Программа учебной дисциплины
«Технология построения защищенных систем обработки информации»

Утверждена
Академическим советом ООП
Протокол № 2 от «19» апреля 2017 г.

Автор	Баранова Елена Константиновна
Число кредитов	6
Контактная работа (час.)	72
Самостоятельная работа (час.)	156
Курс	2 курс, магистерская программа: «Управление информационной безопасностью»
Формат изучения дисциплины	без использования онлайн курса

I. ЦЕЛЬ, РЕЗУЛЬТАТЫ ОСВОЕНИЯ ДИСЦИПЛИНЫ И ПРЕРЕКВИЗИТЫ

Целями освоения дисциплины «Технология построения защищенных систем обработки информации» является приобретение учащимися навыков и знаний в области обеспечения защиты информации на объекте информатизации; способность оценивать эффективность защиты, анализировать и оценивать риски информационной безопасности на объекте оценки и принимать эффективные управленческие решения при выборе проектов построения защищенных систем обработки информации.

В результате освоения дисциплины студент должен

знать:

- научные основы и методику работы с источниками информации;
- основные методики выявления и оценки угроз при построении защищенных информационных систем;
- методики анализа, оценки и управления рисками на объекте информатизации;
- методы концептуального проектирования защищенных систем обработки информации;
- современные методы обеспечения защиты информации на объекте информатизации на основе отечественных и международных стандартов;
- методы и средства проектирования, моделирования и экспериментальной отработки систем, средств и технологий обеспечения защиты информации в информационных системах;

уметь:

- организовывать работы по совершенствованию, модернизации и унификации технологий обеспечения защиты информации в информационных системах;
- применять современные программные инструментарии для моделирования угроз, анализа и оценки рисков информационной безопасности, а также использовать системы поддержки принятия решений при выборе эффективных проектов защиты;
- применять эффективные методы управления безопасностью информационных систем;

владеть:

- навыками организации работ по совершенствованию, модернизации, унификации систем, средств и технологий обеспечения защиты информации в соответствии с правовыми актами и нормативно-методическими документами.

Дисциплина «Технология построения защищенных систем обработки информации» относится к вариативной части блока дисциплин, обеспечивающих подготовку магистров по программе: «Управление информационной безопасностью».
Изучение данной дисциплины базируется на следующих дисциплинах:

- «Организационно-правовое обеспечение информационной безопасности»;
- «Методика и инструментарий моделирования бизнес-процессов»;
- «Экономико-математическое моделирование»;
- «Системный анализ и проектирование»;
- «Безопасность информации в государственном и частном секторах».

Для освоения учебной дисциплины, студенты должны владеть следующими знаниями и компетенциями:

- основами выявления рисков в системе обеспечения информационной безопасности предприятий государственного и частного сектора;
- применять понятийно-категориальный аппарат, основные законы гуманитарных и социальных наук в профессиональной деятельности;
- ориентироваться в системе рисков в сфере информационной безопасности и организационно-технических средств по их минимизации;
- использовать правовые нормы в профессиональной и общественной деятельности;
- защищать права на интеллектуальную собственность;
- владеть навыками философского мышления для выработки системного, целостного взгляда на проблемы общества;
- навыками публичной речи, аргументации, ведения дискуссии.

Основные положения дисциплины должны быть использованы в дальнейшем при подготовке выпускной квалификационной работы по магистерской программе: «Управление информационной безопасностью».

II. СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

Тема 1. Основные понятия, определения и проблемы в области построения защищенных систем обработки информации

Акуальность защиты систем обработки информации. Предпосылки кризиса обеспечения безопасности компьютерных систем. Основные регуляторы в сфере построения защищенных систем обработки информации.

