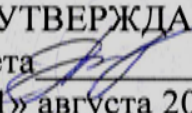


**МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ
ФЕДЕРАЦИИ**

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

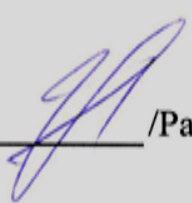
Квалификация выпускника специалист по защите информации

Нормативный период обучения 5 лет

Форма обучения очная

Год начала подготовки 2016

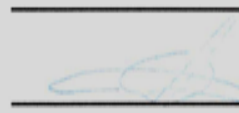
Автор программы


/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.Задачiosoвoениядисциплины

приобретение 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»относитсяк дисциплинамбазовойчастиблокаБ1.

3.ПЕРЕЧЕНЬПЛАНИРУЕМЫХРЕЗУЛЬТАТОВОБУЧЕНИЯПОДИСЦИПЛИНЕ

Процессизучениядисциплины«Управлениеинформационнойбезопасностью»направленнаформированиеследующихкомпетенций:

ПК-2-способностьюсоздаватьиисследоватьмоделиавтоматизированных систем;

ПК-4-способностьюразрабатыватьмоделиугрозимоделинарушителяинформационнойбезопасностиавтоматизированнойсистемы;

ПК-11-способностьюразрабатыватьполитикуинформационнойбезопасностиавтоматизированнойсистемы;

ПК-19-способностьюразрабатыватьпредложенияпосовершенствованию системыуправленияинформационнойбезопасностьюавтоматизированнойсистемы;

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

	владеть навыками 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 разрабатывать модели угроз модели нарушителя информационной безопасности автоматизированной системы;
ПК-11	знать принципы построения систем управления информационной безопасностью (СУИБ) и особенности отдельных процессов управления ИБ в рамках СУИБ
	уметь формировать политики информационной безопасности организации
ПК-19	знать основные документы по стандартизации в сфере управления ИБ
	уметь определять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности автоматизированных систем;
	владеть методами мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем
ПК-28	знать способы управления информационной безопасностью автоматизированной системы
	уметь определять цели и задачи, решаемые разрабатываемыми процессами управления ИБ

4. ОБЪЕМ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины «Управление информационной безопасностью» составляет 33 з.е.

Распределение трудоемкости дисциплины по видам занятий
очная форма обучения

Виды учебной работы	Всего часов	Семестры
		9
Аудиторные занятия (всего)	80	80
В том числе:		
Лекции	40	40
Практические занятия (ПЗ)	40	40
Самостоятельная работа	28	28
Виды промежуточной аттестации - зачет	+	+
Общая трудоемкость:		

академические часы	108	108
зач.ед.	3	3

5.СОДЕРЖАНИЕДИСЦИПЛИНЫ(МОДУЛЯ)

5.1Содержаниеразделовдисциплиныираспределениетрудовыхнагрузокпо видамзанятий

очнаяформаобучения

№ п/ п	Наименованиетем ы	Содержаниераздела	Ле кц	П ра к за н.	С Р С	Все го, 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. Управление конфигурациями, изменениями и обновлениями.	8	6	4	18
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. Отраслевые стандарты в области управления ИБ.	8	6	4	18
3	Политика информационной безопасности и	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	6	4	16
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	6	4	16
5	Управление и	Необходимость управления	6	8	6	20

	система управления информационной безопасностью	обеспечением ИБ организации. Деятельность по обеспечению 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. Компетентностные уровни профессионалов в области ИБ	6	8	6	20
Итого			40	40	28	108

5.2 Перечень лабораторных работ

Непредусмотрено учебным планом

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

В соответствии с учебным планом освоение дисциплины не предусматривает выполнения курсового проекта (работы) или контрольной работы.

7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

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

7.1.1 Этап текущего контроля

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

«аттестован»;

«неаттестован».

