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

«Управление информационной безопасностью»

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 _____ /Разинкин К.А./

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

Руководитель ОПОП _____ /А.Г. Остапенко/

Воронеж 2017

1.ЦЕЛИИЗАДАЧИДИСЦИПЛИНЫ

1.1.Целидисциплиныявляется изучение основных понятий, методологии и практических приемов управления технической и организационной инфраструктурой обеспечения информационной безопасности на предприятии.

1.2.Задачиосвоениядисциплиныприобретение обучаемыми необходимого объема знаний и практических навыков в области стандартизации и нормотворчества в управлении информационной безопасностью, оценки рисков информационных ресурсов предприятия и аудита информационной безопасности, организации работы и разграничения полномочий персонала, ответственного за информационную безопасность

формирование у обучаемых целостного представления об организации и содержании процессов управления информационной безопасностью на предприятии как результата внедрения системного подхода к решению задач обеспечения информационной безопасности (ИБ) автоматизированных систем

2.МЕСТОДИСЦИПЛИНЫВСТРУКТУРЕОПОП

Дисциплина«Управлениеинформационнойбезопасностью»относитсякдисциплинамбазовойчастиблокаБ1.

3.ПЕРЕЧЕНЬПЛАНИРУЕМЫХРЕЗУЛЬТАТОВОБУЧЕНИЯПОДИСЦИПЛИНЕ

Процессизучениядисциплины«Управлениеинформационнойбезопасностью»направленаформированиеследующихкомпетенций:

ПК-2-способностьюосоздаватьиисследоватьмоделиавтоматизированныхсистем

ПК-4-способностьюразрабатыватьмоделиугрозимоделинарушителяинформационнойбезопасностиавтоматизированнойсистемы

ПК-11-способностьюразрабатыватьполитикуинформационнойбезопасностиавтоматизированнойсистемы

ПК-19-способностьюразрабатыватьпредложенияпосовершенствованиюсистемыуправленияинформационнойбезопасностьюавтоматизированнойсистемы

ПК-28-способностьюуправлятьинформационнойбезопасностьюавтоматизированнойсистемы

Компетенция	**Результатыобучения,характеризующие сформированностькомпетенции**
ПК-2	знать основные методы управления информационной безопасностью
	уметь пользоваться моделями безопасности КС при управлении доступом и информационными потоками

	владетьнавыками анализа информационной инфраструктуры автоматизированной системы и ее безопасности
ПК-4	знать требования информационной безопасности при эксплуатации автоматизированной системы
	уметь оценивать информационные риски в автоматизированных системах и разрабатыватьмоделиугрозимоделинарушителяинформационнойбезопасностиавтоматизированнойсистемы;
ПК-11	знать принципы построения систем управления информационной безопасностью (СУИБ) и особенности отдельных процессов управления ИБ в рамках СУИБ
	умеет формировать политики информационной безопасности организации
ПК-19	знать основные документы по стандартизации в сфере управления ИБ
	уметьопределять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности автоматизированных систем;
	владетьметодами мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем
ПК-28	знать способыуправлятьинформационнойбезопасностьюавтоматизированнойсистемы
	уметь определять цели и задачи, решаемые разрабатываемыми процессами управления ИБ

4. ОБЪЕМ ДИСЦИПЛИНЫ

Общаятрудоемкостьдисциплины«Управлениеинформационнойбезопасностью»составляет4з.е.

Распределениетрудоемкостидисциплиныповидамзанятий

очнаяформаобучения

Видыучебнойработы	Всегочасов	Семестры
		9
Аудиторныезанятия (всего)	60	60
В томчисле:		
Лекции	40	40
Лабораторныеработы (ЛР)	20	20
Самостоятельнаяработа	84	84

Виды промежуточной аттестации - зачет с оценкой	+	+
Общая трудоемкость: академические часы зач.ед.	 144 4	 144 4

5.СОДЕРЖАНИЕДИСЦИПЛИНЫ(МОДУЛЯ)

