Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Смирнов Сергей Николаевич
Должность: врио ректора
Дата подписания: 13.10.2023 13:56:10
Уникальный программный ключ:
69e375c64f7e975d4e8830e7b4fcc2ad1bf35f08

Министерство науки и высшего образования Российской Федерации

ФГБОУ ВО «Тверской государственный университет»

Утверждаю:
Руководитель ООП:
_____ Н.А. Семыкина
«_9_» _06_ 2023 г.

Рабочая программа дисциплины (с аннотацией)

МОДЕЛИ БЕЗОПАСНОСТИ КОМПЬЮТЕРНЫХ СИСТЕМ

Специальность
10.05.01 Компьютерная безопасность

Специализация
Математические методы защиты информации

Для студентов 4 курса очной формы обучения

Составитель: _____ к.ф.-м.н, доцент *Семыкина Н. А.*

Тверь 2023

I. Аннотация

1. Наименование дисциплины (или модуля) в соответствии с учебным планом

Модели безопасности компьютерных систем

2. Цель и задачи дисциплины (или модуля)

Целью освоения дисциплины является раскрытие содержания основных понятий и формальных моделей обеспечения безопасности компьютерных систем (моделей компьютерной безопасности), а также сформировать у обучаемых теоретико-методологические основы профессиональной деятельности в сфере компьютерной безопасности в контексте всех трех ее составляющих видов — производственно-технологической, организационно-управленческой и экспериментально-исследовательской.

Задачи дисциплины – дать основы:

• исходных понятий и формализации в сфере компьютерной безопасности;

• представления, анализа и обоснования моделей, методов и механизмов обеспечения компьютерной безопасности;

• методологии анализа архитектурных (схемно-технических) и программно-алгоритимических решений, применяемых в системах защиты информации современных компьютерных систем.

3. Место дисциплины (или модуля) в структуре ООП

Дисциплина «Модели безопасности компьютерных систем» относится к дисциплинам базовой части ООП. Для успешного изучения данной дисциплины необходимо знание основ следующих дисциплин «Основы информационной безопасности», «Компьютерные сети», «Операционные системы».

Модели безопасности компьютерных систем является базовой для изучения дисциплин: «Защита в операционных системах», «Техническая защита информации».

4. Объем дисциплины (или модуля):

3 зачетные единицы, 108 академических часов, **в том числе**

контактная работа: лекции 36 часов, практические занятия 36 часов, лабораторные работы 0 часов, **самостоятельная работа:** 36 часов.

5. Перечень планируемых результатов обучения по дисциплине (или модулю), соотнесенных с планируемыми результатами освоения образовательной программы

Планируемые результаты освоения образовательной программы (формируемые компетенции)	**Планируемые результаты обучения по дисциплине (или модулю)**
ОПК-9. способностью разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации	**Владеть:** научным представлением о формальных моделях политик безопасности, методами формирования политик безопасности, классификацией информационных систем по требованиям защиты информации. **Уметь:** исследовать формализованные модели в области автоматизации информационно-аналитической деятельности, разрабатывать модели угроз безопасности информации, формировать политики безопасности компьютерных систем и сетей. **Знать:** модели безопасности компьютерных систем, виды политик безопасности компьютерных систем, методы построения и исследования математических моделей в области автоматизации информационно-аналитической деятельности в сфере безопасности.
ПК-4. способностью проводить анализ и участвовать в разработке математических моделей безопасности компьютерных систем	**Владеть:** навыками определения видов политик безопасности компьютерных систем, основными методами построения моделей безопасности компьютерных систем. **Уметь:** формировать политики безопасности компьютерных систем и сетей. **Знать:** виды политик безопасности компьютерных систем, модели безопасности компьютерных систем, критерии безопасности и условия применения моделей безопасности

