МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования
«Воронежский государственный технический университет»

УТВЕРЖДАЮ
Декан факультета_____ С.А. Баркалов
«31» августа 2017 г.

РАБОЧАЯ ПРОГРАММА

дисциплины

«Информационная безопасность»

Специальность 38.05.01 ЭКОНОМИЧЕСКАЯ БЕЗОПАСНОСТЬ

Специализация Экономико-правовое обеспечение экономической безопасности

Квалификация выпускника экономист

Нормативный период обучения 5 лет / 6 лет

Форма обучения очная / заочная

Год начала подготовки 2016

Автор программы _____/Белоусов В.Е./

Заведующий кафедрой
Управления строительством _____/Баркалов С.А./

Руководитель ОПОП _____/Морозов В.П./

Воронеж 2017

1. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ

1.1. Цели дисциплины

изучение комплекса проблем информационной безопасности предпринимательских структур различных типов и направлений деятельности, построения, функционирования и совершенствования правовых, организационных, технических и технологических процессов, обеспечивающих информационную безопасность и формирующих структуру системы защиты ценной и конфиденциальной информации в сферах охраны интеллектуальной собственности предпринимателей и сохранности, их информационных ресурсов.

1.2. Задачи освоения дисциплины

овладение теоретическими, практическими и методическими вопросами обеспечения информационной безопасности и освоение системных комплексных методов защиты предпринимательской информации от различных видов объективных и субъективных угроз в процессе ее возникновения, обработки, использования и хранения:

– изучение концепции инженерно-технической защиты информации;

– изучение теоретических основ инженерно - технической защиты информации;

– изучение физических основ инженерно-технической защиты информации;

– изучение технических средств добывания и защиты информации;

– изучение организационных основ инженерно-технической защиты информации;

– изучение методического обеспечения инженерно-технической защиты информации.

Изучаемые вопросы рассматриваются в широком диапазоне современных проблем и затрагивают предметные сферы защиты как документированной информации (на бумажных и технических носителях), циркулирующей в традиционном или электронном документообороте, находящейся в компьютерных системах, так и недокументированной информации, распространяемой персоналом в процессе управленческой (деловой) или производственной деятельности.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина «Информационная безопасность» относится к дисциплинам базовой части блока Б1. В результате изучения дисциплины студенты должны иметь общее представление о методах обеспечения безопасности информационных ресурсов, ведения аналитической работы по выявлению угроз несанкционированного доступа к информации, ее утраты, функциональные возможности и предпосылки эффективного использования различных типов технологических систем и способов обработки и хранения традиционных и электронных конфиденциальных документов . Полученные знания и навыки могут применяться в процессе подготовки выпускной

квалификационной работы.

В результате изучения дисциплины студенты должны знать: средства и методы предотвращения и обнаружения вторжений; технические каналы утечки информации; возможности технических средств перехвата информации; способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации; организацию защиты информации от утечки по техническим каналам на объектах информатизации; уметь: пользоваться нормативными документами по противодействию технической разведке; оценивать качество готового программного обеспечения; владеть: методами и средствами технической защиты информации; методами расчета и инструментального контроля показателей технической защиты информации.

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Процесс изучения дисциплины «Информационная безопасность» направлен на формирование следующих компетенций:

ОК-12 - способностью работать с различными информационными ресурсами и технологиями, применять основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации

ПК-20 - способностью соблюдать в профессиональной деятельности требования, установленные нормативными правовыми актами в области защиты государственной тайны и информационной безопасности, обеспечивать соблюдение режима секретности

Компетенция	**Результаты обучения, характеризующие сформированность компетенции**
ОК-12	знать способностью работать с различными информационными ресурсами и технологиями, применять основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации
	уметь способностью работать с различными информационными ресурсами и технологиями, применять основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации
	владеть способностью работать с различными информационными ресурсами и технологиями, применять основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации
ПК-20	знать требования, установленные нормативными правовыми актами в области защиты государственной тайны и информационной безопасности

	уметь обеспечивать соблюдение режима секретности
	владеть способностью соблюдать в профессиональной деятельности требования, установленные нормативными правовыми актами в области защиты государственной тайны и информационной безопасности, обеспечивать соблюдение режима секретности

4. ОБЪЕМ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины «Информационная безопасность» составляет 5 з.е.

Распределение трудоемкости дисциплины по видам занятий

очная форма обучения

Виды учебной работы	Всего часов	Семестры
		9
Аудиторные занятия (всего)	95	95
В том числе:		
Лекции	19	19
Практические занятия (ПЗ)	38	38
Лабораторные работы (ЛР)	38	38
Самостоятельная работа	49	49
Курсовая работа	+	+
Часы на контроль	36	36
Виды промежуточной аттестации - экзамен	+	+
Общая трудоемкость: академические часы зач.ед.	 180 5	 180 5

заочная форма обучения

Виды учебной работы	Всего часов	Семестры
		11
Аудиторные занятия (всего)	28	28
В том числе:		
Лекции	6	6
Практические занятия (ПЗ)	10	10
Лабораторные работы (ЛР)	12	12
Самостоятельная работа	143	143
Курсовая работа	+	+
Часы на контроль	9	9
Виды промежуточной аттестации - экзамен	+	+
Общая трудоемкость: академические часы зач.ед.	 0 5	 180 5