5.1Содержаниеразделовдисциплиныираспределениетрудоемкостиповидамзанятий

очнаяформаобучения

№ п/п	Наименованиетемы	Содержаниераздела	Лекц	Лаб. зан.	СРС	Всего, час
1	Основные понятия и подходы к управлению информационной безопасностью	Базовая терминология. Системный и процессный подходы к управлению ИБ. Управление логическим доступом к активам организации. Управление защищенной передачей данных и организационной деятельностью. Управлениеконфигурациями, изменениями и обновлениями.	8	4	14	26
2	Стандартизация систем и процессов управления информационной безопасностью	Серия стандартов ISO/IEC 27000 «Информационные технологии. Методы обеспечения безопасности». Стандарты на отдельные процессы управления ИБ и оценку безопасности ИТ. Отраслевыестандарты в областиуправления ИБ.	8	4	14	26
3	Политикаинформационнойбезопасности	Понятие политики обеспечения ИБ и политики ИБ организации. Причины разработки политики. Основные требования и принципы, учитываемые при разработке и внедрения политики ИБ. Содержание политики ИБ. Жизненный цикл политики ИБ. Ответственность за исполнение политики.	6	4	14	24
4	Модели управления доступом и информационными потоками	Модели дискреционного управления доступом. Модели изолированной программной среды. Модели с мандатным управлением доступом. Модели безопасности информационных потоков. Модели с ролевым управлением доступом	6	4	14	24
5	Управление и система управ-	Необходимость управления обеспечением ИБ организации. Деятельность по обеспе-	6	2	14	22

	ления информационной безопасностью	чению ИБ организации как процесс. Определение управления ИБ организации. Управление ИБ информационно-телекоммуникационных технологий организации. Система управления ИБ организации. Область действия СУИБ. Документальное обеспечение СУИБ. Документальное обеспечение СУИБ. Процессный подход в рамках управления ИБ. Работа с процессами СУИБ организации. Стратегии построения и внедрения СУИБ.				
6	Организационные и кадровые вопросы управления информационной безопасностью	Модели организационного управления ИБ. Организационная инфраструктура ИБ. Служба ИБ организации. Компетентностныеуровнипрофессионалов в области ИБ	6	2	14	22
		Итого	**40**	**20**	**84**	**144**

5.2Переченьлабораторныхработ

1.Модель решётки

2.Дискреционное управлением доступом

(модели Харрисона-Руззо-Ульмана и типизированнаяматрицы доступов)

3.Управление распространением прав доступа на основе классической модели Take-Grant

4.Управление распространением прав доступа на основе расширенной модели Take-Grant

5.Модель Белла-ЛаПадулы. Мандатное управление доступом

6. Ролевое и мандатное ролевое управление доступом

7. Изучение средств управления безопасностью на уровне операционной системы на примере WindowsServer 2003.

8. Управления учетными записями пользователей

9. Изучение средств управления безопасностью на уровне операционной системы на примере WindowsServer 2003.

10. Настройка политик безопасности

6.ПРИМЕРНАЯТЕМАТИКАКУРСОВЫХПРОЕКТОВ(РАБОТ) ИКОНТРОЛЬНЫХРАБОТ

Всоответствиисучебнымпланомосвоениедисциплинынепредусматриваетвыполнениекурсовогопроекта(работы)иликонтрольнойработы.

7.ОЦЕНОЧНЫЕМАТЕРИАЛЫДЛЯПРОВЕДЕНИЯПРОМЕЖУТОЧНО

ЙАТТЕСТАЦИИОБУЧАЮЩИХСЯПОДИСЦИПЛИНЕ

7.1.Описаниепоказателейикритериевоцениванияикомпетенцийнаразличныхэтапахихформирования,описаниешкалоценивания

7.1.1Этаптекущегоконтроля

Результатытекущегоконтролязнанийимежсессионнойаттестацииоцениваютсяпоследующейсистеме:

«аттестован»;

«неаттестован».

Компетенция	Результатыобучения,характеризующие сформированностькомпетенции	Критерии оценивания	Аттестован	Неаттестован
ПК-2	знать основные методы управления информационной безопасностью	знаниеосновных методов управления информационной безопасностью	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	уметь пользоваться моделями безопасности КС при управлении доступом и информационными потоками	умение пользоваться частными политиками безопасности, в том числе, основанными на формальных моделях дискреционного, мандатного и ролевого управления доступом, моделях ИПС и ИП	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	владеть навыками анализа информационной инфраструктуры автоматизированной системы и ее безопасности	владениенавыкамиадминистрирования информационной инфраструктуры автоматизированной системы и ее безопасности	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
ПК-4	знать требования информационной безопасности при эксплуатации автоматизированной системы	знание основных принципов организации технического, программного и информационного обеспечения эксплуатации защищённых автоматизированной системы	Выполнение работ в срок, предусмотренный в рабочих про-	Невыполнение работ в срок, предусмотренный в рабочих программах