Литература

1. Андрианов В.В., Зефиров С.Л., Голованов В.Б., Голдуев Н.А. - Обеспечение информационной безопасности бизнеса. – М.: Изд.центр “Альпина Паблишерз”, 2011.
2. Башлы П.Н., Бабаш А.В., Баранова Е.К. Информационная безопасность: учебно-практическое пособие. – М.: Изд.центр ЕАОИ, 2010.
3. Баранова Е.К., Бабаш А.В. Информационная безопасность и защита информации. – М.: РИОР: ИНФРА-М, 2018.
4. Руководящие документы ФСТЭК РФ. [Электронный ресурс] URL: http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty#

Тема 2. Обзор и сравнительный анализ стандартов в области защиты информационных систем

Критерии безопасности компьютерных систем министерства обороны США («Оранжевая книга»). Европейские критерии безопасности информационных технологий. Руководящие документы ФСТЭК в области построения защищенных систем обработки информации. Федеральные критерии безопасности информационных технологий. Обзор серии стандартов ИСО/МЭК 27000. Сравнительный анализ международных и национальных стандартов в области защиты информационных систем.

Литература

1. Грибунин В.Г., Чудовский В.В. Комплексная система защиты информации на предприятии – М.: Академия, 2009.
2. Руководящие документы ФСТЭК РФ. [Электронный ресурс] URL: http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty#

Тема 3. Исследование причин нарушений безопасности информационных систем

Нарушения безопасности информационных систем и уязвимости в системе защиты. Классификация уязвимостей системы защиты по источнику появления и по этапу возникновения. Классификация уязвимостей защиты по размещению в информационной системе. Результаты исследования таксономии уязвимостей и их практическое применение.

Литература

1. Баранова Е.К., Бабаш А.В. Информационная безопасность и защита информации. – М.: РИОР: ИНФРА-М, 2018.
2. Зегжда Д. П., Ивашко А.М. Основы безопасности информационных систем. , СПб, Горячая Линия – Телеком, 2012.
3. Шаньгин В.Ф. Комплексная защита информации в корпоративных системах. – М.: ИНФРА-М, 2010.

Тема 4. Анализ и оценка информационных рисков, угроз и уязвимостей информационной системы

Классификация и характеристика угроз информационной безопасности ИС. Методики и программный инструментарий для анализа и оценки рисков информационной безопасности. Современные программные комплексы для анализа рисков информационной безопасности: MSAT, RA2 art of risk, vsRisk – ISO 27001 и другие. Методология COBIT и программный инструментарий CORAS. Методология OCTAVE. Методы и программные продукты, используемые в международной практике для анализа и оценки рисков, угроз и уязвимостей информационной системы. Учет угроз и рисков при построении защищенной системы обработки информации. Особенности анализа и оценки рисков информационной безопасности в малом и среднем бизнесе. Управление инцидентами информационной безопасности. Основные задачи управления инцидентами информационной безопасности. Примеры международных стандартов в области управления инцидентами информационной безопасности.

Литература

1. Астахов А. Искусство управления информационными рисками. – М.: ДМК Пресс, 2010.
2. Баранова Е.К., Бабаш А.В. Информационная безопасность и защита информации. – М.: ИНФРА-М_РИОР, 2018.
3. Баранова Е.К., Бабаш А.В. Моделирование системы защиты информации. Практикум. – М.: РИОР: ИНФРА-М, 2016.
4. Баранова Е.К., Забродоцкий А.С. Процедура применения методологии анализа рисков OCTAVE в соответствии со стандартами серии ИСО/МЭК 27000-27005. – Вестник Московского университета им. С.Ю. Витте. Серия 3: Образовательные ресурсы и технологии. 2015, №3(11), С.73-77.
5. Баранова Е.К., Чернова М.В. Сравнительный анализ программного инструментария для анализа и оценки рисков информационной безопасности. – Проблемы информационной безопасности. Ком-

пьютерные системы. СПб. Институт информационных технологий и управления // под редакцией проф. Зегжды П.Д № 4, 2014 г. С.160-168.
6. Баранова Е.К., Зубровский Г.Б. Управление инцидентами информационной безопасности. Проблемы информационной безопасности / Труды I Международной научно-практической конференции "Проблемы информационной безопасности". Крымский федеральный университет им. В.И.Вернадского, 26-28 февраля 2015 г. С.27-33
7. The logic behind CRAMM's assessment of measures of risk and determination of appropriate countermeasures. [Электронный ресурс] URL: http://www.cramm.com/downloads/techpapers.htm
8. RiskWatch users manual. [Электронный ресурс] URL: http://www.riskwatch.com

