МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ,
СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФ. М.А. БОНЧ-БРУЕВИЧА»
(СПбГУТ)

Кафедра Безопасности информационных систем
(полное наименование кафедры)

СПбГУТ))) Документ подписан простой электронной подписью
Сертификат: 009b47d8b89b08d0f6
Владелец: Киричек Руслан Валентинович
Действителен с 13.02.2023 по 12.02.2028

УТВЕРЖДАЮ
Первый проректор – проректор по учебной работе
_____ А.В. Абилов
«23» 06 2023 г.

Регистрационный №_23.02/265-Д

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Инструментальный анализ защищенности
(наименование дисциплины)

образовательная программа высшего образования

09.03.02 Информационные системы и технологии
(код и наименование направления подготовки / специальности)

бакалавр
(квалификация)

Технологии проектирования защищенных систем обработки данных
(направленность / профиль образовательной программы)

очная форма, очно-заочная форма
(форма обучения)

Санкт-Петербург

Рабочая программа дисциплины составлена на основе требований Федерального государственного образовательного стандарта высшего образования по направлению (специальности) подготовки «09.03.02 Информационные системы и технологии», утвержденного приказом Министерства образования и науки Российской Федерации от 19.09.2017 № 926, и в соответствии с рабочим учебным планом, утвержденным ректором университета.

1. Цели и задачи дисциплины

Целью преподавания дисциплины «Инструментальный анализ защищенности» является:

подготовка обучающихся к применению методов и программных средств проверки безопасности компьютерных систем с целью обнаружения уязвимостей и выработки рекомендаций по их устранению.

Эта цель достигается путем решения следующих(ей) задач(и):

изучения основных понятий и аспектов информационной безопасности, классов угроз информационной безопасности, направлений атаки на компьютерные системы, программных средств и способов, которые применяются злоумышленниками для компрометации целевой системы.

2. Место дисциплины в структуре образовательной программы

Дисциплина «Инструментальный анализ защищенности» Б1.В.ДВ.02.01 является дисциплиной по выбору части, формируемой участниками образовательных отношений блока 1 учебного плана подготовки бакалавриата по направлению «09.03.02 Информационные системы и технологии». Исходный уровень знаний и умений, которыми должен обладать студент, приступая к изучению данной дисциплины, определяется изучением таких дисциплин, как «Инфокоммуникационные системы и сети»; «Информационные технологии»; «Криптографическая защита информации»; «Методы и средства защиты информации».

3. Перечень планируемых результатов обучения, соотнесенных с планируемыми результатами освоения образовательной программы

Процесс изучения дисциплины направлен на формирование следующих компетенций:

Таблица 1

№ п/п	Код компетенции	Наименование компетенции
1	ПК-31	Способность обеспечивать информационную безопасность хранилищ и баз данных, баз знаний

Индикаторы достижения компетенций

Таблица 2

ПК-31.1	Знать: угрозы и мероприятия по обеспечению информационной безопасности хранилищ и баз данных, баз знаний
ПК-31.2	Уметь: выявлять угрозы и разрабатывать мероприятия по обеспечению информационной безопасности хранилищ и баз данных, баз знаний
ПК-31.3	Иметь навыки: идентификации угроз и реализации мероприятий по обеспечению информационной безопасности хранилищ и баз данных, баз знаний

4. Объем дисциплины и виды учебной работы

Очная форма обучения

Таблица 3

Вид учебной работы		Всего часов	Семестры
			7
Общая трудоемкость	3 ЗЕТ	108	108
Контактная работа с обучающимися		50.25	50.25
в том числе:			
Лекции		16	16
Практические занятия (ПЗ)		34	34
Лабораторные работы (ЛР)			-
Защита контрольной работы			-
Защита курсовой работы			-
Защита курсового проекта			-
Промежуточная аттестация		0.25	0.25
Самостоятельная работа обучающихся (СРС)		57.75	57.75
в том числе:			
Курсовая работа			-
Курсовой проект			-
И / или другие виды самостоятельной работы: подготовка к лабораторным работам, практическим занятиям, контрольным работам, изучение теоретического материала		49.75	49.75
Подготовка к промежуточной аттестации		8	8
Вид промежуточной аттестации			Зачет

