имени ее номером в алфавите. Получилось 46151. Как зовут мальчика?

2. Используя кодировочную таблицу, зашифруйте свое имя и фамилию.

А	Б	В	Г	Д	Е	Ж	З	И	К	Л	М	Н	О	П	Р
21	37	14	22	01	24	62	73	46	23	12	08	27	53	35	04
40	26	63	47	31	83	88	30	02	91	72	32	77	68	60	44
10	03	71	82	15	70	11	55	90	69	38	61	54	09	84	45

С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	
20	13	59	25	75	43	19	29	06	65	74	48	36	28	16	
52	39	07	49	33	85	58	80	50	34	17	56	78	64	41	
89	67	93	76	18	51	87	66	81	92	42	79	86	05	57	

3. «Шифр Цезаря». Этот шифр реализует следующее преобразование текста: каждая буква исходного текста заменяется третьей после нее буквой в алфавите, который считается написанным по кругу. Используя этот шифр, зашифруйте слова ИНФОРМАЦИЯ, КОМПЬЮТЕР, ЧЕЛОВЕК.

4. Расшифруйте слово НУЛТХСЁУГЧЛВ, закодированное с помощью шифра Цезаря.

5. «Шифр Виженера». Это шифр представляет шифр Цезаря с переменной величиной сдвига. Величину сдвига задают ключевым словом. Например, ключевое слово ВАЗА означает следующую последовательность сдвигов букв исходного текста: 31913191и т.д. Используя в качестве ключевого слово ВАГОН, закодируйте слова: АЛГОРИТМ, ПРАВИЛА, ИНФОРМАЦИЯ.

6. Слово НССРХПЛСГХСА получено с помощью шифра Виженера с ключевым словом ВА-ЗА. Восстановите исходное слово.

7. «Шифр перестановки». Кодирование осуществляется перестановкой букв в слове по одному и тому же общему правилу. Восстановите слова и определите правило перестановки: ЛБКО, ЕРАВШН, УМЫЗАК, АШНРРИ, РКДЕТИ.

8. Угадайте правило шифровки и расшифруйте слова: ТКАФЕТРА, ТКНИТСНИ, ТИ-ЦАРТНА, ЛАНИГИРО.

### *Часть III Шифрование данных.*

1) Создать файл-документ MS Office Word и установить ограничение изменений форматирования.

2) Создать файл-документ MS Office Word и записать в него любую личную конфиденциальную информацию. Поместить этот файл в архив, добавить пароль к архиву, включив шифрование файлов и блокировку архива.

## **5 Учебно-методическое обеспечение дисциплины**

### **5.1 Основная литература**

1 Прохорова, О.В. Информационная безопасность и защита информации: учебник [Электронный ресурс] / О.В. Прохорова; Министерство образования и науки РФ, Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Самарский гос. архитектурно-строительный ун-т». - Самара: Самарский гос. архитектурно-строительный ун-т, 2014. - 113 с. - ISBN 978-5-9585-0603-3. – Режим доступа: <http://biblioclub.ru/index.php?page=book&id=438331>

### **5.2 Дополнительная литература**

Щербаков, А. Современная компьютерная безопасность. Теоретические основы. Практические аспекты: учеб. пособие [Электронный ресурс] / А. Щербаков. - Москва: Книжный мир, 2009. - 352 с. - (Высшая школа). - ISBN 978-5-8041-0378-2. – Режим доступа: <http://biblioclub.ru/index.php?page=book&id=89798>.

Фефилов, А.Д. Методы и средства защиты информации в сетях [Электронный ресурс] / А.Д. Фефилов. - Москва: Лаборатория книги, 2011. - 105 с. - ISBN 978-5-504-00608-6. – Режим доступа: <http://biblioclub.ru/index.php?page=book&id=140796>

Кришталюк, А.Н. Правовые аспекты системы безопасности: курс лекций [Электронный ресурс] / А.Н. Кришталюк; Межрегиональная Академия безопасности и выживания. - Орел: МАБИВ, 2014. - 204 с. – Режим доступа: <http://biblioclub.ru/index.php?page=book&id=428612>

Кирпичников, А.П. Криптографические методы защиты компьютерной информации: учеб. пособие [Электронный ресурс] / А.П. Кирпичников, З.М. Хайбуллина; Министерство образования и науки России, Казанский национальный исследовательский технологический университет. - Казань: КНИТУ, 2016. - 100 с. - ISBN 978-5-7882-2052-9. – Режим доступа: <http://biblioclub.ru/index.php?page=book&id=560536>

Загинайлов, Ю.Н. Теория информационной безопасности и методология защиты информации: учеб. пособие [Электронный ресурс] / Ю.Н. Загинайлов. - Москва; Берлин: Директ-Медиа, 2015. - 253 с. - ISBN 978-5-4475-3946-7. – Режим доступа: <http://biblioclub.ru/index.php?page=book&id=276557>

### 5.3 Периодические издания

Информатика и образование: журнал. – Москва: Образование и информатика, 2011-2019.

### 5.4 Интернет-ресурсы

<http://orencode.info/> – Ресурс о компьютерах, интернете, информационных технологиях, программировании на различных языках.

<https://www.securitylab.ru/> – Информационный портал, рассказывающий о событиях в области защиты информации, интернет права и новых технологиях

<http://citforum.ru/security/> – Ресурс, содержащий материалы о информационной безопасности

[www.biblioclub.com](http://www.biblioclub.com) – Электронно-библиотечная система «Университетская библиотека онлайн»

### 5.5 Программное обеспечение, профессиональные базы данных и информационные справочные системы современных информационных технологий

Операционная система Microsoft Windows

Офисные приложения Microsoft Office

Веб-приложение «Универсальная система тестирования БГТИ»

Яндекс-браузер

СПС «Консультант Плюс» – Режим доступа: <http://www.consultant.ru/>

Федеральная университетская компьютерная сеть России RUNNet.– Режим доступа – <http://www.runnet.ru/>

Федеральный образовательный портал. – Режим доступа – <http://www.edu.ru>

Большая российская энциклопедия. - Режим доступа: <https://bigenc.ru/>

### 6 Материально-техническое обеспечение дисциплины

Перечень основного оборудования учебных аудиторий для проведения занятий лекционного типа: стационарный мультимедиа-проектор и проекционный экран, переносной ноутбук, кафедра, посадочные места для обучающихся, рабочее место преподавателя, учебная доска.

Учебные аудитории для проведения лабораторных занятий используются компьютерные классы, оснащенные стационарным мультимедиа-проектором и проекционным экраном, оборудованием для организации локальной вычислительной сети, персональными компьютерами, рабочим местом преподавателя, учебной доской.

Аудитории для проведения групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, помещение для самостоятельной работы обучающихся оснащены компьютерной техникой, подключенной к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду ОГУ, электронные библиотечные системы