МИНОБРНАУКИ РОССИИ

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

УТВЕРЖДАЮ
Декан (директор)

_____
__ _____ _____г.

Основы управления информационной безопасностью

рабочая программа дисциплины (модуля)

Закреплена за кафедрой **Кафедра прикладной физики, электроники и информационной безопасности**

Учебный план 10_03_01_ИБ-1234-2017.plx
10.03.01 Информационная безопасность: Безопасность автоматизированных систем

Форма обучения **очная**

Общая трудоемкость **3 ЗЕТ**

Часов по учебному плану 108
в том числе:
аудиторные занятия 54
самостоятельная работа 27
экзамены 27

Виды контроля в семестрах:
экзамены 8

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**8 (4.2)**		Итого	
Недель	3			
Вид занятий	УП	РПД	УП	РПД
Лекции	18	18	18	18
Практические	36	36	36	36
Итого ауд.	54	54	54	54
Контактная работа	54	54	54	54
Сам. работа	27	27	27	27
Часы на контроль	27	27	27	27
Итого	108	108	108	108

Программу составил(и):
д.ф.-м.н., профессор Минакова Н.Н. _____

Рецензент(ы):
к.ф.-м.н., доцент Рудер Д.Д. _____

Рабочая программа дисциплины
Основы управления информационной безопасностью

разработана в соответствии с ФГОС:
· Федеральный государственный образовательный стандарт высшего образования по направлению подготовки 10.03.01 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ (уровень бакалавриата) (приказ Минобрнауки России от 01.12.2016г. №1515)

составлена на основании учебного плана:
10.03.01 Информационная безопасность: Безопасность автоматизированных систем
утвержденного учёным советом вуза от _____ протокол № ____.

Рабочая программа одобрена на заседании кафедры
Кафедра прикладной физики, электроники и информационной безопасности

Протокол от __ _____ _____ г. № __
Срок действия программы: 2017-2018 уч.г.
Зав. кафедрой д.ф.-м.н., профессор Поляков В.В. _____

Визирование РПД для исполнения в очередном учебном году

Утверждаю: Декан (директор)

__ _____ _____ г.

Рабочая программа пересмотрена, обсуждена и одобрена для
исполнения в _____-_____ учебном году на заседании кафедры

Кафедра прикладной физики, электроники и информационной безопасности

Протокол от __ _____ _____г. № __
Зав. кафедрой д.ф.-м.н., профессор Поляков В.В.

Визирование РПД для исполнения в очередном учебном году

Утверждаю: Декан (директор)

__ _____ _____ г.

Рабочая программа пересмотрена, обсуждена и одобрена для
исполнения в _____-_____ учебном году на заседании кафедры

Кафедра прикладной физики, электроники и информационной безопасности

Протокол от __ _____ _____ г. № __
Зав. кафедрой д.ф.-м.н., профессор Поляков В.В.

Визирование РПД для исполнения в очередном учебном году

Утверждаю: Декан (директор)

__ _____ _____ г.

Рабочая программа пересмотрена, обсуждена и одобрена для
исполнения в - учебном году на заседании кафедры
Кафедра прикладной физики, электроники и информационной безопасности

Протокол от __ _____ _____ г. № __
Зав. кафедрой д.ф.-м.н., профессор Поляков В.В.

Визирование РПД для исполнения в очередном учебном году

Утверждаю: Председатель НМСС

__ _____ _____ г.

Рабочая программа пересмотрена, обсуждена и одобрена для
исполнения в _____-_____ учебном году на заседании кафедры

Кафедра прикладной физики, электроники и информационной безопасности

Протокол от __ _____ _____ г. № __
Зав. кафедрой д.ф.-м.н., профессор Поляков В.В.