Компетенция	Результаты обучения, характеризующие сформированность компетенции	Критерии оценивания	Аттестован	Неаттестован
ПК-2	знать основные методы управления информационной	знание основных методов управления	Выполнение работ	Невыполнение работ в

	безопасностью	информационной безопасностью	в срок, предусмотренный в рабочих программах	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	владение навыками администрирования 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 защищенных автоматизированной системы	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 модели угроз модели нарушителя информационной безопасности автоматизированной системы;	умение оценивать информационные риски в автоматизированных системах и разрабатывать модели угрозы модели нарушителя информационной безопасности автоматизированной системы	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	знание основных инструкций, регламентов, положений и	Выполнение работ	Невыполнение работ в

	управления ИБ	приказов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем	в срок, предусмотренный в рабочих программах	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 аудита, выявления угроз информационной безопасности автоматизированных систем	владеет навыками обработки, оценки и представления результатов исследования эффективности решений по управлению информационной безопасностью	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
ПК-28	знать способы управления информационной безопасностью автоматизированной системы	знает способы управления информационной безопасностью автоматизированной системы	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	умеет определять цели и задачи, решаемые разрабатываемыми процессами управления ИБ	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах

7.1.2 Этап промежуточного контроля знаний

Результаты промежуточного контроля знаний оцениваются в 9 семестре для очной формы обучения по двухбалльной системе:

«зачтено»

«незачтено»

Компетенция	Результаты обучения, характеризующие сформированность компетенции	Критерии оценивания	Зачтено	Незачтено
ПК-2	знать основные методы управления информационной безопасностью	Тест	Выполнение теста на 70-100%	Выполнение менее 70%
	уметь пользоваться моделями безопасности КС при управлении доступом и информационными	Решение стандартных практических задач	Продемонстрирован верный	Задача не решена

	потоками		ход решения в большин стве задач	
	владеть навыками анализа информационной инфраструктуры автоматизированной системы и ее безопасности	Решение прикладных задач в конкретной предметной области	Продемо нстриров а н верный ход решения в большин стве задач	Задачинер ешены
ПК-4	знать требования информационной безопасности при эксплуатации автоматизированной системы	Тест	Выполне ниетеста на 70-100%	Выполнен иенее 70%
	уметь оценивать информационные риски в автоматизированных системах и разрабатывать модели угрозы модели нарушителя информа ционной безопасности автома тизированной системы;	Решение стандартных практически х задач	Продемо нстриров а н верный ход решения в большин стве задач	Задачинер ешены
ПК-11	знать принципы построения систем управления информационной безопасностью (СУИБ) и особенности отдельных процессов управления ИБ в рамках СУИБ	Тест	Выполне ниетеста на 70-100%	Выполнен иенее 70%
	умеет формировать политики информационной безопасности организации	Решение стандартных практически х задач	Продемо нстриров а н верный ход решения в большин стве задач	Задачинер ешены
ПК-19	знать основные документы по стандартизации в сфере управления ИБ	Тест	Выполне ниетеста на 70-100%	Выполнен иенее 70%
	уметь определять комплекс мер (правила, процедуры, практические приемы, руководящие принципы,	Решение стандартных практически х задач	Продемо нстриров а н верный	Задачинер ешены

	методы, средства) для обеспечения информационной безопасности автоматизированных систем;		ход решения в большинстве задач	
	владеть методами мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем	Решение прикладных задач в конкретной предметной области	Продемонстрирован верный ход решения в большинстве задач	Задачи решены
ПК-28	знать способы управления информационной безопасностью автоматизированной системы	Тест	Выполнение теста на 70-100%	Выполнено не менее 70%
	уметь определять цели и задачи, решаемые разрабатываемыми процессами управления ИБ	Решение стандартных практически задач	Продемонстрирован верный ход решения в большинстве задач	Задачи решены

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

7.2.1 Примерный перечень заданий для подготовки к тестированию

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-Grant являются: (несколько вариантов ответов)

- **take**
- **grant**
- **create**
- **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 процессов;**

- 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 стандарта ISO/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

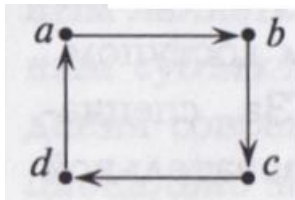
CMS

7.2.2 Примерный перечень заданий для решения стандартных задач

(тема «Модели управления доступом и информационными потоками»)

Практическое задание № 1.