Тема 5. Специальные методы моделирования, используемые при построении защищенных систем обработки информации

Схема воздействия угроз на информационную систему. Декомпозиция общей задачи оценки эффективности функционирования системы защиты. Макромоделирование. Модель элементарной, многозвенной и многоуровневой защиты. Модель "черного ящика". Описание модели безопасности с полным перекрытием множества угроз. Достоинства и недостатки модели безопасности с полным перекрытием, рекомендации по ее использованию. Примеры эффективного использования модели с полным перекрытием угроз и модели "куб безопасности" для построения системы защиты информации в организациях малого и среднего бизнеса.

Общие принципы построения модели "куб безопасности" в координатах: основы, направления, этапы. Достоинства и недостатки модели "куб безопасности" в координатах: основы, направления, этапы. Как оценить эффективность создаваемой или уже функционирующей СЗИ с использованием модели "куб безопасности" в координатах: основы, направления, этапы.

IDEF – методологии. Основные понятия, стандарты и назначение. IDEF0 – методология многофункционального моделирования. Основные элементы и правила построения диаграмм для процессов в системе защиты информации в ИС.

Графовые модели. Возможности использования сетей Петри для моделирования в системах защиты информации. Примеры построения сценария действий нарушителя на объекте информатизации с использованием сети Петри.

Литература

1. Баранова Е.К., Бабаш А.В. Моделирование системы защиты информации. Практикум.– М.: РИОР: ИНФРА-М, 2016.
2. Баранова Е.К., Бабаш А.В. Информационная безопасность и защита информации. – М.: ИНФРА-М_РИОР, 2018.
3. Советов Б.Я., Яковлев С.А. Моделирование систем. Учебник для вузов. М,: Высшая школа. 2011.
4. Шумский А.А. Системный анализ в защите информации: учеб.пособие для студентов вузов, обучающихся по специальностям в обл.информ.безопасности / А.А.Шумский, А.А.Шелупанов. – М.: Гелиос АРВ, 2010.

Тема 6. Методы принятия решений, используемые при выборе эффективных проектов защиты информации в информационной системе

Классификация задач и методов принятия решений. Принятие решений на основе метода анализа иерархий. Иерархическое представление проблемы. Структуризация задачи построения защищенной информационной системы в виде иерархии. Парное сравнение альтернатив (метод парных сравнений). Метод сравнения объектов относительно стандартов.

Методы принятия решений, основанные на исследовании операций. Рекомендации по практическому использованию различных методов принятия управленческих решений в сфере построения защищенных систем обработки информации.

Технология Data Mining, как процесс поддержки принятия решений, при построении защищенных систем обработки информации.

Особенности использования технологии оперативной аналитической обработки OLAP для визуализаций решений при проектировании защищенных систем обработки информации.

Литература

1. Баранова Е.К., Бабаш А.В. Информационная безопасность и защита информации. – М.: ИНФРА-М_РИОР, 2018.
2. Баранова Е.К., Бабаш А.В. Моделирование системы защиты информации. Практикум. – М.: РИОР: ИНФРА-М, 2016.
3. Барсегян А.А., Куприянов М.С., Степаненко В.В., Холод И.И. Технологии анализа данных. Data Mining, Visual Mining, Text Mining, OLAP (+CD). Учебное пособие, БХВ-Петербург, 2012.
4. Ногин В.Д.. Принятие решений при многих критериях. Учебно-методическое пособие. – СПб: Издательство «ЮТАС», 2011.
5. Розен В.В. Математические модели принятия решений в экономике. Учебное пособие. – М.: Книжный дом "Университет". Высшая школа, 2012.
6. Поддержка принятия решений при проектировании систем защиты информации: Монография / В.В.Бухтояров и др. – М.: ИНФРА-М, 2014.

