Министерство науки и высшего образования РФ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Национальный исследовательский университет «МЭИ»

«УТВЕРЖДАЮ»
Проректор по научной работе
д.т.н. проф. _____ Драгунов В.К.
«23» декабря 2022 г.

РАБОЧАЯ ПРОГРАММА
специальной дисциплины 1.2.4. Кибербезопасность
профиль: Кибербезопасность объектов критической информационной инфраструктуры

Москва 2022

Программа составлена на основе паспорта специальности научных работников и программы - минимум кандидатского экзамена по специальности «Кибербезопасность» в действующей редакции и в соответствии с Положением о подготовке научных и научно- педагогических кадров в аспирантуре (адьюнктуре), утвержденным постановлением Правительства Российской Федерации от 30 ноября 2021г. № 2122.

ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целью изучения дисциплины является подготовка к сдаче кандидатского экзамена по направленности (специальности) 1.2.4 – Кибербезопасность.

Задачами дисциплины является приобретение общих сведений и навыков в следующих научно-технических областях.

1. Изучение научных основ анализа уязвимостей и разработка современных методов поиска новых классов уязвимостей, методов проектирования, моделирования, анализа, трансформации программ для выявления потенциальных уязвимостей в программных системах.
2. Освоение механизмов и разработка алгоритмов моделирования политик информационной безопасности, оценки угроз безопасности информации и формирования сценариев компьютерных атак.
3. Изучение и применение методов, алгоритмов и средств анализа защищенности программно-аппаратного обеспечения.
4. Изучение и разработка научных методов интеграции средств защиты на уровне аппаратуры и на уровне программного обеспечения, а также методов, алгоритмов и средств обеспечения устойчивого функционирования программно-аппаратных систем.
5. Разработка масштабируемых способов мониторинга инцидентов информационной безопасности и средств интеллектуального анализа данных и процессов.
6. Научное обоснование разработки методических основ формирования метрик оценки защищенности, определения уровня доверия к компьютерным системам и совершенствования стандартов в области кибербезопасности.

МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ПРОГРАММЫ АСПИРАНТУРЫ

Специальная дисциплина в структуре программы аспирантуры входит в Блок 2 «Образовательный компонент. Общая трудоемкость составляет 7 зачетных единиц (з.е.).

Формула специальности

нет

Области исследований

1. Анализ известных и вновь выявляемых уязвимостей, их систематизация, разработка методов интеллектуального поиска новых классов уязвимостей.

2. Моделирование политик информационной безопасности, угроз и атак, методические основы разработки профилей защиты.

3. Методы проектирования, моделирования, анализа, трансформации программ для выявления потенциальных уязвимостей в программных системах с учетом специфики фаз жизненного цикла: разработки требований, проектирования архитектуры, разработки программного кода, тестирования, верификации, сертификации и эксплуатации.

4. Методы, алгоритмы и средства пострелизного глубокого анализа защищенности программно-аппаратного обеспечения.

5. Методы интеграции средств защиты на уровне аппаратуры и на уровне программного обеспечения.

6. Методы, алгоритмы и средства обеспечения устойчивого функционирования программно-аппаратных систем в условиях злонамеренного воздействия включая методы обфускации и безопасной компиляции программ.

7. Интеллектуальный масштабируемый мониторинг инцидентов безопасности в распределенных программно-аппаратных системах, методы оперативного реагирования на выявленные угрозы.

8. Масштабируемые средства интеллектуального анализа данных и процессов в распределенных системах, включая социальные сети.

9. Разработка методических основ для создания и развития метрик оценки защищенности, уровня доверия компьютерных систем и стандартов в области кибербезопасности.

Отрасль науки

– физико-математические науки

Технологии анализа рисков информационной безопасности

Понятие «риск информационной безопасности» и методы оценки его параметров.

Методы представления оценок показателей рисков информационной безопасности.

Оценка ценности информационных активов. Понятие «информационный

актив» и методы его представления. Методы оценки ценности активов. Моделирование и анализ информационных активов.

Моделирование угроз. Понятие «угроза информационной безопасности». Описательное моделирование. Параметрические модели описания угроз. Методы оценки возможного ущерба.

Моделирование уязвимостей. Модель уязвимости в концепции ГОСТ Р 56545-2015. Модель уязвимости в концепции ГОСТ Р ИСО/МЭК 27005. Обобщенная модель угроз и уязвимостей.

Методика оценки угроз безопасности информации согласно методического документа ФСТЭК от 5 февраля 2021 г.

Методология моделирования рисков информационной безопасности.

Основные цели и задачи моделирования рисков информационной безопасности.

Анализ существующих подходов к моделированию рисков информационной безопасности. Процессы управления рисками в концепции стандарта ГОСТ Р ИСО/МЭК 27005. Установление контекста организации. Анализ рисков информационной безопасности. Оценка рисков. Обработка рисков. Коммуникация рисков. ГОСТ Р ИСО/МЭК 31010-2011 Менеджмент риска. Методы оценки риска.

Информационные технологии моделирования рисков информационной безопасности. Алгоритм обработки рисков в концепции цифровой экономики.

Имитационная модель определения влияния стратегии управления рисками на эффективность систем информационной безопасности.

Безопасность информационных технологий

Основные требования безопасности информационных технологий. Подходы к разработке критериев оценки безопасности информационных технологий. (Зарубежный опыт). Подходы к разработке критериев оценки безопасности информационных технологий. (Зарубежный опыт). Единые критерии оценки безопасности информационных технологий.

Стандарты серии ГОСТ Р ИСО/МЭК 15408 «Общие критерии». Систематизированные каталоги функциональных компонент безопасности и доверия к безопасности информационных технологий. Общая модель критериев оценки безопасности информационных технологий.

Критерии оценки безопасности информационных технологий. Функциональные компоненты безопасности. Функциональные компоненты безопасности.

Критерии оценки безопасности информационных технологий. Компоненты доверия к безопасности. Компоненты доверия к безопасности информационных технологий.

Практическое применение «Общих критериев» оценки безопасности информационных технологий. Практическое применение подходов «Общих» критериев при разработке задания по безопасности для конкретного класса информационных технологий

Методология оценки безопасности информационных технологий.

Стандарт ГОСТ Р 57628-2017 Информационная технология. Методы и средства обеспечения безопасности Руководство по разработке профилей защиты и заданий по безопасности.

Стандарт ГОСТ Р ИСО/МЭК 18045-2013 Информационная технология. Методы и средства обеспечения безопасности.

Методология оценки безопасности информационных технологий. Минимум действий, выполняемых оценщиком при проведении оценки по ИСО/МЭК 15408 с использованием критериев и свидетельств оценки, определенных в ИСО/МЭК 15408. Процесс оценки и соответствующие задачи, требования и методология оценки профиля защиты, объекта оценки и задания по безопасности. Описание архитектуры безопасности. Исследование и оценка «Описания архитектуры безопасности».

Методы и средства контроля эффективности защищенности компьютерных систем

Методы анализа и оценки защищенности компьютерных систем.

Методы, критерии и шкалы оценки защищенности (безопасности) компьютерных систем

Понятие измерения величин и оценки объектов как отображения множеств с отношениями. Процесс измерения (оценки) и шкала измерения (оценки). Точные измерения и измерения с погрешностями. Типы шкал (шкалирования) - номинальные шкалы, порядковые (ранговые) шкалы, шкалы интервалов, шкалы отношений, шкалы разностей и абсолютные шкалы.

Многомерное оценивание сложных объектов и его целевые разновидности - определение сравнительного предпочтения объектов, определение сходства и различия объектов, типизация (классификация и группирование) объектов. Матрица "Объекты-признаки". Снижение размерности пространства признаков путем их агрегирования в оценочные факторы для определения предпочтений. Расстояния в пространстве признаков для определения схожести объектов. Сгущения в пространстве признаков и выделение классов (группирование) объектов.

Оценка защищенности (безопасности) компьютерных систем как задача многомерного шкалирования свойств КС в аспекте безопасности. Иерархический (древовидный) характер системы критериев анализа КС (параметров, свойств, функций), обеспечивающих составляющие безопасности (конфиденциальность, целостность и доступность информации). Номинальный или иной (порядковый, абсолютный и т.д.) характер шкалирования параметров, свойств и функций безопасности КС. Безопасность (защищенность) компьютерных систем как обобщенный (абстрактный) фактор, агрегирующий результаты оценки параметров, свойств и функций безопасности. Порядковое (ранговое) шкалирование компьютерных систем в аспекте безопасности на основе группирования (классификации) в пространстве шкалирования первичных факторов оценки.

Примеры многомерных номинально-ранговых систем оценки защищенности компьютерных систем, закрепленные в стандартах безопасности.