6. Форма промежуточной аттестации зачет

7. Язык преподавания русский**.**

II. Содержание дисциплины (или модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

1. Для студентов очной формы обучения

Учебная программа – наименование разделов и тем	Всего (час.)	Контактная работа (час.)		Самостоятельная работа (час.)
		Лекции	Практические (лабораторные) занятия	
Основные понятия и определения. Угрозы безопасности в компьютерных системах. Виды политики безопасности. Основные виды моделей безопасности.	7	3	2	2
Модели систем дискретного разграничения доступа. Модель матрицы доступов ХРУ	7	3	2	2
Модель распространения прав доступа TAKE - GRANT	11	3	4	4
Расширенная модель TAKE-GRANT	11	3	4	4
Модели безопасности на основе мандатной политики. Модель Белла – ЛаПадулы	11	3	4	4
Основные расширения модели Белла-ЛаПадулы	7	3	2	2
Модель систем военных сообщений (MMS)	7	3	2	2
Модели безопасности на основе ролевой политики	9	3	3	3

Модели безопасности на основе тематической политики	9	3	3	3
Модель тематико-иерархического разграничения доступа	6	2	2	2
Модель системы индивидуально-групповых назначений доступа к иерархически организованным объектам	10	2	4	4
Субъектно – ориентированная модель изолированной программной среды	7	3	2	2
Стандарты в информационной безопасности	8	4	2	2
ИТОГО	108	36	36	36

III. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

Методические рекомендации по организации самостоятельной работы студентов

Самостоятельная работа студентов по изучаемой дисциплине призвана, не только, закреплять знания, полученные во время аудиторных занятий, но и способствовать развитию у студентов творческих навыков, инициативы, умению организовывать свое время.

Все виды самостоятельной работы и планируемые на их выполнение затраты времени в часах исходят из того, что студент достаточно активно работал в аудитории, слушая лекции и решая задачи на практических занятиях. В случае пропуска лекций и практических занятий студенту потребуется сверхнормативное время на освоение пропущенного материала.

При выполнении плана самостоятельной работы студенту необходимо прочитать теоретический материал, содержащийся в указанной учебной

литературе и Интернет-ресурсах. Составить словарь основных терминов и тематические конспекты, в которые необходимо включить теоретическое описание метода и привести примеры алгоритмов.

Планы практических занятий и методические рекомендации к ним

Раздел 1. Исходные положения теории компьютерной безопасности.

Определение информации. Понятие компьютерной и информационной безопасности, угрозы, уязвимости. Классификация угроз. Принципы обеспечения компьютерной безопасности в автоматизированных системах. Угрозы конфиденциальности, целостности, доступности автоматизированных систем. Понятие политики безопасности.

Раздел 2. Классические модели безопасности компьютерных систем. Математические основы моделей безопасности

Граф. Решётка. Алгоритмически разрешимые и алгоритмически неразрешимые проблемы. Проблема адекватности реализации модели безопасности в реальной компьютерной системе. Модель системы безопасности HRU. Основные положения модели. Теорема об алгоритмической неразрешимости задачи проверки безопасности произвольной системы HRU. Модель распространения прав доступа Take-Grant. Теоремы о передаче прав в графе доступов, состоящем из субъектов, и произвольном графе доступов. Расширенная модель Take-Grant и ее применение для анализа информационных потоков в АС. Модель Белла-Лападулы как основа построения систем мандатного разграничения доступа. Основные положения модели. Базовая теорема безопасности (BST). Политика low-watermark в модели Белла-ЛаПадулы. Применение модели Биба для реализации мандатной политики целостности. Применение модели систем военных сообщений для систем приема, передачи и обработки почтовых сообщений, реализующих мандатную политику безопасности.

Примеры тестов для самоконтроля по разделу 2

1.Какие виды политик информационной безопасности рассматриваются в теории компьютерной безопасности (отметьте один или несколько ответов).

1*) мандатная
2) древовидная
3) многоуровневая
4*) ролевая
5*) дискреционная
6) дискретизированная
7) ничего из перечисленного

2. Как формулируется основная аксиома теории компьютерной безопасности?

1) Все вопросы безопасности информации в КС описываются перечнем субъектов и объектов;

2) Все вопросы безопасности информации в КС описываются уровнями субъектов и объектов;

3*) Все вопросы безопасности информации в КС описываются доступами субъектов к объектам;

4) Все вопросы безопасности информации в КС описываются доступами субъектов к субъектам;

5) Все вопросы безопасности информации в КС описываются уровнями доступа субъектов и уровнями безопасности объектов;

6) ничего из перечисленного.

