МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

(МОСКОВСКИЙ ПОЛИТЕХ)

Факультет информационных технологий

УТВЕРЖДЕНО
Декан факультета
Информационных технологий
_____ / Д.Г. Демидов /
«16» ____02_____ 2023 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Аудит информационной безопасности»

Направление подготовки
09.03.01 Информатика и вычислительная техника

Профиль
«Кибербезопасность автоматизированных систем»

Квалификация
Бакалавр

Формы обучения
очная

Москва, 2023 г.

Разработчик(и):

степень, звание, должность /Кесель С. А. /

Согласовано:
И.о. заведующего кафедрой «Информационная безопасность», /А.Ю. Гневшев/

Руководитель образовательной программы, /А.Ю. Гневшев/

Содержание

1 Цели, задачи и планируемые результаты обучения по дисциплине

К **основным целям** освоения дисциплины «Аудит информационной безопасности» следует отнести:

- изучение студентами видов, практических методов и средств проведения аудита информационной безопасности (ИБ).

К **основным задачам** освоения дисциплины «Аудит информационной безопасности» следует отнести:

- формирование понимания процессов проверки и оценки ИБ, принципов организации процессов аудита и анализа рисков ИБ и подготовки отчетных документов;
- ознакомление с основными стандартами в области аудита ИБ, практическими приемами проведения аудита, методами сбора данных, оценки рисков и анализа защищенности;
- обучение инструментальным средствам проведения аудита ИБ.

Обучение по дисциплине «Аудит информационной безопасности» направлено на формирование у обучающихся следующих компетенций:

Код и наименование компетенций	Индикаторы достижения компетенции
ПК-2. Способен осуществлять администрирование процесса управления безопасностью сетевых устройств и программного обеспечения	ИПК-2.1. Знать: Общие принципы функционирования и архитектуру аппаратных, программных и программно-аппаратных средств администрируемой сети; Классификация ОС согласно классам безопасности; Средства защиты от несанкционированного доступа ОС и СУБД; ИПК-2.2. Уметь: Применять аппаратные и программные средства защиты сетевых устройств от несанкционированного доступа Настраивать параметры и сегментировать элементы администрируемой сети ИПК-2.3. Владеет: Планированием защиты и оценкой безопасности и защиты приложений и ОС от несанкционированного доступа Установкой специализированных программных и аппаратных средств защиты сетевых устройств администрируемой сети от несанкционированного доступа Настройка средств обеспечения безопасности удаленного доступа (операционной системы и специализированных протоколов)

	Документирование настроек средств обеспечения безопасности удаленного

2 Место дисциплины в структуре образовательной программы

Дисциплина «Аудит информационной безопасности» относится к числу профессиональных учебных обязательной части цикла (Б1.1) основной образовательной программы (Б1.1.37).

Изучение дисциплины опирается на знания, умения и навыки, приобретенные в предшествующих дисциплинах: «Организационное и правовое обеспечение информационной безопасности», «Физические основы информационной безопасности», «Разработка технических текстов и документации», «Введение в аналитику информационной безопасности», «Аналитика информационной безопасности».

3 Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 4 зачетных единицы, т.е. **144** академических часов (лабораторные занятия – 54 часа, лекции - 18 часов, самостоятельная работа - 72 часа, форма контроля – экзамен) в 6 семестре.

Структура и содержание дисциплины «Аудит информационной безопасности» по срокам и видам работы отражены в приложении.

1.1 Виды учебной работы и трудоемкость (по очной форме обучения)

№ п/п	Вид учебной работы	Количество часов	Семестры	
			6	
1	**Аудиторные занятия**	**72**	72	
	В том числе:			
1.1	Лекции	18	18	
1.2	Семинарские/практические занятия			
1.3	Лабораторные занятия	54	54	
2	**Самостоятельная работа**	72	72	
	В том числе:			
2.1	Домашние контрольные работы (ДКР)			
3	**Промежуточная аттестация**			
	Экзамен			
	Итого:	**144**	144	

3.1 Тематический план изучения дисциплины (по формам обучения)

3.2.1 Очная форма обучения

№ п/п	Разделы/темы дисциплины	Трудоемкость, час					
		Всего	Аудиторная работа				Самостоятельная работа
			Лекции	Семинарские/ практические занятия	Лабораторные занятия	Практическая подготовка	
1	Классификация информации в соответствии с российским законодательством	32	3		8		10
2	Типовые угрозы безопасности автоматизированных систем (АС)	24	3		7		10
3	Настройка и эксплуатация средств обеспечения безопасности АС.	32	3		8		10
4	Средства и методы проектирования и построения защищенных АС.	16	3		8		10
5	Средства выявления и нейтрализации попыток нарушения безопасности АС.	24	2		7		10
6	Виды моделей угроз. Разработка и внедрение.	8	2		8		10
7	Разработка организационно-распорядительной и нормативно-технической документации для защищенных АС	8	2		8		12
Итого		**144**	**18**		**54**		**72**

3.2 Содержание дисциплины

Тема 1. Классификация информации в соответствии с российским законодательством.