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ	
1.1	приобретение необходимого объема знаний и практических навыков по управлению информационной безопасностью, оценки рисков информационных ресурсов организации и аудита информационной безопасности, организации работы и разграничения полномочий персонала, ответственного за информационную безопасность;
1.2	– формирование представления о содержании процессов управления информационной безопасностью организации как результата внедрения системного подхода к решению задач обеспечения информационной безопасности

• •

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП	
Цикл (раздел) ООП:	Б1.Б.05
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Для успешного освоения дисциплины студент должен иметь базовую подготовку по направлению подготовки 10.03.01
2.2	**Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	организационное и правовое обеспечение информационной безопасности, основы управленческой деятельности, основы информационной безопасности, программно-аппаратные средства обеспечения информационной безопасности, документоведение

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
ПК-3: способностью администрировать подсистемы информационной безопасности объекта защиты	
Знать:	
Уровень 1	О необходимости администрирования подсистем информационной безопасности
Уровень 2	О роли администрирования при решении вопросов защиты информации и основных проблемах
Уровень 3	Разновидности и основные особенности подсистем информационной безопасности
Уметь:	
Уровень 1	уметь анализировать текущее состояние с целью оценки необходимости администрирования подсистем информационной безопасности
Уровень 2	выделять объекты и субъекты управления при решении простейших задач администрирования
Уровень 3	применять процессный подход при решении задач администрирования
Владеть:	
Уровень 1	навыками представления процесса управления в виде совокупности различных этапов
Уровень 2	навыками подбора вида администрирования под субъекты и объекты управления в простейшей информационной системе
Уровень 3	навыками подбора вида администрирования под субъекты и объекты управления в основных подсистемах

ПК-6: способностью принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	
Знать:	
Уровень 1	О необходимости проверок работоспособности и эффективности средств защиты информации, о возможных последствиях при отсутствии таких проверок
Уровень 2	Основные критерии оценки работоспособности и эффективности средств защиты информации
Уровень 3	Общие метолы и средства контроля работоспособности и эффективности средств защиты информации
Уметь:	
Уровень 1	Выбирать подходы к оценке работоспособности и эффективности средств защиты информации
Уровень 2	Оценивать эффективности распространенных средств защиты информации (парольная защита, антивирусная защита)
Уровень 3	Разрабатывать предложения о необходимости проверок работоспособности и эффективности средств защиты информации
Владеть:	
Уровень 1	Основной профессиональной терминологией, касающейся оценки работоспособности и эффективности средств защиты информации
Уровень 2	Основными представлениями в решении вопросов оценки работоспособности и эффективности средств защиты информации
Уровень 3	Навыками подбора критериев оценки эффективности средств защиты информации

В результате освоения дисциплины обучающийся должен

3.1	**Знать:**
3.1.1	структуру системы управления информационной безопасность;
3.1.2	приемы управлению информационной безопасностью
3.1.3	методы управления комплексной системой защиты информации, применяемые к конкретной структуре угроз
3.2	**Уметь:**
3.2.1	выделять процессы управления информационной безопасностью защищаемых объектов,
3.2.2	разрабатывать предложения по совершенствованию системы управления информационной безопасностью;
3.2.3	выявлять угрозы информационной безопасности для конкретных объектов с учетом применяемых методов организации и управления службами защиты информации;
3.2.4	обосновывать структуру системы управления информационной безопасностью в зависимости от характера угроз на объекте.
3.3	**Владеть:**
3.3.1	правилами, процедурами, практические приемы и пр. для управления информационной безопасности
3.3.2	системой проектирования системы управления информационной безопасностью с учетом особенностей объектов защиты
3.3.3	методами и средствами минимизации угроз за счет совершенствования процессов управления

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Компетен-ции	Литература
	Раздел 1. Введение				
1.1	Цели и задачи курса. Рекомендуемая литература. Основные понятия и определения. Содержание и задачи процесса управления информационной безопасностью автоматизированных систем и организации в целом /Пр/	8	4		Л1.2 Л2.2 Л2.4
1.2	Задачи процесса управления информационной безопасностью автоматизированных систем и организации в целом /Пр/	8	4		Л1.4 Л2.3 Л2.4
	Раздел 2. Система управления информационной безопасностью				
2.1	Системный подход к управлению информационной безопасностью. Стандартизация в сфере управления информационной безопасностью. /Лек/	8	6		Л1.3 Л2.4 Л2.3
2.2	Стандартизация в сфере управления информационной безопасностью. /Пр/	8	6		Л2.2
2.3	Системный подход к управлению информационной безопасностью. Стандартизация в сфере управления информационной безопасностью. /Ср/	8	4		Л1.3
	Раздел 3. Аудит информационной безопасности				
3.1	Назначение, цели и виды аудита ИБ. Требования к аудитору ИБ, особенности взаимодействия в процессе аудита. Оценка работы аудитора. Стандартизация в сфере аудита информационной безопасности. Содержание и организация процесса аудита информационной безопасности. Оценка рисков информационной безопасности. Отчетные документы по результатам аудита. Выполнение рекомендаций по итогам проведения аудита информационной безопасности. /Лек/	8	6		Л1.2 Л2.2 Л2.4
3.2	Аудит информационной безопасности /Лаб/	8	8		
3.3	Оценка рисков информационгой безопасности /Пр/	8	8		
3.4	Назначение, цели и виды аудита ИБ. Требования к аудитору ИБ, особенности взаимодействия в процессе аудита. Оценка работы аудитора. Стандартизация в сфере аудита информационной безопасности. Содержание и организация процесса аудита информационной безопасности. Оценка рисков информационной безопасности. Отчетные документы по результатам аудита. Выполнение рекомендаций по итогам проведения аудита информационной безопасности. /Ср/	8	6		Л1.3 Л1.1 Л1.2 Л2.2 Л2.4 Л2.3
	Раздел 4. Средства поддержки процессов управления информационной безопасностью				