3.Какие из перечисленных моделей являются дискреционными?

1) Модель Биба;
2*) Модель Харрисона-Руззо-Ульмана;
3) Модель Белла-ЛаПадулы;
4*) Модель Take-Grant;
5) Модель систем военных сообщений;
6) Модель изолированной программной среды.

4. Существует ли алгоритм проверки безопасности систем ХРУ?

1) Да, существует для общего случая;

2) Нет, не существует ни для каких ХРУ;

3) Существует только для монооперационных ХРУ;

4) Существует для некоторых разновидностей ХРУ, а в общем случае – возможно существует, но не найден;

5*) Существует для некоторых разновидностей ХРУ, а в общем случае доказано, что не существует.

6) Вопрос о существовании или не существовании такого алгоритма не решен ни для каких ХРУ.

5. Какие из перечисленных правил являются де-факто правилами расширенной модели Take-Grant?

1) take	2) grant
3) write	4) read
5*) spy	6*) find
7*) post	8*) pass
9) invoke	10) observe

Раздел 3. Модели компьютерных систем с ролевым управлением. Модели изолированной программной среды.

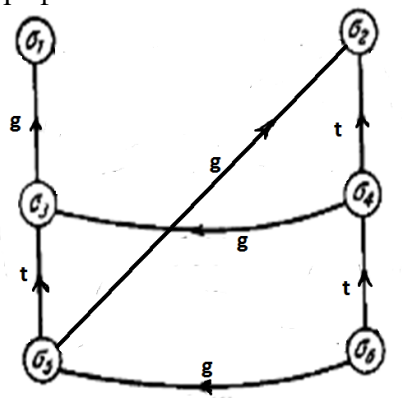
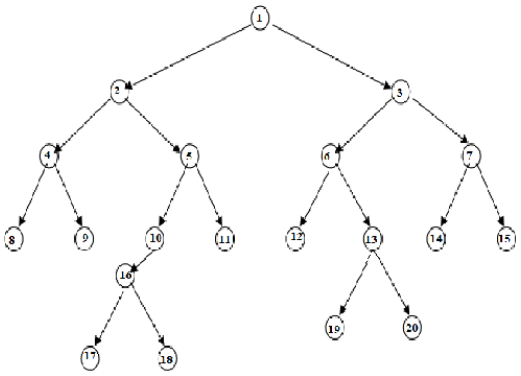
Понятие ролевого управления доступом. Базовая модель ролевого управления доступом. Понятие администрирования ролевого управления доступом. Администрирование иерархии ролей. Монитор безопасности объектов. Монитор безопасности субъектов. Теоремы о достаточных условиях гарантированного выполнения политики безопасности в компьютерных системах. Базовая теорема изолированной программной среды.

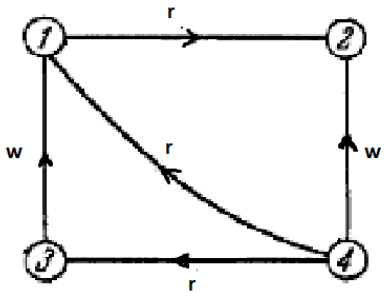
Раздел 4. Стандарты в информационной безопасности

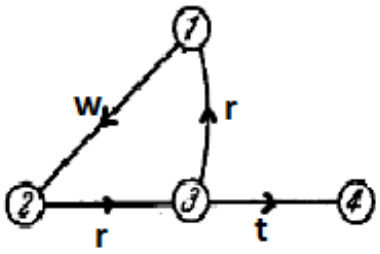
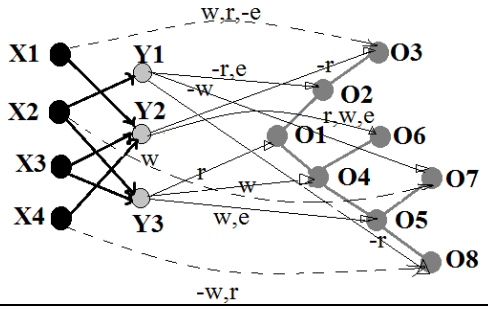
Классические стандарты информационной безопасности. Оранжевая книга. Руководящие документы ФСТЭК (Гостехкомиссии при Президенте РФ). Классы защищенности автоматизированных систем. Единые критерии безопасности информационных технологий (ГОСТ Р ИСО 15408). Сертификация средств защиты в РФ. Верификация защиты.

