МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»
(МОСКОВСКИЙ ПОЛИТЕХ)

Факультет информационных технологий

УТВЕРЖДАЮ
Декан факультета
информационных технологий
/Д. Г. Демидов/
"28" апреля 2022 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Введение в аналитику информационной безопасности»

Направление подготовки
10.05.03 «Информационная безопасность автоматизированных систем»

Профиль
«Безопасность открытых информационных систем»

Квалификация
Специалист по защите информации

Формы обучения
Очная

Москва, 2022 г.

Разработчик(и):

Доцент, к.т.н., доцент  /И.В. Калуцкий/

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 4
2 Место дисциплины в структуре образовательной программы 4
3 Структура и содержание дисциплины 4
3.1 Виды учебной работы и трудоемкость 5
3.2 Тематический план изучения дисциплины 5
3.3 Содержание дисциплины 5
3.4 Тематика семинарских/практических и лабораторных занятий 6
3.5 Тематика курсовых проектов (курсовых работ) 6
4 Учебно-методическое и информационное обеспечение 6
4.1 Нормативные документы и ГОСТы 6
4.2 Основная литература 7
4.3 Дополнительная литература 7
4.4 Электронные образовательные ресурсы 8
4.5 Лицензионное и свободно распространяемое программное обеспечение 8
4.6 Современные профессиональные базы данных и информационные справочные системы 8
5 Материально-техническое обеспечение 9
6 Методические рекомендации 9
6.1 Методические рекомендации для преподавателя по организации обучения 9
6.2 Методические указания для обучающихся по освоению дисциплины 9
7 Фонд оценочных средств 10
7.1 Методы контроля и оценивания результатов обучения 10
7.2 Шкала и критерии оценивания результатов обучения 10
7.3 Оценочные средства 12

1. Цели, задачи и планируемые результаты обучения по дисциплине

К **основным целям** освоения дисциплины «Введение в аналитику информационной безопасности» следует отнести:

• формирование комплекса теоретических знаний и практических навыков по аналитике информационной безопасности.

К **основным задачам** освоения дисциплины «Введение в аналитику информационной безопасности» следует отнести:

- усвоение основных понятий аналитики и аудита информационной безопасности;
- выработка навыков аналитики информационной безопасности;
- выработка навыков классифицировать и оценивать угрозы безопасности информации для объектов информации.

Обучение по дисциплине «Введение в аналитику информационной безопасности» направлено на формирование у обучающихся следующих компетенций:

Код и наименование компетенций	Индикаторы достижения компетенции
ОПК-15 Способен осуществлять администрирование и контроль функционирования средств и систем защиты информации автоматизированных систем, инструментальный мониторинг защищенности автоматизированных систем	ОПК-15.1 Обладает знаниями о методах контроля и администрирования вычислительных сетей в том числе средств защиты информации. ОПК-15.2 Применяет инструменты администрирования оборудования вычислительных сетей. Использует системы журналирования событии для узлов вычислительной сети. ОПК-15.3 Обладает навыками анализа системных конфигураций и журналов узлов вычислительной сети

2. Место дисциплины в структуре образовательной программы

Дисциплина «Введение в аналитику информационной безопасности» относится к числу профессиональных учебных дисциплин обязательной части цикла (Б.1) основной образовательной программы (Б1.1.24).

Изучение дисциплины опирается на знания, умения и навыки, приобретенные в предшествующих дисциплинах: «Организационное и правовое обеспечение информационной безопасности», «Основы сетевых технологий», «Основы ИКТ», «Системы управления базами данных».

3. Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 4 зачетных единицы, т.е. **144** академических часов (лекции – 18 часов, лабораторные занятия – 54 часа, самостоятельная работа - 72 часов, форма контроля – дифференцированный зачёт) в 3 семестре.

3.1. Виды учебной работы и трудоемкость
(по формам обучения)

3.1.1 Очная форма обучения

№ п/п	Вид учебной работы	Количество часов	Семестры	
			Семестр	Неделя семестра
1	**Аудиторные занятия**	**72**	3	1-19
	В том числе:			
1.1	Лекции	18	3	1-19
1.2	Семинарские/практические занятия	-	-	-
1.3	Лабораторные занятия	**54**	3	1-19
2	**Самостоятельная работа**	**72**	3	1-19
3	**Промежуточная аттестация**			
	Дифференцированный зачёт		3	По расписанию
	Итого	**144**		

3.2. 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	Основные определения. Методы обеспечения ИБ. Угрозы ИБ. Построение системы ИБ. Построение СИБ.	18	2	-	8	-	10
2	Моделирование угроз.	18	2	-	8	-	10
3	Управление рисками ИБ.	18	2	-	8	-	10
4	Основные принципы создания политик по ИБ.	18	2	-	8	-	10
5	Аудит ИБ организаций.	18	2	-	8	-	10
6	Управление инцидентами ИБ. (Стандарты)	22	4	-	8	-	10
7	Управление инцидентами ИБ.	22	4	-	6	-	12
Итого		**144**	**18**		**54**		**72**

3.3. Содержание дисциплины

Раздел 1. Основные определения. Методы обеспечения ИБ. Угрозы ИБ. Построение системы ИБ. Построение СИБ..

