Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«Национальный исследовательский ядерный университет «МИФИ»

ИНСТИТУТ ИНТЕЛЛЕКТУАЛЬНЫХ КИБЕРНЕТИЧЕСКИХ СИСТЕМ

КАФЕДРА СТРАТЕГИЧЕСКИХ ИНФОРМАЦИОННЫХ ИССЛЕДОВАНИЙ

ОДОБРЕНО УМС ИИКС

Протокол № 8/1/2024

от 28.08.2024 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

ТЕХНОЛОГИИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБЪЕКТОВ

Направление подготовки (специальность) [1] 10.04.01 Информационная безопасность

Семестр	**Трудоемкость, кред.**	**Общий объем курса, час.**	**Лекции, час.**	**Практич. занятия, час.**	**Лаборат. работы, час.**	**В форме практической подготовки/ В**	**СРС, час.**	**КСР, час.**	**Форма(ы) контроля, экз./зач./КР/КП**
1, 3	3	108	16	16	32		8	0	Э
Итого	3	108	16	16	32	12	8	0	

АННОТАЦИЯ

Изучение дисциплины «Технологии обеспечения информационной безопасности объектов» предполагает изучение основных понятий, принципов и особенностей технологий обеспечения информационной безопасности объектов.

Дисциплина «Технологии обеспечения информационной безопасности объектов» реализует требования Федерального государственного образовательного стандарта (ФГОС3++) по специальности 10.04.01 «Информационная безопасность» (квалификация (степень) выпускника «Магистр») и содействует формированию у студентов профессиональных компетенций, необходимых для решения задач, относящихся к определенному виду профессиональной деятельности.

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Курс занимает важное место в общей системе профильной подготовки выпускника, являясь своего рода мостом, связывающим общенаучные и общеобразовательные дисциплины с профильными для будущего специалиста курсами.

В свою очередь дисциплина обеспечивает необходимую подготовку студентов для выполнения проектирования.

Целью освоения учебной дисциплины «Технологии обеспечения информационной безопасности объектов»» является формирование общих представлений и знаний в области построения систем информационной безопасности с использованием технических средст, освоение дисциплинарных компетенций, связанных с раскрытием базовых и расширенных технологий информационной безопасности сложных технических объектов и систем.

Задачи изучения дисциплины:

- изучение основных положений, понятий и категорий, относящихся к базовым и расширенным технологиям информационной безопасности сложных технических объектов и систем;

– изучение основы правовых, организационно-распорядительных, нормативных и информационных документов в области информационных технологий, средств защиты информации и безопасности;

- изучение принципов организации, комплексного подхода к выбору средств и технологий обеспечения информационной безопасности объектов защиты;

- изучение принципов работы технических средств и определение критериев защищенности охраняемого объекта;

- освоение механизмов защиты объектов;

- формирование правильного подхода к проблемам информационной безопасности объектов.

Таким образом, дисциплина «Технологии обеспечения информационной безопасности объектов» является неотъемлемой составной частью профессиональной подготовки магистров по направлению подготовки 10.04.01 «Информационная безопасность». Вместе с другими дисциплинами общенаучного и профессионального циклов дисциплин изучение данной дисциплины призвано формировать специалиста, и в частности, вырабатывать у него такие качества, как:

- строгость в суждениях,

- творческое мышление,

- организованность и работоспособность,
- дисциплинированность,
- самостоятельность и ответственность.

2. МЕСТО УЧЕБНОЙ ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП ВО

Данная учебная дисциплина входит в базовую часть профессионального модуля ООП «Обеспечение безопасности значимых объектов критической информационной инфраструктуры» ОС НИЯУ МИФИ 10.04.01 «Информационная безопасность».

В процессе изучения дисциплины студенты получают возможность последовательно рассмотреть технологии и систему построения защищенных автоматизированных систем и её основные элементы и др. От студентов требуется знание основ защиты информации. Дисциплина «Технологии обеспечения информационной безопасности объектов» относится к числу дисциплин специализации «Обеспечение безопасности значимых объектов критической информационной инфраструктуры».

Для усвоения учебной дисциплины «Технологии обеспечения информационной безопасности объектов» студенты должны знать следующие дисциплины: «Общая алгебра»; «Математический анализ»; «Линейная алгебра»; «Теория вероятностей и математическая статистика»; «Дискретная математика»; «Информатика»; «Теория информации».