IV. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине (или модулю)

Типовые контрольные задания для проверки уровня сформированности компетенции ОПК-9. способностью разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации

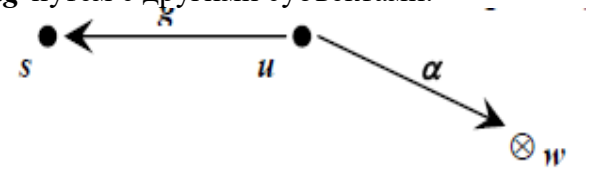
Этап формирования компетенции, в котором участвует дисциплина	**Типовые контрольные задания для оценки знаний, умений, навыков (2-3 примера)**	**Показатели и критерии оценивания компетенции, шкала оценивания**
Базовый, **Владеть** научным представлением о формальных моделях политик безопасности, методами формирования политик безопасности, классификацией информационных систем по требованиям защиты информации.	1. Истинен ли предикат «возможен доступ (σ_1,σ_2,q_0)» для следующего графа?  2. Пусть имеется иерархический тематический рубрикатор. Использованы мультирубрики: $T^м_1$= {τ_3,τ_7}, $T^м_2$= {τ_{10},τ_7}, $T^м_3$= {τ_5,τ_{13}}, $T^м_4$= {τ_4,τ_7}, $T^м_5$= {$\tau_{17},\tau_{18},\tau_{14},\tau_{15}$}, $T^м_6$= {τ_6,τ_{16}}.  а) Определить отношения доминирования (уже, шире, несравнимо) между следующими мультирубриками: $T^м_1$ и $T^м_4$; $T^м_3$ и $T^м_6$; $T^м_5$ и $T^м_2$; $T^м_6$ и $T^м_5$	Имеется полное верное решение, включающее правильный ответ – 5 балла В решении имеются лишние или неверные записи, не отделенные от решения – 3 балла Решение не дано или дано неверное решение – 0 баллов

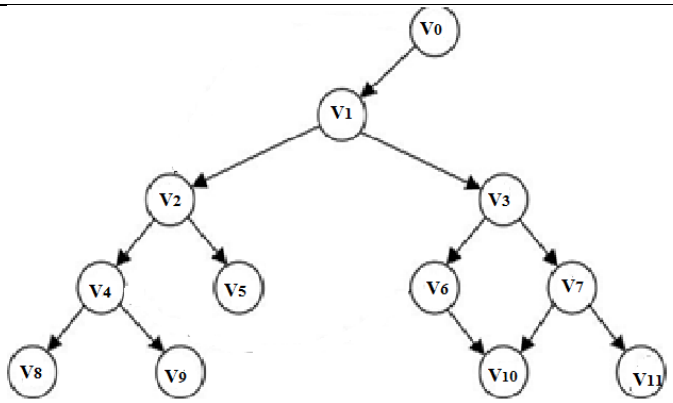
	б) Построить объединение следующих мультирубрик: $T^{м}_{1} \cup_{м} T^{м}_{4}$; $T^{м}_{3} \cup_{м} T^{м}_{6}$; $T^{м}_{2} \cup_{м} T^{м}_{5}$; $T^{м}_{5} \cup_{м} T^{м}_{6}$; $T^{м}_{1} \cup_{м} T^{м}_{6}$. в) Построить пересечение следующих мультирубрик: $T^{м}_{1}$ и $T^{м}_{4}$; $T^{м}_{3}$ и $T^{м}_{6}$; $T^{м}_{5}$ и $T^{м}_{2}$; $T^{м}_{6}$ и $T^{м}_{5}$.	
Базовый, **Уметь** исследовать формализованные модели в области автоматизации информационно-аналитической деятельности, разрабатывать модели угроз безопасности информации, формировать политики безопасности компьютерных систем и сетей.	1. Пусть неявные каналы записи, генерируемые различными командами де-факто имеют следующую стоимость: r_{spy} =5, r_{post} =3, r_{find} =7, r_{pass} =2. Применяя команды де-факто сгенерировать все возможные неявные каналы чтения субъектом x3 информации из субъекта x2 , и сравнить их стоимость.  2. Пусть имеется мандатная система доступа, в которой решетка уровней безопасности Λ_L является линейной и имеет три уровня – $l1$, $l2$, $l3$; $l1 > l2 > l3$. На предприятии есть следующие должности: директор, заместитель директора, ведущий инженер и главный конструктор, в подчинении у них инженеры и специалисты. Имеется следующая система объектов доступа: документ «Новые разработки конструкторского бюро предприятия»; Ведомость покупных изделий, Ведомость технического проекта, Эксплуатационные документы, Чертежи деталей, Инструкция. Обосновать и составить систему уровней допусков пользователей, грифов секретности объектов доступа и матрицу доступа $\boldsymbol{A}[\boldsymbol{u},\boldsymbol{o}]$.	Имеется полное верное решение, включающее правильный ответ – 5 балла В решении имеются лишние или неверные записи, не отделенные от решения – 3 балла Решение не дано или дано неверное решение – 0 баллов
Базовый, **Знать** модели безопасности компьютерных систем,	1. Построить де-юре-замыкание графа доступов	Имеется полное верное решение, включающее правильный ответ – 5 балла В решении