Теоретико-графовые модели комплексной оценки защищенности компьютерных систем.

Теоретико-графовая модель систем защиты с полным перекрытием (угроз) на основе двудольного графа "Угрозы-Объекты". Модель Клементса.

Разновидности теоретико-графового подхода к моделированию систем комплексной оценки защищенности в виде трехдольных ("Угрозы-Средства/МерыЗащиты-Объекты" и взвешенных графов (взвешенность вершин-объектов по ценности, взвешенность вершин " Средств/мер защиты" по стоимости осуществления, взвешенность дуг "угрозы-объекты" по вероятности реализации угроз, взвешенность дуг "средства/меры_защиты-угрозы" по степени снижения вероятности реализации угроз). Векторно-матричное представление взвешенного графа "Угрозы-Средства/МерыЗащиты-Объекты".

Технико-экономическое обоснование (анализ) систем защиты. Критерий эффективности как отношение величины снижения потенциального ущерба от реализации угроз при выбранных средствах/мерах защиты к сумме стоимости объектов защиты и стоимости задействования средств/мер защиты. Выражения для вычисления критерия технико-экономической эффективности на основе векторно-матричного представления графа "Угрозы-Средства/МерыЗащиты-Объекты".

Тактико-техническое обоснование систем защиты. Критерий эффективности как вероятности преодоления системы защиты и его вычисление на основе взвешенного графа "Угрозы-Средства/МерыЗащиты-Объекты".

Проблемы методов и шкал оценки ценности (стоимости) объектов, стоимости защитных мер, вероятности реализации угроз. Ранговые шкалы оценки рисков от реализации угроз безопасности.

Методы анализа и оптимизации индивидуально-групповых систем разграничения доступа.

Проблемы проектирования (синтеза) и анализа систем индивидуально-группового доступа.

Теоретико-графовая формализация (модель) систем индивидуально-группового назначения пользователям (субъектам доступа) прав доступа к иерархически организованным ресурсам (объектам доступа). Матричное выражение графа индивидуально-групповых назначений доступа.

Матричные соотношения для вычисления итоговых прав доступа. Коэффициенты дублирования прав доступа, превышения и недостатка прав доступа как количественные параметры оптимизации систем индивидуально-группового доступа и их матричные выражения.

Методы проектирования системы рабочих групп пользователей - "сверху" (по организационно-функциональной структуре коллектива пользователей) и "снизу" (по схожести индивидуальных потребностей пользователей в правах доступа к объектам). Выражение для вычисления меры близости пользователей по требуемым правам доступа.

Мера близости рабочих групп пользователей по составу пользователей и итоговым правам доступа с учетом вхождения одних рабочих групп в другие и иерархической организации объектов доступа как параметр оптимизации систем индивидуально-группового доступа.

Теоретические основы компьютерной безопасности

Модуль 1. Содержание и основные понятия компьютерной безопасности

История развития теории и практики обеспечения компьютерной безопасности. Понятия "информационная безопасность" и компьютерная безопасность. Безопасность информации в компьютерных системах и ее составляющие - конфиденциальность, целостность и правомерная доступность (сохранность) информации.

Субъекты и объекты безопасности. Угрозы безопасности. Нарушители безопасности.

Общие принципы обеспечения компьютерной безопасности.

Систематика методов и механизмов обеспечения компьютерной безопасности. Методы и механизмы, непосредственно обеспечивающие конфиденциальность, целостность и доступность информации — разграничение доступа к данным, контроль, управления информационной

структурой данных, установление и контроль ограничений целостности данных, шифрование данных, механизмы ЭП данных в процессах их передачи и хранения, защита/удаление остаточной информации на носителях данных и в освобождаемых областях оперативной памяти.

Методы и механизмы общеархитектурного характера — идентификация/аутентификация пользователей, устройств, данных, управление памятью, потоками, изоляция процессов, управление транзакциями.

Методы и механизмы инфраструктурного характера — управление (контроль) конфигурацией, управление сеансами, управление удаленным доступом с рабочих станций, управление сетевым соединениями, управление инфраструктурой сертификатов криптоключей.

Методы и механизмы обеспечивающего (профилактирующего) характера — протоколирование и аудит событий, резервирование данных, журнализация процессов изменения данных, профилактика, учет и контроль использования носителей данных, нормативно-организационная регламентация использования КС, обучение, нормативно-административное побуждение и принуждение пользователей по вопросам информационной безопасности КС.

Угрозы безопасности в компьютерных системах

Понятие угрозы. Угрозы безопасности информации в компьютерных системах.

Понятия "идентификация", "аутентификация", "авторизация", "спецификация", "классификация", "категорирование" и "каталогизация".

Классификационные схемы (каталогизация) угроз. Теоретические (формальные) основы классификации — критерии выделения и таксономия классов (алгебраическая полнота в операциях пересечения и объединения классов). Примеры и проблемы теоретического обоснования каталогов угроз по зарубежным, отечественным и международным стандартам.

Идентификация и спецификация (описание) угроз — выявление угрозы определенного типа и присвоение ей уникального идентификатора, определение и описания источника (природы) угрозы, активов/объектов, подверженных воздействию угрозы, способов и особенностей реализации/осуществления.

Общая схема оценивания угроз — оценка реализации угрозы и оценка ущерба от реализации угрозы. Оценка рисков, методы и шкалы оценки. Методы экспертной оценки вероятности реализации и/или степени опасности угроз.

Человеческий фактор в угрозах безопасности и модель нарушителя

информационной безопасности.

Политика и модели безопасности в компьютерных системах

Понятие политики безопасности. Модель безопасности как формализованное выражение политики безопасности. Модель безопасности как основа архитектурных, схемотехнических и программно-алгоритмических решений при создании защищенных КС, анализа систем защиты информации в КС.

Составляющие модели безопасности — модель (формализация) компьютерной системы в аспекте безопасности информации, критерии, формализованные правила, алгоритмы, механизмы безопасного функционирования КС.

Класс моделей конечных состояний. Компьютерная система как автомат (процесс) с дискретным временем функционирования.

Теоретико-множественная субъектно-объектная формализация (модель) компьютерной системы. Понятие субъекта и объекта, потока информации и доступа субъекта к объекту, методов и прав доступа, разграничения доступа.

Основные типы политик безопасности — дискреционная, мандатная, тематическая, ролевая, временная, маршрутная.

Программно-техническая структура компьютерной системы в контексте безопасности. Понятие и функции монитора (ядра) безопасности. Требования к монитору безопасности. Монитор безопасности объектов (монитор ссылок) и монитор безопасности субъектов (монитор приложений).

Гарантирование выполнения политики безопасности. Тождественность объектов и тождественность субъектов доступа (неизменность свойств). Модель и теоремы гарантирования безопасности (по Щербакову). Изолированная программная среда.

Модуль 2. Модели безопасности компьютерных систем

Модели безопасности на основе дискреционной политики

Общая характеристика политики дискреционного доступа. Тройки доступа: субъект-операция-объект. Модели дискреционного (избирательного) разграничения доступа и модели распространения прав доступа.

Пятимерное пространство Хартсона как пример выражения дискреционного разграничения доступа на языке реляционной алгебры.

Модели разграничения доступа на основе матрицы доступа. Принудительный и добровольный принцип управления доступом. Администраторы системы и владельцы объектов. Привилегии и предоставление (распространение) прав доступа. Способы организации информационной структуры матрицы доступа — централизованная структура (системные таблицы доступа в реляционных СУБД, биты доступа в ОС UNIX)

и децентрализованная структура (списки доступа объектов в ОС Windows).

Модель распространения прав доступа Харисона-Руззо-Ульмана. Примитивные операции и команды изменения матрицы доступа. Монотонные, монооперационные и одноусловные системы. Теорема безопасности Харисона-Руззо-Ульмана для монооперационных систем и в общем случае. Троянские программы. Сценарий атаки троянской программой в нотации модели ХарисонаРуззо-Ульмана.

Модель типизованной матрицы доступа как расширение модели Харисона-Руззо-Ульмана и способ разрешения проблемы троянских программ. Типы субъектов и объектов. Родительские и дочерние типы. Граф отношений (порождений) наследственности. Теорема безопасности для ацикличных реализаций систем на основе типизованной матрицы доступа.

Теоретико-графовая модель TAKE-GRANT для исследования распространения прав доступа в системах с добровольным управлением доступом. Специфичные права субъектов доступа take и grant. Граф доступа. Примитивные операции (команды), изменяющие состояние графа доступа. tg-связность вершин графа доступа, "острова" и "мосты" в графе доступа. Условия и теорема возможности санкционированного получения субъектом прав доступа на какой-либо объект. Условия и теорема возможности несанкционированного получения субъектом прав доступа на какой-либо объект ("похищения" прав доступа).