3. ФОРМИРУЕМЫЕ КОМПЕТЕНЦИИ И ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

Универсальные и(или) общепрофессиональные компетенции:

Код и наименование компетенции	Код и наименование индикатора достижения компетенции

Профессиональные компетенции в соотвествии с задачами и объектами (областями знаний) профессиональной деятельности:

Задача профессиональной деятельности (ЗПД)	**Объект или область знания**	**Код и наименование профессиональной компетенции; Основание (профессиональный стандарт-ПС, анализ опыта)**	**Код и наименование индикатора достижения профессиональной компетенции**
контрольно-аналитический			
Контроль защищенности ЗО КИИ по требованиям безопасности информации; аттестация ЗО КИИ по требованиям безопасности	Объекты информатизации, информационные ресурсы и информационные технологии, компьютерные, автоматизированные, телекоммуникационные,	ПК-4 [1] - Способен участвовать в планировании и реализации процессов контроля ИБ или процессов информационно-аналитических систем безопасности	З-ПК-4[1] - Знать: методы и методики оценки безопасности программно-аппаратных средств защиты информации; принципы построения программно-аппаратных средств

информации; проведение сертификационных испытаний средств защиты информации ЗО КИИ на соответствие требованиям по безопасности информации	информационные и информационно-аналитические системы, обеспечивающие безопасность критических процессов значимых объектов критической информационной инфраструктуры	*Основание:* Профессиональный стандарт: 06.032, 06.034	защиты информации; принципы построения подсистем защиты информации в компьютерных системах; методы и методики контроля защищенности информации от утечки за счет побочных электромагнитных излучений и наводок; средства контроля защищенности информации от утечки за счет побочных электромагнитных излучений и наводок; средства контроля защищенности информации от несанкционированного доступа порядок аттестации объектов информатизации на соответствие требованиям по защите информации; способы организации работ при проведении сертификации программно-аппаратных средств защиты; нормативные правовые акты, методические документы, национальные стандарты в области защиты информации ограниченного доступа и сертификации средств защиты информации на соответствие требованиям по безопасности информации. ; У-ПК-4[1] - Уметь: оценивать эффективность защиты информации;

			применять разработанные методики оценки защищенности программно-аппаратных средств защиты информации; оформлять материалы аттестационных испытаний (протоколов аттестационных испытаний и заключения по результатам аттестации объектов вычислительной техники на соответствие требованиям по защите информации); анализировать компьютерную систему с целью определения уровня защищенности и доверия; применять инструментальные средства проведения сертификационных испытаний; разрабатывать программы и методики сертификационных испытаний программных (программно-технических) средств защиты информации от несанкционированного доступа на соответствие требованиям по безопасности информации; проводить экспертизу технических и эксплуатационных документов на сертифицируемые программные

			(программно-технические) средства защиты информации от несанкционированного доступа и материалов сертификационных испытаний. ; В-ПК-4[1] - Владеть: определением уровня защищенности и доверия программно-аппаратных средств защиты информации; основами проведения аттестационных испытаний объектов вычислительной техники на соответствие требованиям по защите информации; основами проведения экспериментальных исследований уровней защищенности компьютерных систем и сетей; основами подготовки протоколов испытаний и технического заключения по результатам сертификационных испытаний программных (программно-технических) средств защиты информации от несанкционированного доступа на соответствие требованиям по безопасности информации; основами проведения экспертизы технических и эксплуатационных документов на сертифицируемые

			программные (программно-технические) средства защиты информации от несанкционированного доступа и материалов сертификационных испытаний.

4. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

Разделы учебной дисциплины, их объем, сроки изучения и формы контроля:

№ п.п	Наименование раздела учебной дисциплины	Недели	Лекции/ Практ. (семинары)/ Лабораторные работы, час.	Обязат. текущий контроль (форма*, неделя)	Максимальный балл за раздел**	Аттестация раздела (форма*, неделя)	Индикаторы освоения компетенции
	1 Семестр						
1	Раздел 1. Межсетевые экраны (МЭ) и	1-8	8/8/16		25	КИ-8	З-ПК-4, У-ПК-4, В-ПК-4
2	Раздел 2. Средства обеспечения ИБ в открытых системах	9-16	8/8/16		25	КИ-16	З-ПК-4, У-ПК-4, В-ПК-4
	Итого за 1 Семестр		16/16/32		50		
	Контрольные мероприятия за 1 Семестр				50	Э	З-ПК-4, У-ПК-4, В-ПК-4

* – сокращенное наименование формы контроля

** – сумма максимальных баллов должна быть равна 100 за семестр, включая зачет и (или) экзамен

Сокращение наименований форм текущего контроля и аттестации разделов:

Обозначение	Полное наименование
КИ	Контроль по итогам
Э	Экзамен

КАЛЕНДАРНЫЙ ПЛАН

Недели	Темы занятий / Содержание	Лек., час.	Пр./сем., час.	Лаб., час.
	1 Семестр	16	16	32
1-8	**Раздел 1. Межсетевые экраны (МЭ) и**	8	8	16
1 - 3	**Межсетевые экраны (МЭ)**	Всего аудиторных часов		