виды политик безопасности компьютерных систем, методы построения и исследования математических моделей в области автоматизации информационно-аналитической деятельности в сфере безопасности.	 2. Пусть имеется иерархически организованная система объектов доступа О и система субъектов Х, объединенных в рабочие группы. Вхождение пользователей в рабочие группы показаны на рисунке. Определите общий коэффициент дублирования прав доступа в системе по записи и коэффициент дублирования прав доступа по записи для пользователя x_4 . 	имеются лишние или неверные записи, не отделенные от решения – 3 балла Решение не дано или дано неверное решение – 0 баллов

Типовые контрольные задания для проверки уровня сформированности компетенции ПК-4. способностью проводить анализ и участвовать в разработке математических моделей безопасности компьютерных систем

Этап формирования компетенции, в котором участвует дисциплина	**Типовые контрольные задания для оценки знаний, умений, навыков (2-3 примера)**	**Показатели и критерии оценивания компетенции, шкала оценивания**
Базовый, **Владеть** навыками определения видов политик безопасности компьютерных систем, основными	1. Пусть имеется система субъектов и объектов доступа, представленная графом доступов Установленная для системы политика безопасности запрещает любым субъектам (владельцам) предоставлять право α на "свои" объекты другим субъектам (но не запрещает субъектам, которые владеют правами ***t*** ("брать") на какие-либо субъекты брать у них права на их объекты).	Имеется полное верное решение, включающее правильный ответ – 5 балла В решении имеются лишние или неверные записи, не