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

5.1 Содержание разделов дисциплины и распределение трудоемкости по видам занятий

очная форма обучения

№ п/п	Наименование темы	Содержание раздела	Лекц	Прак зан.	Лаб. зан.	СРС	Всего, час
1	Информационная безопасность в системе национальной безопасности Российской Федерации	Основные термины и определения. Классификация защищаемой информации . Некоторые проблемы обеспечения информационной безопасности в Российской Федерации. Основные положения документов «О стратегии национальной безопасности Российской федерации до 2020 года» и «Доктрина информационной безопасности Российской Федерации». Основные составляющие национальных интересов Российской Федерации в информационной сфере. Основные направления федерального законодательства в области защиты информации ограниченного доступа. Проблемы региональной информационной безопасности .	3	6	8	8	25
2	Критерии и классы защищенности средств вычислительной техники и автоматизированных информационных систем	. Стандарты по оценке защищенных систем. Критерии безопасности компьютерных систем. Европейские «Критерии безопасности информационных технологий». Федеральные критерии безопасности информационных технологий. Канадские критерии безопасности компьютерных систем. Обзор серии стандартов ISO/IEC 17799. Стандарты ISO/IEC 17799:2002 (BS 7799:2000). Стандарт ISO/IEC 27001. Российский стандарт ГОСТ Р ИСО/МЭК 27001-2006. Стандарты ISO/IEC 15408 и ГОСТ Р ИСО/МЭК 15408. Российская классификация средств вычислительной техники и автоматизированных систем и требования по защите информации согласно РД ФСТЭК	4	6	6	8	24
3	Абстрактные модели обеспечения информационной безопасности	Ранние модели управления доступом. . Модель матрицы доступов Харрисона – Руззо – Ульмана. Модель Белла и Лападула. Модель систем военных сообщений. Понятие контроля доступа, базирующегося на ролях	4	6	6	8	24
4	Основные угрозы информационной безопасности автоматизированных систем	Анализ и классификация угроз информационной безопасности автоматизированных систем. Причины, виды, каналы утечки и искажения информации. Угрозы программно-математических воздействий и нетрадиционных информационных каналов. Угрозы,	4	6	6	8	24

		основанные на информационных сетевых атаках					
5	Основы построения систем защиты информации	Основные принципы обеспечения информационной безопасности предприятий. Основные методы и средства защиты информации. Порядок построения защищенной автоматизированных системах управления предприятия (АСУП). Аттестация объектов информатизации по требованиям безопасности информации	2	6	6	8	22
6	Основы обеспечения информационной безопасности в автоматизированных системах управления	Проблемы обеспечения информационной безопасности в АСУП. Основные термины и определения. Основные угрозы безопасности АСУП. Правовые основы защиты информации. Цели защиты информации. Режимы защиты информации. Классификация компьютерных преступлений	2	8	6	9	25
		Итого	**19**	**38**	**38**	**49**	**144**

заочная форма обучения

№ п/п	Наименование темы	Содержание раздела	Лекц	Прак зан.	Лаб. зан.	СРС	Всего, час
1	Информационная безопасность в системе национальной безопасности Российской Федерации	Основные термины и определения. Классификация защищаемой информации . Некоторые проблемы обеспечения информационной безопасности в Российской Федерации. Основные положения документов «О стратегии национальной безопасности Российской федерации до 2020 года» и «Доктрина информационной безопасности Российской Федерации». Основные составляющие национальных интересов Российской Федерации в информационной сфере. Основные направления федерального законодательства в области защиты информации ограниченного доступа. Проблемы региональной информационной безопасности .	2	-	2	24	28
2	Критерии и классы защищенности средств вычислительной техники и автоматизированных информационных систем	. Стандарты по оценке защищенных систем. Критерии безопасности компьютерных систем. Европейские «Критерии безопасности информационных технологий». Федеральные критерии безопасности информационных технологий. Канадские критерии безопасности компьютерных систем. Обзор серии стандартов ISO/IEC 17799. Стандарты ISO/IEC 17799:2002 (BS 7799:2000). Стандарт ISO/IEC 27001. Российский стандарт ГОСТ Р ИСО/МЭК 27001-2006. Стандарты ISO/IEC 15408 и ГОСТ Р ИСО/МЭК 15408. Российская классификация	2	2	2	24	30

		средств вычислительной техники и автоматизированных систем и требования по защите информации согласно РД ФСТЭК					
3	Абстрактные модели обеспечения информационной безопасности	Ранние модели управления доступом. . Модель матрицы доступов Харрисона – Руззо – Ульмана. Модель Белла и Лападула. Модель систем военных сообщений. Понятие контроля доступа, базирующегося на ролях	2	2	2	24	30
4	Основные угрозы информационной безопасности автоматизированных систем	Анализ и классификация угроз информационной безопасности автоматизированных систем. Причины, виды, каналы утечки и искажения информации. Угрозы программно-математических воздействий и нетрадиционных информационных каналов. Угрозы, основанные на информационных сетевых атаках	-	2	2	24	28
5	Основы построения систем защиты информации	Основные принципы обеспечения информационной безопасности предприятий. Основные методы и средства защиты информации. Порядок построения защищенной автоматизированных системах управления предприятия (АСУП). Аттестация объектов информатизации по требованиям безопасности информации	-	2	2	24	28
6	Основы обеспечения информационной безопасности в автоматизированных системах управления	Проблемы обеспечения информационной безопасности в АСУП. Основные термины и определения. Основные угрозы безопасности АСУП. Правовые основы защиты информации. Цели защиты информации. Режимы защиты информации. Классификация компьютерных преступлений	-	2	2	23	27
		Итого	**6**	**10**	**12**	**143**	**171**