			граммах	
	уметь оценивать информационные риски в автоматизированных системах и разрабатыватьмоделиугрозимоделинарушителяинформационной безопасностиавтоматизированнойсистемы;	умениеоценивать информационные риски в автоматизированных системах и разрабатыватьмоделиугрозимоделинарушителяинформационнойбезопасностиавтоматизированнойсистемы	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
ПК-11	знать принципы построения систем управления информационной безопасностью (СУИБ) и особенности отдельных процессов управления ИБ в рамках СУИБ	знает принципы построения систем управления информационной безопасностью (СУИБ) и особенности отдельных процессов управления ИБ в рамках СУИБ	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	умеет формировать политики информационной безопасности организации	умение разрабатывать технические задания на создание подсистем обеспечения информационной безопасности	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
ПК-19	знать основные документы по стандартизации в сфере управления ИБ	знание основных инструкций, регламентов, положений и приказов, регламентирующих работу по обеспечению информационной безопасности автоматизированныхсисте	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	уметь определять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности автоматизированных систем;	умение проводить выбор, исследовать эффективность, проводить технико-экономическое обоснование проектных решений в области построения систем обеспечения информационной безопасности	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	владеть методами мониторинга и	владеет навыками обработки,	Выпол-	Невыпол-

	аудита, выявления угроз информационной безопасности автоматизированных систем	оценки и представления результатов исследования эффективности решений по управлению информационной безопасностью	нение работ в срок, предусмотренный в рабочих программах	нение работ в срок, предусмотренный в рабочих программах
ПК-28	знать способыуправлятьинформационнойбезопасностьюавтоматизированнойсистемы	знает способовуправлятьинформационнойбезопасностьюавтоматизированнойсистемы	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	уметь определять цели и задачи, решаемые разрабатываемыми процессами управления ИБ	умеетопределять цели и задачи, решаемые разрабатываемыми процессами управления ИБ	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах

7.1.2Этаппромежуточногоконтролязнаний

Результатыпромежуточногоконтролязнанийоцениваютсяв9семестредля очнойформыобученияпочетырехбалльнойсистеме:

«отлично»;

«хорошо»;

«удовлетворительно»;

«неудовлетворительно».

Компетенция	**Результатыобучения,характеризующие сформированностькомпетенции**	**Критерии оценивания**	**Зачтено**	**Незачтено**
ПК-2	знать основные методы управления информационной безопасностью	Тест	Выполнение тестана 70-100%	Выполнениеменее 70%
	уметь пользоваться моделями безопасности КС при управлении доступом и информационными потоками	Решениестандартныхпрактическихзадач	Продемонстрирова н верный ход решения в большинстве задач	Задачине решены

	владеть навыками анализа информационной инфраструктуры автоматизированной системы и ее безопасности	Решение прикладных задач в конкретной предметной области	Продемонстрирова н верный ход решения в большинстве задач	Задачине решены
ПК-4	знать требования информационной безопасности при эксплуатации автоматизированной системы	Тест	Выполнение тестана 70-100%	Выполнениеменее 70%
	уметь оценивать информационные риски в автоматизированных системах и разрабатыватьмоделиугрозимоделинарушителяинформационнойбезопасностиавтоматизированнойсистемы;	Решениестандартныхпрактическихзадач	Продемонстрирова н верный ход решения в большинстве задач	Задачине решены
ПК-11	знать принципы построения систем управления информационной безопасностью (СУИБ) и особенности отдельных процессов управления ИБ в рамках СУИБ	Тест	Выполнение тестана 70-100%	Выполнениеменее 70%
	умеет формировать политики информационной безопасности организации	Решениестандартныхпрактическихзадач	Продемонстрирова н верный ход решения в большинстве задач	Задачине решены
ПК-19	знать основные документы по стандартизации в сфере управления ИБ	Тест	Выполнение тестана 70-100%	Выполнениеменее 70%
	уметь определять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности автоматизированных систем;	Решениестандартныхпрактическихзадач	Продемонстрирова н верный ход решения в большинстве задач	Задачине решены
	владеть методами мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем	Решение прикладных задач в конкретной предметной области	Продемонстрирова н верный ход решения в большинстве задач	Задачине решены
ПК-28	знать способыуправлятьинформационнойбезопасностьюавтоматизированнойсистемы	Тест	Выполнение тестана 70-100%	Выполнениеменее 70%
	уметь определять цели и задачи, решаемые разрабатываемыми процессами управления ИБ	Решениестандартныхпрактическихзадач	Продемонстрирова н верный ход решения в большинстве задач	Задачине решены

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

7.2.1Примерныйпереченьзаданийдляподготовкиктестированию

1.К моделям КС с дискреционным управлением доступом относятся:

- **модель матрицы доступов Харрисона-Рузо-Ульмана**
- модель Белла-ЛаПадулы
- автоматная модель безопасности информационных потоков
- вероятностная модель контроля информационных потоков

2.Математические понятия, относящиеся к моделям безопасности: (несколько вариантов ответов)

- **граф;**
- **автомат;**
- **решётка;**
- дифференциальное уравнения
- уравнение в конечных разностях.

3. Дайте правильное определение основной аксиомы компьютерной безопасности:

-в рамках субъект сущностного подхода все вопросы безопасности информации в КС описываются доступами субъектов к сущностям;

- информационным потоком от сущности к источнику к сущности-приемнику называется преобразование данных в сущности-приемнике;
- все действия в КС, в том числе выполнение операций над сущностями, могут быть инициированы только субъектами КС с использованием доступов к сущностям КС.

