МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

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

УТВЕРЖДАЮ
Декан факультета _____ С.М. Пасмурнов
«31» августа 2017 г.

РАБОЧАЯ ПРОГРАММА
дисциплины

«Информационное противоборство в мультисетевом пространстве»

Специальность 10.05.03 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

Специализация Обеспечение информационной безопасности распределенных информационных систем

Квалификация выпускника специалист по защите информации

Нормативный период обучения 5 лет

Форма обучения очная

Год начала подготовки 2017

Автор программы _____ /А. Г. Остапенко /

Заведующий кафедрой Систем информационной безопасности _____ / А.Г. Остапенко /

Руководитель ОПОП _____ / А.Г. Остапенко /

Воронеж 2017

1.ЦЕЛИИЗАДАЧИДИСЦИПЛИНЫ

1.1. Целидисциплины

Изучение подходов к определению информационного противоборства в мультисетевом пространстве, как составной части национальной безопасности любого государства с учѐтом новых методов и средств взаимодействия противоборствующих сторон.

1.2. Задачиосвоениядисциплины

- познакомить студентов с формами информационной борьбы «второго» поколения, связанными с использованием в качестве информационной инфраструктуры мультисетевого пространства как арены организации противодействия;
- сформировать у студентов устойчивую систему взглядов на необходимость повышения эффективности ведения информационного взаимодействия в мультисетевом пространстве с учѐтом современных видов, методов и средств организации и ведения кибервойн.

2.МЕСТОДИСЦИПЛИНЫВСТРУКТУРЕОПОП

Дисциплина«Информационноепротивоборствовмультисетевомпространстве»относится кдисциплинамвариативнойчастиблокаФТД.

3.ПЕРЕЧЕНЬПЛАНИРУЕМЫХРЕЗУЛЬТАТОВОБУЧЕНИЯПОДИСЦИПЛИНЕ

Процессизучениядисциплины«Информационноепротивоборствовмультисетевомпространстве»направленнаформированиеследующихкомпетенций:

ПК-5-способностьюпроводитьанализрисковинформационнойбезопасностиавтоматизированнойсистемы

ПК-11-способностьюразрабатыватьполитикуинформационнойбезопасностиавтоматизированнойсистемы

ПК-17-способностьюпроводитьинструментальныймониторингзащищенностиинформациивавтоматизированнойсистемеивыявлятьканалыутечкиинформации

ПК-22-способностьюучаствоватьвформированииполитикиинформационнойбезопасностиорганизацииииконтролироватьэффективностьеереализации

ПСК-7.2-способностьюпроводитьанализрисковинформационнойбезопасностииразрабатывать,руководитьразработкойполитикибезопасностивраспределенныхинформационныхсистемах

Компетенция	Результатыобучения,характеризующие сформированностькомпетенции
ПК-5	Знать: - основные риски информационной безопасности в

	мультисетевом пространстве; - основные этапы анализа рисков информационной безопасности в мультисетевом пространстве.
	Уметь: - рассчитывать риски информационной безопасности в условиях сетевого противоборства; -разрабатывать методику анализа рисков информационной безопасности в мультисетевом пространстве.
	Владеть: -расчётами рисков информационной безопасности в условиях сетевого противоборства; - разработкой методики анализа рисков информационной безопасности в мультисетевом пространстве.
ПК-11	Знать: -основные составляющие политики безопасности; - принципы разработки политики безопасности.
	Уметь: - разрабатывать политику безопасности; - применять комплексный подход к обеспечению информационной безопасности в условиях информационного противоборства.
	Владеть: -навыками разработки политики безопасности; -способностью применения комплексного подхода к обеспечению информационной безопасности в условиях информационного противоборства.
ПК-17	Знать: - методику анализа информационной безопасности; - современные стандарты в области информационной безопасности.
	Уметь: -разрабатывать методику анализа информационной безопасности; - использовать стандарты в области информационной безопасности.
	Владеть: -умением использования стандартов в области информационной безопасности.
ПК-22	Знать: -основные составляющие политики безопасности; - принципы разработки политики безопасности.
	Уметь: - разрабатывать политику безопасности.

	- применять комплексный подход к обеспечению информационной безопасности.
	Владеть: - навыками разработки политики безопасности; - способностью применения комплексного подхода к обеспечению информационной безопасности.
ПСК-7.2	знать методики оценки рисков ИБ, включая такие этапы как: идентификация активов, определение риска несоответствия требований законодательства в области ИБ, разработка модели угроз, количественная оценка рисков ИБ, определение допустимого уровня риска
	уметьумеет оценивать информационные риски в автоматизированных системах и разрабатывать политики безопасности компьютерных систем, в том числе политики управления доступом и информационными потоками в распределенных информационных системах
	владеть навыками анализа рисков информационной безопасности, правилами построения оптимальной политики безопасности в соответствии с требованиями уровня безопасности, стоимости и сроков реализации разработки

4. ОБЪЕМ ДИСЦИПЛИНЫ

Общаятрудоемкостьдисциплины«Информационноепротивоборствовмультисетевомпространстве»составляет2з.е.