	Введение. Базовые сведения о межсетевых экранах (МЭ). Примеры МЭ.	3	3	0
		Онлайн		
		0	0	0
1 - 3	**Лабораторная работа №1** Исследование уязвимости "Man in the Middle"	Всего аудиторных часов		
		0	0	6
		Онлайн		
		0	0	0
3 - 5	**Лабораторная работа №2** Исследование уязвимости "SQL-injection"	Всего аудиторных часов		
		0	0	4
		Онлайн		
		0	0	0
3 - 5	**Виртуальные частные сети (VPN)** Базовые сведения о VPN. Туннелирование. Варианты построения VPN.	Всего аудиторных часов		
		2	2	0
		Онлайн		
		0	0	0
5 - 8	**Стандартные протоколы создания VPN** Протоколы создания VPN 2-го уровня модели OSI. Протоколы создания VPN 3-го уровня модели OSI.	Всего аудиторных часов		
		3	3	0
		Онлайн		
		0	0	0
5 - 8	**Лабораторная работа №3** Исследование уязвимости "XSS"	Всего аудиторных часов		
		0	0	6
		Онлайн		
		0	0	0
9-16	**Раздел 2. Средства обеспечения ИБ в открытых системах**	8	8	16
9 - 10	**Стандартные протоколы создания VPN** Протоколы создания VPN 5-го уровня модели OSI.	Всего аудиторных часов		
		2	2	0
		Онлайн		
		0	0	0
9 - 11	**Лабораторная работа №4** Изучение инструментов поиска уязвимостей в веб-приложениях	Всего аудиторных часов		
		0	0	6
		Онлайн		
		0	0	0
11 - 12	**Базовые сведения о виртуальных локальных сетях (VLAN)** Виды виртуальных локальных сетей. VLAN с группировкой портов, VLAN с маркированными кадрами, VLAN на основе протоколов высокого уровня. Этапы перехода к VLAN. Протокол VTP. Безопасность в VLAN. Преимущества VLAN.	Всего аудиторных часов		
		2	2	0
		Онлайн		
		0	0	0
12 - 13	**Лабораторная работа №5** Изучение стандартных утилит для исследования сетевых инфраструктур и мониторинга ИБ	Всего аудиторных часов		
		0	0	4
		Онлайн		
		0	0	0
13 - 14	**Адаптивное управление ИБ объектов** Аудит и мониторинг ИБ в открытых системах. Средства анализа защищенности (САЗ) и их место в защите открытых систем. Классификации САЗ. Сетевые сканеры: размещение агентов, принципы работы, этапы работы; сравнение современных реализаций. Системные сканеры. САЗ для приложений. Критерии выбора САЗ. Методы	Всего аудиторных часов		
		2	2	0
		Онлайн		
		0	0	0

	отражения вторжений: предотвращение, прерывание, сдерживание, отклонение, обнаружение, устранение последствий. Системы обнаружения/предотвращения вторжений (СОВ/СПВ). Классификация и структура СОВ/СПВ. Системные и сетевые СОВ/СПВ: принципы работы, достоинства и недостатки. Размещение сетевых СОВ/СПВ. Интеллектуальные и поведенческие СОВ. Обнаружение вторжений/злоупотреблений; обнаружение аномалий/сопоставление с образцом. СОВ, их выбор, применение, ограниченность и примеры систем. СПВ, их применение и примеры систем. Сохранение доказательств вторжений. Стандарты в области обнаружения вторжений.			
14 - 16	**Другие средства обеспечения ИБ в открытых системах** Защита от спама. Защита от спама в электронной почте: определение, методы детектирования, архитектура защищенной от спама электронной почты, примеры систем. Другие средства защиты информации. Многофункциональные устройства защиты от сетевых атак. Системы анализа и управления рисками. Системы обеспечения ИБ на уровне предприятия.	Всего аудиторных часов		
		2	2	0
		Онлайн		
		0	0	0
15 - 16	**Лабораторная работа №6** Ознакомление с основами PostgreSQL	Всего аудиторных часов		
		0	0	6
		Онлайн		
		0	0	0

Сокращенные наименования онлайн опций:

Обозначение	**Полное наименование**
ЭК	Электронный курс
ПМ	Полнотекстовый материал
ПЛ	Полнотекстовые лекции
ВМ	Видео-материалы
АМ	Аудио-материалы
Прз	Презентации
Т	Тесты
ЭСМ	Электронные справочные материалы
ИС	Интерактивный сайт