Очно-заочная форма обучения

Таблица 4

Вид учебной работы		Всего часов	Семестры
			8
Общая трудоемкость	3 ЗЕТ	108	108
Контактная работа с обучающимися		36.25	36.25
в том числе:			
Лекции		12	12
Практические занятия (ПЗ)		24	24
Лабораторные работы (ЛР)			-
Защита контрольной работы			-
Защита курсовой работы			-
Защита курсового проекта			-
Промежуточная аттестация		0.25	0.25
Самостоятельная работа обучающихся (СРС)		71.75	71.75
в том числе:			
Курсовая работа			-
Курсовой проект			-
И / или другие виды самостоятельной работы: подготовка к лабораторным работам, практическим занятиям, контрольным работам, изучение теоретического материала		63.75	63.75
Подготовка к промежуточной аттестации		8	8
Вид промежуточной аттестации			Зачет

5. Содержание дисциплины

5.1. Содержание разделов дисциплины.

Таблица 5

№ п/п	Наименование раздела дисциплины	Содержание раздела	№ семестра		
			очная	очно-заочная	заочная
1	Раздел 1. Основы аудита информационной безопасности	Принципы системности, комплексности, непрерывности защиты, гибкости управления и применения защитных механизмов, открытости алгоритмов и механизмов защиты, простоты применения защитных мер и средств. Правовые (законодательные), аппаратно-программные меры обеспечения безопасности компьютерных систем.	7	8	
2	Раздел 2. Требования к информационной безопасности	Классы защищенности автоматизированных систем. Основные требования и рекомендации по защите информации, составляющей служебную или коммерческую тайну, а также персональных данных. Требования к защите информации в автоматизированных системах, локальных вычислительных сетях, на рабочих местах пользователей ПК. Аутентификации подлинности его автора, возможности злоумышленника при реализации угроз, направленных на нарушение целостности передаваемых сообщений и подлинность их авторства, метод решения данных проблем.	7	8	
3	Раздел 3. Элементы информационной безопасности	Элементы информационной безопасности. Угрозы информационной безопасности и векторы атак. Классы угроз информационной безопасности.Типы атак. Меры противодействия. Изучение защищаемой системы с позиции злоумышленника. Тестирование на проникновение.	7	8	
4	Раздел 4. Инструментальные средства оценки безопасности компьютерных систем	Средства и способы предварительной разведки и сбора информации. Средства сканирования сетей. Средства перечисления локальных и сетевых ресурсов. Средства, используемые для взлома системы. Средства прослушивание сети — снифферы. Средства организации атаки "Отказ в обслуживании".	7	8	
5	Раздел 5. Защита от разрушающих программных воздействий	Понятие и виды активизирующих событий. Модели взаимодействия прикладной программы и программы с потенциально опасными последствиями. Общие и специализированные методы защиты программного обеспечения от разрушающих программных воздействий	7	8	

5.2. Междисциплинарные связи с обеспечиваемыми (последующими) дисциплинами.

Таблица 6

№ п/п	Наименование обеспечиваемых (последующих) дисциплин
1	Интеллектуальные информационные системы и технологии
2	Системы ведения хранилищ данных

5.3. Разделы дисциплин и виды занятий.