Расширенная (extended) модель TAKE-GRANT. Неявные (вероятностные) каналы утечки информации и "мнимые" дуги в графе доступов. Примитивные (элементарные) команды преобразования графа доступов для генерации мнимых дуг (команды де-факто). Графовые пути возможностей утечки информации по графу доступа.

Модели безопасности на основе мандатной политики

Общая характеристика политики мандатного (полномочного) доступа. Парадигма градуированного доверия пользователям (субъектам доступа) и градуированной степени конфиденциальности данных (объектов доступа). Уровни безопасности субъектов и объектов доступа. Правила безопасного мандатного доступа — запрет чтения вверх (NRU) и запрет записи вниз (NWD). Рефрексивность, антисимметричность и транзитивность отношений доступа. Функция уровня безопасности субъектов и объектов доступа. Решетка уровней безопасности. Классы безопасных информационных потоков и матрица доступа.

Модель безопасности Белла-ЛаПадулы. Критерий безопасного состояния системы. Функция перехода системы из одного состояния в другое. Основная теорема безопасности (теорема безопасности БеллаЛаПадулы).

Недостатки и "абстрактность" систем на основе модели Белла-ЛаПадулы (Z-системы и др.).

Расширения модели Белла-ЛаПадулы. Безопасная функция перехода МакЛина и теорема безопасности МакЛина, разрешение проблемы Z-системы. Уполномоченные (доверенные) субъекты и авторизованная функция перехода МакЛина. Групповые субъекты доступа. Модель совместного доступа МакЛина. Правила безопасного доступа NRU и NWD для групповых субъектов.

Другие расширения модели Белла-ЛаПадулы. Модель Low-WaterMark.

Модели безопасности на основе тематической политики

Общая характеристика политики тематического доступа. Тематическое классификационное множество и ее разновидности. Способы тематической классификации субъектов и объектов доступа на основе дескрипторных, иерархических и фасетных классификационных множеств. Критерии безопасности информационных потоков в системах тематического разграничения доступа.

Тематические решетки на основе классификационных множеств. Решетка подмножеств множества тематических рубрик при дескрипторной классификации. Тематическая решетка на корневом дереве рубрикатора при монорубрицированной иерархической классификации и ее изоморфный вариант в виде решетки листовых подмножеств.

Тематические мультирубрики при мультирубрицированной иерархической классификации субъектов и объектов доступа. Алгебра (решетка) мультирубрик. Отношения доминирования мультирубрик, операции (механизмы) наименьшей верхней и наибольшей нижней границ мультирубрик.

Модель тематико-иерархического разграничения доступа в системах с мультирубрицированной тематической классификацией субъектов и объектов доступа.

Модели безопасности на основе ролевой политики

Общая характеристика политики ролевого (типизованного) доступа. Роль как типовой субъект доступа (функционально обособленное агрегирование прав доступа и полномочий выполнения процедур над данными). Две фазы организации ролевого доступа — создание ролей как типовых субъектов доступа с наделением их правами (полномочиями) доступа на основе дискреционной, мандатной, тематической или иной политики безопасности и назначение ролей пользователям. Сеансовый характер функционирования компьютерной системы с ролевым доступом. Сеансовая авторизация пользователя с одной или группой назначенных ему в системе

ролей и доступ к объектам системы в соответствующей (соответствующих) роли (ролях).

Разновидности ролевых систем по отношениям ролей, принципам назначения ролей пользователям и сеансовой авторизации пользователей с назначенными ролями.

Системы с иерархической организацией ролей, с взаимоисключающими в системе ролями (статическое распределение обязанностей), с взаимоисключающими в рамках одного сеанса ролями (динамическое распределение обязанностей) и др. Способы наделения правами доступа ролей (ролевых субъектов доступа) в системах с иерархической организацией ролей.

Модель индивидуально-группового доступа. Отличия рабочих групп от ролей. Теоретикомножественная формализация индивидуально-группового доступа.

MMS-модель (military message system) Лендвера-МакЛина как пример сочетания дискреционной, мандатной и ролевой политики безопасности.

Модуль 3. Формальные методы и механизмы безопасности компьютерных систем

Автоматные и теоретико-вероятностные модели информационного невлияния и информационной невыводимости

Понятие и общая характеристика скрытых каналов утечки информации. Скрытые каналы " по памяти", скрытые каналы " по времени", статистические скрытые каналы (" по статистике"). Примеры реализации скрытых каналов утечки информации. Понятие емкости (пропускной способности) скрытых каналов передачи данных.

Автоматная модель информационного невлияния Гогена-Мессигера. Функция истории вводов и функция очищения. Модель Гогена-Мессигера как теоретико-методологическая база интерфейса защищенных КС в аспекте устранения (перекрытия) скрытых каналов утечки информации "по времени".

Теоретико-вероятностная трактовка информационного потока (по К.Шеннону). Модели информационной невыводимости и информационного невлияния как теоретико-методологическая основа анализа (выявления) и перекрытия скрытых каналов "по памяти" и "по статистике". Теоретико-вероятностная трактовка автоматной модели Гогена-Мессигера.

Технологии представлений (views) в реляционных СУБД как пример реализации подходов информационной невыводимости и информационного невлияния.

Модели и механизмы обеспечения целостности данных

Понятие целостности данных и общая характеристика методов и механизмов обеспечения целостности данных.

Дискреционная модель обеспечения целостности данных Кларка-Вильсона. Объекты, требующие контроля целостности (constrained data items), процедуры проверки целостности (integrity verification procedures), корректно сформированные транзакции (не нарушающие ограничения целостности), тройки "субъект-транзакция-объект".

Мандатная модель К.Биба. Уровни целостности данных. Уровни доверия пользователям. Правила мандатного доступа, не нарушающие целостность данных (запрет "чтения вниз", запрет " записи вверх") как инверсия правилам мандатного доступа, не нарушающим конфиденциальность данных (в модели БеллаЛападулы).

Проблемы и разновидности совместимости в практической реализации моделей Белла-ЛаПадулы и К.Биба: на основе двух разных решеток безопасности (отдельных систем уровней конфиденциальности и целостности), на основе одной общей решетки, но с двумя отдельными метками для объектов и субъектов (на чтение, на запись).

Транзакционная парадигма коллективной (одновременной) обработки данных в клиент-серверных системах. Принципы "атомарности" (неделимости), "изоляции" транзакций. Нарушения целостности, возникающие при совместной обработке данных, одновременном (параллельном) выполнении транзакций пользователей. Понятие и виды "грязных" (dirty) данных - "грязное чтение" (dirty read), "потерянные изменения" (lost update) и "неповторяющееся чтение" (unrepeatable read). Протоколы выполнения и фиксации транзакций.

Протоколы, основанные на "захватах" блокировках объектов. Двухфазной протокол выполнения и фиксации транзакций ("пессимистичный" режим выполнения транзакций). Тупики (Deadlock), их обнаружение и разрушение. Механизмы изоляции транзакций, основанные на временных метках объектов ("оптимистичный" режим выполнения транзакций).

Методы и технологии обеспечения доступности (сохранности) данных

Резервирование, архивирование и журнализация данных. Организационные, технологические и программно-технические принципы политики резервирования и архивирования БД.

Оперативное сохранение (журнализация) изменений данных. Восстановление данных из архивной копии и по журналу изменений данных. Синхронная и асинхронная журнализация. Полное и инкрементное сохранение измененных данных. Сценарии архивирования/журнализации.

Системы реального времени. "Горячее" резервирование. Главный/резервный серверы. "Прозрачность" для приложений. Автоматическое переключение серверов, "поднятие" " упавшего" сервера.

Системы репликации данных. Обеспечение непрерывности согласованного состояния данных, синхронная и асинхронная репликации. Программно-техническая структура систем репликации данных. Обеспечение непрерывности согласованного состояния структуры данных, системы с " главной" и частичными репликами.

Политика и модели безопасности в распределенных компьютерных системах

Понятие "распределенности" компьютерных систем в аспекте безопасности. Дополнительные аспекты политики безопасности в распределенных компьютерных системах.

Структура распределенных компьютерных систем в аспекте политики безопасности. Понятие локального сегмента и удаленного доступа субъекта к объектам. Локальная и общесетевая (общесистемная) политика безопасности. Субъект (субъекты) реализации политики безопасности в распределенных компьютерных системах.

Модель безопасности Варахаратжана. Фазы доступа.

Зональная политика безопасности и ее теоретико-множественное формализация (модель). Внутризональные и межзональные (общесистемные) аспекты политики безопасности. Доверительные отношения зон безопасности (локальных сегментов с обособленным монитором безопасности). Реализация зонально-межзональных принципов политики безопасности в распределенных компьютерных системах на примере доменно-групповой архитектуры сетей на основе ОС Windows.