ТЕМЫ ЛАБОРАТОРНЫХ РАБОТ

Недели	**Темы занятий / Содержание**
	1 Семестр
3 - 4	**Лабораторная работа №1** Исследование уязвимости "Man in the Middle"
5 - 6	**Лабораторная работа №2** Исследование уязвимости "SQL-injection"
7 - 8	**Лабораторная работа №3** Исследование уязвимости "XSS"
11 - 12	**Лабораторная работа №4** Изучение инструментов поиска уязвимостей в веб-приложениях
13 - 14	**Лабораторная работа №5**

	Изучение стандартных утилит для исследования сетевых инфраструктур и мониторинга ИБ
15 - 16	**Лабораторная работа №6** Ознакомление с основами PostgreSQL

ТЕМЫ ПРАКТИЧЕСКИХ ЗАНЯТИЙ

Недели	**Темы занятий / Содержание**
	1 Семестр
1 - 3	**Практическое занятие № 1** Базовые сведения о межсетевых экранах (МЭ). Примеры МЭ
4 - 5	**Практическое занятие № 2** Базовые сведения о VPN. Туннелирование. Варианты построения VPN
6 - 8	**Практическое занятие № 3** Протоколы создания VPN 2-го уровня модели OSI. Протоколы создания VPN 3-го уровня модели OSI
9 - 11	**Практическое занятие № 4** Протоколы создания VPN 5-го уровня модели OSI
12 - 13	**Практическое занятие № 5** Виды виртуальных локальных сетей. VLAN с группировкой портов, VLAN с маркированными кадрами, VLAN на основе протоколов высокого уровня. Этапы перехода к VLAN. Протокол VTP. Безопасность в VLAN. Преимущества VLAN
14 - 16	**Практическое занятие № 6** Защита от спама. Защита от спама в электронной почте: определение, методы детектирования, архитектура защищенной от спама электронной почты, примеры систем. Другие средства защиты информации. Многофункциональные устройства защиты от сетевых атак. Системы анализа и управления рисками. Системы обеспечения ИБ на уровне предприятия

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Цель обучения достигается сочетанием применения традиционных и инновационных педагогических технологий, направленных на развитие познавательной активности, творческой самостоятельности студентов.

В соответствии с целью формирования и развития профессиональных навыков студентов и требованиями ОС ВО по направлению подготовки реализация компетентностного подхода предусматривает в учебном процессе широкое использование активных и интерактивных форм проведения занятий в сочетании с внеаудиторной работой.

Цель обучения достигается сочетанием применения традиционных и инновационных педагогических технологий, направленных на развитие познавательной активности, творческой самостоятельности студентов. Последовательное и целенаправленное выдвижение перед студентом познавательных задач, решая которые студенты активно усваивают знания. Поисковые методы; постановка познавательных задач. С целью формирования и развития профессиональных навыков студентов в дисциплине используются активные и интерактивные формы проведения занятий: лабораторные работы и доклады и презентации с их обсуждением в сочетании с внеаудиторной работой. В соответствии со спецификой ВУЗа в процессе преподавания дисциплины методически целесообразно в каждом разделе выделить наиболее важные темы и акцентировать на них внимание обучаемых. В рамках дисциплины

предусмотрены встречи с представителями государственных и общественных организаций, мастер-классы экспертов и специалистов в области технологий обеспечения ИБ, а также российских и зарубежных компаний – разработчиками средств обеспечения ИБ.

6. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

Фонд оценочных средств по дисциплине обеспечивает проверку освоения планируемых результатов обучения (компетенций и их индикаторов) посредством мероприятий текущего, рубежного и промежуточного контроля по дисциплине.

Связь между формируемыми компетенциями и формами контроля их освоения представлена в следующей таблице:

Компетенция	**Индикаторы освоения**	**Аттестационное мероприятие (КП 1)**
ПК-4	З-ПК-4	Э, КИ-8, КИ-16
	У-ПК-4	Э, КИ-8, КИ-16
	В-ПК-4	Э, КИ-8, КИ-16

Шкалы оценки образовательных достижений

Шкала каждого контрольного мероприятия лежит в пределах от 0 до установленного максимального балла включительно. Итоговая аттестация по дисциплине оценивается по 100-балльной шкале и представляет собой сумму баллов, заработанных студентом при выполнении заданий в рамках текущего и промежуточного контроля.