4. Правилами (де-юре) классической модели Take-Grantявляются:(несколько вариантов ответов)

- **take**
- **grant**
- **crteate**
- **remove**
- delete
- post
- pass
- spy

5. Стоимость правила в модели Take-Grant может:

- **являться константой**
- не зависеть от специфики правила
- зависеть от степени требуемого взаимодействия и не зависеть от числа и состава участников при применении правила.

6. Процессный подход это:

- **систематическая идентификация и менеджмент применяемых организацией бизнес-процессов и особенно взаимодействия таких про-**

цессов;

- менеджмент применяемых организацией бизнес-процессов и особенно взаимодействия таких процессов;

- внесистемная организация бизнес-процессов, в части идентификации и особенно взаимодействия таких процессов

7. Определение инцидента (выберите правильное, согласно стандартаISO/IEC 27000:201):

- событие или серия нежелательных или непредвиденных событий ИБ, которые могут с большой долей вероятности привести к компрометации бизнес-операций или созданию угрозы ИБ;

- последовательность событий;

- единичное событие;

- событие, обусловленное действиями субъекта-нарушителя;

- событие, приводящее к компрометации бизнес-операций или созданию угрозы ИБ

8. Основные признаки инцидента (выбирайте несколько вариантов ответов):

− вероятностный характер события;

− неблагоприятные последствия;

−изменение профилей защиты СЗИ**;**

−маппинг физических смещений на виртуальные адреса**;**

− изменение имён открытых файлов для каждого процесса.

9. Целью какого процесса является определение и контроль компонентов услуг и конфигурационных единиц, а также предоставление достоверной информации о состоянии услуг и инфраструктур?

планирование и поддержка внедрения

управление изменениями

управление активами и конфигурациями

управление релизами и развертыванием

10. В рамках какого элемента Управления информационной безопасностью происходит выбор метрик информационной безопасности?

планирование

реализация

оценка

контроль

поддержка

11. Как называется процесс, отвечающий за допуск пользователей к использованию услуг, данных или других активов?

управление конфигурациями

управление доступом

управление информационной безопасностью

управление инцидентами

12. Какую аббревиатуру носит система политик, процессов, стандартов, руководящих документов и средств, которые обеспечивают организации достижение целей управления информационной безопасностью?

SKWIT

ISMS

SMIS

CMS

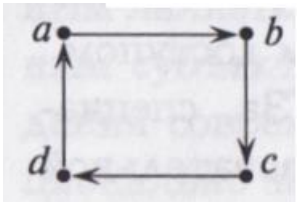
7.2.2Примерныйпереченьзаданийдлярешениястандартныхзадач

(минимум10вопросовдлятестированиясвариантамиответов)

(тема «Модели управления доступом и информационными потоками»)

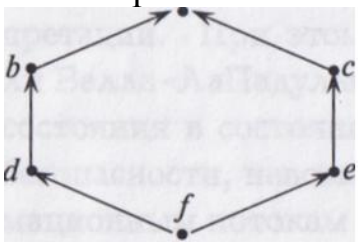
Практическое задание № 1.

Модель решётки. Задает ли решетку граф на рис.?



Так как выполняются условия $a \le b, b \le c$ и $a \ne b$, то не выполняется свойство антисимметричности отношения частичного порядка «≤» на множестве {a, b, c,d}. Следовательно, по определению граф не задает решетку.

Практическое задание № 2.

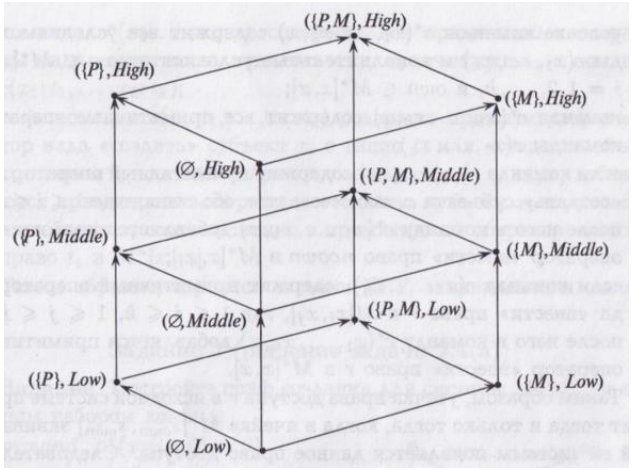


Задает ли решетку граф?