Модель решётки. Задаёт ли решётку граф на рис.?



Так как выполняются условия $a \leq b, b \leq c$ и $a \neq b$, то не выполняется свойство антисимметричности отношения частичного порядка « $\leq$ » на множестве $\{a, b, c, d\}$. Следовательно, по определению граф не задаёт решётку.

Практическое задание № 2.



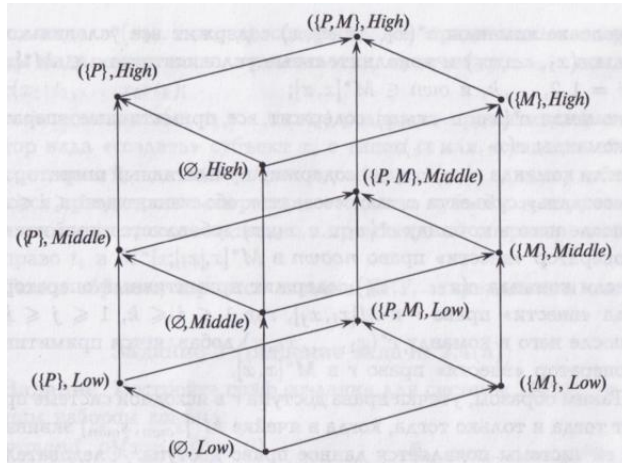
Задаёт ли решётку граф?

Решение. В соответствии с определением выполнены все свойства отношения частичного порядка « $\leq$ » на множестве $\{a, b, c, d, e, f\}$. Для каждой пары вершин, соединённых в графе путем, существует наименьшая верхняя и наибольшая нижняя границы. Например, справедливы равенства $f \oplus b = b$ и $f \otimes b = f$. Для каждой пары, не соединённых 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 ($X \times L, \leq$), для решетки $(L, \leq) = \{Low, Middle, High\}$ и $(X, \leq)$ — решетки подмножеств множества $U = \{Political, Military\}$.



Решение. Построим граф, задающий решетку $(X \times L, \leq)$. 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 γ для заданной пары субъект s и 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 $q^* = (S^*, O^*, M^*)$, соответствующем состоянию $q = (S, O, M)$, справедливы равенства:

$$S^* = S \cup \{s_{own}\};$$

$$O^* = O \cup \{s_{own}\};$$

$$R^* = R \cup \{own, noown\}.$$

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

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

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: $noown \in M^*[x, x_i], i = 1, 2, \dots, k, own \in M^*[x, x]$; 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 $1 \leq i \leq k$, 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 $1 \leq i \leq k, 1 \leq j \leq k$ 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 $M^*[s_{own}, s_{own}]$ эквивалентной ей системы появляется данное право доступа. Следовательно, если бы существовал алгоритм проверки возможности утечки права доступа для заданной пары субъект s и 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 $q = (S, O, T, M)$, 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 $M^*[s, o] = M[s, o]$,
 $M[s_{own}, o] = \{t(o)\}, M^*[s_{own}, s_{own}] = \{own\}$.
 Для каждой команды $c(x_1: t_1, \dots, x_k: t_k) \in C$ системы ТМД в систему ХРУ добавим команду $c^*(x_1, \dots, x_k, x)$, 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_i или «создать» объект X_i с типом t_i , где $1 \leq i \leq k$, то в команду $c^*(x_1, \dots, x_k, x)$ добавляются примитивные операторы «создать» субъект X_i или «создать» объект X_i соответственно и примитивный оператор «внести» право t_i в $M^*[x, x_i]$. 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?

- ☐ А. Угрозы x Риски x Ценность актива
- ☐ В. (Угрозы x Ценность актива x Уязвимости) x Риски
- ☐ С. SLE x 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**
- ☐ В. Количественная оценка воздействия потенциальных угроз
- ☐ С. 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?