Методы и средства защиты информации в условиях информационного противоборства

Основы теории информационного противоборства.

Методы информационного противоборства. Концепции и цели информационного противоборства. Модели и методы информационного противоборства. Информационная война.

Технические средства, применяемые в информационном противоборстве. Информационное оружие. Средства, применяемые в качестве информационного оружия в информационном противоборстве. Основные цели информационного противоборства. Модели и методы информационного противоборства. Информационная война. Определение информационного оружия. Средства, применяемые в качестве информационного оружия в информационном противоборстве, их классификация.

Методы защиты информации, реализуемые специальными СЗИ.

Методы защиты информации, реализуемые СЗИ от НСД. Методы ограничения доступа и управления доступом. Замкнутая программная среда, управление доступом к устройствам, контроль целостности, контроль аппаратной конфигурации, регистрация событий безопасности, контроль работоспособности, дополнительные функции СЗИ. Реализация требований по защите информации с помощью СЗИ контроля доступа. СЗИ от НСД, реализующие методы защиты информации. Типовые функции.

Методы защиты информации, реализуемые средствами защиты от вредоносного программного обеспечения. Статические и динамические способы защиты информации. Методы борьбы с воздействием вредоносного программного обеспечения. Защита от изменения и контроль целостности. Создание доверенной программной среды. Защита от изменения и контроль целостности.

Методы защиты информации, реализуемые СЗИ, обеспечивающими безопасное межсетевое взаимодействие. Реализация требований по защите информации с помощью средств обеспечения безопасного межсетевого взаимодействия. Трансляция сетевых адресов. Фильтрация сетевого трафика. Применение криптографических методов защиты информации. Управление доступом.

Методы защиты информации, реализуемые средствами контроля и предотвращения утечек информации. Контроль содержимого информации. Применение цифровых отпечатков. Лингвистические и статистические методы контроля. Контроль содержания графической информации. Реализация требований по защите информации с помощью средств контроля и предотвращения утечек информации.

Методы и средства, применяемые для контроля и оценки эффективности функционирования СЗИ. Методы контроля и оценки эффективности функционирования программных СЗИ. Программно-аппаратные средства, применяемые для контроля и оценки эффективности.

Защита информации в виртуальных инфраструктурах.

Технологии виртуализации. Виртуализация: термины и определения. Виды виртуализации, классификация видов виртуализации. Основные компоненты среды виртуализации. Основные платформы виртуализации. Механизмы защиты информации, реализуемые платформами виртуализации

Методы и средства защиты информации, применяемые для защиты виртуальных инфраструктур. Методы защиты виртуальных инфраструктур, реализуемые платформами виртуализации, встроенные механизмы безопасности. Специальные СЗИ, применяемые для защиты виртуальных

инфраструктур. Реализация требований по ЗИ с помощью средств защиты виртуальных инфраструктур.

Методы защиты информации, реализуемые в операционных системах.

Методы защиты информации, реализуемые ОС общего назначения. Механизмы обеспечения ИБ, реализованные в ОС общего назначения: идентификация и аутентификация, парольные системы, управление доступом, политики безопасности.

Методы защиты информации, реализуемые специализированными ОС. Сертифицированные защищенные ОС. Механизмы обеспечения ИБ, реализованные в защищенных ОС.

Технологии и методы защиты информационных систем от кибератак

Методологические основы защиты от кибератак.

Основы защиты информационных систем от кибератак. Введение в защиту от кибератак. Понятие атаки на компьютерные системы. Классификация уязвимостей и кибератак. Примеры кибератак на компьютерные системы. База данных CVE и CWE. Ретроспектива киберинцидентов в России и мире. Описание реальных реализаций кибератак: WannaCry, Stuxnet, NonPetya, Mirai, BEC, Zeus, Lazarus (атаки группировки), Industroyer, Cobalt, Dark Hotel, Turla (атаки группировки), DarkVishnya, KoffeyMaker.

Модель угроз и модель нарушителя информационной безопасности в типовых информационных системах. Модель оценки угроз ФСТЭК России. Цели злоумышленника. Квалификация злоумышленника. Основной инструментарий киберпреступника.

Структура кибератаки на информационную систему объекта информатизации. Кибератаки на корпоративные информационные системы компаний (КИС). Типовая структура КИС с точки зрения безопасности. Типовые сценарии атак на КИС: преодоление периметра (Сценарий 1. Подбор учетных данных;сценарий; Сценарий 2. Эксплуатация веб-уязвимостей; Сценарий 3. Эксплуатация известных уязвимостей; Сценарий 4. Социальная инженерия; Сценарий 5. Открытые данные; Сценарий 6. Выход из песочницы) и получение контроля над КИС (Сценарий 1. Подбор доменной учетной записи; Сценарий 2. Атаки на протоколы сетевого и канального уровней; Сценарий 3. Атака SMB Relay; Сценарий 4. Чтение памяти процесса; Сценарий 5. Групповые политики; Сценарий 6. Золотой билет Kerberos; Сценарий 7. Pass the hash и pass the ticket. Атака на двухфакторную аутентификацию). Типовые защитные меры от кибератак на КИС.

Атаки на промышленные предприятия (АСУ ТП). Типовая структура АСУ ТП с точки зрения безопасности. Примеры кибератак на АСУ ТП. Типовые защитные меры. Разработка защитных мер для предприятия АСУ ТП на основе созданной модели нарушителя.

Обнаружение кибератак на информационные системы. Технология анализа атак на информационные системы. Методы обнаружения атак (признаки компрометации систем). Средства обнаружения атак (системы обнаружения вторжений). Технологии анализа атак (этапы, необходимая информация, средства, техники и тактики сценарии атак).

Кибератаки на информационные системы. DoS/DDoS. Понятие DoS/DDoS атаки, их особенность. Технология обнаружения атаки. Методы и средства защиты от DDoS. Вводная информация по темам предстоящих докладов: Детальный разбор методов и средств обнаружения и защиты от DoS/DDoS атак.

Кибератаки на информационные системы с использованием социальной инженерии. Понятие социальной инженерии, примеры. Технология обнаружения атаки. Методы и средства защиты от социальной инженерии. Методы социальной инженерии (фишинг, претекстинг и т.д.).

Структура кибератаки на веб-приложения и ресурсы сети "Интернет". Выявление и эксплуатация SQL-инъекций в приложениях. Причины возникновения SQL-инъекций. Техники, применяемые при эксплуатации SQLинъекций. Процесс обнаружения и эксплуатации SQL-инъекций.

Защита веб-приложений от инъекций команд. Характеристика основ внедрения опасных команд. Методы обнаружения внедрения опасных команд. OWASP CheatSheet.

Защита веб-приложений от атак типа XSS. Общее понятие XSS. Виды XSS. Контексты выполнения. Common Weakness Enumeration.

Меры предотвращения stored и reflected XSS. CSRF. SSRF. Меры предотвращения stored и reflected XSS. Меры предотвращения DOM-based XSS. Использование CSP.

Применение подхода DevSecOps в современных системах разработки программного обеспечения. Понятие DevSecOps. Организация фаззинга исходного кода. Сравнение некоторых SCA.

Математические модели защиты информационных систем.

Вопросы, включенные в билеты для проведения экзамена, а также для самоконтроля:

1. Понятие «риск информационной безопасности».

2. Методы оценки параметров риска информационной безопасности.
3. Методы представления оценок показателей рисков информационной безопасности.
4. Оценка ценности информационных активов.
5. Понятие «информационный актив».
6. Методы оценки ценности активов.
7. Моделирование и анализ информационных активов.
8. Моделирование угроз.
9. Параметрические модели описания угроз.
10. Методы оценки возможного ущерба.
11. Модель уязвимости в концепции ГОСТ Р 56545-2015.
12. Модель уязвимости в концепции ГОСТ Р ИСО/МЭК 27005.
13. Методика оценки угроз безопасности информации согласно методического документа ФСТЭК от 5 февраля 2021 г.
14. Методология моделирования рисков информационной безопасности.
15. Основные цели и задачи моделирования рисков информационной безопасности.
16. Процессы управления рисками в концепции стандарта ГОСТ Р ИСО/МЭК 27005.
17. Анализ рисков информационной безопасности. Оценка рисков. Обработка рисков. Коммуникация рисков.
18. Управление рисками в концепции стандарта ГОСТ Р ИСО/МЭК 31010-2011 Менеджмент риска. Методы оценки риска.
19. Информационные технологии моделирования рисков информационной безопасности.
20. Алгоритм обработки рисков в концепции цифровой экономики.
21. Имитационная модель определения влияния стратегии управления рисками на эффективность систем информационной безопасности.
22. Подходы к разработке критериев оценки безопасности информационных технологий.
23. Подходы к разработке критериев оценки безопасности информационных технологий.
24. Единые критерии оценки безопасности информационных технологий.
25. Общая модель критериев оценки безопасности информационных технологий. в концепции стандарта ГОСТ Р ИСО/МЭК 15408 «Общие критерии».