Решение. В соответствии с определением выполнены все свойства отношения частичного порядка «≤» на множестве {a, b, c, d, e, f}. Для каждой пары вершин, соединенных в графе путем, существует наименьшая верхняя и наибольшая нижняя границы. Например, справедливы равенства $f \oplus b = b$к $f \otimes b = f$.Для каждой пары, не соединенных в графе путем, приведем значения наименьших верхних и наибольших нижних границ: $d \oplus$e = a, $d \otimes$e = f; $b \oplus$e=a, $b \otimes e$=f; $d \oplus c$ = a, $d \otimes c$=f;b$\oplus$c = a, b$\otimes c$=f.Следовательно, по определению граф задает решетку.

Практическое задание №3

Нарисуйте граф, соответствующий решетке многоуровневой безопасности (X x L, ≤), для решетки (L, ≤) = $\{Low, Middle, High\}$и (X, ≤) — решетки подмножеств множества $U=\{Political, Military\}$.



Решение. Построим граф, задающий решетку (X x L, ≤). При этом используем сокращения: P (*Political*), *M (Military)*.

Практическое задание №4

Докажите, что для общего случая систем ХРУ не существует алгоритма проверки возможности утечки права доступа г для заданной пары субъект sи объект o.

Решение. Пусть задана система ХРУ, в которой определены множества *R, Q, C.* Построим эквивалентную ей систему ХРУ, определив множества *R*, Q*, C*.*

Пусть в каждом состоянии $q^*= (S^*,0^*, M^*)$, соответствующем состоянию $q= (S,0,M)$,справедливы равенства:

$$S^* = S \cup \{s_{owm}\};$$
$$O^* = O \cup \{s_{oum}\};$$
$$R^* = R \cup \{own, noown\}.$$

Кроме того, для $s \in S$, $o \in O$ справедливы равенства

$$M^*[s,o] = M[s,o], M^*[s_{own}, o] = \{noown\}, M^*[Sown, Sown] = \{own\}.$$

Каждую команду $c(x_1,\dots ,x_k) \in C$ исходной системы ХРУ заменим командой $c(x_1,\dots ,x_k,x)$, которая удовлетворяет следующим условиям:

условие команды $c^*(x_1,\dots ,x_k,x)$содержит все условия команды $c(x_1,\dots ,x_k)$и дополнительные условия: $noown \in M^*[x, x_i]$, $i=1,2,\dots k$, $uown \in M^*[x,x]$; команда $c^*(x_1,\dots,x_k,x)$содержит все примитивные операторы команды $c(x_1,\dots ,x_k)$

если команда $c(x_1,\dots ,x_k)$содержит примитивный оператор вида «создать» субъекта x_i или «создать» объект x_i, где $1 \le i \le \kappa$, то после него в команду $c^*(x_1,\dots ,x_k,x)$ добавляется примитивный оператор «внести» право $noown$в $M^*[x,x_i]$;

если команда $c(x_1,\dots ,x_k)$содержит примитивный оператор вида «внести» право r в $M[x_i,X_j]$, где $1 \le i \le \kappa$, $1 \le j \le \kappa$ то после него в команду $c^*(x_1,\dots ,x_k,x)$добавляется примитивный оператор «внести» право r в $M^*[x,x]$.

Таким образом, утечка права доступа r в исходной системе происходит тогда и только тогда, когда в ячейке $M^*[s_{own},s_{oum}]$ эквивалентной ей системы появляется данное право доступа. Следовательно, если бы существовал алгоритм проверки возможности утечки права доступаr для заданной пары субъект sи объект o (в данном случае для пары s_{own},S_{own}), то существовал бы алгоритм проверки безопасности произвольных систем ХРУ, что противоречит утверждению теоремы.

Практическое задание №5.Представьте произвольную систему ТМД системой ХРУ.

Решение. Пусть задана система ТМД, в которой определены множества *R, Q, T, C.* Построим эквивалентную ей систему ХРУ, определив множества *R*, Q*, C*.*

Пусть в каждом состоянии $q^*= (S^*,O^*,M^*)$ системы ХРУ, соответствующем состоянию $q= (S,0,t, M)$, справедливы равенства:

$S^* = S \cup \{s_{otxw}\}$; $o^* = O \cup \{s_{own}\}$,$R^*= R \cup T \cup \{own\}$.

Кроме того, для $s \in S$, $o \in O$ справедливы равенства $M^*[s,o] = M[s,o]$, $M[s_{ou;n},o]=\{t(o)\}$,$M^*\{s_{own}, s_{own}\}=\{own\}$.