4.1	Программные средства автоматизации процедур управленияинформационной безопасности и анализа политики информационной безопасности. Программные средства поддержки процессов управления информационной безопасности /Лек/	8	6		Л1.3 Л1.2 Л2.2 Л2.4 Л2.3
4.2	Средства управления информационнйо безопасностью /Лаб/	8	4		
4.3	Средства поддержки процессов управления информационной безопасностью /Пр/	8	14		
4.4	Программные средства автоматизации процедур информационной безопасности и анализа политики информационной безопасности. Программные средства поддержки процессов управления информационной безопасности /Ср/	8	17		Л1.1 Л2.1 Л2.2 Л2.4

5. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

5.1. Контрольные вопросы и задания

1. Понятие управления информационной безопасностью. Факторы, от которых зависит система управления
2. Сущность управления информационной безопасностью
3. Значение обеспечения и управления информационной безопасностью
4. Информационные риски: основные представления
5. Основные способы управления системой защиты информации
6. Основные правила, применяемые при реализации процесса управления информационной безопасностью
7. Процедуры, используемые для управления информационной безопасностью
8. Практические приемы, применяемые для управления информационной безопасностью

5.2. Темы письменных работ

1. Способы качественной оценки информационных рисков
2. Способы количественной оценки информационных рисков
3. Управление защитой информации в зависимости от конкретной компьютерной системы
4. Основные направления совершенствования сисмы управления информационной безопасностью

5.3. Фонд оценочных средств

Аудит средствами операционных систем. Журналы аудита. Примеры выявления неправомерных действий.
2. Выявление уязвимостей с помощью Microsoft Baseline Security Analyzer. Настройка локальной политики паролей"
3. Управление разрешениями на файлы и папки. Примеры
4. Программы ЭВМ для контроля и протоколирования доступа пользователя к устройствам и портам ввода вывода (инфракрасные параллельные и последовательные порты, внешние съемные носители и т.д.)
5. Управление информационной безопасностью: условия, при которых необходимо изменять первоначально настроенную систему защиты информации, обоснование необходимости изменений
6. Свободно распространяемые программы – снятие логов с персонального компьютера.
7. Свободно распространяемые программы – анализаторы логов. Примеры применения в управлении информационной безопасностью
8. Свободно распространяемые утилиты для автоматического анализа логов пользователя персонального компьютера (именно утилиты, в предыдущем задании – программы)
9. Свободно распространяемые программы мониторинга подключений к персональному компьютеру. Примеры применения в управлении информационной безопасностью
10. Свободно распространяемые программы беспроводных мониторинга подключений к персональному компьютеру. Примеры применения в управлении информационной безопасностью
11. Утилиты оперативного реагирования: утилита идентификации, сбора и анализа временных файлов
12. Утилиты оперативного реагирования: утилита идентификации, сбора и анализа cookies
13. Утилиты оперативного реагирования: анализ сетевых подключений на предмет отклонения от обычного состояния
14. Утилиты просмотра реестра на предмет отклонения от обычного состояния
15. Инцидент «несанкционированный доступ»: программные средства выявления и доказательств инцидента.
16.Инцидент «компрометация информации»: программные средства выявления и доказательств инцидента.
17. Инцидент «удаление информации»: программные средства выявления и доказательств инцидента.
18. Инцидент «аномальное поведение бизнес-приложений»: программные средства выявления и доказательств инцидента.
19. Инцидент «сканирование сети»: программные средства выявления и доказательств инцидента.
20. Инцидент «перехват и подмена трафика»: программные средства выявления и доказательств инцидента.
21. Инцидент «письма с угрозами»: программные средства выявления и доказательств инцидента.
22. Инцидент «перехват и подмена трафика»: программные средства выявления и доказательств инцидента.
23. База данных известных ошибок, ее использование при управлении инцидентами
24. Журналы оповещений систем, их роль в управлении инцидентами. Примеры анализа