Тема 7. Современные тенденции в области создания и эксплуатации центров обработки данных (ЦОД)

Место информационно-коммуникационных технологий (ИКТ) в современных экономических отношениях. ИКТ в деятельности предприятий. Технологии Arcnet, Token Ring, Ethernet. Протоколы TCP/IP. Конвергенция вычислительных сетей и сетей хранения данных. Передача данных внутри и между ЦОД. Особенности обеспечения защиты информации при использовании облачных сервисов. Технологии сетей хранения данных Fibre Channel, iSCSI, FCoE. Мониторинг и управление в вычислительных сетях.

Общие принципы организации системы хранения данных (СХД). Типы СХД: дисковые; ленточные (кассетные); флэш. Технологии хранения данных: с использованием аппаратного Redundant array of independent disks (RAID); с использованием программного RAID. Структура и организация RAID (Redundant Array of Independed Disks) – избыточных массивов независимых дисков. Устройства хранения: DAS; NAS; SAN. Разработчики СХД.

Литература

1. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. Учебник для вузов. – М.: РИОР: ИНФРА-М, 2014.
2. Вычислительные сети. Развитие ВС, их основные принципы, классификация. [Электронный ресурс] URL: http://csd.faculty.ifmo.ru/files/seti-wiki-book.pdf
3. Основы сетей передачи данных. [Электронный ресурс] URL: http://www.intuit.ru/studies/courses/1/1/info
   Fibre Channel and iSCSI Configuration Guide for the Data ONTAP 8.0 Release Family. [Электронный ресурс]
   URL: http://netappsky.com/wp-content/uploads/2010/12/fc_iscsi_config_guide_80.pdf
4. Storage Area Network Fundamentals; Gupta, Meeta; 2002; Cisco Press
5. Обработка и хранение информации. [Электронный ресурс] URL: http://www.intuit.ru/studies/courses/13860/1257/lecture/24002?page=1
6. Principles of SAN Design, Second Edition; Judd, Josh; 2007; Infinity Publishing

Тема 8. Сети хранения данных на базе интерфейса Fibre Channel

Сферы применения технологии Fibre Channel. Топологии Fibre Channel: точка-точка; кольцо с разделяемым доступом; коммутируемая связная архитектура. Структура и особенности протокола Fibre Channel. Различные устройства и компоненты, которые используются для создания сетей хранения данных Fibre Channel.

Обеспечение целостности и доступности данных. Планирование защиты данных. Методы и средства резервного копирования данных. Использование протокола NDMP (Network Data Management Protocol) для резервного копирования. Ленточные библиотеки для больших ЦОД. Защита данных средствами СХД: мгновенные снимки; клонирование; копирование; зеркалирование; синхронная и асинхронная репликация.

Литература

1. Fibre Channel and iSCSI Configuration Guide for the Data ONTAP 8.0 Release Family. [Электронный ресурс] URL: http://netappsky.com/wp-content/uploads/2010/12/fc_iscsi_config_guide_80.pdf
2. Interoperability Matrix Tool. [Электронный ресурс] URL: http://now.netapp.com/matrix/mtx/login.do
3. Principles of SAN Design, Second Edition; Judd, Josh; 2007; Infinity Publishing
4. Storage Area Network Fundamentals; Gupta, Meeta; 2002; Cisco Press

Тема 9. Перспективные направления в области проектирования защищенных систем обработки информации

Современные технологии построения защищенных систем обработки информации на конкретных примерах перспективных разработок.

Литература

1. Баранова Е.К., Бабаш А.В. Информационная безопасность и защита информации. – М.: ИНФРА-М_РИОР, 2018.
2. Баранова Е.К., Бабаш А.В. Моделирование системы защиты информации. Практикум. – М.: РИОР: ИНФРА-М, 2016.
3. Руководящие документы ФСТЭК РФ. [Электронный ресурс] URL: http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty#

Образовательные технологии

В рамках проведения семинаров разбираются задачи по темам лекций, рассматриваются и анализируются ситуационные задачи, выполняются практические работы по индивидуальным заданиям.

