МИНОБРНАУКИ РОССИИ
Ярославский государственный университет им. П.Г. Демидова

Кафедра компьютерной безопасности и математических методов обработки информации

УТВЕРЖДАЮ
Декан математического факультета

Нестеров П.Н.
20 июня 2023 г.

Рабочая программа дисциплины
Комплексная защита объектов информатизации

Направление подготовки (специальности)
10.03.01 Информационная безопасность

Направленность (профиль)
«Безопасность компьютерных систем»

Форма обучения очная

Программа рассмотрена
на заседании кафедры
от 14 апреля 2023 г., протокол № 8

Программа одобрена НМК
математического факультета
протокол № 9 от 3 мая 2023 г.

Ярославль

1. **Цели освоения дисциплины**

Дисциплина «Комплексное обеспечение защиты информации объекта информатизации» имеет целью подготовить выпускника к деятельности, связанной с выработкой предложений по вопросам комплексного обеспечения информационной безопасности объектов информатизации, разработке предложений по совершенствованию и повышению эффективности такого комплекса мер.

2. **Место дисциплины в структуре образовательной программы**

Дисциплина «Комплексная защита объектов информатизации» относится к обязательной части образовательной программы. (Б1.О.42)

Для успешного усвоения данной дисциплины необходимо, чтобы студент овладел знаниями, умениями и навыками, сформированными в процессе изучения дисциплин:

«Программно-аппаратные средства защиты информации» - базовые знания об угрозах информационной безопасности, а также о средствах и методах защиты от них;

«Информатика» – работа с программными средствами общего назначения;

«Основы информационной безопасности» – знание основ обеспечения информационной безопасности в Российской Федерации.

Знания и навыки, полученные в результате изучения дисциплины «Комплексная защита объектов информатизации», используются студентами для дальнейшего изучения дисциплин в этом же модуле, а также для продолжения обучения в магистратуре по направлению Информационная безопасность.

3. **Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения образовательной программы**

Процесс изучения дисциплины направлен на формирование следующих элементов компетенций в соответствии с ФГОС ВО, ООП ВО и приобретения следующих знаний, умений, навыков и (или) опыта деятельности:

Формируемая компетенция (код и формулировка)	**Индикатор достижения компетенции (код и формулировка)**	**Перечень планируемых результатов обучения**
Общепрофессиональные компетенции		
ОПК- 5 Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности;	**И-ОПК-5_1.** Знает и понимает нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации;	**Знать** особенности комплексного подхода к обеспечению информационной безопасности, а также нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации.

ОПК-6 Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;	**И-ОПК-6_2** знает основные угрозы безопасности информации и модели нарушителя объекта информатизации	**Знать** характерные угрозы безопасности информации; способы реализации атак на объект информатизации.
ОПК- 8 Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности;	**И-ОПК-8_1** знает способы поиска и обработки информации, методы работы с научной информацией, принципы и правила построения суждений и оценок	**Знать** способы поиска и обработки информации, методы работы с научной информацией, принципы и правила построения суждений и оценок.
	И-ОПК-8_2 умеет обобщать, анализировать и систематизировать научную информацию в области информационной безопасности	**Уметь** анализировать исходные данные для проектирования подсистем и средств обеспечения информационной безопасности.

ОПК-1.4 Способен оценивать уровень безопасности компьютерных систем и сетей, в том числе в соответствии с нормативными и корпоративными требованиями	**И-ОПК-1.4_1** знает источники угроз информационной безопасности в компьютерных сетях и меры по их предотвращению	**Знать** источники угроз информационной безопасности в компьютерных сетях и меры по их предотвращению.
	И-ОПК-1.4_2 умеет оценивать угрозы безопасности информации в компьютерных сетях	**Уметь** оценивать угрозы информационной безопасности предприятия, а также уровень безопасности компьютерных систем и сетей в соответствии с политикой безопасности предприятия.
	И-ОПК-1.4_3 владеет управлением средствами межсетевого экранирования в компьютерных сетях в соответствии с действующими требованиями	**Владеть навыками** администрирования межсетевого экранирования в компьютерных сетях с учетом политики безопасности предприятия.

4. Объем, структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 5 зачетных единиц, 180 акад. часов.