Для каждой команды $c(x_1:t_1,\dots,x_k:t_k) \in C$ системы ТМД в систему ХРУ добавим команду $\overline{c^*(x_1,\dots,x_k,x)}$, которая удовлетворяет следующим условиям:

условие команды $c^*(x_1,\dots ,x_k,x)$содержит все условия команды $c(x_1:t_1,\dots,x_k:t_k) \in C$ и дополнительные условия: $t_i \in M^*[x,x_i]$, $i = 1,2,\dots,k$, и $own \in M^*[x,x]$;

команда $c^*(x_1,\dots,x_k,x)$содержит все примитивные операторы вида «внести»..., «удалить»..., «уничтожить»... команды $c(x_1{:}t_1,\dots,x_k{:}t_k)\in C$
если команда $c(x_1{:}t_1,\dots,x_k{:}t_k)\in C$содержит примитивный оператор вида «создать» субъект x_i с типом t_iили «создать» объект Xiс типом t_iгде $1\le i\le\kappa$, то в команду $c^*(x_1,\dots,x_k,x)$добавляются примитивные операторы «создать» субъект Xiили «создать» объект Xiсоответственно и примитивный оператор «внести» право t_iв $M^*[x,x_i]$.Таким образом, строится система ХРУ, эквивалентная системе ТМД.

Практическое задание 6. Ответьте на вопросы теста (тема «Управление и система управления информационной безопасностью»)

1. Как рассчитать остаточный риск?

- A. Угрозы x Риски x Ценность актива
- B. (Угрозы x Ценность актива x Уязвимости) x Риски
- C. SLEx Частоту = ALE
- **D. (Угрозы x Уязвимости x Ценность актива) x Недостаток контроля**

2. Что из перечисленного не является целью проведения анализа рисков?

- **A. Делегирование полномочий**
- B. Количественная оценка воздействия потенциальных угроз
- C. Выявление рисков
- D. Определение баланса между воздействием риска и стоимостью необходимых контрмер

3. Что из перечисленного не является задачей руководства в процессе внедрения и сопровождения безопасности?

- A. Поддержка
- **B. Выполнение анализа рисков**
- C. Определение цели и границ
- D. Делегирование полномочий

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

- A. Чтобы убедиться, что проводится справедливая оценка
- B. Это не требуется. Для анализа рисков следует привлекать небольшую группу специалистов, не являющихся сотрудниками компании, что позволит обеспечить беспристрастный и качественный анализ
- **C. Поскольку люди в различных подразделениях лучше понимают риски в своих подразделениях и смогут предоставить максимально полную и достоверную информацию для анализа**
- D. Поскольку люди в различных подразделениях сами являются одной из причин рисков, они должны быть ответственны за их оценку

5. Что является наилучшим описанием количественного анализа рисков?

A. Анализ, основанный на сценариях, предназначенный для выявления различных угроз безопасности

B. Метод, используемый для точной оценки потенциальных потерь, вероятности потерь и рисков

C. Метод, сопоставляющий денежное значение с каждым компонентом оценки рисков

D. Метод, основанный на суждениях и интуиции

Практическое задание 7. Тема «Политика информационной безопасности»

Пусть имеем множество из 3 пользователей-субъектов O={Администратор, Гость, Пользователь_1} и множество из 4 объектов U={Файл_1, Файл_2, CD-RW, Флоппи-Дисковод}.

Пусть множество возможных действий включает следующие: S={Чтение, Запись, Передача прав}.

Кроме этого, существует два дополнительных типа операций -«Полные права», «Полный запрет». Действие «Полные права» разрешает выполнение всех из перечисленных 3 действий, «Полный запрет» запрещает выполнение всех из вышеперечисленных действий. Право «Передача прав» позволяет передавать субъекту свои права на объект другому субъекту.В данном случае, матрица доступа, описывающая дискреционную политику безопасности, может выглядеть, например, следующим образом.

Таблица 1

Объект / Субъект	Файл_1	Файл_2	CD-RW	Флоппи-дисковод
Администратор	Полные права	Полные права	Полные права	Полные права
Гость	Запрет	Чтение	Чтение	Запрет
Пользователь_1	Чтение, передача прав	Чтение, запись	Полные права	Полный запрет

Например, Пользователь_1 имеет права на чтение и запись в Файл_2. Пользователь_1 может передать свое право на чтение из Файла_1 другому пользователю. Если Пользователь_1 передает право на чтение к Файлу_1 пользователю Гость, то у пользователя Гость появляется право чтения из Файла_1, соответственно модифицируется матрица доступов.

Порядок выполнения работы.

Пусть множество Sвозможных операций субъектов над объектами компьютерной системы задано в виде: S= {«Доступ на чтение», «Доступ на запись», «Передача прав»}.

1.Получите из таблицы 2 информацию о количестве субъектов и объектов компьютерной системы, соответственно Вашему варианту.

2.Реализуйте программный модуль, формирующий матрицу доступов субъектов к объектам компьютерной системы в виде, аналогичном таблице 1.