Тема 2. Типовые угрозы безопасности автоматизированных систем (АС).

Тема 3. Настройка и эксплуатация средств обеспечения безопасности автоматизированных систем (АС).

Тема 4. Средства и методы проектирования и построения защищенных автоматизированных систем (АС).

Тема 5. Средства выявления и нейтрализации попыток нарушения безопасности автоматизированных систем (АС).

Тема 6. Виды моделей угроз. Разработка и внедрение.

Тема 7. Разработка организационно-распорядительной и нормативно-технической документации для защищенных автоматизированных систем (АС).

4 Учебно-методическое и информационное обеспечение

4.1 Основная литература

- Экономическая информатика : учебник и практикум для бакалавриата и магистратуры / Ю. Д. Романова [и др.] ; ответственный редактор Ю. Д. Романова. — Москва : Издательство Юрайт, 2023. — 495 с. — (Высшее образование). — ISBN 978-5-9916-3770-1. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/533745.
- Нетесова, О. Ю. Информационные системы и технологии в экономике : учебное пособие для вузов / О. Ю. Нетесова. — 4-е изд., испр. и доп. — Москва : Издательство Юрайт, 2023. — 178 с. — (Высшее образование). — ISBN 978-5-534-15926-4. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/510292.
- Петренко, В.И. Защита персональных данных в информационных системах : учебное пособие / В.И. Петренко ; Министерство образования и науки Российской Федерации, Федеральное государственное автономное образовательное учреждение высшего профессионального образования «Северо-Кавказский федеральный университет». – Ставрополь : СКФУ, 2016. – 201 с. : схем. – Режим доступа: по подписке. – URL: http://biblioclub.ru/index.php?page=book&id=459205. – Текст : электронный.
- Милешко, Л. П. Экономика и менеджмент безопасности : учебное пособие для вузов / Л. П. Милешко. — Москва : Издательство Юрайт, 2023. — 99 с. — (Высшее образование). — ISBN 978-5-534-13764-4. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/519758.
- Новая парадигма защиты и управления персональными данными в Российской Федерации и зарубежных странах в условиях развития систем обработки данных в сети Интернет : монография / А.С. Дупан, А.К. Жарова, В.М. Елин и др. ; под ред. А.С. Дупан ; Высшая школа экономики, Национальный исследовательский университет. – Москва : Издательский дом Высшей школы экономики, 2016. – 343 с. – Режим доступа: по подписке. – URL:

http://biblioclub.ru/index.php?page=book&id=486427 (дата обращения: 18.08.2019). – Библиогр. в кн. – ISBN 978-5-7598-1386-6 (в обл.). – Текст : электронный.

4.2 Дополнительная литература

- Аверченков, В.И. Защита персональных данных в организации : монография / В.И. Аверченков, М.Ю. Рытов, Т.Р. Гайнулин. – 3-е изд., стер. – Москва : Флинта, 2016. – 124 с. – Режим доступа: по подписке. – URL: http://biblioclub.ru/index.php?page=book&id=93260 (дата обращения: 18.08.2019). – Библиогр.: с. 107-109. – ISBN 978-5-9765-1273-3. – Текст : электронный.
- Загинайлов, Ю.Н. Теория информационной безопасности и методология защиты информации : учебное пособие / Ю.Н. Загинайлов. – Москва ; Берлин : Директ-Медиа, 2015. – 253 с. : ил. – Режим доступа: по подписке. – URL: http://biblioclub.ru/index.php?page=book&id=276557 (дата обращения: 18.08.2019). – Библиогр. в кн. – ISBN 978-5-4475-3946-7. – DOI 10.23681/276557. – Текст : электронный.

4.3 Электронные образовательные ресурсы

Электронный образовательный ресурс на разработке.

5 Материально-техническое обеспечение

5.1 Требования к оборудованию и помещению для занятий

Для проведения всех видов занятий необходимо презентационное оборудование (мультимедийный проектор, экран) – 1 комплект.

Для проведения лабораторных занятий необходимо наличие компьютерных классов оборудованных современной вычислительной техникой из расчета одно рабочее место на одного обучаемого.

5.2 Требования к программному обеспечению

1. Компьютер с операционной системой Microsoft Windows.
2. Веб-браузер Chrome.
3. Microsoft Office.

6 Методические рекомендации

6.1 Методические рекомендации для преподавателя по организации обучения

1. При подготовке к занятиям следует предварительно проработать материал занятия, предусмотрев его подачу точно в отведенное для этого время занятия. Следует подготовить необходимые материалы – теоретические сведения, задачи и др. При проведении занятия следует контролировать подачу материала и решение заданий с учетом учебного времени, отведенного для занятия.

2. При проверке работ и отчетов следует учитывать не только правильность выполнения заданий, но и оптимальность выбранных методов решения, правильность выполнения всех его шагов.