№ п/п	Темы (разделы) дисциплины, их содержание	Семестр	Виды учебных занятий, включая самостоятельную работу студентов, и их трудоемкость (в академических часах)						Формы текущего контроля успеваемости Форма промежуточной аттестации *(по семестрам)*
			Контактная работа						
			лекции	практические	лабораторные	консультации	аттестационные испытания	Самостоятельная работа	
1	Комплексное обеспечение информационной безопасности	7	8	4		2		20	Опрос на практических занятиях
2	Управление доступом в автоматизированных системах	7	6	6		1		14	Опрос на практических занятиях
3	Межсетевые экраны и виртуальные частные сети	7	14	18		4		26	Опрос на практических занятиях
4	Защита электронного документооборота	7	4	4		1		12	Опрос на практических занятиях
						2	0,5	33,5	Экзамен
	Всего	180	32	32		10	0,5	105.5	

Содержание разделов дисциплины:

Раздел №1. «Комплексное обеспечение информационной безопасности».

Тема 1.1 Архитектура корпоративной информационной системы.

Тема 1.2 Структура системы защиты информации в корпоративной информационной системе.

Тема 1.3 Комплексный подход к обеспечению информационной безопасности корпоративной системы.

Тема 1.4 Подсистемы информационной безопасности корпоративной информационной системы.

Раздел №2. «Управление доступом в автоматизированных системах».

Тема 2.1 Идентификация, аутентификация, авторизация, подотчетность.

Тема 2.2 Модели управления доступом.

Тема 2.3 Техники и технологии управления доступом.

Тема 2.4 Администрирование доступа.

Тема 2.5 Методы управления доступом.

Тема 2.6 Мониторинг управления доступом.

Тема 2.7 Протоколы аутентификации.

Тема 2.8 Серверы аутентификации.

Раздел №3. «Межсетевые экраны».

Тема 3.1 Средства и методы сегментирования сети.

Тема 3.2 Функции межсетевых экранов.

Тема 3.3 Типы межсетевых экранов. Экранирующие концентраторы. Пакетные фильтры.

Тема 3.4 Основные компоненты межсетевых экранов.

Тема 3.5 Схемы подключения межсетевых экранов.

Тема 3.6 Уязвимости межсетевых экранов.

Раздел №4. «Защита электронного документооборота».

Тема 4.1 Концепция электронного документооборота.

Тема 4.2 Особенности защиты электронного документооборота.

Тема 4.3 Защита корпоративного почтового документооборота.

5. Образовательные технологии, в том числе технологии электронного обучения и дистанционные образовательные технологии, используемые при осуществлении образовательного процесса по дисциплине

В процессе обучения используются следующие образовательные технологии:

Вводная лекция – дает первое целостное представление о дисциплине и ориентирует студента в системе изучения данной дисциплины. Студенты знакомятся с назначением и задачами курса, его ролью и местом в системе учебных дисциплин и в системе подготовки в целом. Дается краткий обзор курса, история развития науки и практики, достижения в этой сфере, имена известных ученых, излагаются перспективные направления исследований. На этой лекции высказываются методические и организационные особенности работы в рамках данной дисциплины, а также дается анализ рекомендуемой учебно-методической литературы.

Академическая лекция (или лекция общего курса) – последовательное изложение материала, осуществляемое преимущественно в виде монолога преподавателя. Требования к академической лекции: современный научный уровень и насыщенная информативность, убедительная аргументация, доступная и понятная речь, четкая структура и логика, наличие ярких примеров, научных доказательств, обоснований, фактов.

Практические занятия – занятия, посвященные освоению конкретных умений и навыков и закреплению полученных на лекции знаний.

Консультации – вид учебных занятий, являющийся одной из форм контроля самостоятельной работы студентов. На консультациях по просьбе студентов рассматриваются наиболее сложные моменты при освоении материала дисциплины, преподаватель отвечает на вопросы студентов, которые возникают у них в процессе самостоятельной работы.

6. Перечень лицензионного и (или) свободно распространяемого программного обеспечения, используемого при осуществлении образовательного процесса по дисциплине

В процессе осуществления образовательного процесса используются:

- программное обеспечение для создания и демонстрации презентаций, иллюстраций и

других учебных материалов:

- Microsoft Windows (в составе Microsoft Imagine Premium Electronic Software Delivery);

- Microsoft OfficeSTD 2013;
- ViPNet Administrator 4.x (КС3;
- Сеть 11565. ViPNet Client for Windows 4.x (КС3);
- XSpyder 7.8.;
- СЗИ НСД Dallas Lock 8.0-K.;
- Средства защиты информации Secret Net 7;
- Linux (GNU GPL v.3).
- Academic VMware Fusion 10 Pro ESd.
- Academic VMware Workstation 14 Pro for Linux and Windows ESD.
- Virtual Box (GNU GPL v.2).