Итоговая оценка выставляется в соответствии со следующей шкалой:

<table>
<tr><th>Сумма баллов</th><th>Оценка по 4-ех балльной шкале</th><th>Оценка ECTS</th><th>Требования к уровню освоению учебной дисциплины</th></tr>
<tr><td>90-100</td><td>5 – «отлично»</td><td>A</td><td>Оценка «отлично» выставляется студенту, если он глубоко и прочно усвоил программный материал, исчерпывающе, последовательно, четко и логически стройно его излагает, умеет тесно увязывать теорию с практикой, использует в ответе материал монографической литературы.</td></tr>
<tr><td>85-89</td><td rowspan="3">4 – «хорошо»</td><td>B</td><td rowspan="3">Оценка «хорошо» выставляется студенту, если он твёрдо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос.</td></tr>
<tr><td>75-84</td><td>C</td></tr>
<tr><td>70-74</td><td rowspan="2">D</td></tr>
<tr><td>65-69</td><td rowspan="2">3 – «удовлетворительно»</td><td rowspan="2">Оценка «удовлетворительно» выставляется студенту, если он имеет знания только основного материала, но не усвоил его деталей, допускает неточности, недостаточно правильные формулировки, нарушения логической последовательности в изложении программного материала.</td></tr>
<tr><td>60-64</td><td>E</td></tr>
<tr><td>Ниже 60</td><td>2 – «неудовлетворительно»</td><td>F</td><td>Оценка «неудовлетворительно» выставляется студенту, который не знает</td></tr>
</table>

			значительной части программного материала, допускает существенные ошибки. Как правило, оценка «неудовлетворительно» ставится студентам, которые не могут продолжить обучение без дополнительных занятий по соответствующей дисциплине.

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

ОСНОВНАЯ ЛИТЕРАТУРА:

1. ЭИ П 84 Информационная безопасность и защита информации : учебное пособие, Прохорова О. В., Санкт-Петербург: Лань, 2021

2. 004 М48 Информационная безопасность открытых систем : учебник, Мельников Д.А., Москва: Флинта, 2013

3. ЭИ Д84 Оценка защищенности речевой информации Ч.1 Выявление акустических и вибрационных каналов утечки речевой информации, Дураковский А.П., Москва: НИЯУ МИФИ, 2015

4. ЭИ Д84 Оценка защищенности речевой информации Ч.2 Проведение инструментального контроля в канале низкочастотного акустоэлектрического преобразования, Дураковский А.П., Москва: НИЯУ МИФИ, 2015

5. ЭИ Д84 Оценка защищенности речевой информации Ч.3 Проведение инструментального контроля в канале акустоэлектромагнитного преобразования, Дураковский А.П., Москва: НИЯУ МИФИ, 2018

6. ЭИ Д84 Оценка защищенности речевой информации Ч.4 Проведение инструментального контроля в канале высокочастотного навязывания, Дураковский А.П., Москва: НИЯУ МИФИ, 2018

7. ЭИ Д84 Оценка защищенности речевой информации Ч.5 Проведение инструментального контроля в канале высокочастотного облучения, Дураковский А.П., Москва: НИЯУ МИФИ, 2018

8. 004 М48 Системы и сети передачи данных : учебник, Мельников Д.А., Москва: РадиоСофт, 2015

ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА:

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ:

Специальное программное обеспечение не требуется

LMS И ИНТЕРНЕТ-РЕСУРСЫ:

1. Вузовские электронно-библиотечные системы учебной литературы ()

2. База научно-технической информации (например, ВИНИТИ РАН) ()

3. www.fstec.ru; www.gost.ru; www.fsb.ru. ()

4. http://www.scinet.cc ()

5. https://bit.spels.ru/index.php/bit ()

6. http://library.mephi.ru/ ()

https://online.mephi.ru/

http://library.mephi.ru/

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

1. специализированная учебная лаборатория: «Контроль защищенности ЛВС от НСД» ()

9. УЧЕБНО-МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ СТУДЕНТОВ

Общие рекомендации по изучению курса

Студенты должны своевременно спланировать учебное время для поэтапного и системного изучения данной учебной дисциплины в соответствии с планом лекций, лабораторных работ и контроля знаний.

Успешное освоение дисциплины требует от студентов посещения лекций, активной работы во время лабораторных занятий, выполнения всех учебных заданий преподавателя, ознакомления с базовыми учебниками, основной и дополнительной литературой, а также предполагает творческое участие студента путем планомерной, повседневной работы.

Изучение дисциплины следует начинать с проработки учебной программы, особое внимание, уделяя целям и задачам, структуре и содержанию курса.

Во время лекций рекомендуется писать конспект. Запись лекции – одна из форм активной самостоятельной работы студентов, требующая навыков и умения кратко, схематично, последовательно и логично фиксировать основные положения, выводы, обобщения, формулировки. Теория ИБ как наука использует свою терминологию, категориальный, графический и математический аппараты, которыми студент должен научиться пользоваться и применять по ходу записи лекции. Культура записи лекции – один из важнейших факторов успешного и творческого овладения знаниями.