Очная форма обучения

Таблица 7

№ п/п	Наименование раздела дисциплины	Лекции	Практ. занятия	Лаб. занятия	Семинары	СРС	Всего часов
1	Раздел 1. Основы аудита информационной безопасности	2				6	8
2	Раздел 2. Требования к информационной безопасности	2				6	8
3	Раздел 3. Элементы информационной безопасности	4	2			8	14
4	Раздел 4. Инструментальные средства оценки безопасности компьютерных систем	6	28			23.75	57.75
5	Раздел 5. Защита от разрушающих программных воздействий	2	4			6	12
	Итого:	16	34	-	-	49.75	99.75

Очно-заочная форма обучения

Таблица 8

№ п/п	Наименование раздела дисциплины	Лекции	Практ. занятия	Лаб. занятия	Семинары	СРС	Всего часов
1	Раздел 1. Основы аудита информационной безопасности	2				8	10
2	Раздел 2. Требования к информационной безопасности	2				8	10
3	Раздел 3. Элементы информационной безопасности	2				10	12
4	Раздел 4. Инструментальные средства оценки безопасности компьютерных систем	4	22			31	57
5	Раздел 5. Защита от разрушающих программных воздействий	2	2			6.75	10.75
	Итого:	12	24	-	-	63.75	99.75

6. Лекции

Очная форма обучения

Таблица 9

№ п/п	Номер раздела	Тема лекции	Всего часов

1	1	Основы аудита информационной безопасности. Принципы системности, комплексности, непрерывности защиты, гибкости управления и применения защитных механизмов, открытости алгоритмов и механизмов защиты, простоты применения защитных мер и средств. Правовые (законодательные), аппаратно-программные меры обеспечения безопасности компьютерных систем.	2
2	2	Аутентификации подлинности его автора, возможности злоумышленника при реализации угроз, направленных на нарушение целостности передаваемых сообщений и подлинность их авторства, метод решения данных проблем. Классы защищенности автоматизированных систем. Основные требования и рекомендации по защите информации, составляющей служебную или коммерческую тайну, а также персональных данных.	2
3	3	Элементы информационной безопасности. Угрозы информационной безопасности и векторы атак. Классы угроз информационной безопасности.	2
4	3	Типы атак. Меры противодействия. Изучение защищаемой системы с позиции злоумышленника. Тестирование на проникновение.	2
5	4	Средства и способы предварительной разведки и сбора информации. Средства сканирования сетей.	2
6	4	Средства перечисления локальных и сетевых ресурсов. Средства, используемые для взлома системы.	2
7	4	Средства прослушивание сети — снифферы. Средства организации атаки "Отказ в обслуживании".	2
8	5	Понятие и виды активизирующих событий. Модели взаимодействия прикладной программы и программы с потенциально опасными последствиями. Общие и специализированные методы защиты программного обеспечения от разрушающих программных воздействий	2
		Итого:	16

Очно-заочная форма обучения

Таблица 10

№ п/п	Номер раздела	Тема лекции	Всего часов
1	1	Основы аудита информационной безопасности. Принципы системности, комплексности, непрерывности защиты, гибкости управления и применения защитных механизмов, открытости алгоритмов и механизмов защиты, простоты применения защитных мер и средств.	2
2	2	Классы защищенности автоматизированных систем. Основные требования и рекомендации по защите информации, составляющей служебную или коммерческую тайну, а также персональных данных. Требования к защите информации в автоматизированных системах, локальных вычислительных сетях, на рабочих местах пользователей ПК.	2
3	3	Элементы информационной безопасности. Угрозы информационной безопасности и векторы атак. Классы угроз информационной безопасности.	2
4	4	Средства и способы предварительной разведки и сбора информации. Средства сканирования сетей. Средства и способы предварительной разведки и сбора информации.	2

5	4	Средства перечисления локальных и сетевых ресурсов. Средства прослушивание сети — снифферы. Средства организации атаки "Отказ в обслуживании".	2
6	5	Понятие и виды активизирующих событий. Модели взаимодействия прикладной программы и программы с потенциально опасными последствиями. Общие и специализированные методы защиты программного обеспечения от разрушающих программных воздействий	2
		Итого:	12

7. Лабораторный практикум

Рабочим учебным планом не предусмотрено

8. Практические занятия (семинары)