7. Перечень современных профессиональных баз данных и информационных справочных систем, используемых при осуществлении образовательного процесса по дисциплине (при необходимости)

В процессе осуществления образовательного процесса по дисциплине используются:

1. Автоматизированная библиотечно-информационная система «БУКИ-NEXT» - https://www.lib.uniyar.ac.ru/opac/bk_cat_find.php/
2. Электронно-библиотечная система «Юрайт - https://www.biblio-online.ru/
3. Электронно-библиотечная система «Университетская библиотека online» - https://www.biblioclub.ru/
4. Электронно-библиотечная система «Лань» - http://e.lanbook.com/
5. Портал разработчиков клиент-серверных приложений Microsoft Developer Network (MSDN) - https://msdn.microsoft.com/ru-ru/
6. Федеральный банк данных угроз безопасности, ведущийся в разделе «Техническая защита информации» официального сайта ФСТЭК России - https://bdu.fstec.ru/

8. Перечень основной и дополнительной учебной литературы, ресурсов информационно-телекоммуникационной сети «Интернет» (при необходимости), рекомендуемых для освоения дисциплины

а) основная литература

1. Внуков, А. А. Защита информации : учебное пособие для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2022. — 161 с. — (Высшее образование). — ISBN 978-5-534-07248-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/490277 (дата обращения: 25.01.2022).
2. Шаньгин, В. Ф. Информационная безопасность и защита информации / Шаньгин В. Ф. - Москва : ДМК Пресс, 2014. - 702 с. - ISBN 978-5-94074-768-0. - Текст : электронный // ЭБС "Консультант студента" : [сайт]. - URL : https://www.studentlibrary.ru/book/ISBN9785940747680.html (дата обращения: 25.01.2022). - Режим доступа : по подписке
3. Мифтахова, Л. Х. Программно-аппаратные средства защиты информации : учебное пособие / Л. Х. Мифтахова, А. Р. Касимова, В. Н. Красильников, В. А. Богомолов, А. Д. Алехин. - Санкт-петербург : ИЦ Интермедия, 2018. - 408 с. - ISBN 978-5-4383-0157-8. - Текст : электронный // ЭБС "Консультант студента" : [сайт]. - URL : https://www.studentlibrary.ru/book/ISBN9785438301578.html (дата обращения: 25.01.2022). - Режим доступа : по подписке.
4. Платонов, В.В. «Программно-аппаратные средства обеспечения информационной безопасности вычислительных сетей»: учебное пособие для вузов / В. В. Платонов;

УМО по образованию в обл. информационной безопасности. - М.: Академия, 2006. - 239 с. - (Высшее проф. образование. Информационная безопасность).
Режим доступа:
http://www.lib.uniyar.ac.ru/opac/bk_cat_card.php?rec_id=355769&cat_cd=YARSU

б) дополнительная литература

1. Шаньгин, В. Ф. Защита информации в компьютерных системах и сетях / Шаньгин В. Ф. - Москва : ДМК Пресс, 2012. - 592 с. - ISBN 978-5-94074-637-9. - Текст : электронный // ЭБС "Консультант студента" : [сайт]. - URL : https://www.studentlibrary.ru/book/ISBN9785940746379.html (дата обращения: 25.01.2022). - Режим доступа : по подписке.
2. Девянин, П. Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками : учебное пособие для вузов / Девянин П. Н. - Москва : Горячая линия - Телеком, 2012. - 320 с. - ISBN 978-5-9912-0147-6. - Текст : электронный // ЭБС "Консультант студента" : [сайт]. - URL : https://www.studentlibrary.ru/book/ISBN9785991201476.html (дата обращения: 25.01.2022). - Режим доступа : по подписке.

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

Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине включает в свой состав специальные помещения:

- учебные аудитории для проведения занятий лекционного типа;
- учебные аудитории для проведения практических занятий (семинаров);
- учебные аудитории для проведения групповых и индивидуальных консультаций;
- учебные аудитории для проведения текущего контроля и промежуточной аттестации;
- помещения для самостоятельной работы;
- лаборатория программно-аппаратных средств обеспечения информационной безопасности;
- помещения для хранения и профилактического обслуживания технических средств обучения.

