Минобрнауки России

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Оренбургский государственный университет»

Кафедра управления и информатики в технических системах

РАБОЧАЯ ПРОГРАММА

ДИСЦИПЛИНЫ

«Б.1.В.ДВ.2.2 Компьютерная безопасность»

Уровень высшего образования

БАКАЛАВРИАТ

Направление подготовки
27.03.04 Управление в технических системах
(код и наименование направления подготовки)

Управление и информатика в технических системах
(наименование направленности (профиля) образовательной программы)

Тип образовательной программы
Программа академического бакалавриата

Квалификация
Бакалавр

Форма обучения
Очная

Год набора 2018

Рабочая программа рассмотрена и утверждена на заседании кафедры

Кафедра управления и информатики в технических системах
наименование кафедры

протокол № 5 от "16" 01 2018 г.

Заведующий кафедрой
Кафедра управления и информатики в технических системах
наименование кафедры *подпись* А.С. Боровский *расшифровка подписи*

Исполнители:
Доцент *должность* *подпись* А.С Боровский *расшифровка подписи*

должность *подпись* *расшифровка подписи*

СОГЛАСОВАНО:
Председатель методической комиссии по направлению подготовки
27.03.04 Управление в технических системах *код наименование* *личная подпись* А.С. Боровский *расшифровка подписи*

Заведующий отделом комплектования научной библиотеки
личная подпись Н.Н. Грицай *расшифровка подписи*

Уполномоченный по качеству от АКИ
личная подпись А.М. Черноусова *расшифровка подписи*

1 Цели и задачи освоения дисциплины

Цель (цели) освоения дисциплины:

Дисциплина «Компьютерная безопасность» предназначена для изучения методов и средств защиты (аппаратных и программных) компьютерной информации в компьютерных системах (сетях).

Задачи:

Для достижения поставленной цели предусматривается решение следующих основных задач:

- анализировать информационную инфраструктуру;
- определять и анализировать угрозы безопасности информации в зависимости от среды эксплуатации продуктов информационных технологий;
- выбирать и анализировать показатели качества систем и отдельных методов и средств защиты информации;
- принимать адекватные решения при выборе средств защиты информации на основе анализа угроз;
- разрабатывать и создавать типовые схемы защиты информации на основе современных средств обеспечения информационной безопасности;
- пользоваться современной научно-технической информацией по исследуемым проблемам и задачам.

2 Место дисциплины в структуре образовательной программы

Дисциплина относится к дисциплинам (модулям) по выбору вариативной части блока 1 «Дисциплины (модули)»

Пререквизиты дисциплины: *Б.1.Б.13 Информационное обеспечение систем управления*

Постреквизиты дисциплины: *Отсутствуют*

3 Требования к результатам обучения по дисциплине

Процесс изучения дисциплины направлен на формирование следующих результатов обучения

Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций	Формируемые компетенции
Знать: - основные требования информационной безопасности к компьютерным системам; **Уметь:** - использовать навыки работы с компьютером для соблюдения основных требований по информационной безопасности; **Владеть:** - методами информационных технологий для обеспечения требований информационной безопасности;	ОПК-9 способностью использовать навыки работы с компьютером, владеть методами информационных технологий, соблюдать основные требования информационной безопасности
Знать: -методы построения моделей безопасности для выполнения экспериментов на объектах аттестации; **Уметь:** - выполнять эксперименты на объектах аттестации на соответсвие требованиям информационной безопасности; **Владеть:** -методикой применения информационных технологий и технических средств для выполнения экспериментов на соответствие объектов информационной безопасности;	ПК-1 способностью выполнять эксперименты на действующих объектах по заданным методикам и обрабатывать результаты с применением современных информационных технологий и технических средств

4 Структура и содержание дисциплины

4.1 Структура дисциплины

Общая трудоемкость дисциплины составляет 6 зачетных единиц (216 академических часов).