методами построения моделей безопасности компьютерных систем.	Кроме субъекта ***s***, субъект ***u*** может быть связан ***tg***-путем с другими субъектами.  Построить систему команд получения субъектом ***s*** прав доступа α на объект ***w*** от субъекта ***u***, при условии того, что команда ***grants***(α, ***u***, ***s***, ***w***) не может быть задействована 2. Составить и обосновать систему допусков и грифов секретности для двух состояний системы: Состояние I – Подготовка (разработка) документа «Стратегия выхода предприятия на новый уровень». Состояние II – Документ «Стратегия выхода предприятия на новый уровень» утвержден и введен в действие.	отделенные от решения – 3 балла Решение не дано или дано неверное решение – 0 баллов
Базовый, **Уметь** формировать политики безопасности компьютерных систем и сетей.	1. Множество уровней контроля достоверности определено следующим образом: *A*={около научная пресса, нестрогий контроль, строгий контроль}. Представлены печатные издания: Известия академии наук России, Сборник научных трудов «Вестник ТвГУ», Сборник студенческих докладов, Журнал «Занимательная математика». Существуют три источника информации: Профессор, студент, учитель математики. Обосновать и составить систему уровней достоверности, грифов достоверности объектов доступа и матрицу доступа ***A***. **2.** Ввести административные роли: старший офицер безопасности, офицер безопасности. а) Определить значение функций can-assign() и can-revoke() для административных ролей. б) Определить значения функций $can\text{-}assign_a$, $can\text{-}revoke_a$ для административных ролей. с) Определить значение функции can-modify() для административных ролей.	Имеется полное верное решение, включающее правильный ответ – 5 балла В решении имеются лишние или неверные записи, не отделенные от решения – 3 балла Решение не дано или дано неверное решение – 0 баллов
Базовый, **Знать** виды политик безопасности компьютерных систем, модели безопасности компьютерных систем, критерии безопасности и условия применения	1. Пусть имеется система иерархически организованных ролей ***V***. Ролям назначены полномочия из конечного множества. Определить полномочия роли $\mathbf{v_1}$ и роли $\mathbf{v_3}$. $P(v_0)=\{p_7\}$, $P(v_1)=\{p_3\}$, $P(v_2)=\{p_2,p_4\}$, $P(v_3)=\{p_5\}$, $P(v_4)=\{p_8\}$, $P(v_5)=\{p_6,p_8\}$, $P(v_6)=\{p_8\}$, $P(v_7)=\{p_1\}$, $P(v_8)=\{p_2\}$, $P(v_9)=\{p_6\}$, $P(v_{10})=P(v_{11})=\{p_1\}$.	Имеется полное верное решение, включающее правильный ответ – 5 балла В решении имеются лишние или неверные записи, не отделенные от решения – 3 балла

моделей безопасности		Решение не дано или дано неверное решение – 0 баллов

V. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины (или модуля)

а) Основная литература

Богульская, Н. А. Модели безопасности компьютерных систем : учебное пособие / Н. А. Богульская, М. М. Кучеров. — Красноярск : СФУ, 2019. — 206 с. — ISBN 978-5-7638-4008-7. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/157578

Пушкарёв, В. В. Защита информационных процессов в компьютерных системах : учебное пособие / В. В. Пушкарёв, В. П. Пушкарёв. — Москва : ТУСУР, 2012. — 131 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/4925

Информационная безопасность и защита информации: Учебное пособие. / Баранова Е.К., Бабаш А.В. — 3-е изд., перераб. и доп. — М.: РИОР: ИНФРА-М, 2017. — 322 с. — (Высшее образование). [Электронный ресурс]. – Режим доступа: http://znanium.com/go.php?id=763644

б) Дополнительная литература:

Щербаков, А. Современная компьютерная безопасность. Теоретические основы. Практические аспекты : учебное пособие / А. Щербаков. – Москва : Книжный мир, 2009. – 352 с. – (Высшая школа). – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=89798

Петров А.А. Компьютерная безопасность. Криптографические методы защиты [Электронный ресурс]/ А.А. Петров.— Электрон. текстовые данные.— Саратов: Профобразование, 2017.— 446 с.— Режим доступа: http://www.iprbookshop.ru/63800.html

VI. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. 1. ЭБС Лань https://e.lanbook.com/ Договор № 4-е/23 от 02.08.2023 г.

2. 2. ЭБС Znanium.com https://znanium.com/ Договор № 1106 эбс от 02.08.2023 г.
3. 3. ЭБС Университетская библиотека online https://biblioclub.ru Договор № 02-06/2023 от 02.08.2023 г.
4. 4. ЭБС ЮРАЙТ https://urait.ru/ Договор № 5-е/23 от 02.08.2023 г.
5. 5. ЭБС IPR SMART https://www.iprbookshop.ru/ Договор № 3-е/23К от 02.08.2023г.
6. 6. https://cyberleninka.ru/ научная электронная библиотека «Киберленинка».
7. 7. Научная электронная библиотека eLIBRARY.RU (подписка на журналы) https://elibrary.ru/projects/subscription/rus_titles_open.asp;
8. 8. Репозитарий ТвГУ http://eprints.tversu.ru
9. Библиотека информационной безопасности
10. Библиотека сетевой безопасности
11. Компьютерная безопасность: уязвимости, ошибки и эксплоиты
12. Построение безопасности в сетях
13. openPGP в России
14. Защита информации

VII. Методические указания для обучающихся по освоению дисциплины

Требования к рейтинг-контролю

Модуль 1.