Специальные помещения укомплектованы средствами обучения, служащими для представления учебной информации большой аудитории.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде ЯрГУ.

Автор:
Ассистент кафедры КБ и ММОИ. К. Ю. Герасимова

1

Приложение № 1 к рабочей программе дисциплины
«Комплексная защита объектов информатизации»

Фонд оценочных средств
для проведения текущего контроля успеваемости
и промежуточной аттестации студентов
по дисциплине

10.
11.

1. Типовые контрольные задания и иные материалы, используемые в процессе текущего контроля успеваемости

Перечень вопросов для опросов на практических занятиях:

1. Укажите преимущества электронного документооборота по сравнению с бумажным документооборотом. Укажите различия между понятиями «система электронного документооборота» (СЭД) и ECM (Enterprise Content Management).
2. Охарактеризуйте базовые составляющие системы электронного документооборота.
3. Укажите особенности построения и функционирования системы распределенного электронного документооборота.
4. Назовите угрозы информационной безопасности для СЭД и охарактеризуйте источники этих угроз.
5. Назовите основные угрозы ИБ баз данных. Укажите методы и средства защиты СУБД.
6. Охарактеризуйте методы и средства защиты корпоративного почтового документооборота.
7. Опишите функциональные возможности и архитектуру системы электронного документооборота DIRECTUM.
8. Охарактеризуйте приемы и методы защиты, реализованные в системе DIRECTUM.
9. Сформулируйте основополагающие принципы построения современных КИС.
10. Охарактеризуйте четыре уровня управления КИС.
11. Укажите необходимые условия обеспечения санкционированного доступа к информационным ресурсам предприятия.
12. Какие важные системные функции может выполнять КИС при реализации в ней принципа централизованного управления?
13. Объясните значение управления рисками предприятия для создания системы эффективной защиты информации на этом предприятии.
14. Какие требования необходимо учитывать при разработке архитектуры КСЗИ?
15. Перечислите меры и средства защиты, применяемые при построении комплексной системы защиты информации КИС.
16. Укажите основные подсистемы информационной безопасности, входящие в состав КСЗИ.
17. Опишите особенности подсистемы защиты информации от несанкционированного доступа.
18. Опишите назначение и особенности подсистемы контроля эффективности защиты информации.
19. Опишите назначение особенности подсистемы мониторинга и управления инцидентами ИБ.
20. Опишите назначение и особенности подсистемы обеспечения непрерывности функционирования средств защиты.
21. Сформулируйте понятия «межсетевое экранирование» и «межсетевой экран».

22. Объясните суть фильтрации информационного потока межсетевым экраном.
23. Какие параметры могут использоваться в качестве критериев анализа информационного потока?
24. Какие варианты решений принимаются при интерпретации правил фильтрации информационного потока?
25. Что представляют собой функции посредничества МЭ и программы посредники? Перечислите функции, которые могут выполнять программы посредники.
26. Назовите дополнительные возможности МЭ.
27. Укажите достоинства программно-аппаратного варианта исполнения межсетевых экранов.
28. Сформулируйте принципы формирования политики межсетевого взаимодействия, реализуемой системой МЭ.
29. Назовите основные схемы подключения межсетевых экранов. Опишите функционирование схемы с защищаемой закрытой и незащищаемой открытой подсетями.
30. Сформулируйте тенденции дальнейшего развития межсетевых экранов.
31. Назовите задачи системы управления ИБ КИС.
32. Как осуществляется управление учетными записями и правами доступа к рабочим станциям, серверам и другим активным устройствам КИС?

2. Список вопросов и (или) заданий для проведения промежуточной аттестации

Список вопросов к экзамену:

1. Комплексное обеспечение информационной безопасности.
2. Архитектура корпоративной информационной системы.
3. Структура системы защиты информации в корпоративной информационной системе.
4. Комплексный подход к обеспечению информационной безопасности корпоративной системы.
5. Подсистемы информационной безопасности корпоративной информационной системы.
6. Идентификация, аутентификация, авторизация, подотчетность в автоматизированных системах.
7. Модели управления доступом.
8. Техники и технологии управления доступом.
9. Администрирование доступа.
10. Методы управления доступом.
11. Мониторинг управления доступом.
12. Протоколы аутентификации.
13. Серверы аутентификации.
14. Средства аутентификации
15. Средства и методы сегментирования сети.
16. Функции межсетевых экранов.
17. Типы межсетевых экранов.
18. Экранирующие концентраторы.
19. Пакетные фильтры.
20. Основные компоненты межсетевых экранов.
21. Схемы подключения межсетевых экранов.
22. Уязвимости межсетевых экранов.
23. Концепция электронного документооборота.
24. Особенности защиты электронного документооборота.
25. Защита корпоративного почтового документооборота.