Распределениетрудоемкостидисциплиныповидамзанятий

очнаяформаобучения

Видыучебнойработы	Всегочасов	Семестры
		9
Аудиторныезанятия (всего)	54	54
В томчисле:		
Лекции	36	36
Практическиезанятия (ПЗ)	18	18
Самостоятельнаяработа	18	18
Видыпромежуточнойаттестации - зачет	+	+
Общая трудоемкость: академические часы зач.ед.	 72 2	 72 2

5.СОДЕРЖАНИЕДИСЦИПЛИНЫ(МОДУЛЯ)

5.1Содержаниеразделовдисциплиныираспределениетрудоемкости повидамзанятий

очнаяформаобучения

№ п/п	Наименование темы	Содержание раздела	Лекц	Прак зан.	СРС	Всего, час
1.	Основы анализа процессов информационного противоборства, протекающих в телекоммуникационных сетях	Определения. Объекты и субъекты информационного противоборства. Средства информационного противоборства. Формализация описания сетевого конфликта и информационного противоборства в телекоммуникационных сетях. Разновидности сетевых конфликтов. Динамика развития сетевого конфликта.Риск-модель сетевой конфликтологии и информационного противоборства, протекающих в телекоммуникационных сетях. Основы топологического моделирования сетей. Метрики топологии сетей. Структурно-функциональное многообразие сетей.	6	2	2	10
2.	Модели влияния в социальных сетях	Влияние и индексы влиятельности. Влияние. Классификация моделей.Влиятельность агентов в сети. Ценность агента.Каскадные и другие модели влияния.Индексы влияния Общее знание. Коллективные действия Роль информированности.Общественные блага и индивидуальная специализация. Коммуникация и координация.Социальный кон-	6	2	2	10

		троль и коллективное действие. Стабильность сети				
3.	Модели информационного управления и информационного противоборства в социальных сетях	Марковская модель информационного влияния. Информационное управление и мнения членов сети Унифицированное информационное управление в однородных сетях. Роль СМИ. Информационное управление и репутация членов сети Информационное управление и доверие членов сети Информационное противоборство: распределенный контроль и согласование интересов. Информационная эпидемия и защита от нее	6	2	2	10
4	Стратегия устранения и взвешенные беспроводные информационные сети	Живучесть атакуемых сетевых структур при блокировании их элементов Оценка ущерба.Оценка пользы.Временная зависимость динамического ресурса вершины сети при атаке без восстановления.Временная зависимость динамического ресурса вершины сети при атаке с восстановлением.	6	4	4	14
5	Структурно-функциональная специфика блокирования элементов атакуемой беспроводной сети	Беспроводные сети, их иерархическая система. Методы и актуальные атаки блокирования элементов сети, их классификация. Риск-анализ реализации данных методов и разработка соответствующих мер противодействия на примере сотового оператора	6	4	4	14
6	Риск-анализ блокирования элементов беспроводной сети	Составляющие рисков блокирования элементов для уровней иерархии сети. Оценка эффективности применяемых средств защиты в условиях реализации угроз	6	4	4	14

		блокирования элементов сети.				
			Итого	36	18	18	72

5.2 Перечень лабораторных работ

Непредусмотреноучебнымпланом

6.ПРИМЕРНАЯТЕМАТИКАКУРСОВЫХПРОЕКТОВ(РАБОТ) ИКОНТРОЛЬНЫХРАБОТ

Всоответствиисучебнымпланомосвоениедисциплинынепредусматриваетвыполнениекурсовогопроекта(работы)иликонтрольнойработы.

7.ОЦЕНОЧНЫЕМАТЕРИАЛЫДЛЯПРОВЕДЕНИЯПРОМЕЖУТОЧНОЙАТТЕСТАЦИИОБУЧАЮЩИХСЯПОДИСЦИПЛИНЕ

7.1.Описаниепоказателейикритериевоцениваниякомпетенцийнаразличныхэтапахихформирования,описаниешкалоценивания

7.1.1Этаптекущегоконтроля

Результатытекущегоконтролязнанийимежсессионнойаттестациионениваютсяпоследующейсистеме:

«аттестован»;«неаттестован».

Компетенция	Результатыобучения,характеризующие сформированностькомпетенции	Критерии оценивания	Аттестован	Неаттестован
ПК-5	знать -основные риски информационной безопасности в мультисетевом пространстве; - основные этапы анализа рисков информационной безопасности в мультисетевом пространстве.	знание основных рисков информационной безопасности в мультисетевом пространстве; знание основных этапов анализа рисков информационной безопасности в мультисетевом пространстве.	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	уметь - рассчитывать риски информационной безопасности в условиях сетевого противоборства; - разрабатывать методику анализа рисков информационной безопасности в мультисетевом пространстве.	умение рассчитывать риски информационной безопасности в условиях сетевого противоборства; умение разрабатывать методику анализа рисков информационной безопасности в мультисетевом пространстве	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	владеть -расчётами рисков информационной безопасности в условиях сетевого противоборства; - разработкой методики анализа рисков информационной	владение расчётами рисков информационной безопасности в условиях сетевого противоборства; владение разработкой методики анализа рисков информационной безопасности в мультисетевом пространстве.	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах

	безопасности в мультисетевом пространстве.			
ПК-11	знать - основные составляющие политики безопасности; - принципы разработки политики безопасности.	знаниеосновных составляющих политики безопасности; знание принципов разработки политики безопасности.	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	уметь - разрабатывать политику безопасности; - применять комплексный подход к обеспечению информационной безопасности в условиях информационного противоборства.	умение разрабатывать политику безопасности; умение применять комплексный подход к обеспечению информационной безопасности в условиях информационного противоборства	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	владеть - навыками разработки политики безопасности; - способностью применения комплексного подхода к обеспечению информационной безопасности в условиях информационного противоборства.	владение навыками разработки политики безопасности; владение способностью применения комплексного подхода к обеспечению информационной безопасности в условиях информационного противоборства.	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
ПК-17	знать - методику анализа информационной безопасности; - современные стандарты в области информационной безопасности.	знание методики анализа информационной безопасности; знание современных стандартов в области информационной безопасности.	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	уметь - разрабатывать методику анализа информационной безопасности; - использовать стандарты в области информационной безопасности.	умение разрабатывать методику анализа информационной безопасности; умение использовать стандарты в области информационной безопасности	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	владеть - разработкой анализа информационной безопасности; - умением использования стандартов в области информационной безопасности.	владение разработкой анализа информационной безопасности; умением использования стандартов в области информационной безопасности.	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
ПК-22	знать	знание основных состав-	Выполнение работ в	Невыполнение ра-

	- основные составляющие политики безопасности; -: принципы разработки политики безопасности.	ляющих политик безопасности и принципов разработки политики безопасности.	срок, предусмотренный в рабочих программах	бот в срок, предусмотренный в рабочих программах
	уметь - разрабатывать политику безопасности. -: применять комплексный подход к обеспечению информационной безопасности.	умение разрабатывать политику безопасности и применять комплексный подход к обеспечению информационной безопасности.	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	владеть - навыками разработки политики безопасности; - способностью применения комплексного подхода к обеспечению информационной безопасности.	владение навыками разработки политики безопасности, а также способностью применения комплексного подхода к обеспечению информационной безопасности.	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
ПСК-7.2	знать методики оценки рисков ИБ, включая такие этапы как: идентификация активов, определение риска несоответствия требований законодательства в области ИБ, разработка модели угроз, количественная оценка рисков ИБ, определение допустимого уровня риска	знание методики оценки рисков ИБ, включая такие этапы как: идентификация активов, определение риска несоответствия требований законодательства в области ИБ, разработка модели угроз, количественная оценка рисков ИБ, определение допустимого уровня риска	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	уметь оценивать информационные риски в автоматизированных системах и разрабатывать политики безопасности компьютерных систем, в том числе политики управления доступом и информационными потоками в распределенных информационных системах	умение оценивать информационные риски в автоматизированных системах и разрабатывать политики безопасности компьютерных систем, в том числе политики управления доступом и информационными потоками в распределенных информационных системах	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	владеть навыками анализа рисков информационной безопасности, правилами построения оптимальной политики безопасности в соответствии с требованиями уровня безопасности, стои-	владение навыками анализа рисков информационной безопасности, правилами построения оптимальной политики безопасности в соответствии с требованиями уровня безопасности, стоимости и сроков реализации разработки	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах

	мости и сроков реализации разработки			

7.1.2Этаппромежуточногоконтролязнаний

Результатыпромежуточногоконтролязнанийоцениваютсяв9семестредлячнойформыобученияподвухбалльнойсистеме:

«зачтено»/«незачтено»

Компетенция	Результатыобучения,характеризующие сформированностькомпетенции	Критерии оценивания	Зачтено	Незачтено
ПК-5	знать - основные риски информационной безопасности в мультисетевом пространстве; - основные этапы анализа рисков информационной безопасности в мультисетевом пространстве.	Тест	Выполнениетестана 70-100%	Выполнениеменее 70%
	уметь - рассчитывать риски информационной безопасности в условиях сетевого противоборства; - разрабатывать методику анализа рисков информационной безопасности в мультисетевом пространстве.	Решениестандартныхпрактическихзадач	Продемонстрирована верный ход решения в большинстве задач	Задачинерешены
	владеть -рассчетами рисков информационной безопасности в условиях сетевого противоборства; - разработкой методики анализа рисков информационной безопасности в мультисетевом пространстве.	Решение прикладных задач в конкретной предметной области	Продемонстрирована верный ход решения в большинстве задач	Задачинерешены
ПК-11	знать - основные составляющие политики безопасности; - принципы разработки политики безопасности.	Тест	Выполнениетестана 70-100%	Выполнениеменее 70%
	уметь - разрабатывать политику безопасности; - применять комплексный подход к обеспечению информационной безопасности в ус-	Решениестандартныхпрактическихзадач	Продемонстрирована верный ход решения в большинстве задач	Задачинерешены

	ловиях информационного противоборства.			
	владеть - навыками разработки политики безопасности; - способностью применения комплексного подхода к обеспечению информационной безопасности в условиях информационного противоборства.	Решение прикладных задач в конкретной предметной области	Продемонстрирова н верный ход решения в большинстве задач	Задачинерешены
ПК-17	знать - методику анализа информационной безопасности; - современные стандарты в области информационной безопасности.	Тест	Выполнениетестана 70-100%	Выполнениеменее 70%
	уметь - разрабатывать методику анализа информационной безопасности; - использовать стандарты в области информационной безопасности.	Решениестандартныхпрактическихзадач	Продемонстрирова н верный ход решения в большинстве задач	Задачинерешены
	владеть - разработкой анализа информационной безопасности; - умением использования стандартов в области информационной безопасности.	Решение прикладных задач в конкретной предметной области	Продемонстрирова н верный ход решения в большинстве задач	Задачинерешены
ПК-22	знать - основные составляющие политики безопасности; - принципы разработки политики безопасности.	Тест	Выполнениетестана 70-100%	Выполнениеменее 70%
	уметь - разрабатывать политику безопасности. - применять комплексный подход к обеспечению информационной безопасности.	Решениестандартныхпрактическихзадач	Продемонстрирова н верный ход решения в большинстве задач	Задачинерешены
	владеть - навыками разработки политики безопасности; - способностью	Решение прикладных задач в конкретной предметной области	Продемонстрирова н верный ход решения в большинстве задач	Задачинерешены