26. Критерии оценки безопасности информационных технологий. Функциональные компоненты безопасности. Функциональные компоненты безопасности.

27. Критерии оценки безопасности информационных технологий. Компоненты доверия к безопасности. Компоненты доверия к безопасности информационных технологий.

28. Методология оценки безопасности информационных технологий в концепции стандарта ГОСТ Р ИСО/МЭК 18045-2013 Информационная технология. Методы и средства обеспечения безопасности.

29. Методология оценки безопасности информационных технологий используемая оценщиком при проведении оценки по ГОСТ Р ИСО/МЭК 15408 с использованием критериев и свидетельств оценки, определенных в ИСО/МЭК 15408.

30. Методы анализа и оценки защищенности компьютерных систем.

31. Методы, критерии и шкалы оценки защищенности (безопасности) компьютерных систем

32. Понятие измерения величин и оценки объектов как отображения множеств с отношениями. Процесс измерения (оценки) и шкала измерения (оценки).

33. Многомерное оценивание сложных объектов и его целевые разновидности - определение сравнительного предпочтения объектов, определение сходства и различия объектов, типизация (классификация и группирование) объектов.

34. Оценка защищенности (безопасности) компьютерных систем как задача многомерного шкалирования свойств КС в аспекте безопасности.

35. Иерархический (древовидный) характер системы критериев анализа компьютерных систем (параметров, свойств, функций), обеспечивающих составляющие безопасности (конфиденциальность, целостность и доступность информации).

36. Безопасность (защищенность) компьютерных систем как обобщенный (абстрактный) фактор, агрегирующий результаты оценки параметров, свойств и функций безопасности.

37. Теоретико-графовая модель систем защиты с полным перекрытием (угроз) на основе двудольного графа "Угрозы-Объекты". Модель Клементса.

38. Тактико-техническое обоснование систем защиты. Критерий эффективности как вероятности преодоления системы защиты и его вычисление на основе взвешенного графа "Угрозы-Средства/МерыЗащиты-Объекты".

39. Проблемы методов и шкал оценки ценности (стоимости) объектов,

стоимости защитных мер, вероятности реализации угроз. Ранговые шкалы оценки рисков от реализации угроз безопасности.

40. Методы анализа и оптимизации индивидуально-групповых систем разграничения доступа.

41. Проблемы проектирования (синтеза) и анализа систем индивидуально-группового доступа.

42. Безопасность информации в компьютерных системах и ее составляющие - конфиденциальность, целостность и правомерная доступность (сохранность) информации.

43. Субъекты и объекты безопасности. Угрозы безопасности. Нарушители безопасности.

44. Общие принципы обеспечения компьютерной безопасности.

45. Систематика методов и механизмов обеспечения компьютерной безопасности.

46. Методы и механизмы, непосредственно обеспечивающие конфиденциальность, целостность и доступность информации (общеархитектурного. инфраструктурного, профилактирующего).

47. Угрозы безопасности в компьютерных системах

48. Классификационные схемы (каталогизация) угроз. Теоретические (формальные) основы классификации — критерии выделения и таксономия классов (алгебраическая полнота в операциях пересечения и объединения классов.

49. Идентификация и спецификация (описание) угроз.

50. Общая схема оценивания угроз.

51. Понятие политики безопасности. Модель безопасности как формализованное выражение политики безопасности.

52. Модель безопасности, как основа архитектурных, схемотехнических и программно-алгоритмических решений при создании защищенных компьютерной системы.

53. Составляющие модели безопасности — модель (формализация) компьютерной системы в аспекте безопасности информации, критерии, формализованные правила, алгоритмы, механизмы безопасного функционирования КС.

54. Основные типы политик безопасности — дискреционная, мандатная, тематическая, ролевая, временная, маршрутная.

55. Понятие и функции монитора (ядра) безопасности. Требования к монитору безопасности. Монитор безопасности объектов (монитор ссылок) и монитор безопасности субъектов (монитор приложений).

56. Модель и теоремы гарантирования безопасности (по Щербакову).

Изолированная программная среда.

57. Общая характеристика политики дискреционного доступа. Тройки доступа: субъект-операция-объект.

58. Модели дискреционного (избирательного) разграничения доступа и модели распространения прав доступа.

59. Пятимерное пространство Хартсона как пример выражения дискреционного разграничения доступа на языке реляционной алгебры.

60. Модели разграничения доступа на основе матрицы доступа. Принудительный и добровольный принцип управления доступом.

61. Модель распространения прав доступа Харисона-Руззо-Ульмана. Примитивные операции и команды изменения матрицы доступа. Монотонные, монооперационные и одноусловные системы.

62. Теорема безопасности Харисона-Руззо-Ульмана для монооперационных систем и в общем случае.

63. Троянские программы. Сценарий атаки троянской программой в нотации модели ХарисонаРуззо-Ульмана.

64. Модель типизованной матрицы доступа как расширение модели Харисона-Руззо-Ульмана и способ разрешения проблемы троянских программ.

65. Теоретико-графовая модель TAKE-GRANT для исследования распространения прав доступа в системах с добровольным управлением доступом.

66. Расширенная (extended) модель TAKE-GRANT.

67. Модели безопасности на основе мандатной политики

68. Общая характеристика политики мандатного (полномочного) доступа.

69. Правила безопасного мандатного доступа.

70. Рефрексивность, антисимметричность и транзитивность отношений доступа.

71. Модель безопасности Белла-ЛаПадулы. Критерий безопасного состояния системы.

72. Расширения модели Белла-ЛаПадулы. Безопасная функция перехода МакЛина и теорема безопасности МакЛина, разрешение проблемы Z-системы.

73. Общая характеристика политики тематического доступа. Тематическое классификационное множество и ее разновидности.

74. Способы тематической классификации субъектов и объектов доступа на основе дескрипторных, иерархических и фасетных классификационных множеств.

75. Критерии безопасности информационных потоков в системах

тематического разграничения доступа.

76. Модель тематико-иерархического разграничения доступа в системах с мультирубрицированной тематической классификацией субъектов и объектов доступа.

77. Общая характеристика политики ролевого (типизованного) доступа. Роль как типовой субъект доступа (функционально обособленное агрегирование прав доступа и полномочий выполнения процедур над данными).

78. Разновидности ролевых систем по отношениям ролей, принципам назначения ролей пользователям и сеансовой авторизации пользователей с назначенными ролями.

79. Системы с иерархической организацией ролей, с взаимоисключающими в системе ролями (статическое распределение обязанностей), с взаимоисключающими в рамках одного сеанса ролями (динамическое распределение обязанностей) и др.

80. Модель индивидуально-группового доступа.

81. MMS-модель (military message system) Лендвера-МакЛина как пример сочетания дискреционной, мандатной и ролевой политики безопасности.

82. Автоматные и теоретико-вероятностные модели информационного невлияния и информационной невыводимости

83. Автоматная модель информационного невлияния Гогена-Мессигера.

84. Теоретико-вероятностная трактовка информационного потока (по К.Шеннону).

85. Модели и механизмы обеспечения целостности данных. Понятие целостности данных и общая характеристика методов и механизмов обеспечения целостности данных.

86. Дискреционная модель обеспечения целостности данных Кларка-Вильсона.

87. Мандатная модель Биба. Уровни целостности данных. Уровни доверия пользователям. Правила мандатного доступа, не нарушающие целостность данных.

88. Методы и технологии обеспечения доступности (сохранности) данных. Резервирование, архивирование и журнализация данных. Организационные, технологические и программно-технические принципы политики резервирования и архивирования БД.

89. Оперативное сохранение (журнализация) изменений данных. Восстановление данных из архивной копии и по журналу изменений данных. Синхронная и асинхронная журнализация. Полное и инкрементное сохранение

измененных данных. Сценарии архивирования/журнализации.

90. Системы реального времени. "Горячее" резервирование. Главный/резервный серверы. "Прозрачность" для приложений. Автоматическое переключение серверов, "поднятие" " упавшего" сервера.

91. Системы репликации данных. Программно-техническая структура систем репликации данных. Обеспечение непрерывности согласованного состояния структуры данных, системы с " главной" и частичными репликами.

92. Политика и модели безопасности в распределенных компьютерных системах

93. Структура распределенных компьютерных систем в аспекте политики безопасности.

94. Модель безопасности Варахаратжана. Фазы доступа.