5.2 Перечень лабораторных работ

№ п/п	№ раздела дисциплины	Наименование практических работ	Трудо-емкость (час) очно/заочно
1.	1	Математические аспекты применения формальных моделей	8/2
2	2	Практическая реализация и оценка формальных моделей	6/2
3	3	Исследование корректности систем защиты	6/2
4	4	Инсталляция и настройка штатных средств операционных систем, предназначенных для защиты от НСД и	6/2

		программно-аппаратных комплексов защиты от НСД	
5	5	Инсталляция и настройка МЭ, программно-аппаратных средств защиты информации при передаче по открытым каналам связи и разграничения доступа к сетевым ресурсам	6/2
6	6	Анализ состояния информационных систем и организация защиты от хакерских атак	6/2

6. ПРИМЕРНАЯ ТЕМАТИКА КУРСОВЫХ ПРОЕКТОВ (РАБОТ) И КОНТРОЛЬНЫХ РАБОТ

В соответствии с учебным планом освоение дисциплины предусматривает выполнение курсовой работы в 9 семестре для очной формы обучения, 11.

Примерная тематика курсовой работы: ««Разработка мероприятий информационной безопасности специализированного объекта».

Примерные темы курсовых проектов

1. Разработка мероприятий по защите информации для системы управления ООО « Воронежсельмаш».
2. Разработка мероприятий по защите информации для системы управления ЗАО «Рудгормаш».
3. Разработка мероприятий по защите информации для системы управления ЗАО ВКСМ.
4. Разработка мероприятий по защите информации для системы управления ООО завод им. Тельмана.
5. Разработка мероприятий по защите информации для системы управления ОАО Электроприбор.
6. Разработка мероприятий по защите информации для системы управления ООО Финист-мыловар.
7. Разработка мероприятий по защите информации для системы управления ООО Ангстрем.
8. Разработка мероприятий по защите информации для системы управления ООО ВЭКС.
9. Разработка мероприятий по защите информации для системы управления ООО Воронежский шинный завод.

Разработка мероприятий по защите информации для системы управления ООО Воронежский станкостроительный завод.

Задачи, решаемые при выполнении курсовой работы:

1. Проанализировать общую характеристику объекта защиты, оформленную в виде «Паспорта предприятия»;

2.Построить модель бизнес-процессов с целью выявления конфиденциальной информации;

3. Составить «Перечень сведений конфиденциального характера»;

4. Выявить объекты защиты, оформленные в виде «Списка объектов, подлежащих защите»;

5.Выявить угрозы, уязвимости и произвести расчет рисков для ключевых объектов защиты;

6.Построить модель злоумышленника;

7. Проанализировать степень защищенности объектов защиты по каждому из видов защиты информации (ЗИ) (правовая ЗИ, организационная ЗИ, программно-аппаратная ЗИ, инженерно-физическая ЗИ, криптографическая ЗИ).

Курсовая работа включат в себя графическую часть и расчетно-пояснительную записку.

7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

7.1. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

7.1.1 Этап текущего контроля

Результаты текущего контроля знаний и межсессионной аттестации оцениваются по следующей системе:

«аттестован»;

«не аттестован».

Компе-тенция	Результаты обучения, характеризующие сформированность компетенции	Критерии оценивания	Аттестован	Не аттестован
ОК-12	знать способностью работать с различными информационными ресурсами и технологиями, применять основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации	укажите критерий	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	уметь способностью работать с различными информационными ресурсами и технологиями, применять основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации	укажите критерий	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	владеть способностью работать с	укажите критерий	Выполнение работ в срок, предусмотренный в	Невыполнение работ в срок, предусмотренный в

	различными информационными ресурсами и технологиями, применять основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации		рабочих программах	рабочих программах
ПК-20	знать требования, установленные нормативными правовыми актами в области защиты государственной тайны и информационной безопасности	укажите критерий	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	уметь обеспечивать соблюдение режима секретности	укажите критерий	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	владеть способностью соблюдать в профессиональной деятельности требования, установленные нормативными правовыми актами в области защиты государственной тайны и информационной безопасности, обеспечивать соблюдение режима секретности	укажите критерий	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах

7.1.2 Этап промежуточного контроля знаний

Результаты промежуточного контроля знаний оцениваются в 9 семестре для очной формы обучения, 11 семестре для заочной формы обучения по четырехбалльной системе:

«отлично»;

«хорошо»;

«удовлетворительно»;

«неудовлетворительно».