Раздел 2. Моделирование угроз.

Раздел 3. Управление рисками ИБ.

Раздел 4. Основные принципы создания политик по ИБ.

Раздел 5. Аудит ИБ организаций.

Раздел 6. Управление инцидентами ИБ. (Стандарты)

Раздел 7. Управление инцидентами ИБ.

3.4. Тематика семинарских/практических и лабораторных занятий

3.4.1 Семинарские/практические занятия

Не предусмотрены программой.

3.4.2 Лабораторные занятия

Лабораторная работа 1. Основные определения. Методы обеспечения ИБ. Угрозы ИБ. Построение системы ИБ. Построение СИБ.**.**

Лабораторная работа 2. Моделирование угроз.

Лабораторная работа 3. Управление рисками ИБ.

Лабораторная работа 4. Основные принципы создания политик по ИБ.

Лабораторная работа 5. Аудит ИБ организаций.

Лабораторная работа 6. Управление инцидентами ИБ. (Стандарты)

Лабораторная работа 7. Управление инцидентами ИБ.

3.5. Тематика курсовых проектов (курсовых работ)

Не предусмотрены программой.

4. Учебно-методическое и информационное обеспечение

4.1. Нормативные документы и ГОСТы

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) // Российская газета. № 237. 25.12.1993.

2. Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне» // СЗ РФ. 2004. № 32. ст. 3283.

3. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // СЗ РФ. 2006. № 31 (1 ч.).ст. 3448.

4. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» // СЗ РФ. 2006. № 31 (1 ч.).ст. 3451.

5. Приказ ФСТЭК России от 11 февраля 2013 г. N 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»

6. "Методический документ. Методика оценки угроз безопасности информации" (утв. ФСТЭК России 05.02.2021)

7. ГОСТ Р ИСО/МЭК 27005-2010 Национальный стандарт российской федерации информационная технология методы и средства обеспечения безопасности менеджмент риска информационной безопасности

8. "ГОСТ Р ИСО/МЭК 27001-2021. Национальный стандарт Российской

Федерации. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования"

4.2. Основная литература

1. Конкин, Ю. В. Основы информационной безопасности : учебное пособие / Ю. В. Конкин, Ю. М. Кузьмин, В. Н. Пржегорлинский. — Рязань : РГРТУ, 2021. — 96 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/220418

2. Чесалин, А. Н. Основы искусственного интеллекта с приложениями в информационной безопасности : учебное пособие / А. Н. Чесалин. — Москва : РТУ МИРЭА, 2021. — 155 с. — ISBN 978-5-7339-1589-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/182429

3. Аудит безопасности информационных систем / Николай Скрабцов. – Санкт-Петербург : Питер,, 2017. – 272 с. – ISBN 978-5-4461-0662-2. 2. Аверченков, В. И. Аудит информационной безопасности : учебное пособие : [16+] / В. И. Аверченков. – 4-е изд., стер. – Москва : ФЛИНТА, 2021. – 269 с. : ил., схем., табл. – Режим доступа: по подписке. – URL: https://lib.biblioclub.ru/index.php?page=book&id=93245

4.3. Дополнительная литература

1. Нестеров, С.А. Основы информационной безопасности : учебное пособие / С.А. Нестеров ; Министерство образования и науки Российской Федерации, Санкт-Петербургский государственный политехнический университет. – Санкт-Петербург : Издательство Политехнического университета, 2014. – 322 с. : схем., табл., ил. – Режим доступа: по подписке. – URL: http://biblioclub.ru/index.php?page=book&id=363040 (дата обращения: 28.08.2019). – ISBN 978-5-7422-4331-1. – Текст : электронный.

2. Аудит информационной безопасности органов исполнительной власти : учебное пособие / В.И. Аверченков, М.Ю. Рытов, А.В. Кувыклин, М.В. Рудановский. – 4-е изд., стер. – Москва : Флинта, 2016. – 100 с. – (Организация и технология защиты информации). – Режим доступа: по подписке. – URL: http://biblioclub.ru/index.php?page=book&id=93259 (дата обращения: 28.08.2019). – Библиогр.: с. 83-84. – ISBN 978-5-9765-1277-1. – Текст : электронный.