В конце лекции преподаватель оставляет время (5 минут) для того, чтобы студенты имели возможность задать уточняющие вопросы по изучаемому материалу.

Лекции имеют в основном обзорный характер и нацелены на освещение наиболее трудных и дискуссионных вопросов, а также призваны способствовать формированию навыков работы с научной литературой. Предполагается также, что студенты приходят на лекции, предварительно проработав соответствующий учебный материал по источникам, рекомендуемым программой.

Конспект лекций для закрепления полученных знаний необходимо просмотреть сразу после занятий. Хорошо отметить материал конспекта лекций, который вызывает затруднения для понимания. Можно попытаться найти ответы на затруднительные вопросы, используя рекомендуемую литературу. Если самостоятельно не удалось разобраться в материале, рекомендуется сформулировать вопросы и обратиться за помощью к преподавателю на консультации или ближайшей лекции.

В процессе изучения учебной дисциплины необходимо обратить внимание на самоконтроль. Требуется регулярно отводить время для повторения пройденного материала, проверяя свои знания, умения и навыки по контрольным вопросам.

Перед выполнением лабораторных работ студент должен заранее изучить теоретический и учебно-методический материалы, относящиеся непосредственно к выполнению данной работы. После этого составляется план выполнения работы в соответствии с ее сценарием и готовятся рабочие материалы, необходимые для выполнения работы и для оформления отчета по ней. По имеющимся у студента контрольным вопросам осуществляется самоконтроль уровня подготовки к выполнению работы. При необходимости студент может обратиться к преподавателю за консультацией по вопросам, относящимся к выполнению данной лабораторной работы.

После допуска преподавателем студента к лабораторной работе, он выполняет все задания, готовит отчет и защищает его.

Систематическая индивидуальная работа, постоянная активность на занятиях, готовность ставить и обсуждать актуальные проблемы курса – залог успешной работы и положительной оценки.

Со стороны преподавателя должен быть установлен контакт со студентами, и они должны быть информированы о порядке прохождения курса, его особенностях, учебно-методическом обеспечение по данной дисциплине. Преподаватель дает методические рекомендации обучаемым по самостоятельному изучению проблем, характеризуя пути и средства достижения поставленных перед ними задач, высказывает советы и рекомендации по изучению учебной литературы, самостоятельной работе и лабораторных работах.

В рамках дисциплины предусмотрены встречи с представителями государственных и общественных организаций, мастер-классы экспертов и специалистов в области обеспечения ИБ, а также российских и зарубежных компаний – разработчиками средств обеспечения ИБ объектов.

В конце занятия преподаватель подводит его итоги, даёт оценку активности студентов и уровня их знаний.

Методические рекомендации по организации самостоятельной работы студента

Для эффективного достижения указанных выше целей обучения по дисциплине «Технологии обеспечения информационной безопасности объектов» процесс изучения материала курса предполагает достаточно интенсивную работу не только на лекциях и семинарах, но и с различными текстами и информационными ресурсами в ходе самостоятельной работы.

Самостоятельная работа по дисциплине «Технологии обеспечения информационной безопасности объектов» делится на аудиторную и внеаудиторную. Вопросы организации самостоятельной работы в ходе аудиторных занятий рассмотрены в предыдущих разделах предлагаемых методических рекомендаций. Поэтому рассмотрим процесс организации самостоятельной внеаудиторной работы студентов. Весь материал темы или отдельных ее вопросов, выносимых на самостоятельное изучение, разбивается на небольшие части. В конце

каждой части приводятся вопросы для самоконтроля, отвечая на которые студент может проверить степень усвоения им изучаемого материала. Внеаудиторная самостоятельная работа включает также выполнение индивидуальных контрольных заданий. По результатам работы студента на практических занятиях проставляется оценка в ведомость текущего контроля успеваемости и посещаемости студентов, а также передаются сведения в автоматизированную систему контроля самостоятельной и аудиторной работы студентов в Учебный Департамент НИЯУ «МИФИ».

Подготовка к зачету и порядок его проведения

Итоговой формой контроля знаний студентов в семестре по дисциплине «Технологии обеспечения информационной безопасности объектов» является зачет. Перед проведением зачета студенту необходимо восстановить в памяти теоретический материал по всем темам курса. Для этого следует обратиться к соответствующим конспекту лекций, главам учебника и другим источникам. Зачет по курсу «Технологии обеспечения информационной безопасности объектов» может быть проведен в традиционной устной форме, но с обязательной записью основных формулировок по каждому вопросу в зачетном листе. Данный лист может служить документом при подаче аппеляции. В качестве методической помощи студентам при подготовке к зачету рекомендуется перечень вопросов для подготовки к зачету. Зачет по курсу может быть проведен также в письменной форме: в форме письменных ответов на вопросы (на усмотрение преподавателя). Вопросы должны в обязательном порядке охватывать все дидактические единицы дисциплины «Технологии обеспечения информационной безопасности объектов». Форма проведения зачета сообщается студентам на последних занятиях.