95. Зональная политика безопасности и ее теоретико-множественное формализация (модель).

96. Доверительные отношения зон безопасности (локальных сегментов с обособленным монитором безопасности). Реализация зонально-межзональных принципов политики безопасности в распределенных компьютерных системах на примере доменно-групповой архитектуры сетей на основе ОС Windows.

97. Методы ограничения доступа и управления доступом. Идентификация и аутентификация.

98. Методы ограничения доступа и управления доступом. Дискреционное управление доступом.

99. Методы ограничения доступа и управления доступом. Мандатное управление доступом.

100. Методы ограничения доступа и управления доступом. Ролевое управление доступом.

101. Структура и функции программно–аппаратных средств обеспечения информационной безопасности.

102. Основные принципы создания средств защиты информации.

103. Концепция построения программно–аппаратных средств обеспечения информационной безопасности.

104. Типовая структура и функции СЗИ от НСД.

105. Современные СЗИ от НСД и их применение для ЗИ в УИП

106. Разрушающие программные воздействия. Определение. Классификация. Основные функции.

107. Разрушающие программные воздействия. Методы и средства защиты от разрушающих программных воздействий.

108. Сертифицированные средства антивирусной защиты

109. Методы ЗИ, применяемые для обеспечения безопасного межсетевого взаимодействия

110. СЗИ, применяемые для обеспечения безопасного межсетевого взаимодействия

111. Общая характеристика систем контроля и предотвращения утечек информации. Контролируемые каналы утечки информации.

112. Типовые функциональные возможности. Анализ информации при контроле каналов передачи. Применяемые технологии.

113. Системы контроля и предотвращения утечек информации. Типовая структура. Основные компоненты.

114. Системы контроля и предотвращения утечек информации. Концепция применения. Основные стадии применения.

115. Классификация видов виртуализации.

116. Структура платформы виртуализации. Основные компоненты.

117. Угрозы безопасности виртуальной инфраструктуры.

118. Механизмы безопасности, реализуемые платформами виртуализации.

119. Специальные СЗИ, применяемые для защиты виртуальных инфраструктур.

120. Методы контроля и оценки эффективности функционирования программных СЗИ.

121. Программно-аппаратные средства, применяемые для контроля и оценки эффективности.

122. Защитные механизмы, реализованные в типовых ОС общего назначения.

123. Защитные механизмы, реализованные в сертифицированных защищенных ОС.

124. Методологические основы защиты от кибератак.

125. Основы защиты информационных систем от кибератак

126. Классификация уязвимостей и кибератак. База данных CVE и CWE.

127. Модель угроз и модель нарушителя информационной безопасности в типовых информационных системах.

128. Структура кибератаки на информационную систему объекта информатизации.

129. Кибератаки на корпоративные информационные системы компаний.

130. Типовые сценарии атак на корпоративную информационную систему.

131. Типовые защитные меры от кибератак на корпоративную информационную систему.

132. Тиковые кибератаки на промышленные предприятия (АСУ ТП).

133. Защитные меры от кибератак для предприятия АСУ ТП на основе созданной модели нарушителя.

134. Методы обнаружения кибератак (признаки компрометации систем). Средства обнаружения атак (системы обнаружения вторжений).

135. Технологии анализа атак (этапы, необходимая информация, средства, техники и тактики сценарии атак).

136. Кибератаки DoS/DDoS на информационные системы Технология обнаружения атаки. Методы и средства защиты от DDoS.

137. Кибератаки на информационные системы с использованием социальной инженерии (фишинг, претекстинг и т.д.). Методы и средства защиты от социальной инженерии. Методы социальной инженерии

138. Структура кибератаки на веб-приложения и ресурсы сети "Интернет".

139. Выявление и эксплуатация SQL-инъекций в приложениях.

140. Причины возникновения SQL-инъекций. Техники, применяемые при эксплуатации SQLинъекций. Процесс обнаружения и эксплуатации SQL-инъекций.

141. Защита веб-приложений от инъекций команд. Характеристика основ внедрения опасных команд. Методы обнаружения внедрения опасных команд. OWASP CheatSheet.

142. Защита веб-приложений от атак типа XSS. Общее понятие XSS. Виды XSS. Контексты выполнения. Common Weakness Enumeration.

143. Меры предотвращения stored и reflected XSS. CSRF. SSRF.

144. Меры предотвращения stored и reflected XSS.

145. Меры предотвращения DOM-based XSS. Использование CSP.

146. Применение подхода DevSecOps в современных системах разработки программного обеспечения. Организация фаззинга исходного кода. Сравнение некоторых SCA.

147. Математические модели защиты информационных систем.

ПРОМЕЖУТОЧНАЯ АТТЕСТАЦИЯ ПО ДИСЦИПЛИНЕ

Промежуточная аттестация проводится в форме экзамена.

Требования и критерии оценивания ответов экзамена

В процессе экзамена оценивается уровень научно-исследовательской компетентности аспиранта, что проявляется в квалифицированном представлении результатов обучения.

При определении оценки учитывается грамотность представленных ответов, стиль изложения и общее оформление, способность ответить на поставленный вопрос по существу.

Критерии выставления оценки на экзамене:

Оценка «ОТЛИЧНО» выставляется аспиранту, который показал при ответе на вопросы экзаменационного билета и на дополнительные вопросы, что владеет материалом изученной дисциплины, свободно применяет свои знания для объяснения различных явлений и решения задач.

Оценка «ХОРОШО» выставляется аспиранту, в основном правильно ответившему на вопросы экзаменационного билета и на дополнительные вопросы, но допустившему при этом непринципиальные ошибки.

Оценка «УДОВЛЕТВОРИТЕЛЬНО» выставляется аспиранту, который в ответах на вопросы экзаменационного билета допустил существенные и даже грубые ошибки, но затем исправил их сам

Оценка «НЕУДОВЛЕТВОРИТЕЛЬНО» выставляется аспиранту, который:

а) не ответил на вопросы экзаменационного билета

б) при ответе на дополнительные вопросы обнаружил незнание большого раздела экзаменационной программы.

Данные критерии указаны Инструктивном письмом И-23 от 14 мая 2012 г.

УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Основная литература:

1. ГОСТ Р 51897-2011/Руководство ИСО 73:2009 Менеджмент риска. Термины и определения.

2. ГОСТ Р ИСО 31000-2019 Менеджмент риска. Принципы и руководство.

3. МЭК 31010:2019 «Менеджмент риска. Технологии оценки риска» (IEC 31010:2019 «Risk management — Risk assessment techniques». NEQ).

4. ГОСТ Р 58771-2019/ Менеджмент риска. Технологии оценки риска.

5. ГОСТ Р 51901.7-2017. Менеджмент риска. Руководство по внедрению ИСО 31000

6. Информационная технология. Методы и средства обеспечения информационной безопасности. Менеджмент риска информационной безопасности. ГОСТ Р ИСО/МЭК 27005-2010.

7. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология. ГОСТ Р ИСО/МЭК 27000-2012.

8. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования ГОСТ Р ИСО/МЭК 27001-2021.

9. Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил мер обеспечения информационной безопасности ГОСТ Р ИСО/МЭК 27002-2021.

10. Доктрина информационной безопасности Российской Федерации (утверждена Указом Президента РФ № 646 от 5 декабря 2016 г.).

11. Приказ ФСТЭК России № 17 от 11 февраля 2013 г «Специальные требования и рекомендации по технической защите конфиденциальной информации».

12. Приказ Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 года № 21 "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных".

13. Приказ ФСТЭК России от 14 марта 2014 г. N 31 «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды».

14. Методический документ. Методика оценки угроз безопасности информации. Утвержден ФСТЭК России 5 февраля 2021 г.

15. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка). ФСТЭК России, 2008 год.

16. Объект информатизации. Факторы, воздействующие на информацию. ГОСТ Р 51275—2006.

17. Петренко С. А. Управление информационными рисками. Экономически оправданная безопасность / Петренко С. А., Симонов С. В. - М.: Компания АйТи ; ДМК Пресс, 2004. - 384 с.: ил. - (Информационные технологии для инженеров).

18. Система менеджмента качества. Требования. ГОСТ ИСО 9001-2015.

19. COBIT 5: Бизнес-модель по руководству и управлению ИТ на предприятии: http://www.isaca.org/COBIT/Pages/COBIT-5-russian.aspx

20. Ингланд Роб Овладевая ITIL / Пер. с англ. — М.: Лайвбук, 2011. — 200 с.

21. ГОСТ Р ИСО/МЭК 15408-1-2012 — Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель.

22. ГОСТ Р ИСО/МЭК 15408-2-2013 — Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности.

23. ГОСТ Р ИСО/МЭК 15408-3-2013 — Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности.