3. Прохорова, О.В. Информационная безопасность и защита информации : учебник / О.В. Прохорова ; Министерство образования и науки РФ, Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Самарский государственный архитектурно-строительный университет». – Самара : Самарский государственный архитектурно-строительный университет, 2014. – 113 с. : табл., схем., ил. – Режим доступа: по подписке. – URL: http://biblioclub.ru/index.php?page=book&id=438331 (дата обращения: 28.08.2019). – Библиогр. в кн. – ISBN 978-5-9585-0603-3. – Текст : электронный.

4. Голиков, А.М. Защита информации в инфокоммуникационных системах и сетях : учебное пособие / А.М. Голиков ; Министерство образования и науки Российской Федерации, Томский Государственный Университет Систем Управления и Радиоэлектроники (ТУСУР). – Томск : Томский государственный университет систем управления и радиоэлектроники, 2015. – 284 с. : схем., табл., ил. – Режим доступа: по

подписке. – URL: http://biblioclub.ru/index.php?page=book&id=480637 (дата обращения: 28.08.2019). – Библиогр. в кн. – Текст : электронный.

4.4. Электронные образовательные ресурсы

Электронный образовательный ресурс разрабатывается.

4.5 Лицензионное и свободно распространяемое программное обеспечение

1. Компьютер с операционной системой Microsoft Windows.
2. Microsoft Office.

4.6 Современные профессиональные базы данных и информационные справочные системы

1. eLIBRARY.RU: Научная электронная библиотека: сайт. - Москва, 2000 -. - URL: https://www.elibrary.ru (дата обращения: 16.03.2021). – Текст: электронный.

2. ЛАНЬ: электронно-библиотечная система: сайт. – Санкт-Петербург,2010 -. - URL: https://e.lanbook.com (дата обращения: 10.03.2021). - Текст: электронный.

3. ФСТЭК России: Государственный реестр сертифицированных средств защиты информации. – Москва, 2014. - . - URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty-po-sertifikatsii/153-sistema-sertifikatsii (дата обращения: 10.03.2021). - Текст: электронный.

4. Библиографическая и реферативная база данных научной периодики «Scopus» - www.scopus.com.

5. Сайт Федеральной службы безопасности России (ФСБ России). - http://www.fsb.ru.

6. Сайт Федеральной службы по техническому и экспортному контролю (ФСТЭК России). - http://www.fstec.ru.

7. Портал технического комитета по стандартизации «Защита информации». – http://tk.gost.ru/wps/portal/tk362

8. Информационно-аналитический Интернет-портал ISO27000.ru. – http://www.iso27000.ru/.

5. Материально-техническое обеспечение

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.

6. Методические рекомендации

6.1 Методические рекомендации для преподавателя по организации обучения

При подготовке к лабораторным работам следует предварительно проработать теоретический материал занятия, предусмотрев его подачу точно в отведенное для этого время занятия.

При проведении занятия следует контролировать подачу материала и решение заданий с учетом учебного времени, отведенного для занятия.

При проверке работ и отчетов следует учитывать правильность выполнения лабораторных работ на всех этапах.

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, дорабатывают конспекты лекций, готовятся к зачету, а также самостоятельно изучают отдельные темы учебной программы.

Лабораторные работы проводятся по наиболее важным темам дисциплины. Осуществляется закрепление знаний, полученных студентами на лекциях и в процессе самостоятельной работы. Особое внимание обращается на развитие умений и навыков установления связи положений теории с профессиональной деятельностью будущего специалиста по ИБ. Лабораторные работы проводятся по теоретическим и проблемным вопросам ИБ. Лабораторные работы предполагает творческие дискуссии, активный обмен мнениями по поставленным вопросам, заслушивание и обсуждение докладов по предложенным преподавателем темам.

Текущий контроль осуществляется на практических занятиях, промежуточный контроль осуществляется на экзамене в письменной (устной) форме.

Самостоятельная работа осуществляется индивидуально.

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:

- проведение лабораторных работ (практических занятий с использованием спецтехники) и их защита;
- самостоятельная подготовка и проведение презентаций по темам дисциплины;
- экзамен.