Зачет определяется на основе суммы баллов, полученных по всем разделам по результатам самостоятельной работы при условии, что студент по каждому виду набрал количество баллов не менее зачетного минимума. Так зачет проставляется если студент в сумме набрал от 60-100 баллов. Неудовлетворительно - ниже 60 баллов.

Сумма баллов Оценка (ECTS) Градация

90 - 100 A отлично

85 - 89 B очень хорошо

75 - 84 C хорошо

70 - 74 D хорошо

65 - 69 D удовлетворительно

60 - 64 E удовлетворительно

Ниже 60 F неудовлетворительно

В основу разработки данной бально-рейтинговой системы положены принципы, в соответствии с которыми формирование рейтинга студента осуществляется постоянно в процессе его обучения в университете. Настоящая система оценки успеваемости студентов основана на использовании совокупности контрольных точек, оптимально расположенных на всем временном интервале изучения дисциплины. При этом предполагается разделение всего курса на ряд более или менее самостоятельных, логически завершенных блоков и модулей и проведение по ним промежуточного контроля.

10. УЧЕБНО-МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ ПРЕПОДАВАТЕЛЕЙ

Методические рекомендации для преподавателя по организации изучения дисциплины «Технологии обеспечения информационной безопасности объектов»

Целью методических рекомендаций являются формирование теоретико-методологических знаний и закрепление профессиональных навыков в области построения, проектирования и создания защищенных автоматизированных систем, а также навыков и умения в применении знаний для конкретных условий.

Методологические подходы к изучению дисциплины «Технологии обеспечения информационной безопасности объектов»

- Направленность обучения на получение студентами качественных знаний, которые являются средством развития мышления и культуры, основой воспитания и поведения, будующего практического применения в различных сферах профессиональной деятельности.

- Реализация возможностей студентов в процессе выявления дискуссионных вопросов и комплексных проблем, определения взаимосвязей, анализа разнообразной информации.

- Развитие самостоятельности и способности принятия эффективных решений, определения выбора тех или иных действий с точки зрения их результативности.

Средства обеспечения освоения дисциплины «Технологии обеспечения информационной безопасности объектов»

Общий подход к реализации всего программного комплекса предполагает широкое использование активных методических форм преподавания материала.

Необходимо также обратить внимание на сочетание различных форм и методов обучения, включая лекционную форму подачи наиболее фундаментальных положений, изложение доступного материала в виде непрерывного диалога, проведение практикумов, закрепляющих полученные теоретические знания посредством конкретных расчетов и принятия решений.

При изучении курса рекомендуется широко использовать наглядные пособия, презентации, фрагменты учебных кинофильмов по отдельным разделам дисциплины и обучающие программы.

Формы проведения учебных занятий:

• Практикумы (теоретические и практические задания).

• Ситуационные (творческие) задачи, вопросы для обсуждения (закрепление представлений учащихся об экономических понятиях и явлениях, навыков формирования конструктивных и конкретных вопросов).

• Тестовые задания (тестирование).

Педагогические функции преподавания дисциплины реализуются через совокупность педагогических приемов. В качестве основных можно выделить следующие:

Дидактические (способность к передаче знаний в краткой и интересной форме, т. е. умение делать учебный материал доступным для студентов, опираясь на взаимосвязь теории и практики, учебного материала и реальной экономической действительности).

Рефлексивно-гностические (способность понимать студентов, базирующаяся на интересе к ним и личной наблюдательности; самостоятельный и творческий склад мышления; находчивость или быстрая и точная ориентировка).

Интерактивно-коммуникативные (педагогически волевое влияние на студентов, требовательность, педагогический такт, организаторские способности, необходимые как для обеспечения работы самого преподавателя, так и для создания хорошего психологического климата в учебной группе).

Речевые (содержательность, яркость, образность и убедительность речи преподавателя; способность ясно и четко выражать свои мысли и чувства с помощью речи, а также мимики и жестов).

Материально-техническое обеспечение дисциплины «Технологии обеспечения информационной безопасности объектов»

При выполнении заданий, самостоятельных работ и подготовке учебно-методических комплексов предусматривается применение ПК. Возможно обращение к сети Интернет.