Реализация данного модуля подразумевает реализацию следующих шагов:

2.1.Выбрать идентификаторы пользователей, которые будут использоваться

при их входе в компьютерную систему (по одному идентификатору для каждого пользователя, количество пользователей задано для Вашего варианта). Например, множество из 3 идентификаторов пользователей {Ivan, Sergey, Boris}. Один из данных идентификаторов должен соответствовать администратору компьютерной системы (пользователю, обладающему полными правами ко всем объектам).

2.2.Создать и случайным образом заполнить матрицу доступа субъектов к объектам в виде, аналогичном таблице 1.

При заполнении матрицы учесть следующее:

2.2.1.Один из пользователей-субъектов должен являться администратором системы. Для него права доступа ко всем объектам системы должны быть выставлены как полные.

2.2.2.Пользователь может иметь несколько прав доступа к некоторому объекту компьютерной системы, иметь полные права, либо совсем не иметь прав.

Замечание по реализации

Для реализации программной модели матрицы доступов можно использовать массив размерности MxN, где M–количество субъектов, N–количество объектов.

Права доступов в ячейках матрицы доступов можно кодировать трехбитными числами от 0 до 7, например, в следующем виде:

Бит доступа по чтению	Бит доступа по записи	Бит передачи прав

Тогда, соответствие множеств типов доступов и соответствующих значений в матрице доступов будет следующее:

Десятичное число	**Двоичное число**	**Разрешенные типы доступов**
0	000	Полный запрет
1	001	Передача прав
2	010	Запись
3	011	Запись, Передача прав
4	100	Чтение
5	101	Чтение, Передача прав
6	110	Чтение, Запись
7	111	Полный доступ

Таблица 2

Вариант	Количество субъектов доступа (пользователей)	Количество объектов доступа
1	5	5
2	4	4
3	5	4
4	6	5
5	7	6
6	8	3
7	9	4
8	10	4
9	3	5
10	4	6

7.2.4Примерныйпереченьвопросовдляподготовкикзачету
Непредусмотреноучебнымпланом

7.2.5Примерныйпереченьзаданийдлярешенияприкладныхзадач

1. Элементы теории защиты информации: объект, субъект, доступ. Основная аксиома теории защиты информации
2. Понятие ролевого разграничения доступа. Базовая модель ролевого разграничения доступа.
3. Классификация угроз безопасности информации: основные определения. Информационный поток по памяти и по времени.
4. Автоматная модель безопасности информационных потоков.
5. Виды политик безопасности. Общая характеристика дискреционной политики безопасности.
6. Классическая модель Белла-ЛаПадула мандатного разграничения доступа. Базовая теорема безопасности.
7. Виды политик безопасности. Общая характеристика мандатной политика безопасности.
8. Похищение прав доступа в рамках модели *Take-Grant.*
9. Виды политик безопасности. Общая характеристика политики безопасности информационных потоков.
10. Санкционированное получение прав доступа в рамках модели *Take-Grant*
11. Виды политик безопасности. Общая характеристика политики ролевого разграничения доступа и изолированной программной среды.
12. Модель распространения прав доступа *Take-Grant* (основные положения классической модели).

13.Модель решетки как важнейшее понятие теории информационной безопасности.

14.Дискреционная модель - типизированная матрица доступов.

15.Элементы теории защиты информации: объект, субъект, доступ. Основная аксиома теории защиты информации

16.Модель матрицы доступов Харисона-Руззо-Ульмана как модель систем дискреционного разграничения доступа.

17.Классификация угроз безопасности информации: основные определения. Информационный поток по памяти и по времени.

18.Классическая модель Белла-ЛаПадула мандатного разграничения доступа. Базовая теорема безопасности.

19.Виды политик безопасности. Общая характеристика дискреционной политики безопасности.

7.2.6.Методикавыставленияоценкиприпроведенииипромежуточной аттестации

(Например:Экзаменпроводитсяпотест-билетам,каждыйизкоторыхсодержит10вопросовизадачу.Каждыйправильныйответнавопросвтестеоценивается1баллом,задачаоценивается10баллов(5балловверноерешениеи5балловзаверныйответ).Максимальноеколичествонабранныхбаллов–20.

1.Оценка«Неудовлетворительно»ставитсявслучае,еслистудентнабралменее6баллов.

2.Оценка«Удовлетворительно»ставитсявслучае,еслистудентнабралот6до10баллов

3.Оценка«Хорошо»ставитсявслучае,еслистудентнабралот11до15баллов.

4.Оценка«Отлично»ставится,еслистудентнабралот16до20баллов.)