III. ОЦЕНИВАНИЕ

В соответствии с рабочим учебным планом, формами текущего контроля являются контрольная работа, реферат и домашнее задание. Каждая из форм текущего контроля оценивается по 10-балльной шкале. Общая оценка за текущий контроль (по 10-балльной шкале) рассчитывается по формуле:

$$O_{текущий} = 0,2 \cdot O_{к/р} + 0,3 \cdot O_{реф} + 0,5 \cdot O_{дз},$$

где $O_{к/р}$ – оценка за контрольную работу;
$O_{реф}$ – оценка за реферат;
$O_{дз}$ – оценка за домашние задания.

При определении накопленной оценки (по 10-балльной шкале) аудиторная работа и самостоятельная внеаудиторная работа не оцениваются. Поэтому накопленная оценка совпадает с оценкой за текущий контроль и рассчитывается по формуле:

$$O_{накопленная} = 1,0 \cdot O_{текущий} + 0,0 \cdot O_{ауд} + 0,0 \cdot O_{сам.работа},$$

где $O_{текущий}$ – оценка за текущий контроль;
$O_{ауд}$ – оценка за аудиторную работу;
$O_{сам.работа}$ – оценка за самостоятельную работу.

Результирующая оценка (выставляется в диплом) формируется на основе итоговой оценки за зачет (по 10-балльной шкале) и накопленной оценки. Результирующая оценка рассчитывается по формуле:

$$O_{результ} = 0,2 \cdot O_{экзамен} + 0,8 \cdot O_{накопленная},$$

где $O_{экзамен}$ – оценка за итоговый контроль (экзамен);
$O_{накопленная}$ – накопленная оценка.

При формировании оценок на основе весовых коэффициентов применяется округление до целого числа в большую сторону.

IV. ПРИМЕРЫ ОЦЕНОЧНЫХ СРЕДСТВ

Оценочные средства для текущего контроля студента

Перечень тем рефератов по курсу ТПЗСОИ

1. Этапы и общие принципы разработки защищенных информационных систем.
2. Предпосылки отнесения информации к категории конфиденциальной и выявление конфиденциальных сведений.
3. Сценарии последовательности действий нарушителя системы защиты информации. Пример построения сценария действий нарушителя с использованием графов.
4. Международные стандарты в области защиты информационных систем.
5. Цели, задачи и стадии проведения аудита информационной безопасности.
6. Оценка ущерба от нарушений информационной безопасности на различных этапах жизненного цикла объекта информатизации.
7. Методы оценки рисков информационной безопасности.
8. Шкалы оценки ущерба при нарушении информационной безопасности на объекте оценки.
9. Управление рисками. Модель безопасности с полным перекрытием.
10. Концепция управление рисками согласно ISO-15408.
11. Lifecycle Security – обобщенная схема построения комплексной защиты компьютерной сети предприятия.
12. Методика управления рисками, предлагаемая Microsoft (MSAT).
13. Обзор современных программных продуктов для анализа и оценки рисков.
14. Особенности моделирования сложных организационно-технических систем.
15. Моделирование процесса защиты информации в информационной системе с использованием графовых структур.
16. Пример использования графов для расчета защищенности от физического проникновения.
17. Генерирование множества альтернатив с применением экспертных методов при построении защищенной системы обработки информации.
18. Модель процесса защиты информации в виде трёхдольного графа.
19. Оценка альтернативных проектов организации системы защиты информации с использованием критериального метода.
20. Оценка альтернативных проектов организации системы защиты информации с использованием метода парных сравнений.
21. Информационные технологии, используемые в системах поддержки управленческих решений в области построения защищенных систем обработки информации.
22. Основные направления развития информатизации как глобального процесса.
23. Приоритетные направления развития ИКТ в России в условиях глобализации.
24. Конвергенция вычислительных сетей и сетей хранения данных.
25. Облачные технологии – это способ увеличения пропускной способности сетей или предоставление ИТ-ресурсов в виде сервиса.
26. Технологии сетей хранения данных Fibre Channel, iSCSI, FCoE.
27. Современное развитие Ethernet и TCP/IP.
28. Устройства хранения: DAS; NAS; SAN.
29. Классификация серверов по типу используемого ЦП.
30. Классификация серверов по типу приложений.
31. Обзор протоколов сетей хранения данных.
32. Fibre Channel SAN сети.
33. IP SAN сети.

