

Минобрнауки России

Федеральное государственное бюджетное образовательное учреждение
высшего образования

«Оренбургский государственный университет»

Кафедра метрологии, стандартизации и сертификации

РАБОЧАЯ ПРОГРАММА

ДИСЦИПЛИНЫ

«Б.1.В.ДВ.9.2 Системы безопасности и защиты информации»

Уровень высшего образования

БАКАЛАВРИАТ

Направление подготовки

27.03.02 Управление качеством
(код и наименование направления подготовки)

Общий профиль

(наименование направленности (профиля) образовательной программы)

Тип образовательной программы

Программа прикладного бакалавриата

Квалификация

Бакалавр

Форма обучения

Заочная

Год набора 2018

Рабочая программа рассмотрена и утверждена на заседании кафедры

Кафедра метрологии, стандартизации и сертификации

наименование кафедры

протокол № 6 от "23" января 2018 г.

Заведующий кафедрой

Кафедра метрологии, стандартизации и сертификации А.Л. Воробьев

наименование кафедры

подпись

расшифровка подписи



Исполнители:

ст. преподаватель кафедры

метрологии, стандартизации и сертификации

должность

подпись

расшифровка подписи

В.А. Гарельский



должность

подпись

расшифровка подписи

СОГЛАСОВАНО:

Председатель методической комиссии по направлению подготовки

27.03.02 Управление качеством

код наименование



А.Л. Воробьев

расшифровка подписи

Заведующий отделом комплектования научной библиотеки

личная подпись

Н.Н. Грицай

расшифровка подписи

Уполномоченный по качеству факультета

личная подпись

Р.Х. Хасанов

расшифровка подписи

№ регистрации _____

© Гарельский В.А., 2018

© ОГУ, 2018

1 Цели и задачи освоения дисциплины

Цель (цели) освоения дисциплины: ознакомление с методами разработки моделей и алгоритмов защиты информации; системами менеджмента с использованием сетей; организационными, техническими, алгоритмическими и другими методами и средствами защиты информации, с законодательством и стандартами в этой области, изучение методов идентификации пользователей; моделями безопасности; политикой безопасности; особенностями реализации систем с различными ключами; использованием иерархического метода построения защищенной системы; моделью политики контроля целостности.

Задачи:

- изучение средств и методов защиты информации;
- освоение безопасного режима работы;
- приобретение навыков по разграничению полномочий между пользователями;
- изучение политики информационной безопасности, моделей безопасности;
- освоение информационных ресурсов и приобретение навыков по документированию информации;
- приобретение навыков по обеспечению безопасности информационных ресурсов;
- изучение государственных информационных ресурсов;
- освоение упрощенной схемы идентификации пользователей;
- изучение аутентификации данных.

2 Место дисциплины в структуре образовательной программы

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

Пререквизиты дисциплины: *Б.1.В.ОД.12 Квалиметрия*

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
<p><u>Знать:</u></p> <ul style="list-style-type: none">- основы теории принятия решений;- основы современных систем поддержки принятия решений;- способы организации процесса принятия решений;- сценарные и математические модели принятия решений. <p><u>Уметь:</u></p> <ul style="list-style-type: none">- собирать данные, необходимые для принятия решений;- анализировать имеющиеся в распоряжении лица, принимающего решение, данные;- организовывать процесс принятия решений;- оптимизировать число возможных решений;- применять соответствующие ситуации сценарные и математические модели принятия решений. <p><u>Владеть:</u></p> <ul style="list-style-type: none">- приемами использования теории принятия решений для практических задач;- навыками использования систем поддержки принятия решений в	ПК-6 способность использовать знания о принципах принятия решений в условиях неопределенности, о принципах оптимизации

Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций	Формируемые компетенции
практической деятельности; - навыками принятия обоснованных анализом решений; - методами рационального выбора информационных систем для управления производством.	
Знать: - правовые, нормативно-технические и организационно-правовые основы обеспечения безопасности и управления риском на предприятиях; - средства и методы повышения безопасности и управления риском; - основные понятия и термины в области управления риском. Уметь: - творчески применять знания о системах безопасности и защиты информации; - вести разработку и внедрение систем управления риском; - применять полученные знания к решению практических задач. Владеть: - нормативно-технологической документацией в части систем управления риском; - актуализированной информацией о путях развития управления риском в РФ и за рубежом - методами управления риском.	ПК-11 способность идти на оправданный риск при принятии решений

4 Структура и содержание дисциплины

4.1 Структура дисциплины

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

Вид работы	Трудоемкость, академических часов	
	8 семестр	всего
Общая трудоёмкость	108	108
Контактная работа:	14,5	14,5
Лекции (Л)	6	6
Практические занятия (ПЗ)	8	8
Промежуточная аттестация (зачет, экзамен)	0,5	0,5
Самостоятельная работа: - выполнение контрольной работы (КонтрР); - самоподготовка (проработка и повторение лекционного материала и материала учебников и учебных пособий); - подготовка к практическим занятиям.)	93,5 +	93,5
Вид итогового контроля (зачет, экзамен, дифференцированный зачет)	зачет	

Разделы дисциплины, изучаемые в 8 семестре

№ раздела	Наименование разделов	Количество часов				
		всего	аудиторная работа			внеауд. работа
			Л	ПЗ	ЛР	
1	Нормативно-правовые основы информационной безопасности в РФ	20	1	1		18

№ раздела	Наименование разделов	Количество часов				
		всего	аудиторная работа			внеауд. работа
			Л	ПЗ	ЛР	
2	Угрозы безопасности информации	21	1	1		19
3	Подходы к обеспечению защиты информации	22	1	2		19
4	Применение риск-ориентированного мышления	23	2	2		19
5	Основы теории принятия решений в условиях неопределенности	22	1	2		19
	Итого:	108	6	8		94
	Всего:	108	6	8		94

4.2 Содержание разделов дисциплины

Раздел 1. Нормативно-правовые основы информационной безопасности в РФ

Программа информационной безопасности России и пути ее реализации. Роль и место системы обеспечения информационной безопасности в системе национальной безопасности РФ. Концепция информационной безопасности. Обзор состояния систем защиты информации в России и в ведущих зарубежных странах. Международные стандарты информационного обмена. Основные понятия и определения защиты информации. Современное состояние правового регулирования в информационной сфере. Правовое обеспечение информационной безопасности. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства. Организационное обеспечение информационной безопасности. Нормативная база менеджмента риска. Государственные стандарты серии «Менеджмент риска».

Раздел 2. Угрозы безопасности информации

Три вида возможных нарушений информационной системы. Понятие угрозы. Анализ угроз безопасности информации. Причины, виды, каналы утечки и искажения информации. Основные методы реализации угроз информационной безопасности: методы нарушения секретности, целостности и доступности информации. Информационная безопасность в условиях функционирования в России глобальных сетей. Методы перехвата и навязывания информации.

Раздел 3. Подходы к обеспечению защиты информации

Общие подходы к построению парольных систем. Выбор паролей. Хранение паролей. Типы алгоритмов шифрования. Особенности реализации систем с симметричными и несимметричными ключами. Защита офисных документов. Способы распространения программного обеспечения. Техническая защита от несанкционированного копирования. Базовые методы нейтрализации систем защиты от несанкционированного копирования. Идентификация параметров персонального компьютера. Идентификация жестких дисков. Идентификация гибких дисков. Оценка уникальности конфигурации компьютера.

Раздел 4. Применение риск-ориентированного мышления

Теоретические основы управления риском. Основные понятия. Взаимосвязь показателей надежности и риска. Функция безопасности – понятие, свойства, количественная оценка. Функция риска – понятие, свойства, количественная оценка. Ущерб – классификация, способы количественного выражения. Взаимосвязь функций безопасности и риска. Методика установления допустимого уровня риска. Управление техногенным риском на предприятии.