7.2.7Паспортоценочныхматериалов

№п/п	Контролируемыеразделы(темы)дисциплины	Кодконтролируемойкомпетенции	Наименованиеоценочногосредства
1	Основные понятия и подходы к управлению информационной безопасностью	ПК-2, ПК-4, ПК- 11, ПК-19, ПК-28	Тест, контрольная работа, защита лабораторных работ, защита реферата,

2	Стандартизация систем и процессов управления информационной безопасностью	ПК-2, ПК-4, ПК- 11, ПК-19, ПК-28	Тест, контрольная работа, защита лабораторных работ, защита реферата,
3	Политикаинформационнойбезопасности	ПК-2, ПК-4, ПК- 11, ПК-19, ПК-28	Тест, контрольная работа, защита лабораторных работ, защита реферата
4	Модели управления доступом и информационными потоками	ПК-2, ПК-4, ПК- 11, ПК-19, ПК-28	Тест, контрольная работа, защита лабораторных работ, защита реферата,
5	Управление и система управления информационной безопасностью	ПК-2, ПК-4, ПК- 11, ПК-19, ПК-28	Тест, контрольная работа, защита лабораторных работ, защита реферата
6	Организационные и кадровые вопросы управления информационной безопасностью	ПК-2, ПК-4, ПК- 11, ПК-19, ПК-28	Тест, контрольная работа, защита лабораторных работ, защита реферата

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

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

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

Решениеприкладныхзадачосуществляет-

ся,либоприпомощикомпьютернойсистемытестирования,либосиспользование мвыданныхзадачнабумажномносите-ле.Времярешениязадач30мин.Затемосуществляетсяпроверкарешениязадачэкзаменаторомивыставляетсяоцен-ка,согласнометодикивыставленияоценкиприпроведенииипромежуточнойаттестации.

8УЧЕБНОМЕТОДИЧЕСКОЕИИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕДИСЦИПЛИНЫ)

8.1Переченьучебнойлитературы,необходимойдляосвоениядисциплины

Основная литература

1. Основы управления информационной безопасностью :Учеб.пособие/ А. П. Курило. - М. : Горячая линия -Телеком, 2012. - 244 с. : ил . - (Вопросы управления информационной безопасностью. Кн. 1). - ISBN 978-5-9912-0271-8 : 300-00.

3.Разинкин К.А.336-2014 Методические указания №336-2014к практическим занятиям No 1–4 по дисциплине «Управление информационной безопасностью» для студентов специальности 090303 «Информационная безопасность автоматизированных систем»очной формы обучения/К.А. Разинкин, 2014, Воронеж, ВГТУ,59 с. Режим доступа: https://cchgeu.ru/upload/iblock/e3f/razinkin_pz_uib_1_4.pdf

4. Разинкин К.А.335-2014 Методические указания №336-2014к практическим занятиям No5–6 по дисциплине «Управление информационной безопасностью» для студентов специальности 090303 «Информационная безопасность автоматизированных систем»очной формы обучения/К.А. Разинкин, 2014, Воронеж, ВГТУ,53 с. Режим доступа: https://cchgeu.ru/upload/iblock/815/razinkin_pz_uib_5_6.pdf

Дополнительная литература

1.Методическое обеспечение оценки и регулирования рисков распределенных информационных систем :Учеб.пособие / Г. А. Остапенко [и др.]. - Воронеж : ФГБОУ ВПО "Воронежский государственный технический университет", 2011. - 178 с. - 182-77; 250 экз.

2. Шилов А.К. Управление информационной безопасностью [Электронный ресурс]: учебное пособие/ Шилов А.К.— Электрон.текстовыеданные.— Ростов-на-Дону, Таганрог: Издательство Южного федерального университета, 2018.— 120 с.— Режим доступа: http://www.iprbookshop.ru/87643.html.— ЭБС «IPRbooks».

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

http://att.nica.ru
http://www.edu.ru/
http://window.edu.ru/window/library
http://www.intuit.ru/catalog/
https://marsohod.org/howtostart/marsohod2
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

Дисплейный класс, оснащенный компьютерными программами для проведения лабораторного практикума.

10.МЕТОДИЧЕСКИЕУКАЗАНИЯДЛЯОБУЧАЮЩИХСЯПООСВОЕНИЮДИСЦИПЛИНЫ(МОДУЛЯ)

Подисциплине«Управлениеинформационнойбезопасностью»читаютсялекции,проводятсялабораторныеработы.

Основойизучениядисциплиныявляютсялекции,накоторыхизлагаютсянаиболеесущественныеитрудныевопросы,атакжевопросы,ненашедшиеотраженияв учебнойлитературе.

Лабораторныеработывыполняютсяналабораторномоборудованиивсоответствиисметодиками,приведеннымивуказанияхквыполнениюработ.

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.
Лабораторнаяработа	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, ре-

	шить 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 промежуточнойаттестации.
Подготовка к промежуточнойа ттестации	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 с оценкой три дня эффективнее всего использовать для повторения и систематизации материала.