24. Нечеткое моделирование и управление [Электронный ресурс] / А. Пегат ; пер. с англ. — 2-е изд. (эл.). — М. : БИНОМ. Лаборатория знаний, 2013. — 798 с. : ил. — (Адаптивные и ин- теллектуальные системы)

25. Дюбуа Д., Прад А. Теория возможностей. Приложения к представлению знаний в информатике: Пер. с фр. - М.: Радио и связь, 1990. - 288 с.

26. Стандарт Банка России: «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0 — 2014» (СТО БР ИББС-1.2-2014).

27. ФСТЭК Приказ от 11 февраля 2013 г. №17. «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах.

28. ФСТЭК Приказ от 18 февраля 2013 г. №21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»

29. ФСТЭК Приказ от 14 марта 2014 г. №31 «Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственным и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни».

30. ГОСТ Р 57580.1-2017 — «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер».

31. ГОСТ Р 57580.2-2018 — «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Методика оценки соответствия».

32. Атаманов Г. А. Азбука безопасности. Информационные вызовы, риски и угрозы //Защита информации. Инсайд. – 2014. – №. 1. – С. 6-12.

33. Минзов А.С. Методология применения терминов и определений в сфере информационной, экономической и комплексной безопасности бизнеса : уч.– мет. Пособие . – М. : ВНИИгеосистем, 2011, – 84 с. : ил.

34. ГОСТ Р 56545-2015 Защита информации. Уязвимости информационных систем. Правила описания уязвимостей. Утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 19 августа 2015 г. №1180-ст

35. ГОСТ Р 56546-2015 Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем. Утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 19 августа 2015 г. №1181-ст

36. Малюк, А. А. Введение в защиту информации в автоматизированных системах / А.А. Малюк, С.В. Пазизин, Н.С. Погожин. - М.: Горячая линия - Телеком, 2011. - 146 с.

37. Мельников В.П., Клейменов С.А., Петраков А.М. Информационная безопасность и защита информации Учебное пособие для студентов учреждения высшего профессионального образования. — 6-е изд., стер. — М.: Академия, 2012. — 330 с. — ISBN: 978-5-7695-9222-

38. Чипига А. Ф. Информационная безопасность автоматизированных систем: учебное пособие для студентов высших учебных заведений, обучающихся по специальности 090105 - "Комплексное обеспечение информационной безопасности автоматизированных систем" / А. Ф. Чипига. - Москва : Гелиос АРВ, 2010. - 334, [1] с. : ил., табл.; 24 см.; ISBN 978-5-85438-183-3

39. Щербаков А.Ю. Современная компьютерная безопасность. Теоретические основы. Практические аспекты. – М.: Высшая школа, 2009. – 352 с.

40. Грушо А.А., Применко Э.А., Тимонина Е.Е. Теоретические основы компьютерной безопасности. – М.: Академия, 2009.

41. Хорев П.Б. Прогаммно-аппаратная защита информации. – М.: Форум, 2009.

42. Роберт Ларсон, Жаник Карбон. Платформа виртуализации Hyper-V. Ресурсы Windows Server 2008. – СПб.: Русская Редакция, БХВ-Петербург, 2010. – 800 стр.

43. К. Кусек, В. Ван Ной, А. Дэниел. Администрирование VMware vSphere 5. Для профессионалов – СПБ.: Питер, 2013. – 384 стр.

44. Михеев М.О. Администрирование VMware vSphere 5. – М.: ДМК Пресс, 2012. – 504 стр.

45. Леандро Карвальо. Windows Server 2012 Hyper-V. Книга рецептов. – М.: ДМК Пресс, 2013. – 302 стр.

46. Расторгуев С.П. Математические модели в информационном противоборстве. Экзистенциальная математика. — М.: АНО ЦСОиП, 2014. — 260 с.

47. Марков А.С. Технические решения по реализации подсистем ГосСОПКА. В книге: Управление информационной безопасностью в современном обществе. СборникнаучныхтрудовVМеждународнойнаучно-практическойконференции.2017. С.85-96.

48. Петренко А.С., Петренко С.А. Проектирование корпоративного сегмента СОПКА.Защита информации. Инсайд. 2016. N 6 (72). С. 28-30.

49. Бегаев А.Н., Бегаев С.Н., Федотов В.А. Тестирование на проникновение. СПб.: Университет ИТМО, 2018. - 45 с.

50. Бирюков Д.Н., Ломако А.Г., Петренко С.А. Порождение сценариев предупреждения компьютерных атак.Защита информации. Инсайд. 2017. N 4 (76). С. 70-79.

51. Дорофеев А.В., Лемберская Е.Х., Рауткин Ю.В. Анализ защищенности: нормативная база, методологии и инструменты.Защита информации. Инсайд. 2018. N 4 (82). С. 63-69.

52. Жуков И.Ю., Михайлов Д.М., Шеремет И.А. Защита автоматизированных систем от информационно-технологических воздействий. М.: МИФИ, 2014. - 176 с.

53. Макаренко С.И. Критерии и показатели оценки качества тестирования на проникновение. Вопросы кибербезопасности. 2021. N 3 (43). С. 43-57.

54. Dorofeev A. V., Rautkin Y. V. Applied Aspects of Security Testing. In CEUR Workshop Proceedings, 2017, Vol-2081 (Selected Papers of the VIII All-Russian Scientific and Technical Conference on Secure Information Technologies, BIT 2017), pp. 49-53.

55. Макаренко С.И. Аудит безопасности критической инфраструктуры специальными информационными воздействиями. Монография. - СПб.: Наукоемкие технологии, 2018. - 122 с.

56. Марков А.С. Летописи кибервойн и величайшего в истории перераспределения богатства.Вопросы кибербезопасности. 2016. N 1 (14). С. 68-74.

57. Марков А.С., Фадин А.А. Организационно-технические проблемы защиты от целевых вредоносных программ типа Stuxnet.Вопро-сы кибербезопасности. 2013. N 1 (1). С. 28-36.

58. Басан Е.С., Басан А.С., Макаревич О.Б., Бабенко Л.К. Исследование влияния активных сетевых атак на группу мобильных робо-тов.Вопросы кибербезопасности. 2019. N 1 (29). С. 35-44.

59. Бойко А.А. Боевая эффективность кибератак: аналитическое моделирование современного боя.Системы управления, связи и безопасности. 2020. N 4. С. 101-133.

60. Васильев В.И., Кириллова А.Д., Вульфин А.М. Когнитивное моделирование вектора кибератак на основе меташаблонов CAPEC. Вопросы кибербезопасности. 2021. N 2 (42). С. 2-16.

61. Дергунов И.Ю., Зима В.М., Глыбовский П.А., Мажников П.В. Модель процесса интеллектуального тестирования АС на проникновение с учетом временных параметров.Защита информации. Инсайд. 2020. N 5 (95). С. 64-67.

62. Добрышин М.М., Закалкин П.В. Модель компьютерной атаки типа «phishing» на локальную компьютерную сеть.Вопросы кибербезопасности. 2021. N 2 (42). С. 17-25.

63. Дроботун Е.Б. Теоретические основы построения систем защиты от компьютерных атак для автоматизированных систем управления. Монография. - СПб.: Наукоемкие технологии, 2017. - 120 с., ил. ISBN 978-5-9909412-2-9.

64. Климов С.М. Имитационные модели испытаний критически важных информационных объектов в условиях компьютерных атак.. Известия ЮФУ. Технические науки. 2016. N 8(181) С. 27-36. DOI 10.18522/2311-3103-2016-8-2736.

65. Котенко Д.И., Котенко И.В., Саенко И.Б. Методы и средства моделирования атак в больших компьютерных сетях: состояние проблемы, Тр. СПИИРАН, 22 (2012), 5-30.

66. Коцыняк М.А., Лаута О.С., Иванов Д.А. Математическая модель таргетированной компьютерной атаки.Наукоемкие технологии в космических исследованиях Земли. 2019. Т. 11. N 2. С. 73-81. DOI: 10.24411/2409-5419-2018-10261.

67. Лаута О.С., Коцыняк М.А., Иванов Д.А., Гудков М.А. Моделирование компьютерных атак на основе метода преобразования стохастических сетей.В сборнике: Радиолокация, навигация, связь. Сборник трудов XXIV Международной научно-технической конференции. В 5-и томах. 2018. С. 137-146.

68. Чечулин А.А. Построение и анализ деревьев атак на компьютерные сети с учетом требования оперативности. Диссертация. -Санкт-Петербург, 2013. - 152 с. : ил. Методы и системы защиты информации, информационная безопасность. Хранение: 61 14-5/933.