	применения комплексного подхода к обеспечению информационной безопасности.			
ПСК-7.2	знать методики оценки рисков ИБ, включая такие этапы как: идентификация активов, определение риска несоответствия требований законодательства в области ИБ, разработка модели угроз, количественная оценка рисков ИБ, определение допустимого уровня риска	Тест	Выполнениетестана70-100%	Выполнениеменее70%
	уметь умеет оценивать информационные риски в автоматизированных системах и разрабатывать политики безопасности компьютерных систем, в том числе политики управления доступом и информационными потоками в распределенных информационных системах	Решениестандартныхпрактическихзадач	Продемонстрирова н верный ход решения в большинстве задач	Задачинерешены
	владеть навыками анализа рисков информационной безопасности, правилами построения оптимальной политики безопасности в соответствии с требованиями уровня безопасности, стоимости и сроков реализации разработки	Решение прикладных задач в конкретной предметной области	Продемонстрирова н верный ход решения в большинстве задач	Задачинерешены

7.2Примерныйпереченьоценочныхсредств(типовыеконтрольныезаданияилииныематериалы,необходимыедляоценкизнаний,умений,навыкови(или)опытадеятельности)

7.2.1Примерныйпереченьзаданийдляподготовкиктестированию

1) Виды информационной безопасности:

+ Персональная, корпоративная, государственная

- Клиентская, серверная, сетевая

- Локальная, глобальная, смешанная

2) Основными рисками информационной безопасности являются:

- Искажение, уменьшение объема, перекодировка информации
- Техническое вмешательство, выведение из строя оборудования сети
+ Потеря, искажение, утечка информации

3) Цели информационной безопасности – своевременное обнаружение, предупреждение:

+ несанкционированного доступа, воздействия в сети
- инсайдерства в организации
- чрезвычайных ситуаций

4) К основным принципам обеспечения информационной безопасности относится:

+ Экономической эффективности системы безопасности
- Многоплатформенной реализации системы
- Усиления защищенности всех звеньев системы

5) К основным функциям системы безопасности можно отнести все перечисленное:

+ Установление регламента, аудит системы, выявление рисков
- Установка новых офисных приложений, смена хостинг-компании
- Внедрение аутентификации, проверки контактных данных пользователей

6) Принципом политики информационной безопасности является принцип:

+ Невозможности миновать защитные средства сети (системы)
- Усиления основного звена сети, системы
- Полного блокирования доступа при риск-ситуациях

7) Политика безопасности строится на основе:

-общих представлений об ИС организации;
- изучения политик родственных организаций;
+ анализа рисков**.**

8) Управление рисками включает в себя следующие виды деятельности:

- определение ответственных за анализ рисков;
+ оценка рисков;
+ выбор эффективных защитных средств.

9) К современным стандартам в области информационной безопасности относятся:

+ГОСТ Р ИСО/МЭК 17799:2005 "Информационная технология. Практические правила управления информационной безопасностью"

-2. ГОСТ Р ИСО/МЭК 17799:2016 "Информационная технология. Практические правила управления информационной безопасностью"

+ГОСТ Р ИСО/МЭК 27001-2006 "Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования"

10) Проранжируйте по времени основные этапы, проводимые при

анализе риска безопасности ИС

Определение уязвимых мест ИС.
Оценка ожидаемых размеров потерь.
Оценка выгоды от применения предполагаемых мер.
Описание компонентов ИС.
Оценка вероятностей проявления угроз безопасности ИС.
Обзор возможных методов защиты и оценка их стоимости.

Описание компонентов ИС.
Оценка вероятностей проявления угроз безопасности ИС.
Обзор возможных методов защиты и оценка их стоимости. Определение уязвимых мест ИС.
Оценка ожидаемых размеров потерь.
Оценка выгоды от применения предполагаемых мер.

Описание компонентов ИС.
Определение уязвимых мест ИС.
Оценка вероятностей проявления угроз безопасности ИС.
Оценка ожидаемых размеров потерь.
Обзор возможных методов защиты и оценка их стоимости.
Оценка выгоды от применения предполагаемых мер.