Компе-тенция	Результаты обучения, характеризующие сформированность компетенции	Критерии оценивания	Отлично	Хорошо	Удовл.	Неудовл.
ОК-12	знать способностью работать с различными информационными ресурсами и	Тест	Выполнение теста на 90-100%	Выполнение теста на 80-90%	Выполнение теста на 70-80%	В тесте менее 70% правильных ответов

	технологиями, применять основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации					
	уметь способностью работать с различными информационными ресурсами и технологиями, применять основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации	Решение стандартных практических задач	Задачи решены в полном объеме и получены верные ответы	Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены
	владеть способностью работать с различными информационными ресурсами и технологиями, применять основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации	Решение прикладных задач в конкретной предметной области	Задачи решены в полном объеме и получены верные ответы	Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены
ПК-20	знать требования, установленные нормативными правовыми актами в области защиты государственной тайны и информационной безопасности	Тест	Выполнение теста на 90-100%	Выполнение теста на 80-90%	Выполнение теста на 70-80%	В тесте менее 70% правильных ответов
	уметь обеспечивать соблюдение режима секретности	Решение стандартных практических задач	Задачи решены в полном объеме и получены верные ответы	Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены

	владеть способностью соблюдать в профессиональной деятельности требования, установленные нормативными правовыми актами в области защиты государственной тайны и информационной безопасности, обеспечивать соблюдение режима секретности	Решение прикладных задач в конкретной предметной области	Задачи решены в полном объеме и получены верные ответы	Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены

7.2 Примерный перечень оценочных средств (типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности)

7.2.1 Примерный перечень заданий для подготовки к тестированию

Укажите основные свойства VPN

Создает туннель, т.е. защищённый канал передачи данных
Использует шифрование данных
Реализуется в незащищенных или слабо защищенных сетях

Каковы функциональные возможности программы Retina WiFi Scanner

Вычисляет WEP-ключи методом brute force
Генерирует отчёты
Обнаруживает IP-адреса и другую сетевую информацию
Обнаруживает неавторизованные беспроводные устройства

64- и 128-битное WEP-шифрование трафика на основе RC4 обеспечивает уровень безопасности

Высокий

Отметьте потенциально опасные с точки зрения утечек внутренней информации действия

Размещение серверов в стороннем дата-центре
Хранение носителей вне офиса
Сервисный ремонт серверов или жестких дисков
Перевозка компьютеров или носителей

Перебор всех слов языка для взлома пароля это

атака Brute Force

Какого типа БД является реестр

иерархическая

IDS - это

система обнаружения вторжений

Какие режимы работы имеет программа Iris

Decode
Capture

Используется ли VPN для защиты беспроводных сетей

да

Какие дополнительные меры обеспечения безопасности могут использоваться в беспроводных сетях

Технология VPN
Использование IPSec для защиты трафика
Защита беспроводного сегмента с помощью L2TP
Выделение беспроводной сети в отдельный сегмент

Инсайдер - это

член какой-либо группы людей, имеющий доступ к секретной, скрытой или какой-либо другой закрытой информации или знаниями, недоступной широкой публике

Сколько root key содержит реестр Windows

5

Решение DeviceLock является

программно-аппаратным

Способ построения одноранговых Wi-Fi сетей называется

Ad-hoc

Какие решения применяются для контроля доступа к внешним устройствам

Secret Disk
ZLock
DeviceLock

7.2.2 Примерный перечень заданий для решения стандартных задач

Какие решения применяются для контроля доступа к внешним устройствам

Secret Disk
ZLock

DeviceLock

Компьютер проверяет 10 млн. паролей в секудну. Сколько примерно времени ему потребуется, чтобы проверить методом словарной атаки все пароли для языка, содержащего 1 млн слов

0,1 секунды

Сколько групп символов должен минимально содержать надежный пароль

3

Тонкий клиент - это

Бездисковый компьютер-клиент в сетях с клиент-серверной или терминальной архитектурой, который переносит все или большую часть задач по обработке информации на сервер

В какой блок файла autorun.inf обычно прописываются вредоносные программы

open

Каково количество популярных паролей, которые остаются неизменными в течение последних 15 лет

500

Какой протокол VPN используется для создания защищенного сегмента локальной сети

IpSec

DLP (Data Leak Prevention) система защищает от

утечек конфиденциальной информации из информационной системы вовне

Что позволяет выполнять программа Process Monitor

Отслеживать сетевую активность процесса
Отслеживать обращение процесса к реестру
Отслеживать работу процесса с файлами

Необходимы ли криптографические ключи для создания VPN-тоннеля

Да

Каковы предпосылки возникновения искусственного интеллекта как науки?

-появление ЭВМ
-развитие кибернетики, математики, философии, психологии и т.д.
-научная фантастика

-нет правильного ответа

В каком году появился термин искусственный интеллект (artificial intelligence)?

-1856
-1956
-1954
-1950
-Нет правильного ответа

Кто считается родоначальником искусственного интеллекта?

-А. Тьюринг
-Аристотель
-Р. Луллий
-Декарт
-правильного ответа

7.2.3 Примерный перечень заданий для решения прикладных задач

Файл рабочей группы MS Access содержит следующие встроенные учётные записи:

-System, Window, Help
-Search, View, Copy
-Run, Project, Tools
-Database, Win32, Standart
+Admins, Admin, Users

Для создания новой рабочей группы в MS Access запускаем программу

+wrkgadmexe
-wrkgadmmdw
-wrkgadmmdb
-wrkgadmcpp
-wrkgadmdoc

Как называется документ в программе MS Access?

-таблица
+база данных
-книга
-форма

Телефонный радио ретранслятор большой мощности работает в диапазоне?