Вид работы	Трудоемкость, академических часов	
	4 семестр	всего
Общая трудоёмкость	**216**	**216**
Контактная работа:	**86,25**	**86,25**
Лекции (Л)	52	52
Лабораторные работы (ЛР)	34	34
Промежуточная аттестация (зачет, экзамен)	0,25	0,25
Самостоятельная работа: *- самоподготовка (проработка и повторение лекционного материала и материала учебников и учебных пособий);* *- подготовка к лабораторным занятиям;* *- - подготовка к рубежному контролю.*	**129,75**	**129,75**
Вид итогового контроля (зачет, экзамен, дифференцированный зачет)	**зачет**	

Разделы дисциплины, изучаемые в 4 семестре

№ раздела	Наименование разделов	Количество часов				
		всего	аудиторная работа			внеауд. работа
			Л	ПЗ	ЛР	
1	Введение	26	6			20
2	Понятие защиты информации. Базовые свойства безопасности информации	30	10			20
3	Меры обеспечения безопасности компьютерных систем	30	10			20
4	Понятие идентификации и аутентификации.	40	8		12	20
5	Проблема обеспечения целостности компьютерной информации	40	8		12	20
6	Понятие и виды разрушающего программного воздействия	50	10		10	30
	Итого:	216	52		34	130
	Всего:	216	52		34	130

4.2 Содержание разделов дисциплины

№ 1. Введение.

Значимость информации в современном мире. Актуальность проблемы информационной безопасности. Предмет, задачи курса «Компьютерная безопасность». Место курса среди других дисциплин учебного плана.

№ 2. Понятие защиты информации. Базовые свойства безопасности информации.

Понятие доступа к информации, субъекта и объекта доступа, санкционированного и несанкционированного доступа, нарушителя. Причины несанкционированного доступа к информации. Последствия несанкционированного доступа к информации. Понятие угрозы, классификация угроз. Понятие уязвимости, атаки на компьютерную систему. Понятие риска. Задача специалиста по информационной безопасности. Виды утечки информации. Понятие канала утечки информации, основные каналы утечки информации. Классификация злоумышленников.

№ 3. Меры обеспечения безопасности компьютерных систем.

Принципы системности, комплексности, непрерывности защиты, разумной достаточности, гибкости управления и применения защитных механизмов, открытости алгоритмов и механизмов защиты, простоты применения защитных мер и средств. Связь затрат на информационную безопасность и уровень достигаемой защищенности. Правовые (законодательные), морально-этические, организационно-административные, физические, аппаратно-программные меры обеспечения безопасности компьютерных систем. Назначение этапа идентификации и аутентификации, подсистемы разграничения доступа к ресурсам. Цели применения криптографических преобразований, электронно-цифровой подписи. Аудит безопасности, резервирование ресурсов и компонентов автоматизированной системы.

№ 4. Понятие идентификации и аутентификации.

Понятие идентификации, идентификатора, авторизации, аутентификации. Определение и назначение подсистемы идентификации и аутентификации. Стойкость ко взлому подсистемы идентификации и аутентификации. Классификация подсистем идентификации и аутентификации. Особенности парольных систем, основные типы угроз безопасности парольных систем. Требования к выбору и использованию паролей.

№ 5. Проблема обеспечения целостности компьютерной информации.

Электронный документооборот: преимущества и недостатки, проблемы, связанные с обеспечением целостности передаваемого документа и аутентификации подлинности его автора, возможности злоумышленника при реализации угроз, направленных на нарушение целостности передаваемых сообщений и подлинность их авторства, метод решения данных проблем. Понятие функции хэширования, дайджест сообщения, свойства необратимости, рассеивания и чувствительности к изменениям. Значение функций хэширования в технологии электронно-цифровой подписи. Понятие электронно-цифровой подписи (ЭЦП), Процедура установки ЭЦП (подписывание документа), процедура проверки ЭЦП (аутентификация документа). Схема установки ЭЦП, схема проверки ЭЦП.

№ 6. Понятие и виды разрушающего программного воздействия.

Понятие опосредованного несанкционированного доступа, программы с потенциально опасными последствиями. Функции, свойственные таким программам, классы данных программ. Понятие и виды активизирующих событий. Модели взаимодействия прикладной программы и программы с потенциально опасными последствиями. Свойства вирусов, фазы исполнения вируса, основные подходы к классификации компьютерных вирусов. Средства борьбы с компьютерными вирусами. Признаки заражения, виды проявлений компьютерных вирусов. Способы обнаружения заражения. Общие и специализированные методы защиты программного обеспечения от разрушающих программных воздействий. Понятие изолированной программной среды, условия создания изолированной программной среды. Потенциально возможные злоумышленные действия.