Описание компонентов ИС.
Определение уязвимых мест ИС. 47336 32
Оценка вероятностей проявления угроз безопасности ИС.
Обзор возможных методов защиты и оценка их стоимости.
Оценка ожидаемых размеров потерь.
Оценка выгоды от применения предполагаемых мер

7.2.2Примерныйпереченьзаданийдлярешениястандартныхзадач

1.Вопрос:Кто является основным ответственным за определение уровня классификации информации?
Варианты ответа:

1. Руководитель среднего звена
2. Высшее руководство
3. **Владелец**
4. Пользователь

2.Вопрос:Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности?
Варианты ответа:

1. **Сотрудники**
2. Хакеры
3. Атакующие
4. Контрагенты (лица, работающие по договору)

3.Вопрос:Если различным группам пользователей с различным уровнем доступа требуется доступ к одной и той же информации, какое из указанных ниже действий следует предпринять руководству?
Варианты ответа:

1. Снизить уровень безопасности этой информации для обеспечения ее доступности и удобства использования
2. Требовать подписания специального разрешения каждый раз, когда человеку требуется доступ к этой информации
3. **Улучшить контроль за безопасностью этой информации**
4. Снизить уровень классификации этой информации

4.Вопрос:Что самое главное должно продумать руководство при классификации данных?
Варианты ответа:

1. Типы сотрудников, контрагентов и клиентов, которые будут иметь доступ к данным
2. **Необходимый уровень доступности, целостности и конфиденциальности**
3. Оценить уровень риска и отменить контрмеры
4. Управление доступом, которое должно защищать данные

5.Вопрос:Кто в конечном счете несет ответственность за гарантии того, что данные классифицированы и защищены?
Варианты ответа:

1. Владельцы данных
2. Пользователи
3. Администраторы
4. **Руководство**

6.Вопрос:Что такое процедура?
Варианты ответа:

1. Правила использования программного и аппаратного обеспечения в компании
2. **Пошаговая инструкция по выполнению задачи**
3. Руководство по действиям в ситуациях, связанных с безопасностью, но не описанных в стандартах
4. Обязательные действия

7. Вопрос:Какой фактор наиболее важен для того, чтобы быть уверенным в успешном обеспечении безопасности в компании?
Варианты ответа:

1. **Поддержка высшего руководства**
2. Эффективные защитные меры и методы их внедрения
3. Актуальные и адекватные политики и процедуры безопасности
4. Проведение тренингов по безопасности для всех сотрудников

8. Вопрос:Когда целесообразно не предпринимать никаких действий в отношении выявленных рисков?
Варианты ответа:

1. Никогда. Для обеспечения хорошей безопасности нужно учитывать и

снижать все риски
2. Когда риски не могут быть приняты во внимание по политическим соображениям
3. Когда необходимые защитные меры слишком сложны
4. **Когда стоимость контрмер превышает ценность актива и потенциальные потери**

9. Вопрос:Что такое политики безопасности?
Варианты ответа:
1. Пошаговые инструкции по выполнению задач безопасности
2. Общие руководящие требования по достижению определенного уровня безопасности
3. **Широкие, высокоуровневые заявления руководства**
4. Детализированные документы по обработке инцидентов безопасности

10.Вопрос:Какая из приведенных техник является самой важной при выборе конкретных защитных мер?
Варианты ответа:
1. Анализ рисков
2. **Анализ затрат / выгоды**
3. Результаты ALE
4. Выявление уязвимостей и угроз, являющихся причиной риска

11.Вопрос:Что лучше всего описывает цель расчета ALE?
Варианты ответа:
1. Количественно оценить уровень безопасности среды
2. Оценить возможные потери для каждой контрмеры
3. Количественно оценить затраты / выгоды
4. **Оценить потенциальные потери от угрозы в год**

12. Вопрос:Тактическое планирование – это:
Варианты ответа:
1. **Среднесрочное планирование**
2. Долгосрочное планирование
3. Ежедневное планирование
4. Планирование на 6 месяцев

13. Вопрос:Что является определением воздействия (exposure) на безопасность?
Варианты ответа:
1. **Нечто, приводящее к ущербу от угрозы**
2. Любая потенциальная опасность для информации или систем
3. Любой недостаток или отсутствие информационной безопасности
4. Потенциальные потери от угрозы

14. Вопрос:Эффективная программа безопасности требует сбалансированного применения:
Варианты ответа:
1. **Технических и нетехнических методов**
2. Контрмер и защитных механизмов
3. Физической безопасности и технических средств защиты

4. Процедур безопасности и шифрования

15. Вопрос:Функциональность безопасности определяет ожидаемую работу механизмов безопасности, а гарантии определяют:

Варианты ответа:

1. Внедрение управления механизмами безопасности
2. Классификацию данных после внедрения механизмов безопасности
3. **Уровень доверия, обеспечиваемый механизмом безопасности**
4. Соотношение затрат / выгод

16. Вопрос:Какое утверждение является правильным, если взглянуть на разницу в целях безопасности для коммерческой и военной организации?

Варианты ответа:

1. Только военные имеют настоящую безопасность
2. **Коммерческая компания обычно больше заботится о целостности и доступности данных, а военные – о конфиденциальности**
3. Военным требуется больший уровень безопасности, т.к. их риски существенно выше
4. Коммерческая компания обычно больше заботится о доступности и конфиденциальности данных, а военные – о целостности

17. Вопрос:Как рассчитать остаточный риск?

Варианты ответа:

1. Угрозы х Риски х Ценность актива
2. (Угрозы х Ценность актива х Уязвимости) х Риски
3. SLE х Частоту = ALE
4. **(Угрозы х Уязвимости х Ценность актива) х Недостаток контроля**

18. Вопрос:Что из перечисленного не является целью проведения анализа рисков?