+65-108 МГц
-65-80 Мгц
-27-28 МГц
-88-108МГц
-30 МГц

Речевой сигнал находится в диапазоне…

+200300 Гц до 46 кГц

-200…400 Гц до 2…6 кГц

-100…300 Гц до 4…6 кГц

-200…300 Гц до 2…6 кГц

-200…400 Гц до 4…6 кГц

Телефонный ретранслятор с питанием от телефонной линии имеет выходную мощность

-10 мВт

-5 мВт

+20 мВт

-30 мВт

-15 мВт

Телефонный радио ретранслятор с ЧМ на одном транзисторе обеспечивает дальность передачи

-До 100 м

+До 200м

-До 300м

-До 50м

-До 400м

Телефонный ретранслятор УКВ диапазона с ЧМ его дальность действия передатчика

+Около 100м

-Около 200м

-Около 300м

-Около 400м

-Около 50м

Отличие конвертера от Миниатюрного конвертера на частоте 430 МГц.

+Позволяет принимать сигнал с частотой до 1 ГГц

-Емкостью С1 до 15 пФ

-Способу подсоединения к телефонной линии

-Позволяет прослушивать телефонный разговор в диапазона 27-28 МГц

Источник: https://yznaika.com/notes/501

Чтобы установить парольную защиту в ОС Windows , необходимо выполнить следующую процедуру?

+Пуск->Панель управления->Учетные записи->Изменение пароля

-Пуск->Учетные записи->Изменение пароля

-Пуск->Справка->Учетные записи->Изменение пароля

-Пуск->Панель управления->Пароли и данные->Изменение пароля

7.2.4 Примерный перечень вопросов для подготовки к зачету

Не предусмотрено учебным планом

7.2.5 Примерный перечень заданий для решения прикладных задач

1. Каким образом десять неформальных свойств модели СВС

реализуются в ее формальном описании?

2. В каком случае система (T, s_0) безопасна?

3. Где в определениях безопасности модели СВС реализовано *ss*-свойство безопасности классической модели Белла-ЛаПадулы?

4. Где в определениях безопасности модели СВС реализовано *-свойство безопасности классической модели Белла-ЛаПадулы?

5. Где в определениях безопасности модели СВС реализовано *ds*-свойство безопасности классической модели Белла-ЛаПадулы?

6. Каким стандартам необходимо следовать при построении СУИБ?

7. Что регламентируется в стандарте ISO 27002?

8. Что регламентируется в стандарте ISO 18044?

9. Что должна обеспечивать СУИБ?

10. Какова главная задача СУИБ?

11. Какой вид политики управления доступом используется в качестве основы автоматной модели безопасности информационных потоков?

12. В каких случаях в КС с мандатным управлением доступом нецелесообразно предотвращение возможности реализации всех информационных потоков от устройств ввода пользователей с высоким уровнем доступа к устройствам вывода пользователей с низким уровнем доступа?

13. В чем отличие информационной невыводимости от информационного невлияния?

14. Почему использование определения требований информационного невлияния (с учетом времени) позволяет обеспечить возможность функционирования в КС монитора ссылок?

15. В каких случаях может являться эффективным моделирование безопасности информационных потов с использованием вероятностных подходов?

16. Что понимается под термином информационная безопасность?

17. Что понимается под термином доступность информации?

18. Что понимается под термином целостность информации?

19. Что понимается под термином конфиденциальность информации?

20. Что понимается под термином комплекс средств автоматизации обработки информации?

21. Что понимается под термином информационная безопасность ИС?

22. Что понимается под термином уничтожение информации?

23. Какие способы защиты от вирусов Вы знаете?

24. Какие способы защиты от несанкционированного доступа Вы можете привести?

25. Анализ источников, каналов распространения и каналов утечки информации (на примере конкретной фирмы).

26. Анализ конкретной автоматизированной системы, предназначенной для обработки и хранения информации о конфиденциальных документах
фирмы.

27. Основы технологии обработки и хранения конфиденциальных документов (по зарубежной литературе).

28. Назначение, виды, структура и технология функционирования системы защиты информации.

29. Поведение персонала и охрана фирмы в экстремальных ситуациях различных типов.

30. Аналитическая работа по выявлению каналов утечки информации фирмы.

31. Анализ функций секретаря-референта небольшой фирмы в области защиты информации.

32. Направления и методы защиты профессиональной тайны.

33. Направления и методы защиты служебной тайны.

34. Направления и методы защиты персональных данных о гражданах.

35. Методы защиты личной и семейной тайны.

7.2.6. Методика выставления оценки при проведении промежуточной аттестации

Экзамен проводится по тест-билетам, каждый из которых содержит 10 вопросов и задачу. Каждый правильный ответ на вопрос в тесте оценивается 1 баллом, задача оценивается в 10 баллов (5 баллов верное решение и 5 баллов за верный ответ). Максимальное количество набранных баллов – 20.

1. Оценка «Неудовлетворительно» ставится в случае, если студент набрал менее 6 баллов.

2. Оценка «Удовлетворительно» ставится в случае, если студент набрал от 6 до 10 баллов

3. Оценка «Хорошо» ставится в случае, если студент набрал от 11 до 15 баллов.

4. Оценка «Отлично» ставится, если студент набрал от 16 до 20 баллов.)

7.2.7 Паспорт оценочных материалов

№ п/п	Контролируемые разделы (темы) дисциплины	Код контролируемой компетенции	Наименование оценочного средства
1	Информационная безопасность в системе национальной безопасности Российской Федерации	ОК-12, ПК-20	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту….
2	Критерии и классы защищенности средств вычислительной техники и автоматизированных информационных систем	ОК-12, ПК-20	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту….
3	Абстрактные модели обеспечения информационной безопасности	ОК-12, ПК-20	Тест, контрольная работа, защита лабораторных

			работ, защита реферата, требования к курсовому проекту….
4	Основные угрозы информационной безопасности автоматизированных систем	ОК-12, ПК-20	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту….
5	Основы построения систем защиты информации	ОК-12, ПК-20	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту….
6	Основы обеспечения информационной безопасности в автоматизированных системах управления	ОК-12, ПК-20	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту….