69. Dorofeev A.V., Markov A.S., Rautkin Y.V. Ethical Hacking Training.CEUR Workshop Proceedings. - Vol. 2522. P. 47-56.

70. . Садердинов А. А. Информационная безопасность предприятия : учеб. пособие / Садердинов, Али Абдулович ; В.А.Трайнёв, А.А.Федулов; Междунар. акад. наук информации, информ. процессов и технологий. - 3-е изд. - М. : Дашков и К, 2006. - 335 с. - ISBN 5-94798-918-2 : 154-00.

71. Шаньгин В. А. Информационная безопасность компьютерных систем и сетей : учеб. пособие для студентов учреждений сред. проф. образования, обуч. по группе специальностей 2200 "Информатика и вычислительная техника" / Шаньгин, Владимир Фёдорович. - М. : ФОРУМ: ИНФРА-М, 2008. - 415 с. - (Профессиональное образование). - Рекомендовано МО РФ. - 194-92.

72. Галатенко В. А. Основы информационной безопасности : учеб. пособие для студентов вузов, обуч. по специальности 351400 "Прикл. информ." / Галатенко, Владимир Антонович. - 4-е изд. - М. : Изд-во Интернет-Ун-та Информ. Технологий: БИНОМ. Лаб. знаний, 2016, 2008, 2006. - 205 с. - (Основы информационных технологий). - Рекомендовано УМО. - ISBN 978-5-94774-821-5 : 230-00.

73. Герман О. Н. Теоретико-числовые методы в криптографии : учеб. для студентов учреждений высш. проф. образования / Герман, Олег Николаевич, Ю. В. Нестеренко. - М. : Академия, 2012. - 270,[1] с. - (Высшее профессиональное образование. Информатика и вычислительная техника). - ISBN 978-5-7695-6786-5 : 603-90.

Дополнительная литература:

1. Managing Information Security Risk Organization, Mission, and Information System View/ NIST Special Publication 800-39 http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf

2. Марков А., Цирлов В. Управление рисками – нормативный вакуум информационной безопасности. //Открытые системы – №8 – 2007.

3. Managing Information Security Risk: Organization, Mission, and Information System View/ NIST Special Publication 800-39. Computer Security Division Information Technology Laboratory National Institute of Standards and Technology Gaithersburg, MD 20899-8930, 2014.

4. Корченко А. Г., Иванченко Е. В., Казмирчук С. В. Интегрированное представление параметров риска //Захист інформації. – 2011. – Т. 13. – №. 1

(50).

5. Корченко А.Г. Анализ и определение понятия риска для его интерпретации в области информационной безопасности / Корченко А.Г., Иванченко Е.В., Казмирчук С.В. // Научно-технический журнал "Защита информации" – 2010. – №3. – С. 5-10.

6. Хорев П.Б. Методы и средства защиты информации в компьютерных системах. – М.: Академия, 2008.

7. Ложников П.С. Обеспечение безопасности сетевой инфраструктуры на основе операционных систем Microsoft : практикум / П. С. Ложников, Е. М. Михайлов. - Москва : Интернет-Ун-т информ. технологий : БИНОМ. Лаб. знаний, 2008. - 245 с.

8. Алексеев, В.М. Обеспечение информационной безопасности на жизненном цикле автоматизированных систем : учебное пособие / В. М. Алексеев, А. Г. Фатеев, М. Ю. Лупанов ; Федеральное агентство по образованию, Гос. образовательное учреждение высш. проф. образования "Пензенский гос. ун-т". - Пенза : Изд-во Пензенского гос. ун-та, 2009. - 290, с.

9. Прохода А.Н. Обеспечение интернет-безопасности. Практикум: Учебное пособие для вузов. – М.: Горячая линия–Телеком, 2007. С.- 142..

10. Шаньгин, В.Ф. Защита компьютерной информации. Эффективные методы и средства [Текст] : [учебное пособие] / Шаньгин В. Ф. - Москва : ДМК Пресс, 2010. - 544 с.

11. Казанцева С.Я.. Правовое обеспечение информационной безопасности : [учеб. пособие для вузов по специальностям 075200 "Компьютер. безопасность", 075500 "Комплекс. обеспечение информ. безопасности и автоматизир. систем", 075600 "Информ. безопасность телекоммуникац. систем" / С.Я.Казанцев и др.]; под ред. С.Я.Казанцева. - М. : Academia, 2005. - 239 с. : ил. ; 22 см. - (Высшее профессиональное образование. Информационная безопасность). - Библиогр.: с. 235-237. - Допущено УМО. - ISBN 5-7695-1209-1 : 129-47.

12. Панасенко С.П. Основы криптографии для экономистов : учеб. пособие / Панасенко, Сергей Петрович ; В.П.Батура; под ред. Л.Г.Гагариной. - М. : Финансы и статистика, 2005. - 173,[1] с. - ISBN 5-279-02938-6 : 120-00.

13. Душин В.К. Теоретические основы информационных процессов и систем : учебник / Душин В.К. - 2-е изд. - М. : Дашков и К, 2006. - 347,[1] с. : ил. - Рекомендовано МО РФ. - ISBN 5-94798-869-0 : 121-33.

14. Филин С.А. Информационная безопасность : учеб. пособие / Филин, Сергей Александрович. - М. : Альфа-Пресс, 2006. - 411 с. - ISBN 5-94280-163-0 : 129-03.

15. Расторгуев С.П. Основы информационной безопасности : учеб.

пособие для студентов вузов, обуч. по специальности "Компьютер. безопасность", "Комплекс. обеспечение информ. безопасности автоматизир. систем" и "Информ. безопасность телеком. систем" / Расторгуев, Сергей Павлович. - М. : Академия, 2007. - 186,[1] с. - (Высшее профессиональное образование. Информационная безопасность). - Допущено УМО. - ISBN 978-5-7695-3098-2 : 150-70.

16. Белов Е. Б. Основы информационной безопасности : [учеб. пособие для вузов] / Е. Б. Белов. - М. : Горячая линия - Телеком, 2006. - 544 с. - ISBN 5-93517-292-5 : 154-00.

17. Корнеев И.К. Защита информации в офисе : учебник / Корнеев, Игорь Константинович, Е. А. Степанов. - М. : Проспект, 2010. - 150-00.

18. Петров С.В. Информационная безопасность : учеб. пособие / С. В. Петров. - Новосибирск: М. : АРТА, 2012. - 439-77.

Лицензионное и свободно распространяемое программное обеспечение: *(программное обеспечение, на которое кафедра или МЭИ имеет лицензию, а также свободно распространяемое программное обеспечение)*

Интернет-ресурсы, включая профессиональные базы данных и информационные справочные системы:

Университетская информационная система «РОССИЯ» https://uisrussia.msu.ru

Справочно-правовая система «Консультант+» http://www.consultant-urist.ru

Справочно-правовая система «Гарант» http://www.garant.ru

База данных Web of Science https://apps.webofknowledge.com/

База данных Scopus https://www.scopus.com

Портал открытых данных Российской Федерации https://data.gov.ru

База открытых данных Министерства труда и социальной защиты РФ https://rosmintrud.ru/opendata

База данных Научной электронной библиотеки eLIBRARY.RU https://elibrary.ru/

База данных профессиональных стандартов Министерства труда и социальной защиты РФ http://profstandart.rosmintrud.ru/obshchiy-informatsionnyy-blok/natsionalnyy-reestr-professionalnykh-standartov/

База открытых данных Росфинмониторинга http://www.fedsfm.ru/opendata

Электронная база данных «Издательство Лань» https://e.lanbook.com

Федеральная государственная информационная система «Национальная электронная библиотека» https://нэб.рф

Национальный портал онлайн обучения «Открытое образование» https://openedu.ru

Электронная база данных "Polpred.com Обзор СМИ" https://www.polpred.com

Официальный сайт Федерального агентства по техническому регулированию и метрологии http://protect.gost.ru/

Электронная библиотека МЭИ https://ntb.mpei.ru/e-library/index.php.

База данных материалов об информационных технологиях и обеспечении ИБ http://www. cnews. ru.

База данных информационных материалов о средствах ИТ и средствах обеспечения ИБ http://www. servernews. ru.

Официальный сайт Федеральной службы по техническому и экспертному контролю http://www. fstec.ru.

Официальный сайт группы компаний Информзащита http:// www. infosec. ru .

Официальный сайт компании ООО «АМ Медиа», Аналитический центр Anti-Malware. Ru https://www. anti-malware. ru.

ПРОГРАММУ СОСТАВИЛ:

Доцент кафедры БИТ
к.т.н., доцент О.Р. Баронов

Зав. кафедрой ВМСС
к.т.н., доцент А.Ю. Невский

Директор ИнЭИ
к.т.н., доцент А.Ю. Невский