Максимальная сумма баллов по модулю – 50, из них 30 баллов отводится на текущий контроль учебной работы студента, 20 баллов на рубежный контроль по модулю.

Текущая работа студента складывается из ответов в аудитории и подготовке сообщений, min – 0 баллов, max - 3 баллов.

Рубежный контроль проводится в форме контрольной работы.

Модуль 2.

Максимальная сумма баллов по модулю – 50, из них 30 баллов отводится на текущий контроль учебной работы студента, 20 баллов на рубежный контроль по модулю.

Текущая работа студента складывается из ответов в аудитории и подготовке сообщений, min – 0 баллов, max - 3 баллов.

Рубежный контроль проводится в форме контрольной работы.

Вопросы для подготовки к зачету

1. Безопасность информации. Безопасности функций КС.

2. Угрозы безопасности в компьютерных системах. Классификация методов защиты информации в компьютерных системах. Основные критерии оценки надежности.

3. Принципы политики безопасности. Виды политики безопасности.

4. Модель матрицы доступов HRU. Элементарные операторы. Безопасность системы HRU.

5. Модель распространения прав доступа TAKE – GRANT. Команды модели TAKE – GRANT. Санкционированное получение прав доступа.

6. Похищение прав доступа в модели TAKE – GRANT.

7. Расширенная модель TAKE-GRANT. Де-факто правила расширения модели Take-Grant.

8. Построение замыкания графа доступов и информационных потоков.

9. Алгоритм построения tg-замыкания.

10. Алгоритм построения де-юре-замыкания.

11. Алгоритм построения де-факто-замыкания. Определение стоимости путей

12. Модель Белла – ЛаПадулы. Основные правила, гарантирующих безопасность. Основная теорема безопасности.

13. Модель Кена Биба. Основные правила, гарантирующих безопасность.

14. Модель систем военных сообщений. Постулаты безопасности модели MMS. Неформальные свойства модели MMS.

15. Базовая модель Ролевого Разграничения Доступа (РРД).

16. Модель администрирования РРД. Администрирование множеств авторизованных ролей пользователей. Администрирование множеств прав доступа, которыми обладают роли. Администрирование иерархии ролей.

17. Модели безопасности на основе тематической политики. Основные способы тематической классификации. Тематические решетки: при дескрипторной тематической классификации и при иерархической тематической классификации.

18. Модель тематико-иерархического разграничения доступа. Критерий безопасности.

19. Правила санкционированных переходов системы с помощью монитора безопасности объектов (МБО).

20. Субъектно – ориентированная модель изолированной программной среды.

21. Стандарты в информационной безопасности.

VIII. Перечень педагогических и информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (или модулю), включая перечень программного обеспечения и информационных справочных систем (по необходимости)

Преподавание учебной дисциплины строится на сочетании лекций, практических занятий и различных форм самостоятельной работы студентов.

Программное обеспечение:

Google Chrome	бесплатно
Kaspersky Endpoint Security 10 для Windows	Акт на передачу прав ПК545 от 16.12.2022
Lazarus	бесплатно
OpenOffice	бесплатно
Многофункциональный редактор ONLYOFFICE бесплатное ПО	бесплатно
ОС Linux Ubuntu бесплатное ПО	бесплатно

IX. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине

Учебная аудитория с мультимедийной установкой (Ноутбук, проектор, колонки), наличие классной доски. Для организации самостоятельной работы класс ПЭВМ.

.

X. Сведения об обновлении рабочей программы дисциплины (или модуля)

№ п.п.	Обновленный раздел рабочей программы дисциплины (или	Описание внесенных изменений	Дата и протокол заседания кафедры, утвердившего изменения

	модуля)		
1.	Вся рабочая программа	Приведена в соответствие с новым стандартом и новым шаблоном	
2.			