Очная форма обучения

Таблица 11

№ п/п	Номер раздела	Тема занятия	Всего часов
1	3	Настройка и тестирование виртуальной лаборатории	2
2	4	Средства предварительной разведки для подготовки атаки на систему	4
3	4	Перехват и анализ сетевого трафика	4
4	4	Перечисление локальных и сетевых ресурсов целевой системы	4
5	4	Сканирование сети для получения профиля атакуемой системы	4
6	4	Изучение средств сканирования сетей	4
7	4	Средства анализа сетевых пакетов	4
8	4	Средства перечисления локальных и сетевых ресурсов	4
9	5	Средства защиты от программно-математического воздействия	4
		Итого:	34

Очно-заочная форма обучения

Таблица 12

№ п/п	Номер раздела	Тема занятия	Всего часов
1	4	Настройка и тестирование виртуальной лаборатории	2
2	4	Средства предварительной разведки для подготовки атаки на систему	2
3	4	Перехват и анализ сетевого трафика	4
4	4	Изучение средств сканирования сетей	2
5	4	Сканирование сети для получения профиля атакуемой системы	4
6	4	Средства анализа сетевых пакетов	2
7	4	Средства перечисления локальных и сетевых ресурсов	2
8	4	Перечисление локальных и сетевых ресурсов целевой системы	4
9	5	Средства защиты от программно-математического воздействия	2
		Итого:	24

9. Примерная тематика курсовых проектов (работ)

Рабочим учебным планом не предусмотрено

10. Самостоятельная работа

Очная форма обучения

Таблица 13

№ п/п	Номер раздела	Содержание самостоятельной работы	Форма контроля	Всего часов
1	1	Основы аудита информационной безопасности. Принципы системности, комплексности, непрерывности защиты, гибкости управления и применения защитных механизмов, открытости алгоритмов и механизмов защиты, простоты применения защитных мер и средств.	Оценка знаний на занятии	6
2	2	Требования к информационной безопасности	Оценка знаний на занятии	6
3	3	Элементы информационной безопасности	Материалы ПЗ	8
4	4	Инструментальные средства оценки безопасности компьютерных систем	Материалы ПЗ	23.75
5	5	Защита от разрушающих программных воздействий	Оценка знаний на занятии	6
			Итого:	49.75

Очно-заочная форма обучения

Таблица 14

№ п/п	Номер раздела	Содержание самостоятельной работы	Форма контроля	Всего часов
1	1	Основы аудита информационной безопасности. Принципы системности, комплексности, непрерывности защиты, гибкости управления и применения защитных механизмов, открытости алгоритмов и механизмов защиты, простоты применения защитных мер и средств.	Оценка знаний на занятии	8
2	2	Требования к информационной безопасности	Оценка знаний на занятии	8
3	3	Элементы информационной безопасности	Материалы ПЗ	10
4	4	Инструментальные средства оценки безопасности компьютерных систем	Материалы ПЗ	31
5	5	Защита от разрушающих программных воздействий	Оценка знаний на занятии	6.75
			Итого:	63.75

11. Перечень учебно-методического обеспечения самостоятельной работы обучающихся по дисциплине

Для самостоятельной работы по дисциплине рекомендовано следующее учебно-методическое обеспечение:

- Положение о самостоятельной работе студентов в Санкт-Петербургском государственном университете телекоммуникаций им. проф. М.А. Бонч-Бруевича;
- рекомендованная основная и дополнительная литература;
- конспект занятий по дисциплине;
- слайды-презентации и другой методический материал, используемый на занятиях;
- методические рекомендации по подготовке письменных работ, требования к их

содержанию и оформлению (реферат, эссе, контрольная работа) ;
- фонды оценочных средств;

12. Фонд оценочных средств для проведения промежуточной аттестации обучающихся

Фонд оценочных средств разрабатывается в соответствии с локальным актом университета «Положение о фонде оценочных средств» и является приложением (Приложение А) к рабочей программе дисциплины.

Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине включает в себя:
- перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы;
- описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания;
- типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы;
- методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций.

Для каждого результата обучения по дисциплине определяются показатели и критерии оценки сформированности компетенций на различных этапах их формирования, шкалы и процедуры оценивания.