34. Планирование защиты данных в СХД.
35. Современные ленточные библиотеки.
36. Обзор методов защиты данных средствами СХД.
37. Перспективные направления в организации и управлении системой защиты информации на предприятии.

Варианты контрольных работ по курсу ТПЗСОИ

Вариант 1
1. Методы оценки рисков информационной безопасности на предприятии.
2. Генерирование множества альтернатив с применением экспертных методов при разработке СЗИ.
3. Основные этапы принятия управленческих решений в области построения защищенных систем обработки информации.

Вариант 2
1. Этапы построения защищенных систем обработки информации.
2. “Куб безопасности” в координатах ОСНОВА, НАПРАВЛЕНИЯ, ЭТАПЫ. Обработка трехмерных матриц для оценки эффективности СЗИ.
3. Пример использования метода строчных сумм для составления матрицы альтернативных проектов СЗИ.

Вариант 3
1. Управление рисками. Модель безопасности с полным перекрытием.
2. Модель элементарной защиты объекта информатизации. Пример расчета прочности защиты.
3. Парное сравнение альтернатив (метод парных сравнений).

Вариант 4
1. Пример использования сетей Петри для построения сценария действий нарушителя и сигнатур атак.
2. Оценка альтернативных проектов организации СЗИ с использованием критериального метода.
3. Обзор современных программных продуктов для оценки рисков.

Вариант 5
1. Модель многозвенной защиты объекта информатизации. Пример расчета прочности защиты.
2. Альтернативы и критерии. Требования к набору критериев. Оценка важности критериев.
3. Пример исследования эффективности СЗИ с использованием морфологической матрицы.

Методические рекомендации, варианты и программный инструментарий для выполнения практических работ по курсу ТПЗСОИ

Приведены в книге:
Баранова Е.К., Бабаш А.В. Моделирование системы защиты информации. Практикум.– М.: РИОР: ИНФРА-М, 2016.

Оценочные средства для промежуточной аттестации по курсу ТПЗСОИ

A_Общие вопросы ТПЗСОИ

1. Системный подход к информационной безопасности. Классы задач по информационной безопасности. Цели и задачи обеспечения защиты систем обработки информации.
2. Требования к современным защищенным системам обработки информации.
3. Этапы построения защищенных систем обработки информации.

B_Моделирование СЗИ

4. Базовые модели СЗИ. Пример использования графовых моделей для оценки эффективности защиты от НСД к локальной сети.
5. Требования к моделям СЗИ. Схема воздействия угроз на информационную систему. Модель “черного ящика”.
6. Базовые модели СЗИ. Пример использования сетей Петри для построения сценария действий нарушителя и сигнатур атак.
7. “Куб безопасности” в координатах ОСНОВА, НАПРАВЛЕНИЯ, ЭТАПЫ. Обработка трехмерных матриц для оценки эффективности СЗИ.
8. Декомпозиция общей задачи оценки эффективности функционирования системы защиты. Модель элементарной защиты объекта информатизации. Пример расчета прочности защиты.
9. Описание модели безопасности с полным перекрытием множества угроз. Достоинства и недостатки модели безопасности с полным перекрытием, рекомендации по ее использованию.
10. Пример использования сетей Петри для построения сценария действий нарушителя и сигнатур атак.
11. Модель многозвенной защиты объекта информатизации. Пример расчета прочности защиты.
12. IDEF0 – методология многофункционального моделирования. Основные элементы и правила построения диаграмм на примере процесса проведения аудита ИБ.
13. IDEF0 – методология многофункционального моделирования. Основные элементы и правила построения диаграмм на примере управления инцидентами ИБ.