4.3 Лабораторные работы

№ ЛР	№ раздела	Наименование лабораторных работ	Кол-во часов
1	4	Программно-аппаратные средства защиты информации – средства контроля учета доступа	12
2	5	Программно-аппаратные средства защиты информации – исследование алгоритма электронной цифровой подписи	12
3	6	Программно-аппаратные средства защиты информации – исследование отечественного алгоритма шифрования ГОСТ 28147-89	10
		Итого:	34

5 Учебно-методическое обеспечение дисциплины

5.1 Основная литература

1. Шаньгин, В.Ф. Защита компьютерной информации. Эффективные методы и средства / В.Ф. Шаньгин. - Москва : ДМК Пресс, 2010. - 544 с. - ISBN 978-5-94074-518-1 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=86475

2. Аверченков, В.И. Аудит информационной безопасности : учебное пособие для вузов / В.И. Аверченков. - 3-е изд., стереотип. - Москва : Издательство «Флинта», 2016. - 269 с. - Библиогр. в кн. - ISBN 978-5-9765-1256-6 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=93245

5.2 Дополнительная литература

1 Мельников, В. П. Информационная безопасность и защита информации [Текст] : учебное пособие для студентов высших учебных заведений, обучающихся по специальности "Информационные системы и технологии" / В. П. Мельников, С. А. Клейменов, А. М. Петраков; под ред. С. А. Клейменова.- 6-е изд., стер. - Москва : Академия, 2012. - 332 с. : ил. - (Высшее профессиональное образование. Информатика и вычислительная техника). - Библиогр.: с. 327-328. - ISBN 978-5-7695-9222-5.

2 Ян, С.Й. Криптоанализ RSA Cryptanalitic Attacks on RSA [Текст] / С.Й. Ян. – М. : Ижевск : Ин-т компьютер. исслед., 2011. – 287 с. : ил. – Библиогр.: с. 259-280. – Предм. указ.: с. 281-285. – ISBN 978-5-93972-873-7.

5.3 Периодические издания

– Вестник компьютерных и информационных технологий: журнал. - М.: Агентство "Роспечать", 2018;

– Информационные технологии: журнал. - М.: Агентство "Роспечать", 2018.

5.4 Интернет-ресурсы

- www.citforum.ru/ - портал аналитических и научных статей в области информационных технологий;

- www.intuit.ru/ - национальный открытый университет «ИНТУИТ»;

− http://window.edu.ru − Информационная система «Единое окно доступа к образовательным ресурсам»;

− http://bigor.bmstu.ru/− База и Генератор Образовательных Ресурсов, автоматизированная обучающая система БиГОР;

− http://CITForum.ru − on-line библиотека свободно доступных материалов по информационным технологиям на русском языке;

− http://www.online-academy.ru/demo/access/ − Центр дистанционного обучения «Онлайн-академия».

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

- Операционная система Microsoft Windows;

- Open Office/LibreOffice – свободный офисный пакет программ, включающий в себя текстовый и табличный редакторы, редактор презентаций и другие офисные приложения.

− Консультант Плюс [Электронный ресурс]: справочно-правовая система / Компания Консультант Плюс. – Электрон. дан. – Москва, [1992– 2017]. – Режим доступа: в локальной сети ОГУ \\fileserver1\! CONSULT\cons.exe;

− Гарант [Электронный ресурс]: справочно-правовая система / НПП Гарант-Сервис. – Электрон. дан. – Москва, [1990–2017]. – Режим доступа в локальной сети ОГУ \\fileserver1\GarantClient\garant.exe.

6 Материально-техническое обеспечение дисциплины

Учебные аудитории для проведения занятий лекционного типа, семинарского типа, курсового проектирования, для проведения групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.

Аудитории оснащены комплектами ученической мебели, техническими средствами обучения, служащими для представления учебной информации большой аудитории.

Для проведения лабораторных занятий используется аудитория оснащенная компьютерной техникой.

Помещение для самостоятельной работы обучающихся оснащены компьютерной техникой подключеной к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду ОГУ.

К рабочей программе прилагаются:

- Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине;
- Методические указания для обучающихся по освоению дисциплины.