13. Перечень основной и дополнительной литературы, необходимой для освоения дисциплины

13.1. Основная литература:

1. Андрианов, В. И.
   Инновационное управление рисками информационной безопасности : [Электронный ресурс] : учеб. пособие / В. И. Андрианов, А. В. Красов, В. А. Липатников ; рец.: С. Е. Душин, Е. В. Стельмашонок ; Федер. агентство связи, Федер. гос. образовательное бюдж. учреждение высш. проф. образования "С.-Петерб. гос. ун-т телекоммуникаций им. проф. М. А. Бонч-Бруевича". - СПб. : СПбГУТ, 2012. - 396 с. : ил. - Библиогр.: с. 394-395. - ISBN 978-5-91891-092-4 (в обл.) : 320.00 р.
2. Новиков, В. К.
   Организационно-правовые основы информационной безопасности (защиты информации). Юридическая ответственность за правонарушения в области информационной безопасности (защиты информации). Учебное пособие : [Электронный ресурс] / В.К. Новиков. - М. : Горячая Линия–Телеком, 2017. - 176 с. : ил. - URL: http://ibooks.ru/reading.php?productid=354366. - ISBN 978-5-9912-0525-2 : Б. ц.

3. Милославская, Н. Г.
Технические, организационные и кадровые аспекты управления информационной безопасностью. Учебное пособие : [Электронный ресурс] / Н. Г. Милославская, М. Ю. Сенаторов, А. И. Толстой. - М. : Горячая Линия–Телеком, 2013. - 216 с. : ил. - URL: http://ibooks.ru/reading.php?productid=334013. - ISBN 978-5-9912-0274-9 : Б. ц.
4. Нестеров, С. А.
Анализ и управление рисками в информационных системах на базе операционных систем Microsoft : [Электронный ресурс] : учебное пособие / С. А. Нестеров. - 2-е изд. - М. : ИНТУИТ, 2016. - 250 с. - URL: https://e.lanbook.com/book/100566. - Б. ц. Книга из коллекции ИНТУИТ - Информатика
5. Абденов, А. Ж.
Методика оценки риска для информационных систем на основе экспертных оценок : [Электронный ресурс] : учеб. пособие / А. Ж. Абденов, С. А. Белкин, Р. Н. Заркумова-Райхель. - Новосибирск : НГТУ, 2014. - 71 с. - URL: https://e.lanbook.com/book/118246. - ISBN 978-5-7782-2588-6 : Б. ц. Книга из коллекции НГТУ - Информатика. Утверждено Редакционно-издательским советом университета в качестве учебного пособия
6. Абденов, А. Ж.
Современные системы управления информационной безопасностью : [Электронный ресурс] : учеб. пособие / А. Ж. Абденов, Г. А. Дронова, В. А. Трушин. - Новосибирск : НГТУ, 2017. - 48 с. - URL: https://e.lanbook.com/book/118224. - ISBN 978-5-7782-3236-5 : Б. ц. Книга из коллекции НГТУ - Информатика. Утверждено Редакционно-издательским советом университета в качестве учебного пособия
7. Ермакова, А. Ю.
Методы и средства защиты компьютерной информации : [Электронный ресурс] : учебное пособие / А. Ю. Ермакова. - М. : РТУ МИРЭА, 2020. - 223 с. - URL: https://e.lanbook.com/book/163844. - Б. ц. Книга из коллекции РТУ МИРЭА - Информатика
8. Никифоров, С. Н.
Методы защиты информации. Защищенные сети : [Электронный ресурс] : учебное пособие / С. Н. Никифоров. - 2-е изд., стер. - Санкт-Петербург : Лань, 2021. - 96 с. - URL: https://e.lanbook.com/book/171868. - ISBN 978-5-8114-8123-1 : Б. ц. Книга из коллекции Лань - Информатика . - [Б. м. : б. и.]. - https://e.lanbook.com/book/169311
9. Никифоров, С. Н.
Методы защиты информации. Защита от внешних вторжений : [Электронный ресурс] : учебное пособие / С. Н. Никифоров. - 4-е изд., стер. - Санкт-Петербург : Лань, 2022. - 96 с. - URL: https://e.lanbook.com/book/200480. - ISBN 978-5-8114-9562-7 : Б. ц. Книга из коллекции Лань - Информатика . - [Б. м. : б. и.]. - https://e.lanbook.com/book/148474
10. Нестеров, С. А.
Основы информационной безопасности : [Электронный ресурс] : учебное пособие