6.2 Методические указания для обучающихся по освоению дисциплины

Изучение дисциплины осуществляется в строгом соответствии с целевой установкой в тесной взаимосвязи учебным планом. Основой теоретической подготовки студентов являются лекции.

В процессе самостоятельной работы студенты закрепляют и углубляют знания, полученные во время аудиторных занятий, готовятся к экзамену, а также самостоятельно изучают отдельные темы учебной программы.

7 Фонд оценочных средств

7.1 Методы контроля и оценивания результатов обучения

В процессе обучения используются следующие оценочные формы самостоятельной работы студентов, оценочные средства текущего контроля успеваемости и промежуточных аттестаций:

- компьютерное тестирование;
- дифференцированный зачет.

7.2 Шкала и критерии оценивания результатов обучения

Показателем оценивания компетенций на различных этапах их формирования является достижение обучающимися планируемых результатов обучения по дисциплине.

Показатель	Критерии оценивания			
	2	3	4	5
ПК-2. Способен осуществлять администрирование процесса управления безопасностью сетевых устройств и программного обеспечения				
ИПК-2.1. Знать: Общие принципы функционирования и архитектуру аппаратных, программных и программно-аппаратных средств администрируемой сети; Классификация ОС согласно классам безопасности;	Обучающийся демонстрирует полное отсутствие или недостаточное соответствие материалу дисциплины знаний, указанных в индикаторах компетенций дисциплины «Знать» (см. п. 3).	Обучающийся демонстрирует неполное соответствие следующих знаний, указанных в индикаторах компетенций дисциплины «Знать» (см. п. 3). Допускаются значительные ошибки, проявляется недостаточность	Обучающийся демонстрирует частичное соответствие следующих знаний, указанных в индикаторах компетенций дисциплины «Знать» (см. п. 3). Но допускаются незначительные ошибки, неточности,	Обучающийся демонстрирует полное соответствие следующих знаний, указанных в индикаторах компетенций дисциплины «Знать» (см. п. 3). Свободно оперирует приобретенным и знаниями.

Средства защиты от несанкционированного доступа ОС и СУБД; ИПК-2.2. Уметь: Применять аппаратные и программные средства защиты сетевых устройств от несанкционированного доступа Настраивать параметры и сегментировать элементы администрируемой сети ИПК-2.3. Владеет: Планированием защиты и оценкой безопасности и защиты приложений и ОС от несанкционированного доступа Установкой специализированных программных и аппаратных средств защиты сетевых устройств администрируемой сети от		знаний, по ряду показателей, обучающийся испытывает значительные затруднения при оперировании знаниями при их переносе на новые ситуации.	затруднения при аналитических операциях.	

несанкционированного доступа Настройка средств обеспечения безопасности удаленного доступа (операционной системы и специализированных протоколов) Документирование настроек средств обеспечения безопасности удаленного				

7.3 Оценочные средства

7.3.1 Список вопросов для экзамена по дисциплине.

1. Аудит ИБ. Концепция IA*4
2. Оценочные стандарты и спецификации ИБ. Состав, основные стандарты и спецификации.

3. В каком нормативном правовом акте закреплены все виды конфиденциальной информации?

4. Что такое персональные данные в соответствии с ФЗ-152?

5. Какую информацию запрещено относить к конфиденциальной в соответствии с законом РФ?

6. Раскройте понятие "конфиденциальный документ"

7. Перечислите 4 вида тайн относящихся к персональным данным. В случае если Вам известно больше видов тайн относящихся к ПД их следует перечислить.

8. В каком случае фотографию можно отнести к биометрическим персональным данным?
9. Может ли являться оператором персональных данных физическое лицо?
10. Какие действия можно производить с персональными данными?

11. Перечислите классификационные группы персональных данных по признаку свободы оборота.
12. Кто является основным ответственным за определение уровня классификации информации?
13. Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности?
14. Если различным группам пользователей с различным уровнем доступа требуется доступ к одной и той же информации, какое из указанных ниже действий следует предпринять руководству?
15. Кто в конечном счете несет ответственность за гарантии того, что данные классифицированы и защищены?
16. Основной документ, на основе которого проводится политика информационной безопасности?
17. Коммерческая тайна это….
18. Государственная тайна это…
19. Банковская тайна это….
20. Профессиональная тайна…
21. Как называется тайна переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений?
22. Элемент аппаратной защиты, где используется резервирование особо важных компьютерных подсистем.
23. Стандарт «Общие Критерии». Концепция, основные понятия и определения.
24. Стандарт «Общие Критерии». Оценочные уровни доверия (ОУД)
25. СТО БР ИББС Структура, концепция, основные понятия и определения.
26. СТО БР ИББС Проведение аудита соответствия кредитно-финансовой организации требованиям СТО БР ИББС.
27.. PCI DSS Структура, концепция, основные понятия и определения.
28. PCI DSS Проведение аудита соответствия требованиям PCI DSS
29. 24. PCI DSS Проведение самооценки соответствия требованиям PCI DSS
30. PCI DSS Основные требования (12 требований)