- ☐ А. Поддержка
- ☒ **В. Выполнение анализа рисков**
- ☐ С. Определение цели и границ
- ☐ D. Делегирование полномочий

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

- ☐ А. Чтобы убедиться, что проводится справедливая оценка
- ☐ В. Это не требуется. Для анализа рисков следует привлекать небольшую группу специалистов, не являющихся сотрудниками компании, что позволит обеспечить беспристрастный и качественный анализ
- ☒ **С. 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?

- ☐ А. Анализ, основанный на сценариях, предназначенный для выявления различных угроз безопасности
- ☐ В. Метод, используемый для точной оценки потенциальных потерь, вероятности потерь и рисков
- ☒ **С. 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 $O = \{\text{Администратор, Гость, Пользователь_1}\}$ и множество из 4 объектов $U = \{\text{Файл_1, Файл_2, CD-RW, Флоппи-Дисковод}\}$.

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

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-диск
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 Возможных операций субъектов над объектами компьютерной системы задано в виде: $S = \{\text{«Доступ на чтение»}, \text{«Доступ на запись»}, \text{«Передача прав»}\}$.

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 $M \times N$, 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

7.2.4 Примерный перечень вопросов для подготовки к зачету

1. Какие определения ПолиБ даются в различных международных стандартах?
2. В чем различие политик, стандартов, правил и процедур ОИБ?
3. Что такое трастовые модели?
4. С каких точек зрения и как можно описать виды ПолиБ?
5. Что понимают под ПолиБ в широком и узком смысле?
6. Для чего разрабатываются организационные (административные) и технические ПолиБ?
7. Перечислите основные требования, предъявляемые в различных источниках к ПолиБ?
8. Каковы основные принципы, позволяющие разработать

эффективную ПолиБ?

9. Каково содержание документа, описывающего корпоративную ПолиБ? Что излагается в каждом из разделов этой политики?

10. Назовите типовые цели корпоративной ПолиБ.

11.11. Каковы отличительные особенности содержания частной ПолиБ для отдельной области, требующей ОИБ, и для отдельной системы, используемой в организации? Что общего между ними подтипами? Что излагается в каждом из разделов этих политик?

12.12. Назовите основные стадии жизненного цикла ПолиБ? Из каких шагов они состоят? Какие из этих шагов выполняются итерационно и почему?

13.13. Отдельно сформулируйте цель к основным мероприятиям, осуществляемым на каждом шаге жизненного цикла ПолиБ.

14. Как происходит процесс информирования в отношении ПолиБ?

15. Для чего и кем осуществляются ревизия, мониторинг и аудит ПолиБ? В чем отличия этих шагов жизненного цикла ПолиБ?

16. Что понимается под исключениями в ПолиБ?

17. Зачем необходим пересмотр ПолиБ?

18. В каких случаях ПолиБ может быть аннулирована?

19. Что такое «роль»? Какие роли связаны с использованием ПолиБ?

20. Какие виды ответственности связаны со всеми стадиями жизненного цикла ПолиБ?

21. Какими принципами необходимо руководствоваться при установлении ответственности в отношении соблюдения ПолиБ?

22. Дайте определения «ОИБ», «управления ИБ» и «СУИБ» организации.

23. Опишите деятельность по ОИБ организации как процесс. Каковы его входные и выходные данные, ресурсы и управляющие воздействия?

24. Как процесс ОИБ организации связан с процессами основной деятельности организации?

25. Каковы основные этапы процесса управления ИБ ИТТ

26. Что является хорошей практикой при выборе области действия СУИБ? Какие стратегии выбора области действия СУИБ существуют?

27. Какие факторы необходимо учитывать при выборе области действия СУИБ?

28. Какие параметры процессов являются наиболее значимыми при выборе области действия проектируемой СУИБ?

29. Что входит в документальное обеспечение СУИБ? Каковы этапы его жизненного цикла?

30. Какие уровни документов включает в себя иерархия документов СУИБ? Какие виды конкретных документов создаются на каждом из уровней?

31. И чем состоит основное отличие между понятиями документ и запись?

32. В чем заключается процесс управления документами и записями?

33. Какова взаимосвязь между понятиями ПолиБ и политика СУИБ?

34. Что должна включать в себя политика СУИБ?