/ С. А. Нестеров. - 5-е изд., стер. - Санкт-Петербург : Лань, 2022. - 324 с. - URL: https://e.lanbook.com/book/206279. - ISBN 978-5-8114-4067-2 : Б. ц. Книга из коллекции Лань - Информатика Предыдущее издание:Нестеров С. А. Основы информационной безопасности : учебное пособие / С. А. Нестеров, 2019. - 324 с. . - [Б. м. : б. и.]. - https://e.lanbook.com/book/114688

11. Никифоров, С. Н.
Методы защиты информации. Шифрование данных : [Электронный ресурс] : учебное пособие / С. Н. Никифоров. - 2-е изд., стер. - Санкт-Петербург : Лань, 2022. - 160 с. - URL: https://e.lanbook.com/book/206285. - ISBN 978-5-8114-4042-9 : Б. ц. Книга из коллекции Лань - Информатика Предыдущее издание:Никифоров С. Н. Методы защиты информации. Шифрование данных : учебное пособие / С. Н. Никифоров, 2019. - 160 с. . - [Б. м. : б. и.]. - https://e.lanbook.com/book/114699

13.2. Дополнительная литература:

1. Зима, В. М.
Безопасность глобальных сетевых технологий : [Электронный ресурс] / В. М. Зима, А. А. Молдовян, Н. А. Молдовян. - 2-е изд. - СПб. : БХВ-Петербург, 2003. - 362, [5] с. : ил. - (Мастер систем). - Библиогр.: с. 351-352. - Предм. указ.: с. 353-362. - ISBN 5-94157-213-1 (в обл.) : 93.00 р.
2. Милославская, Н. Г.
Управление рисками информационной безопасности. Учебное пособие для вузов : [Электронный ресурс] / Н. Г. Милославская, М. Ю. Сенаторов, А. И. Толстой. - М. : Горячая линия-Телеком, 2013. - 130 с. : ил. - URL: http://ibooks.ru/reading.php?productid=334011. - ISBN 978-5-9912-0272-5 : Б. ц.
3. Милославская, Н. Г.
Управление инцидентами информационной безопасности и непрерывностью бизнеса. Учебное пособие для вузов : [Электронный ресурс] / Н. Г. Милославская, М. Ю. Сенаторов, А. И. Толстой. - М. : Горячая линия-Телеком, 2013. - 170 с. : ил. - URL: http://ibooks.ru/reading.php?productid=334012. - ISBN 978-5-9912-0273-2 : Б. ц.
4. Милославская, Н. Г.
Проверка и оценка деятельности по управлению информационной безопасностью. Учебное пособие для вузов : [Электронный ресурс] / Н. Г. Милославская, М. Ю. Сенаторов, А. И. Толстой. - М. : Горячая линия-Телеком, 2013. - 166 с. : ил. - URL: http://ibooks.ru/reading.php?productid=334014. - ISBN 978-5-9912-0275-6 : Б. ц.
5. Душкин, А. В.
Методологические основы построения защищенных автоматизированных систем : [Электронный ресурс] : учебное пособие / А. В. Душкин, О. В. Ланкин, С. В. Потехецкий, А. П. Данилкин. - Воронеж : ВГУИТ, 2013. - 263 с. - URL: http://e.lanbook.com/books/element.php?pl1_id=72890. - ISBN 978-5-89448-981-0 : Б. ц. Книга из коллекции ВГУИТ - Информатика. Утверждено редакционно-издательским советом университета в качестве учебного пособия
6. Милославская, Н. Г.
Сетевые атаки на открытые системы на примере Интранета : [Электронный ресурс] : учебное пособие для вузов / Н. Г. Милославская. - М. : НИЯУ МИФИ,