Методы менеджмента риска в экономике. Методы менеджмента техногенного риска. Применение логико-вероятностной теории для анализа, прогнозирования и оценки риска. Сценарное логико-вероятностное моделирование

Система менеджмента риска промышленного предприятия – состав, структура, разработка и внедрение.

Раздел 5. Основы теории принятия решений в условиях неопределенности

Формальная постановка задачи принятия решения в условиях неопределенности. Этапы принятия решения. Отличие задач, связанных с принятием решений, от традиционных оптимизационных задач. Методологические трудности использования компьютера для поддержки принятия решения. Парадокс Алле. Человеческая система переработки информации и принятия решений. Системы поддержки принятия решений: возможности, основные элементы, примеры использования.

4.3 Практические занятия (семинары)

№ занятия	№ раздела	Тема	Кол-во часов
1	1	Нормативно-правовая база информационной безопасности в РФ	1
2	2	Безопасности информации. Угрозы безопасности информации: виды, способы защиты и устранения	1
3	3	Подходы к обеспечению защиты информации	2
4	4	Применение методов менеджмента риска для анализа, оценки и прогнозирования риска	2
5	5	Поиск альтернатив и критериев для заданной проблемы. Классификация поставленной задачи принятия решения.	2
		Итого:	8

4.4 Контрольная работа (8 семестр)

- 1 Программа информационной безопасности России и пути ее реализации.
- 2 Роль и место системы обеспечения информационной безопасности в системе национальной безопасности РФ.
- 3 Три вида возможных нарушений информационной системы.
- 4 Причины, виды, каналы утечки и искажения информации.
- 5 Общие подходы к построению парольных систем.
- 6 Защита офисных документов.
- 7 Теоретические основы управления риском.
- 8 Функция риска – понятие, свойства, количественная оценка.
- 9 Формальная постановка задачи принятия решения в условиях неопределенности.
- 10 Отличие задач, связанных с принятием решений, от традиционных оптимизационных задач.

5 Учебно-методическое обеспечение дисциплины

5.1 Основная литература

- 1 Аверченков В. И. Аудит информационной безопасности: учебное пособие для вузов [Электронный ресурс] / Аверченков В. И. – М.: Флинта, 2011. – Режим доступа: <http://biblioclub.ru/index.php?page=book&id=93245>.
- 2 Олейников, С.Я. Риск-менеджмент : учебно-методический комплекс / С.Я. Олейников, С.А. Бочаров, А.А. Иванов. – М.: Евразийский открытый институт, 2011. – 303 с. – ISBN 978-5-374-00013-6; То же [Электронный ресурс]. – Режим доступа: <http://biblioclub.ru/index.php?page=book&id=93140>.
- 3 Бородачёв, С.М. Теория принятия решений : учебное пособие / С.М. Бородачёв ; науч. ред. О.И. Никонов ; Министерство образования и науки Российской Федерации, Уральский федеральный университет им. первого Президента России Б. Н. Ельцина. - Екатеринбург : Издательство

Уральского университета, 2014. – 124 с. : ил. – Библиогр. в кн. – ISBN 978-5-7996-1196-5 ; То же [Электронный ресурс]. – Режим доступа: <http://biblioclub.ru/index.php?page=book&id=275740>.

5.2 Дополнительная литература

1 Сычев, Ю. Н. Основы информационной безопасности. Учебно-практическое пособие [Электронный ресурс] / Сычев Ю. Н. - Евразийский открытый институт, 2010. – Режим доступа: <http://biblioclub.ru/index.php?page=book&id=90790>.

2 Островский, Г.М. Технические системы в условиях неопределенности. Анализ гибкости и оптимизация : учебное пособие / Г.М. Островский, Ю.М. Волин. – 3-е изд. (эл.). – Москва : БИНОМ. Лаборатория знаний, 2015. – 322 с. - Библиогр. в кн. – ISBN 978-5-9963-2544-3 ; То же [Электронный ресурс]. – Режим доступа: <http://biblioclub.ru/index.php?page=book&id=95013>.