C_Анализ и оценка рисков ИБ в ИС

14. Методики анализа информационных рисков, угроз и уязвимостей информационной системы.
15. Анализ информационных рисков, угроз и уязвимостей информационной системы. Оценка рисков по двум факторам.
16. Анализ информационных рисков, угроз и уязвимостей информационной системы. Оценка рисков по трем факторам.
17. Сравнительный анализ программного инструментария для анализа рисков ИБ в информационных системах.
18. Достоинства и недостатки моделирования рисков информационной безопасности с использованием программного инструментария CORAS.
19. Уровни зрелости: модель Gartner Group; модель Carnegie Mellon University и их значение при построении защищенных информационных систем.

D_Управление инцидентами ИБ в ИС

20. Основные задачи управления инцидентами информационной безопасности.

21. Примеры международных стандартов в области управления инцидентами информационной безопасности.
22. Примеры инцидентов ИБ согласно ГОСТ Р ИСО/МЭК ТО 18044-2007.

E_Аудит безопасности ИС

23. Виды аудита информационной безопасности информационных систем.
24. Особенности аудита информационных систем методом тестирования на проникновение.
25. Фазы аудита информационной безопасности информационных систем.

F_Методы принятия решений в ТПЗСОИ

26. Характерные черты задачи принятия решений. Классификация задач принятия решений в области проектирования СЗИ.
27. Основные этапы принятия управленческих решений в области построения защищенных систем обработки информации.
28. Метод анализа иерархий. Постановка и этапы решения задачи сравнения альтернативных проектов СЗИ.
29. Пример оценки альтернативных проектов СЗИ с использованием критериального метода.
30. Пример оценки альтернативных проектов СЗИ с использованием метода парных сравнений.
31. Место систем поддержки принятия решений (СППР) среди существующих ИС. Информационные технологии используемые в СППР.

G_Оценка экономической эффективности СЗИ ИС

32. Сложности экономического анализа в сфере информационной безопасности.
33. Методы вычисления оценки возврата инвестиций ROI (Return on Investment) при оценке эффективности проекта защиты информационной системы.
34. Методы вычисления оценки возврата инвестиций в информационную безопасность ИС (ROSI).
35. Оценка экономической эффективности СЗИ с использованием показателя TCO (Total Cost Of Ownership – совокупная стоимость владения).
36. Методика BCP (Business Continuity Management) для оценки экономической эффективности проекта защиты информационной системы.
37. Определение размера целесообразных затрат на ИБ (критерии Лапласа, Вальда, Гурвица, Сэвиджа).

H_ Центры обработки данных (ЦОД)

38. Архитектура и общие задачи VPN.
39. Концепции платформенно-базированного и смешанного решения в архитектуре ИС и оценка их с точки зрения безопасности.
40. Современные подходы к организации ресурсов центров обработки данных (ЦОД). Виды ЦОД по типу и принадлежности.
41. Особенности обеспечения безопасности информации в центрах обработки данных (ЦОД).
42. Центры обработки данных (ЦОД). Стандартизация, задачи и особенности архитектуры ЦОД.
43. Технологии сетей хранения данных (SAN) Fibre Channel, iSCSI, FCoE.
44. Планирование защиты информации в сетях хранения данных (СХД).
45. Конвергенция вычислительных сетей и сетей хранения данных.

V. РЕСУРСЫ

Основная литература

1. Баранова Е.К., Бабаш А.В. Информационная безопасность и защита информации. – М.: ИНФРА-М_РИОР, 2018.
2. Баранова Е.К., Бабаш А.В. Моделирование системы защиты информации. Практикум. – М.: РИОР: ИНФРА-М, 2016.
3. Башлы П.Н., Бабаш А.В., Баранова Е.К. Информационная безопасность: учебно-практическое пособие. – М.: Изд.центр ЕАОИ, 2010.
4. Зегжда Д. П., Ивашко А.М. Основы безопасности информационных систем. СПб, Горячая Линия – Телеком, 2012.
5. Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. - М.: ДМК, 2012.
6. Ярочкин, В. И. Информационная безопасность: учебник для вузов / В. И. Ярочкин. – 3-е изд. – М.: Академический Проект: Трикста, 2005.
7. Руководящие документы ФСТЭК РФ. [Электронный ресурс] URL: http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty#