7.3. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности

Тестирование осуществляется, либо при помощи компьютерной системы тестирования, либо с использованием выданных тест-заданий на бумажном носителе. Время тестирования 30 мин. Затем осуществляется проверка теста экзаменатором и выставляется оценка согласно методики выставления оценки при проведении промежуточной аттестации.

Решение стандартных задач осуществляется, либо при помощи компьютерной системы тестирования, либо с использованием выданных задач на бумажном носителе. Время решения задач 30 мин. Затем осуществляется проверка решения задач экзаменатором и выставляется оценка, согласно методики выставления оценки при проведении промежуточной аттестации.

Решение прикладных задач осуществляется, либо при помощи компьютерной системы тестирования, либо с использованием выданных задач на бумажном носителе. Время решения задач 30 мин. Затем осуществляется проверка решения задач экзаменатором и выставляется оценка, согласно методики выставления оценки при проведении промежуточной аттестации.

Защита курсовой работы, курсового проекта или отчета по всем видам практик осуществляется согласно требованиям, предъявляемым к работе, описанным в методических материалах. Примерное время защиты на одного студента составляет 20 мин.

8 УЧЕБНО МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ)

8.1 Перечень учебной литературы, необходимой для освоения дисциплины

8.1.1. Основная литература

1. . С.А. Баркалов, В.Е. Белоусов, С,А. Колодяжный. Информационная безопасность при управлении техническими системами:/ Учебное пособие. Санкт-Петербург: Изд-во Интермедия, 2016. – 528 с.

2. *Белоусов В.Е.* Средства защиты информации в интегрированных технических системах управления. Методические указания для выполнения курсового проекта [Электронный]// В.Е.Белоусов. Воронеж. гос. арх.–строит. ун–т. -Воронеж, 2014.- 42 с.

3. *Белоусов В.Е.* Средства защиты информации в интегрированных технических системах управления. Методические указания по самостоятельной работе [Электронный]// Е.Белоусов. Воронеж. гос. арх.–строит. ун–т. -Воронеж, 2014.- 33 с.

8.1.2. Дополнительная литература:

4. Алябьева, О. Организация процесса адаптации // Кадровые решения. – 2007. - №6. - С. 81-86.

5. Аминов, В.Л. Кадровая безопасность предприятия // Кадровые решения. – 2009. – № 10. – С.91-99.

6. Бахарева, Е.В. Коммерческая тайна // Секретарь-референт. – 2006. – № 11. – С. 43-50.

7. Громыко, И.А. Общая парадигма защиты информации. Определение терминов: от носителей к каналам утечки информации // Защита информации. Инсайд. – 2008. - № 1. – С.12-15.

8. Доля, А.А. Внутренние ИТ-угрозы в России – 2006 // Защита информации. Инсайд. – 2007. - № 2. – С.60-69.

9. Зенин, Н. Обеспечение конфиденциальности информации – это всегда комплексный подход // Трудовое право. – 2010. – № 1. – С. 41-42.

10. Камаев, В.А., Натров, В.В. Моделирование и анализ состояния информационной безопасности организации // Защита информации. Инсайд. – 2009. - № 4. – С.16-20.

11. Суханова, И.М. Аттестация и комплексная оценка персонала // Кадровые решения. – 2007. - № 4. – С.76-84.

12. Чуковенков, А.Ю. Документы по аттестации служащих // Секретарь-референт. – 2006. - № 11. – С. 17-23.

13. Шубин, А.С. Наша Тайна громко плачет… // Защита информации. Инсайд. – 2008. - № 1. С. 19-27.

14. Янковая, В.Ф. Гриф ограничения доступа к документу // Секретарь-референт. – 2008. - № 1. – С. 17-19.

15. Янковая, В.Ф. Организация конфиденциального делопроизводства // Секретарь-референт. – 2009. - № 12. – С.17 – 20.

Нормативно-правовые источники:

Конституция Российской Федерации // Российская газета. 1993. 25 дек.

О средствах массовой информации. Закон Российской Федерации от 27.12. 1991 № 2124-1// Ведомости съезда народных депутатов РФ и

Верховного Совета РФ. - 1992 . - №7. - С. 378 - 399.

Закон Российской Федерации «О безопасности» от 05.03.92 г. // Ведомости съезда народных депутатов Российской Федерации и Верховного Совета Российской Федерации. 1992. № 15. Ст. 769.

Закон Российской Федерации «О федеральных органах правительственной связи и информации» от 19.02.93 г. №4524-1// Ведомости съезда народных депутатов Российской Федерации и Верховного Совета Российской Федерации.1993. №12. Ст.423.

Федеральный закон «О библиотечном деле» от 29.12.94 г. № 78-ФЗ // Собрание законодательства Российской Федерации. 1995. № 1. Ст. 2.

Федеральный закон «О порядке опубликования и вступления в силу федеральных конституционных законов, федеральных законов, актов палат Федерального Собрания» от 14.06.94 г. № 5-ФЗ // Собрание законодательства Российской Федерации. 1994. № 8. Ст. 801.