Методические рекомендации по организации изучения дисциплины «Технологии обеспечения информационной безопасности объектов»

Методически обосновано изучать дисциплину в аудитории на лекциях и практических занятиях.

Целесообразно для увеличения времени проработки важных тем предусмотреть рассмотрение отдельных вопросов в форме дискуссий и диспутов, на конференциях. Кроме того, необходимо предусмотреть дополнительные консультации по сложным темам.

В качестве форм промежуточного контроля полученных знаний (раздел 1 и 2) используются: контрольная работа и тестирование. Для повышения результатов контроля студентами (по их желанию) могут быть выполнены и использованы письменные работы (рефераты).

В процессе итогового контроля также могут использоваться результаты, полученные студентами на практических занятиях.

При неаттестации хотя бы по одному из разделов, студент не допускается к зачету.

Средства обеспечения освоения учебного курса

При изучении дисциплины рекомендуется использовать следующие средства обучения:

программу учебного курса:

рекомендуемую основную и дополнительную литературу;

методические указания, пособия и учебники (в бумажном виде);

задания для самостоятельной работы для закрепления теоретического материала;

описания лабораторных работ и контрольные вопросы к ним;

методическое обеспечение текущего и итогового контроля знаний.

Со стороны преподавателя должен быть установлен контакт со студентами, и они должны быть информированы о порядке прохождения курса, его особенностях, учебно-методическом обеспечение по данной дисциплине. Преподаватель дает методические рекомендации обучаемым по самостоятельному изучению проблем, характеризуя пути и средства достижения поставленных перед ними задач, высказывает советы и рекомендации по изучению учебной литературы, самостоятельной работе и лабораторных работах.

Основные формы изучения дисциплины

Курс читается на 1 семестре.

Курс рассчитан на 108 часов, из которых 8 часов лекционных занятий, 24 часа лабораторных занятий (ЛР) и 40 часов самостоятельной работы (СР) студента.

Принципы отбора содержания и организации учебного материала дисциплины

Учебный курс строится на интегративной основе и включает в себя как теоретические знания, так и практические навыки, получаемые студентами в ходе выполнения лабораторных работ и самостоятельных занятий.

Данная дисциплина выполняет функции теоретической и практической подготовки студентов. В нем заложен деятельностный компонент, наиболее ярко проявляющийся в системе практических лабораторных занятий.

Содержание дисциплины распределяется между лекционной и практической частями на основе принципа дополняемости: практические занятия, как правило, не дублируют лекции и носят ярко выраженный творческий характер. В лекционном курсе главное место отводится

общетеоретическим проблемам. Практические занятия рекомендуется использовать для выработки у студентов практических навыков защиты в открытых системах.

Содержание учебного курса, его объем и характер обусловливают необходимость оптимизации учебного процесса в плане отбора материала обучения и методики его организации, а также контроля текущей учебной работы. В связи с этим возрастает значимость и изменяется статус внеаудиторной (самостоятельной) работы, которая становится полноценным и обязательным видом учебно-познавательной деятельности студентов. При изучении курса самостоятельная работа включает:

самостоятельное ознакомление студентов с теоретическим материалом, представленным в основной литературе;

самостоятельное изучение тем учебной программы, достаточно хорошо обеспеченных литературой и сравнительно несложных для понимания;

подготовку к практическим занятиям по тем разделам, которые не дублируют темы лекционной части, а потому предполагают самостоятельную проработку материала учебных пособий.

В рамках дисциплины предусмотрены встречи с представителями государственных и общественных организаций, мастер-классы экспертов и специалистов в области обеспечения ИБ, а также российских и зарубежных компаний – разработчиками средств обеспечения ИБ.

Обоснование логики прохождения учебного курса

За основу логического прохождения курса приняты следующие положения.

1. Изложение теоретических основ курса начинается с изучения базовые сведения о технологиях обеспечения ИБ объектов.

2. Далее в качестве одного из базовых вариантов построения ВЧС рассматривается межсетевой экран.

3. После определения основного предмета изучения вводит понятийный аппарат, используемый при дальнейшем изложении, а именно классы ВЧС, туннелирование, схемы построения ВЧС, политика ИБ для ВЧС, стандартные протоколы построения ВЧС и т.д.

4. Также изучается также часто применяемый вид виртуальных сетей – виртуальные локальные сети.

5. Далее рассматриваются САЗ и СОВ/СПВ и другие средства обеспечения ИБ объектов.

Теоретические положения курса подкрепляются иллюстрациями и выработкой практических навыков при выполнении студентами лабораторных работ по всем основным темам курса.

Автор(ы):

Евсеев Владимир Леонович, к.т.н., доцент

Рецензент(ы):

Дураковский А.П.