3 Ефремов, И. Надежность технических систем и техногенный риск : учебное пособие / И. Ефремов, Н. Рахимова ; Министерство образования и науки Российской Федерации, Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Оренбургский государственный университет». - Оренбург : ОГУ, 2013. - 163 с. ; То же [Электронный ресурс]. – Режим доступа: <http://biblioclub.ru/index.php?page=book&id=259179>.

4 Управление рисками проектов / Министерство образования и науки Российской Федерации, Уральский федеральный университет имени первого Президента России Б. Н. Ельцина ; науч. ред. А.В. Гребенкин. - Екатеринбург : Издательство Уральского университета, 2014. - 186 с. : ил. - Библиогр. в кн. - ISBN 978-5-7996-1266-5 ; То же [Электронный ресурс]. – Режим доступа: <http://biblioclub.ru/index.php?page=book&id=276487>.

5.3 Периодические издания

1 Стандарты и качество: журнал. – М.: РИА «Стандарты и качество», 2018.

2 Методы менеджмента качества: журнал. – М.: РИА «Стандарты и качество», 2018.

3 Контроль качества продукции: журнал. – М.: РИА «Стандарты и качество», 2018.

4 Техносферная безопасность: научный электронный журнал. – Екатеринбург: ФГБОУ ВО Уральский институт ГПС МЧС России, 2018.

5 БДИ (Безопасность. Достоверность. Информация): журнал. – С.-Пб., 2018.

5.4 Интернет-ресурсы

- <http://biblioclub.ru/> – университетская библиотека On-line;

- <http://e.lanbook.com/> – электронно-библиотечная система «Издательство «Лань»;

- <http://rucont.ru/> – национальный цифровой ресурс «Руконт» - межотраслевая электронная библиотека на базе технологии Контекстум ;

- <http://artlib.osu.ru> – электронная библиотека научной библиотеки Оренбургского государственного университета;

- www.stq.ru – официальный сайт РИА «Стандарты и качество»;

- www.standart.ru – Федеральный информационный фонд технических регламентов и стандартов;

- www.gost.ru – официальный сайт Федерального агентства по техническому регулированию и метрологии (Росстандарт);

- <http://mirq.ucoz.ru> – официальный сайт Всероссийской организации качества (ВОК);

- <http://www.gosnadzor.ru> – официальный сайт Федеральной службы по экологическому, технологическому и атомному надзору (Ростехнадзор).

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

1 Операционная система Microsoft Windows;

2 Пакет настольных приложений Microsoft Office (Word, Excel, PowerPoint, OneNote, Outlook, Publisher, Access);

3 Бесплатное средство просмотра файлов PDF Adobe Reader;

4 Свободный файловый архиватор 7-Zip;

5 Технорма / Документ [Электронный ресурс] : [система программных продуктов] / ООО Гло-сис-Сервис, ФБУ КВФ Интерстандарт. – Версия 1.11.36. – Электрон. дан. и прогр. – [Москва; Санкт-Петербург], [1999–2013]. – Режим доступа: в локальной сети ОГУ; \\fileserver1\gost\install\tndoc_setup.exe.

6 Консультант Плюс [Электронный ресурс] : справочно-правовая система / Компания Кон-сультант Плюс. – Электрон. дан. – Москва, [1992– 2018]. – Режим доступа: в локальной сети ОГУ <\\fileserver1\CONSULT\cons.exe>;

7 Гарант [Электронный ресурс] : справочно-правовая система / НПП Гарант-Сервис. – Элек-трон. дан. – Москва, [1990–2018].– Режим доступа: <\\fileserver1\GarantClient\garant.exe> в локальной сети ОГУ;

8 Законодательство России [Электронный ресурс] : информационно-правовая система. – Ре-жим доступа: <http://pravo.fso.gov.ru/ips/>, в локальной сети ОГУ.

6 Материально-техническое обеспечение дисциплины

Учебные аудитории для проведения занятий лекционного типа, семинарского типа, 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.

Помещение для самостоятельной работы обучающихся оснащены компьютерной техникой, подключенной к сети «Интернет»; обеспечен доступ в электронную информационно-образовательную среду ОГУ.