Варианты ответа:

1. **Делегирование полномочий**
2. Количественная оценка воздействия потенциальных угроз
3. Выявление рисков
4. Определение баланса между воздействием риска и стоимостью необходимых контрмер

19. Вопрос:Что из перечисленного не является задачей руководства в процессе внедрения и сопровождения безопасности?

Варианты ответа:

1. Поддержка
2. **Выполнение анализа рисков**
3. Определение цели и границ
4. Делегирование полномочий

20. Вопрос:Почему при проведении анализа информационных рисков следует привлекать к этому специалистов из различных подразделений компании?

Варианты ответа:

1. Чтобы убедиться, что проводится справедливая оценка
2. Это не требуется. Для анализа рисков следует привлекать небольшую

группу специалистов, не являющихся сотрудниками компании, что позволит обеспечить беспристрастный и качественный анализ

3. Поскольку люди в различных подразделениях лучше понимают риски в своих подразделениях и смогут предоставить максимально полную и достоверную информацию для анализа

4. Поскольку люди в различных подразделениях сами являются одной из причин рисков, они должны быть ответственны за их оценку

7.2.3Примерныйпереченьзаданийдлярешенияприкладныхзадач

1.Степень центрированности это –

- степень вершины, т.е. число ребер, соединенных с ней;

- метрика позволяет оценить, полезен ли контент в сообществе, верно ли выбрана коммуникативная стратегия, правильно ли настроен таргетинг в рекламе**;**

-метрика показывает примерную долю тех, кто видел публикации сообщества и, так или иначе, отреагировал на них.

2. МетрикаPageRankэто–

- алгоритм применяется к коллекции документов, связанных гиперссылками и назначает каждому из них некоторое численное значение, измеряющее его «важность» или «авторитетность» среди остальных документов;

- метрика позволяет оценить, полезен ли контент в сообществе, верно ли выбрана коммуникативная стратегия, правильно ли настроен таргетинг в рекламе**;**

-метрика показывает примерную долю тех, кто видел публикации сообщества и, так или иначе, отреагировал на них.

3. Центрированность близости это –

–**среднее расстояние от вершины до других вершин;**

–степень вершины, которая лежит на пути между другими вершинами**;**

– степень вершины, т.е. число ребер, соединенных с ней;

4. Средним диаметром (расстоянием) взвешенной сети называется величина:

$$\langle \boldsymbol{D}(\boldsymbol{Net}) \rangle = \frac{\sum_{\boldsymbol{i,j=X,i\neq j}} \boldsymbol{p}(\boldsymbol{x_i}, \boldsymbol{x_j})}{\mathbf{max}|\boldsymbol{A}|}$$

$$D_{wc}(Net) = \frac{\sum_{i=1}^{|X|} [\max_x D_{wc}(x_i) - D_{wc}(x_i)]}{\max_x \sum_{i=1}^{|X|} [\max_x D_{wc}(x_i) - D_{wc}(x_i)]}$$

$$\overline{D}_{wc}(Net) = \frac{\sum_{i=1}^{|X|} \left[\max_x D_{wc}(x_i) - D_{wc}(x_i)\right]}{\sum_{i,j \in X, i \neq j} R_{es}(a_{ij})}$$

5.Стратегия устранения пользователей сети (как объекта атаки) нацелена на:

– исключение и/или переподчинение вершин (пользователей) сети

противника;

–снижение ценности наполнителя, циркулирующего в сети противника**;**

–сокращение объекта наполнителя, циркулирующего в сети противника.

6. К оптимизационным и имитационным моделям влияния в социальных сетях относятся:

- модели с порогами;

- модели независимых каскадов;

- модели взаимной информированности

- модели стабильности сети

- модели информационного влияния и управления

7. Противодействие развитию сети противника означает (направлен)–

- направлен на оказание влияния одной сети на другую с целью ограничения мощностей её множеств вершин и дуг;

- направлен на уменьшение динамического ресурса сети противника за счёт атаки на мостовые (с наиболее высокой пропускной способностью) транспортеры, приводящей к сокращению их пропускной способности**;**

- противодействие развитию может быть реализована за счет препятствий росту структуры сети противника путем понижения положительной (или сделать ее отрицательной) производной мощностей множеств концентраторов и транспортеров сети

8. Нижний уровень гетерогенной беспроводной сетив общем случае представляет:

– **это совокупность пользовательских устройств (планшеты, смартфоны, сотовые телефоны и т.п.), обеспечивающих генерацию всех видов трафика;**

–совокупность базовых станций, имеющих возможность организации беспроводных каналов связи с устройствами нижнего и верхнего уровней, предназначенных для промежуточного накопления и обработки трафика пользователей**;**

- контроллеры базовых станций, предназначенные для координации группы базовых станций в определенном регионе**;**

9. OCTAVE, NIST 800-30 и AS/NZS 4360 являются различными подходами к реализации управления рисками в компаниях. В чем заключаются различия между этими методами?

–NIST и OCTAVE являются корпоративными

–**NIST и OCTAVE ориентирован на ИТ**

–AS/NZS ориентирован на ИТ

–NIST и AS/NZS являются корпоративными

10. Какой из следующих методов анализа рисков пытается определить, где вероятнее всего произойдет сбой?