Правила выставления оценки на экзамене.

В экзаменационные билет включается два теоретических вопроса. На подготовку к ответу дается не менее 1часа.

По итогам экзамена выставляется одна из оценок: «отлично», «хорошо», «удовлетворительно» или «неудовлетворительно».

Оценка «Отлично» выставляется студенту, который демонстрирует глубокое и полное владение содержанием материала; осуществляет межпредметные связи. Студент дает развернутые, полные и четкие ответы на вопросы экзаменационного билета и дополнительные вопросы, соблюдает логическую последовательность при изложении материала. Грамотно использует терминологию.

Оценка «Хорошо» выставляется студенту, ответ которого на экзамене в целом соответствуют указанным выше критериям, но отличается меньшей обстоятельностью, глубиной, обоснованностью и полнотой. В ответе имеют место отдельные неточности (несущественные ошибки), которые исправляются самим студентом после дополнительных и (или) уточняющих вопросов экзаменатора.

Оценка «Удовлетворительно» выставляется студенту, который дает недостаточно полные и последовательные ответы на вопросы экзаменационного билета и дополнительные вопросы, но при этом демонстрирует умение выделить существенные и несущественные признаки и установить причинно-следственные связи. Ответы излагаются в терминах комплексной защиты объектов информатизации, но при этом допускаются ошибки в определении и раскрытии некоторых основных принципов, которые студент затрудняется исправить самостоятельно. При аргументации ответа студент не обосновывает свои суждения. На часть дополнительных вопросов студент затрудняется дать ответ или дает неверные ответы.

Оценка «Неудовлетворительно» выставляется студенту, который демонстрирует разрозненные, бессистемные знания; беспорядочно и неуверенно излагает материал; не умеет выделять главное и второстепенное, не устанавливает межпредметные связи; допускает грубые ошибки при определении сущности раскрываемых понятий, принципов, вследствие непонимания их существенных и несущественных признаков и связей; дает неполные ответы, логика и последовательность изложения которых имеют существенные и принципиальные нарушения, в ответах отсутствуют выводы. Дополнительные и уточняющие вопросы экзаменатора не приводят к коррекции ответов студента. На основную часть дополнительных вопросов студент затрудняется дать ответ или дает неверные ответы.

Оценка «Неудовлетворительно» выставляется также студенту, который взял экзаменационный билет, но отвечать отказался.

Приложение № 2 к рабочей программе дисциплины
«Комплексная защита объектов информатизации»

Методические указания для студентов по освоению дисциплины

Основной формой изложения материала по дисциплине «Комплексная защита объектов информатизации» являются лекции в формате монолога преподавателя с элементами лекции-беседы, во время которых у студентов есть возможность логически размыслить и предложить свое решение проблем или виденье принципов изложенных в материале.

Закрепление теоретического материала проводится на практических занятиях, во время которых студенты приобретают навыки и умения для дальнейшей профессиональной деятельности по своей специализации.

В связи с быстротечностью развития информационных технологий, электронные ресурсы предоставляют более актуальные и глубокие сведения по определенным вопросам курса. Для самостоятельной работы рекомендуется использовать именно их, так как они позволят углубить знания по теме, а также систематизировать полученные на лекции материалы. При появлении трудностей у студентов во время изучения особо сложных вопросов, они могут задать интересующие вопросы на консультациях.

Для проверки и контроля усвоения теоретического материала, приобретенных практических навыков, проводятся мероприятия текущей аттестации в виде опросов на практических занятиях, они учитываются наряду с результатами практических занятий при оценке текущей успеваемости.

В конце изучения дисциплины студенты сдают экзамен. Экзамен принимается по экзаменационным билетам, каждый из которых включает в себя два теоретических вопроса. На самостоятельную подготовку к экзамену выделяется 3 дня, в это время предусмотрена и групповая консультация.