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

6.1. Рекомендуемая литература

6.1.1. Основная литература				
	Авторы, составители	Заглавие	Издательство, год	Эл. адресс
Л1.1	А. Э. Саак, Е. В. Пахомов, В. Н. Тюшняков	Информационные технологии управления: учебник	СПб.: Питер, 2012	
Л1.2	Шаньгин В.	Информационая безопасность и защита информации	М., ДМК Пресс, 2017	
Л1.3	Бирюков А.А.	Информационная безопасность: защита и нападение	ДМК Пресс, 2017	https://e.lanbook.com/book/93278
Л1.4	В. П. Мельников, С. А. Клейменов, А. М. Петраков	Информационная безопасность и защита информации: учеб. пособие для вузов	М.: Академия, 2009	
6.1.2. Дополнительная литература				
	Авторы, составители	Заглавие	Издательство, год	Эл. адресс
Л2.1	В. С. Провалов	Информационные технологии управления: учеб. пособие	М.: Флинта, 2008	
Л2.2	А. А. Перфильев	Управление рисками и страхование: учеб. пособие	Новосибирск, 2009	
Л2.3	А. Б. Петровский	Теория принятия решений: учебник	М.: Академия, 2009	
Л2.4	А. Э. Саак, Е. В. Пахомов, В. Н. Тюшняков	Информационные технологии управления: учебник	СПб.: Питер, 2009	

6.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет"	
Э1	www.gpntb.ru/ Государственная публичная научно-техническая библиотека.
Э2	www.nlr.ru/ Российская национальная библиотека.
Э3	www.nns.ru/ Национальная электронная библиотека.
Э4	www.rsl.ru/ Российская государственная библиотека.
Э5	www.microinform.ru/ Учебный центр компьютерных технологий «Микроинформ».
Э6	www.tests.specialist.ru/ Центр компьютерного обучения МГТУ им. Н.Э.Баумана.
Э7	www.intuit.ru/ Образовательный сайт
Э8	www.window.edu.ru/ Библиотека учебной и методической литературы
Э9	www.osp.ru/ Журнал «Открытые системы»
Э10	www.ihtika.lib.ru/ Библиотека учебной и методической литературы
6.3.1 Перечень программного обеспечения	
7.3.1.1	Операционная система Microsoft Windows 7
7.3.1.2	Офисный пакет Microsoft Office 2007
6.3.2 Перечень информационных справочных систем	

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)	
7.1	Стандартно оборудованные лекционные аудитории, аудитории для проведения интерактивных лекций: видеопроектор, экран настенный и компьютерный класс

8. МЕТОДИЧЕСТКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

Рекомендации по подготовке к лекционным занятиям (теоретический курс):
Перед очередной лекцией необходимо бегло ознакомиться с содержанием очередной лекции по основным источникам литературы в соответствии с рабочей программой дисциплины.
Часть лекционного материала представлена в виде презентаций, ссылок на Интернет-источники. Материалы распределены по разделам курса.

Рекомендации по подготовке к практическим работам:
- необходимо проработать теоретический материал, соответствующий теме работы.
- в начале занятий задать преподавателю вопросы по материалу, вызвавшему затруднения в его понимании и освоении.
- при ответе на вопросы, поставленные для самостоятельной проработки, необходимо его увязывать их с вопросами защиты информации в коммерческой организации.

Рекомендации по подготовке к самостоятельной работе:
- выполнять в установленные сроки все плановые задания, выдаваемые преподавателем, выяснять на консультациях неясные вопросы.
= прорабатывать соответствующие теоретические и практические разделы курса, все неясные моменты фиксировать и

выносить на плановую консультацию.