–Анализ связующего дерева

–AS/NZS

–NIST

–**Анализ сбоев и дефектов**

7.2.4Примерныйпереченьвопросовдляподготовкикзачету

Основы анализа процессов информационного противоборства, протекающих в телекоммуникационных сетях

Определения. Объекты и субъекты информационного противоборства. Средства информационного противоборства. Формализация описания сетевого конфликта и информационного противоборства в телекоммуникационных сетях. Разновидности сетевых конфликтов. Динамика развития сетевого конфликта. Риск-модель сетевой конфликтологии и информационного противоборства, протекающих в телекоммуникационных сетях.

Основы топологического моделирования сетей.Метрики топологии сетей.Структурно-функциональное многообразие сетей.

Модели влияния в социальных сетях Влияние и индексы влиятельности. Влияние. Классификация моделей. Влиятельность агентов в сети. Ценность агента. Каскадные и другие модели влияния. Индексы влияния

Общее знание. Коллективные действия

Роль информированности. Общественные блага и индивидуальная специализация. Коммуникация и координация. Социальный контроль и коллективное действие. Стабильность сети

Модели информационного управления и информационного противоборства в социальных сетях Марковская модель информационного влияния.

Информационное управление и мнения членов сети.

Унифицированное информационное управление в однородных сетях. Роль СМИ.

Информационное управление и репутация членов сети

Информационное управление и доверие членов сети

Информационное противоборство: распределенный контроль и согласование интересов. Информационная эпидемия и защита от нее

Стратегия устранения и взвешенные беспроводные информационные сети Живучесть атакуемых сетевых структур при блокировании их элементов.

Оценка ущерба. Оценка пользы. Временная зависимость динамического ресурса вершины сети при атаке без восстановления. Временная зависимость динамического ресурса вершины сети при атаке с восстановлением.

Структурно-функциональная специфика блокирования элементов атакуемой беспроводной сети. Беспроводные сети, их иерархическая система.

Методы и актуальные атаки блокирования элементов сети, их классификация.Риск-анализ реализации данных методов и разработка соответствующих мер противодействия на примере сотового оператора

Риск-анализ блокирования элементов беспроводной сети. Составляющие рисков блокирования элементов для уровней иерархии сети.

Оценка эффективности применяемых средств защиты в условиях реализации угроз блокирования элементов сети.

7.2.5Примерныйпереченьзаданийдлярешенияприкладныхзадач

Непредусмотреноучебнымпланом

7.2.6.Методикавыставленияоценкиприпроведенииипромежуточной аттестации

(Напри-
мер:Экзаменпроводитсяпотест-билетам,каждыйизкоторыхсодержит10во
просовизада-
чу.Каждыйправильныйответнавопросвтестеоценивается1баллом,задачаоц
енивает-
сяв10баллов(5балловверноерешениеи5балловзаверныйответ).Максимальноек
оличествонабранныхбаллов–20.

1.Оценка«Неудовлетворительно»ставитсявслучае,еслистудентнабра
лменее6баллов.

2.Оценка«Удовлетворительно»ставитсявслучае,еслистудентнабрало
т6до10баллов

3.Оценка«Хорошо»ставитсявслучае,еслистудентнабралот11до15балл
ов.

4.Оценка«Отлично»ставится,еслистудентнабралот16до20баллов.)

7.2.7Паспортоценочныхматериалов

№п/п	Контролируемыеразделы(темы) дисциплины	Кодконтролируемойкомпетенции	Наименованиеоценочного средства
1	Основы анализа процессов информационного противоборства, протекающих в телекоммуникационных сетях	ПК-5, ПК-11, ПК-17, ПК-22, ПСК-7.2	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту….
2	Модели влияния в социальных сетях	ПК-5, ПК-11, ПК-17, ПК-22, ПСК-7.2	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту….
3	Модели информационного управления и информационного противоборства в социальных сетях	ПК-5, ПК-11, ПК-17, ПК-22, ПСК-7.2	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту….
4	Стратегия устранения и взвешенные беспроводные информационные сети	ПК-5, ПК-11, ПК-17, ПК-22, ПСК-7.2	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту….
5	Структурно-функциональная специфика блокирования элементов атакуемой беспроводной сети	ПК-5, ПК-11, ПК-17, ПК-22, ПСК-7.2	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту….

6	Риск-анализ блокирования элементов беспроводной сети	ПК-5, ПК-11, ПК-17, ПК-22, ПСК-7.2	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту….

7.3.Методическиематериалы,определяющиепроцедурыоценивания знаний,умений,навыкови(или)опытадеятельности

Тестированиеосуществляется,либоприпомощикомпьютернойсистемытестирования,либосиспользованием выданных-тест-заданийнабумажномносителе.Времятестирования30мин.Затемосуществляетсяпроверкатестаэкзаменаторомивыставляетсяоценкасогласнометодикивыставленияоценкиприпроведениипромежуточнойаттестации.

Решениестандартныхзадачосуществляется,либоприпомощикомпьютернойсистемытестирования,либосиспользованием выданныхзадачнабумажномносителе.Времярешениязадач30мин.Затемосуществляетсяпроверкарешениязадачэкзаменаторомивыставляетсяоценка,согласнометодикивыставленияоценкиприпроведениипромежуточнойаттестации.

Решениеприкладныхзадачосуществляется,либоприпомощикомпьютернойсистемытестирования,либосиспользованием выданныхзадачнабумажномносителе.Времярешениязадач30мин.Затемосуществляетсяпроверкарешениязадачэкзаменаторомивыставляетсяоценка,согласнометодикивыставленияоценкиприпроведениипромежуточнойаттестации.