Федеральный закон «О федеральной фельдъегерской связи» от 17.12.94 г. № 67-ФЗ // Собрание законодательства Российской Федерации. № 34. Ст. 3547.

Федеральный закон «Об обязательном экземпляре документов» от 29.12.94 г. № 77-ФЗ // Собрание законодательства Российской Федерации. 1995. № 1. Ст. 1.

Федеральный закон «О рекламе» от 18.07.95 г. № 108-ФЗ // Собрание законодательства Российской Федерации. №30. Ст. 2864.

Федеральный закон «О порядке освещения деятельности органов государственной власти в государственных органах массовой информации» от 13.01.95 г. № 7-ФЗ // Собрание законодательства Российской Федерации. № 3. Ст. 170.

Федеральный закон «О почтовой связи» от 09.08.95 г. № 129-ФЗ // Собрание законодательства Российской Федерации. № 33. Ст. 3334.

Закон Российской Федерации «О государственной тайне» от 21.07.93 г. с изменениями и дополнениями от 06.10.97 г. // Собрание законодательства Российской Федерации. 1997. № 41. Ст. 4673.

Федеральный закон «О связи» от 16.02.95 г. № 15-ФЗ // Собрание законодательства Российской Федерации.1995. №8. № Ст. 600.

Федеральный закон «Об основах государственной службы Российской Федерации» от 31.07.95 г. № 119-ФЗ // Собрание законодательства Российской Федерации. № 31. Ст. 2990.

Федеральный закон «Об оперативно-розыскной деятельности» от 12.08.95 г. № 144-ФЗ// Собрание законодательства Российской Федерации. 1995. № 33. Ст. 3349.

Федеральный закон «Об электронной цифровой подписи» от 10.01.02 г. №1-ФЗ // Собрание законодательства Российской Федерации. 2002. № 2. Ст. 127.

Федеральный закон «О коммерческой тайне» от 09.07.04 г. №98-ФЗ // Собрание законодательства Российской Федерации. 2004. № 32. Ст.3283.

Федеральный закон РФ «Об архивном деле в Российской Федерации»

от 22 .10. 2004 . // Собрание Законодательства Российской Федерации. 2004. № 43. Ст. 4169.

Федеральный Закон от 13.03. 2006 . № 38–ФЗ «О рекламе» // Собрание Законодательства Российской Федерации. 2006. № 12. Ст. 1232.

Федеральный Закон от 27.07. 2006 . № 149–ФЗ «Об информации, информационных технологиях и о защите информации» // Собрание Законодательства Российской Федерации. 2006. № 31. (Ч. 1). Ст. 3448.

Федеральный Закон от 27.07. 2006 . № 152–ФЗ «О персональных данных» // Собрание Законодательства Российской Федерации. 2006. № 31. (Ч. 1). Ст. 3451.

Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред.13.05.2008) // Собрание законодательства Российской Федерации. 1996. № 25. Ст. 2954.

Кодекс Российской Федерации об административных правонарушениях от 30.12.2001. № 195-ФЗ (ред.16.05.2008) // Собрание законодательства Российской Федерации. 2002. № 1. (Ч.1). Ст. 1.

Трудовой Кодекс Российской Федерации об от 30.12.2001. № 197-ФЗ (ред.28.02.2008) // Собрание законодательства Российской Федерации. 2002. № 1. (Ч.1). Ст. 3.

Гражданский кодекс Российской Федерации. Часть четвертая от18.12.2006 № 230-ФЗ // Собрание законодательства Российской Федерации. 2006. № 52. Ст. 1232.

Указ Президента Российской Федерации «Об основах государственной политики в сфере информатизации» от 20.01.94 г. № 170 // Собрание актов Президента и Правительства Российской Федерации. 1994. № 4. Ст. 305.

Указ Президента Российской Федерации «О перечне сведений, отнесенных к государственной тайне» от 30.11.95 г. №1203; в редакции Указа Президента РФ от 24.01.98№ 61 от 06.06.01 г. №659 // Собрание законодательства Российской Федерации. 1998. №5. Ст.561; 2001. №24. Ст.2418.

«Положение о Межведомственной комиссии по защите государственной тайны» утверждено Указом Президента Российской Федерации от 20.01.96 г. №71 // Собрание законодательства Российской Федерации. 1996. № 4. Ст. 268.

Указ Президента Российской Федерации «О концепции национальной безопасности Российской Федерации» от 10.01.2000 г. № 24 // Собрание законодательства Российской Федерации. 2000. № 2. Ст. 170.

«Доктрина информационной безопасности Российской Федерации» утверждена Указом Президента Российской Федерации 09.09.00 г. №ПР-1895 // Российская газета №187 от 28.09.00 г.

Указ Президента Российской Федерации «О концепции национальной безопасности Российской Федерации» от 10.01.2000 г. № 24 // Собрание законодательства Российской Федерации. 2000. № 2. Ст. 170.

Постановление Правительства Российской Федерации «Правила отнесения сведений составляющих государственную тайну, к различным

степеням секретности» от 04.09.95 г. № 870 // Собрание законодательства Российской Федерации. 1995. № 37. Ст. 3619.

Постановление Правительства Российской Федерации «О государственном учете и регистрации баз и банков данных» от 28.02.99 г. № 226 // Собрание законодательства Российской Федерации. 1999 №12. Ст.1114.

ГОСТ 6.10.4-84. Унифицированные системы документации. Придание юридической силы документам на машинном носителе и машинограмме, созданным средствами вычислительной техники. М.: Изд-во Стандартов, 1985.