35. На каких этапах руководство организации должно продемонстрировать свою приверженность к разработке, реализации, эксплуатации, мониторингу, анализу, сопровождению и совершенствованию СУИБ?

36. В чем состоит основная необходимость участия высшего руководства в жизненном цикле СУИБ?

37. Каким образом при использовании циклической модели PDCA применительно к СУИБ требования и ожидания к результатам ОИБ преобразуются в управляемую ИБ?

38. Дайте определение «процесс управления ИБ» организации.

39. Какие действия и процессы выполняются на стадии планирования СУИБ? Каковы задачи данного этапа?

40. Специалистов каких подразделений необходимо включать в рабочую группу по построению СУИБ и почему?

41. Какие действия и процессы выполняются на стадии реализации и внедрения СУИБ? Каковы задачи данного этапа?

42. Какие действия и процессы выполняются на стадии проверки СУИБ? Каковы задачи данного этапа?

43. Какие действия и процессы выполняются на стадии совершенствования СУИБ. Каковы задачи данного этапа?

44. В чем разница и сходство между понятиями корректирующего и предупреждающего действия?

45. Почему в рамках процесса подхода к управлению ИБ следует особое внимание уделять мониторингу и анализу результативности и эффективности СУИБ?

46. В чем состоят различия между основными свойствами процессов: эффективность и результативность?

47. Что входит в понятие «задание процесса управления ИБ»?

48. Какие этапы включает в себя идентификация процессов управления ИБ в организации и какие действия необходимо предпринять в рамках этих этапов?

49. Каковы основные преимущества документирования процессов управления ИБ в организации и наличия подробных карт процессов организации?

50. Каковы основные элементы процесса мониторинга процессов управления ИБ организации?

7.2.5 Примерный перечень заданий для решения прикладных задач

Не предусмотрено учебным планом

7.2.6. Методика выставления оценки при проведении промежуточной аттестации

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

1. Оценка «Неудовлетворительно» ставится в случае, если студент набра

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	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	Политика информационной безопасности	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. 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

ле. Время тестирования 30 мин. Затем осуществляется проверка теста экзаменатором и выставляется оценка согласно методике 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 методике 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 методике выставления оценки при проведении промежуточной аттестации.

8 УЧЕБНО МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ)

8.1 Перечень учебной литературы, необходимой для освоения дисциплины

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 №336-2014 к практическим занятиям № 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 №335-2014 к практическим занятиям №5–6 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. текстовые данные. — Ростов-на-Дону, Таганрог: Издательство Южного федерального университета, 2018. — 120 с. — Режим доступа: <http://www.iprbookshop.ru/87643.html>. — ЭБС «IPRbooks».

8.2 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень литературы и программного обеспечения, ресурсов информационно-телекоммуникационной сети «Интернет», современных профессиональных баз данных и информационных справочных 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/> (ЭБС IPRbooks)

9 МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯ БАЗА, НЕОБХОДИМАЯ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА

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

Дисплейный класс, оснащенный компьютерными программами для проведения лабораторного практикума.

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

По дисциплине «Управление информационной безопасностью» читаются лекции, проводятся практические занятия.

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

Практические занятия направлены на приобретение практических навыков по реализации: модели решётки, дискреционного управления доступом (модели Харрисона-Руззо-Ульмана и типизированная матрицы доступов), управления распространением прав доступа на основе классической модели Take-Grant, управление распространением прав доступа на основе расширенной модели Take-Grant, модели Белла-ЛаПадулы, ролевого и мандатного ролевого управления доступом.

А, также изучение средств управления безопасностью на уровне операционной системы на примере Windows Server 2003; управления учетными записями пользователей; изучение средств управления безопасностью на уровне операционной системы на примере

Windows Server 2003; настройке политик безопасности.
Занятия проводятся путем решения конкретных задач в аудитории.

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 удастся 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.
Самостоятельная работа	Самостоятельная работа студентов способствует глубокому усвоению 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 начинаться не позднее, чем за месяц-полтора до промежуточной аттестации. Данные перед зачетом три дня эффективнее всего использовать для повторения и систематизации материала.