8УЧЕБНОМЕТОДИЧЕСКОЕИИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕДИСЦИПЛИНЫ)

8.1Переченьучебнойлитературы,необходимойдляосвоениядисциплины

Основная литература:

1. Остапенко, А.Г. Обнаружение и нейтрализация вторжений в распределенных информационных системах [Электронный ресурс] : Учеб. пособие / А. Г. Остапенко, М. Н. Иванкин. - Электрон. текстовые, граф. дан. (366 Кб). - Воронеж : ФГБОУ ВПО "Воронежский государственный технический университет", 2013. - 1 файл. - 30-00.

2. Остапенко О.А. Риски систем: Оценка и управление [Электронный ресурс] : учеб. пособие / О. А. Остапенко, Д. О. Карпеев, В. Н. Асеев. - Электрон. дан. (1 файл :5250 Кбайта). - Воронеж : ГОУВПО "Воронежский государственный технический университет", 2006. - 1 файл. - 30-00.

3. Кушнир, А.Э. Рефлексивные игры в информационном пространстве социотехнических систем [Электронный ресурс] : Учеб. пособие / А. Э.

Кушнир, О. А. Остапенко, И. В. Сысоев. - Электрон. текстовые дан. (3 230 235 байт). - Воронеж : ГОУВПО "Воронежский государственный технический университет", 2008. - 1 файл. - 30-00.

Дополнительная литература:

1. Демьяненко, Н.Ю. Информационно-психологические воздействия в открытых информационно-телекоммутационных системах [Электронный ресурс] : Учеб. пособие / Н. Ю. Демьяненко. - Электрон. текстовые дан. (1 652 654 байт). - Воронеж : ГОУВПО "Воронежский государственный технический университет", 2008. - 1 файл. - 30-00.
2. Остапенко Г.А. Информационные операции [Электронный ресурс] : учеб. пособие / Г. А. Остапенко, Е. А. Мешкова. - Электрон. дан. (1 файл :3045 Кбайта). - Воронеж : ГОУВПО "Воронежский государственный технический университет", 2006. - 1 файл. - 30-00.
3. Остапенко, О.А. Опасность, ущербы и риски систем : Учеб. пособие / О. А. Остапенко, Р. В. Батищев. - Воронеж : НОУВПО "Междунар. ин-т компьют. технологий", 2007. - 194 с. - 45-00.

8.2Переченьинформационныхтехнологий,используемыхприосуществлениииобразовательногопроцессаподисциплине,включаяперечень лицензионногопрограммногообеспечения,ресурсовинформационно-телекоммуникационнойсети«Интернет»,современныхпрофессиональныхбазданныхиинформационныхсправочных систем:

http://att.nica.ru
http://www.edu.ru/
http://window.edu.ru/window/library
http://www.intuit.ru/catalog/
http://bibl.cchgeu.ru/MarcWeb2/ExtSearch.asp
https://cchgeu.ru/education/cafedras/kafsib/?docs
http://www.eios.vorstu.ru
http://e.lanbook.com/ (ЭБС Лань)
http://IPRbookshop.ru/ (ЭБСIPRbooks)

9МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯБАЗА,НЕОБХОДИМАЯДЛЯОСУЩЕСТВЛЕНИЯОБРАЗОВАТЕЛЬНОГОПРОЦЕССА

Специализированная лекционная аудитория, оснащенная оборудованием для лекционных демонстраций и проекционной аппаратурой.

10.МЕТОДИЧЕСКИЕУКАЗАНИЯДЛЯОБУЧАЮЩИХСЯПООСВОЕНИЮДИСЦИПЛИНЫ(МОДУЛЯ)

Подисциплине«Информационноепротивоборствовмультисетевомпространстве»читаютсялекции,проводятсяпрактическиезанятия.

Основойизучениядисциплиныявляютсялекции,накоторыхизлагаютсянаиболеесущественныеитрудныевопросы,атакжево

просы,ненашедшиеотраженияв учебной литературе.

Практическиезанятиянаправленынаприобретениеследующих практических навыков:

1. Определения ценности информационных активов в распределённом мультисетевом пространстве в денежном выражении.

2. Оценивания в количественном выражении потенциальный ущерб от реализации каждой угрозы в отношении каждого информационного актива.

3. Определения вероятность реализации каждой из угроз ИБ.

Для этого можно использовать статистические данные, опросы сотрудников и заинтересованных лиц. В процессе определения вероятности рассчитать частоту возникновения инцидентов, связанных с реализацией рассматриваемой угрозы ИБ за контрольный период (например, за один год).

4. Определения общего потенциального ущерба от каждой угрозы в отношении каждого актива за контрольный период (за один год).

Значение рассчитывается путем умножения разового ущерба от реализации угрозы на частоту реализации угрозы.

5. Проведения анализа полученных данных по ущербу для каждой угрозы.

По каждой угрозе необходимо принять решение: принять риск, снизить риск либо перенести риск.

Занятияпроводятсяпутемрешенияконкретныхзадачваудитории.

Видучебныхзанятий	Деятельностьстудента
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.
Самостоятельнаяработа	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 промежуточнойаттестации.

Подготовка к промежуточнойаттестации	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 зачетом три дня эффективнее всего использовать для повторения и систематизации материала.