

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 2022

Рабочая программа дисциплины «Б1.Д.В.Э.2.2 Методы и средства защиты информации»
рассмотрена и утверждена на заседании кафедры педагогического образования
наименование кафедры

протокол № 6 от «28» января 2022 г.

Декан факультета


подпись

О.Н. Григорьева

расшифровка подписи

Исполнители:

Старший преподаватель

должность


подпись

С.А. Литвинова

расшифровка подписи

должность

подпись

расшифровка подписи

СОГЛАСОВАНО:

Заместитель директора по НМР




М.А. Зорина

Председатель методической комиссии по направлению подготовки

44.03.01 Педагогическое образование

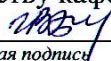
код наименование


личная подпись

Л.А. Омельяненко

расшифровка подписи

Уполномоченный по качеству кафедры


личная подпись

И.В. Балан

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.3 Иностранный язык, Б1.Д.Б.16 Математика, Б1.Д.Б.20 Теоретические основы информатики, Б1.Д.Б.21 Теория и методика обучения информатике, Б1.Д.Б.23 Основы математической обработки информации, Б1.Д.Б.28 Программирование, Б1.Д.В.2 Базы данных и системы управления базами данных, Б1.Д.В.7 Практикум по решению задач на компьютере, 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	Знать: – 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 Уметь: – выбирать инструментальные средства и методы управления средствами сетевой

Код и наименование формируемых компетенций	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций
		безопасности, решать профессиональные задачи по конфигурированию основных средств защиты информации; – применять технологии криптографической защиты информации, технологии аутентификации для защиты информации в компьютерных системах. Владеть: – основными способами, алгоритмами, технологиями в области безопасности компьютерных систем.

4 Структура и содержание дисциплины

4.1 Структура дисциплины

Общая трудоемкость дисциплины составляет 3 зачетные единицы (108 академических часов).

Вид работы	Трудоемкость, академических часов	
	9 семестр	всего
Общая трудоёмкость	108	108
Контактная работа:	10,25	10,25
Лекции (Л)	4	4
Лабораторные работы (ЛР)	6	6
Промежуточная аттестация (зачет, экзамен)	0,25	0,25
Самостоятельная работа: - выполнение индивидуального творческого задания (ИТЗ); - самоподготовка (проработка и повторение лекционного материала и материала учебников и учебных пособий); - подготовка к лабораторным занятиям.	97,75	97,75
Вид итогового контроля (зачет, экзамен, дифференцированный зачет)	зачет	

Разделы дисциплины, изучаемые в 9 семестре

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

№ раздела	Наименование разделов	Количество часов				
		всего	аудиторная работа			внеауд. работа
			Л	ПЗ	ЛР	
	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 Цезаря, Виженера, Вернома.	2
2	3	Особенности защиты информации на узлах компьютерной сети с использованием криптографических методов.	2
3	4	Системы открытого распределения ключей и открытого	2

№ ЛР	№ раздела	Наименование лабораторных работ	Кол-во часов
		шифрования. Системы RSA.	
		Итого:	6

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>

Кристалюк, А.Н. Правовые аспекты системы безопасности: курс лекций [Электронный ресурс] / А.Н. Кристалюк; 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.

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 – Электронно-библиотечная система «Университетская библиотека онлайн»

5.5 Программное обеспечение, профессиональные базы данных и информационные справочные системы

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 Бузулукского гуманитарно-технологического института (филиала) ОГУ, электронные библиотечные системы