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
ОПК-15 Способен осуществлять администрирование и контроль функционирования средств и систем защиты информации автоматизированных систем, инструментальный мониторинг защищенности автоматизированных систем				
ОПК-15.1 Обладает знаниями о методах контроля и администрирования вычислительных сетей в том числе средств защиты информации. ОПК-15.2 Применяет инструменты администрирования оборудования вычислительных сетей. Использует системы журналирования событии для узлов вычислительной сети. ОПК-15.3 Обладает навыками анализа системных конфигураций и журналов узлов вычислительной сети	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 знаний, по ряду показателей, обучающийся испытывает значительные затруднения при оперировании знаниями при их переносе на новые ситуации.	Обучающийся демонстрирует частичное соответствие следующих знаний, указанных в индикаторах компетенций дисциплины «Знать» (см. п. 3). Но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях.	Обучающийся демонстрирует полное соответствие следующих знаний, указанных в индикаторах компетенций дисциплины «Знать» (см. п. 3). Свободно оперирует приобретенными знаниями.

Форма промежуточной аттестации: дифференцированный зачет.

По итогам промежуточной аттестации по дисциплине (модулю) выставляется оценка «отлично», «хорошо», «удовлетворительно» или «неудовлетворительно».

Шкала оценивания	Описание
Отлично	Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует соответствие знаний, умений, навыков приведенным в таблицах показателей, оперирует приобретенными знаниями, умениями, навыками, применяет их в ситуациях повышенной сложности. При этом могут быть допущены незначительные ошибки, неточности, затруднения при аналитических операциях, переносе знаний и умений на новые, нестандартные ситуации.
Хорошо	Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует неполное, правильное соответствие знаний, умений, навыков приведенным в таблицах показателей, либо если при этом были допущены 2-3 несущественные ошибки.
Удовлетворительно	Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует соответствие знаний, в котором освещена основная, наиболее важная часть

	материала, но при этом допущена одна значительная ошибка или неточность.
Неудовлетворительно	Не выполнен один или более видов учебной работы, предусмотренных учебным планом. Студент демонстрирует неполное соответствие знаний, умений, навыков приведенным в таблицах показателей, допускаются значительные ошибки, проявляется отсутствие знаний, умений, навыков по ряду показателей, студент испытывает значительные затруднения при оперировании знаниями и умениями при их переносе на новые ситуации.

7.3 Оценочные средства

7.3. **Список вопросов для экзамена по дисциплине**

1. Проверка состояния организации работ и выполнения организационно-технических требований по защите информации. Оценка правильности классификации и категорирования объекта информатизации.
2. Технологии защиты приложений, баз данных, операционных систем, сетей телекоммуникационного оборудования; песочница и изолирование;
3. Выявления угроз ИБ на основе сведений об уязвимостях (классификация угроз, формирование рекомендаций по устранению уязвимостей и минимизации бизнес-рисков);
4. Распознавание вредоносных программ и защита; безопасность мобильных платформ.
5. Утилизация данных: проблемы повторного использования.
6. P2P-приложения: тенденции развития и аспекты безопасности.
7. Безопасность Web-браузеров. Уязвимости технологии web 2.0.
8. Безопасность беспроводных технологий.
9. Средства взлома парольных систем и противодействие им. СПАМ: способы распространения, принципы и средства противодействия. Проблемы противодействия фишингу и фармингу.
10. Распределенные атаки, отказ в обслуживании и противодействие им. Безопасность информационных систем построенных с использованием с использованием технологий виртуализации. Проблемы безопасности «виртуальных» инфраструктур e-commerce.
11. Принципы тестирования на проникновение и анализа веб-приложений; Тестирование на проникновение (пентест). Нагрузочное тестирование.
12. Управление рисками. Методы численного анализа рисков Оценка и минимизация рисков. Понятие модели нарушителя. Типы моделей.
13. Независимые информационно-аналитические службы и центры.
14. Охарактеризовать актуальную статистику инцидентов на текущий год.
15. Типовые сложности при реализации ГОСТ VPN.
16. Помогут ли рекомендации NIST обеспечить IoT-безопасность в эпоху подключенных устройств.

17. Способы обхода антивирусов с помощью вредоносных файлов Microsoft Office.
18. Обзор систем и сервисов для проверки деловой репутации юридических лиц.
19. Как искусственный интеллект влияет на беспроводные сети и кибербезопасность.
20. Архитектура DaVinci и интеллектуальное обнаружение неизвестных угроз в МСЭ.
21. Облачный SOC (центр мониторинга информационной безопасности) на примере Softline.
22. Категорирование объектов критической информационной инфраструктуры (КИИ).
23. Как защитить от взлома корпоративные сети Wi-Fi.
24. Четыре основные концепции безопасности облачных технологий.
25. Систем противодействия банковскому мошенничеству (антифрод)