Дополнительная литература

1. Андрианов В.В., Зефиров С.Л., Голованов В.Б., Голдуев Н.А. - Обеспечение информационной безопасности бизнеса. – М.: Изд.центр “Альпина Паблишерз”, 2011.
2. Астахов А. Искусство управления информационными рисками. - М,: ДМК Пресс, 2010.
3. Барсегян А.А., Куприянов М.С., Степаненко В.В., Холод И.И. Технологии анализа данных. Data Mining, Visual Mining, Text Mining, OLAP (+CD). Учебное пособие, БХВ-Петербург, 2012.
4. Грибунин В.Г., Чудовский В.В. Комплексная система защиты информации на предприятии – М.: Академия, 2009.
5. Захарчук Т.В., Кузнецова И.П. Аналитико-синтетическая переработка информации. М,: Профессия, 2011.
6. Захарчук Т.В., Кузнецова И.П. Аналитико-синтетическая переработка информации. М,: Профессия, 2011.
7. Ногин В.Д.. Принятие решений при многих критериях. Учебно-методическое пособие. – СПб: Издательство «ЮТАС», 2011.
8. Розен В.В. Математические модели принятия решений в экономике. Учебное пособие. – М.: Книжный дом “Университет”. Высшая школа, 2012.
9. Советов Б.Я., Яковлев С.А. Моделирование систем. Учебник для вузов. М,: Высшая школа. 2011.
10. Поддержка принятия решений при проектировании систем защиты информации: Монография / В.В.Бухтояров и др. – М.: ИНФРА-М, 2014.
11. The logic behind CRAMM’s assessment of measures of risk and determination of appropriate countermeasures. [Электронный ресурс] URL: http://www.cramm.com/downloads/techpapers.htm
12. RiskWatch users manual. [Электронный ресурс] URL: http://www.riskwatch.com

Программное обеспечение

№ п/п	Наименование	Условия доступа
1.	Microsoft Windows 10 Microsoft Windows 8.1 Professional RUS	*Из внутренней сети университета (договор)*
2.	Microsoft Office Professional Plus 2010	*Из внутренней сети университета (договор)*
3.	Специализированное программное обеспечение для моделирования и анализа рисков информационной безопасности СЗИ	Баранова Е.К., Бабаш А.В. Моделирование системы защиты информации. Практикум.– М.: РИОР: ИНФРА-М, 2016. *(free software)*

Профессиональные базы данных, информационные справочные системы, интернет-ресурсы (электронные образовательные ресурсы)

№ п/п	Наименование	Условия доступа
	Профессиональные базы данных, информационно-справочные системы	
1.	Консультант Плюс	*Из внутренней сети университета (договор)*
2.	Электронно-библиотечная система Юрайт	URL: https://biblio-online.ru/
	Интернет-ресурсы (электронные образовательные ресурсы)	
1.	Открытое образование	URL: https://openedu.ru/

Материально-техническое обеспечение дисциплины

Учебные аудитории для лекционных занятий по дисциплине обеспечивают использование и демонстрацию тематических иллюстраций, соответствующих программе дисциплины в составе:

– персональные компьютеры с доступом в Интернет (операционная система, офисные программы, антивирусные программы);

– мультимедийный проектор с дистанционным управлением.

Для успешного освоения дисциплины, студент использует следующие программные средства:

- электронное приложение практикума с исполняемыми модулями:
  Баранова Е.К., Бабаш А.В. Моделирование системы защиты информации. Практикум. – М.: РИОР: ИНФРА-М, 2016.
- программный пакет *CORAS (free software)*;
- программный пакет *MSAT (free software)*;
- демонстрационная версия системы поддержки принятия парето-оптимальных решений в области проектирования защищенных систем обработки информации *(free software)*;
- демонстрационная программа для оценки эффективности защиты информационной системы в виде модели с полным перекрытием угроз *(free software)*;
- электронное приложение для проведения деловой игры *"Моделирование СЗИ"*.

Учебные аудитории для лабораторных и самостоятельных занятий по дисциплине оснащены перечисленным выше ПО, с возможностью подключения к сети Интернет и доступом к электронной информационно-образовательной среде НИУ ВШЭ.