ГОСТ 6.10.1-88. Унифицированные системы документации. Основные положения. М.: Изд-во Стандартов, 1988.

ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритмы криптографического преобразования. М., 1990.

ГОСТ Р-22.0.04-95. Безопасность в чрезвычайных ситуациях. Биолого-социальные чрезвычайные ситуации. Термины и определения. М., 1995.

ГОСТ Р-22.3.05-96. Безопасность в чрезвычайных ситуациях. Жизнеобеспечение населения в чрезвычайных ситуациях. Термины и определения. М.: Изд-во Стандартов, 1996.

ГОСТ Р 50922-96. Защита информации: Основные термины и определения. М., 1996.

ГОСТ Р 6.30-97. Унифицированные системы документации: Система организации норм распорядительной документации: Требования к оформлению документов. М.: Госстандарт. 1998.

ГОСТ 51241-98. Средства и системы контроля и управления доступом. Классификация. Общие технические требования и методы испытания. М.: Изд-во Стандартов, 1999.

ГОСТ 51275-99. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. М., 2000.

ГОСТ Р 6.30-2003. Унифицированные системы документации. Унифицированная система организационно-распорядительной документации. Требования к оформлению документов. М.: Госстандарт, 2003.

8.2 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень лицензионного программного обеспечения, ресурсов информационно-телекоммуникационной сети «Интернет», современных профессиональных баз данных и информационных справочных систем:

Для работы в сети рекомендуется использовать сайты:

1. научная Электронная Библиотека http://www.e-library.ru;.
2. информационная система «Единое окно доступа к образовательным ресурсам» (http://window.edu.ru/);
3. рекомендуемые поисковые системы

http://www.yandex.ru/, http://www.google.ru/, http://www.google.com/ и др.

4. Интернет-библиотека: http://www.twirpx.com

Интернет-библиотека: http://www.sciteclibrary.ru

9 МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯ БАЗА, НЕОБХОДИМАЯ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА

Компьютерный класс 4504а в составе:

- Рабочие станции – Пентиум -4,8 Ггц – 10 комплектов;
- Принтер лазерный -1 комплект;
- Комплект сетевого оборудования для организации ЛВС и доступа к ресурсам сети ВГТУ;
- Мультимедиапроектор и экран;
- Программы: Kerio, Антивирус Касперского – 9.0.

Автоматизированные обучающие системы для изучения прикладных программных продуктов, тестирующий комплекс контроля качества обучения, интегрированная система мониторинга хода учебного процесса кафедры.

10. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

По дисциплине «Информационная безопасность» читаются лекции, проводятся практические занятия и лабораторные работы, выполняется курсовая работа.

Основой изучения дисциплины являются лекции, на которых излагаются наиболее существенные и трудные вопросы, а также вопросы, не нашедшие отражения в учебной литературе.

Практические занятия направлены на приобретение практических навыков расчета уровня безопасности объектов защиты. Занятия проводятся путем решения конкретных задач в аудитории.

Лабораторные работы выполняются на лабораторном оборудовании в соответствии с методиками, приведенными в указаниях к выполнению работ.

Методика выполнения курсовой работы изложена в учебно-методическом пособии. Выполнять этапы курсовой работы должны своевременно и в установленные сроки.

Контроль усвоения материала дисциплины производится проверкой курсовой работы, защитой курсовой работы.

Вид учебных занятий	Деятельность студента
Лекция	Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки, обобщения; помечать важные мысли, выделять ключевые слова, термины. Проверка терминов, понятий с помощью энциклопедий,

	словарей, справочников с выписыванием толкований в тетрадь. Обозначение вопросов, терминов, материала, которые вызывают трудности, поиск ответов в рекомендуемой литературе. Если самостоятельно не удается разобраться в материале, необходимо сформулировать вопрос и задать преподавателю на лекции или на практическом занятии.
Практическое занятие	Конспектирование рекомендуемых источников. Работа с конспектом лекций, подготовка ответов к контрольным вопросам, просмотр рекомендуемой литературы. Прослушивание аудио- и видеозаписей по заданной теме, выполнение расчетно-графических заданий, решение задач по алгоритму.
Лабораторная работа	Лабораторные работы позволяют научиться применять теоретические знания, полученные на лекции при решении конкретных задач. Чтобы наиболее рационально и полно использовать все возможности лабораторных для подготовки к ним необходимо: следует разобрать лекцию по соответствующей теме, ознакомится с соответствующим разделом учебника, проработать дополнительную литературу и источники, решить задачи и выполнить другие письменные задания.
Самостоятельная работа	Самостоятельная работа студентов способствует глубокому усвоения учебного материала и развитию навыков самообразования. Самостоятельная работа предполагает следующие составляющие: - работа с текстами: учебниками, справочниками, дополнительной литературой, а также проработка конспектов лекций; - выполнение домашних заданий и расчетов; - работа над темами для самостоятельного изучения; - участие в работе студенческих научных конференций, олимпиад; - подготовка к промежуточной аттестации.
Подготовка к промежуточной аттестации	Готовиться к промежуточной аттестации следует систематически, в течение всего семестра. Интенсивная подготовка должна начаться не позднее, чем за месяц-полтора до промежуточной аттестации. Данные перед экзаменом, экзаменом три дня эффективнее всего использовать для повторения и систематизации материала.