2012. - 64 с. - URL: http://e.lanbook.com/books/element.php?pl1_id=75789. - ISBN 978-5-7262-1691-1 : Б. ц. Книга из коллекции НИЯУ МИФИ - Информатика. Рекомендовано УМО «Ядерные физика и технологии» в качестве учебного пособия для студентов высших учебных заведений
7. Абденов, А. Ж.
Анализ, описание и оценка функциональных узлов SIEM-системы : [Электронный ресурс] : учеб. пособие / А. Ж. Абденов, В. А. Трушин, К. Сулайман. - Новосибирск : НГТУ, 2018. - 122 с. - URL: https://e.lanbook.com/book/118277. - ISBN 978-5-7782-3603-5 : Б. ц. Книга из коллекции НГТУ - Информатика. Утверждено Редакционно-издательским советом университета в качестве учебного пособия
8. Фот, Ю. Д.
Методы защиты информации : [Электронный ресурс] : учебное пособие для обучающихся по образовательной программе высшего образования по направлению подготовки 02.03.02 фундаментальная информатика и информационные технологии / Ю. Д. Фот. - Оренбург : ОГУ, 2019. - 230 с. - URL: https://e.lanbook.com/book/159977. - ISBN 978-5-7410-2296-2 : Б. ц. Книга из коллекции ОГУ - Информатика. Рекомендовано ученым советом федерального государственного бюджетного образовательного учреждения высшего образования «Оренбургский государственный университет» для обучающихся по образовательной программе высшего образования по направлению подготовки 02.03.02 Фундаментальная информатика и информационные технологии

14. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

- www.sut.ru
- lib.spbgut.ru/jirbis2_spbgut

15. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения и информационных справочных систем.

15.1. Программное обеспечение дисциплины:

- Open Office
- Google Chrome

15.2. Информационно-справочные системы:

- ЭБС iBooks (https://ibooks.ru)
- ЭБС Лань (https://e.lanbook.com/)
- ЭБС СПбГУТ (http://lib.spbgut.ru)

15.3. Дополнительные источники

- ИНТУИТ (https://intuit.ru)

16. Методические указания для обучающихся по освоению дисциплины

16.1. Планирование и организация времени, необходимого для изучения дисциплины

Важным условием успешного освоения дисциплины «Инструментальный анализ защищенности» является создание системы правильной организации труда, позволяющей распределить учебную нагрузку равномерно в соответствии с графиком образовательного процесса. Большую помощь в этом может оказать составление плана работы на семестр, месяц, неделю, день. Его наличие позволит подчинить свободное время целям учебы, трудиться более успешно и эффективно. Нужно осуществлять самоконтроль, который является необходимым условием успешной учебы. Все задания, включая вынесенные на самостоятельную работу, рекомендуется выполнять непосредственно после соответствующего аудиторного занятия (лекции, практического занятия), что способствует лучшему усвоению материала, позволяет своевременно выявить и устранить пробелы в знаниях, систематизировать ранее пройденный материал, на его основе приступить к овладению новыми знаниями и навыками.

Система университетского обучения основывается на рациональном сочетании нескольких видов учебных занятий (в первую очередь лекций и практических занятий), работа на которых обладает определенной спецификой.

16.2. Подготовка к лекциям

Знакомство с дисциплиной происходит уже на первой лекции, где от студента требуется не просто внимание, но и самостоятельное оформление конспекта. При работе с конспектом лекций необходимо учитывать тот фактор, что одни лекции дают ответы на конкретные вопросы темы, другие – лишь выявляют взаимосвязи между явлениями, помогая студенту понять глубинные процессы развития изучаемого предмета, как в истории, так и в настоящее время.

Конспектирование лекций – сложный вид вузовской аудиторной работы, предполагающий интенсивную умственную деятельность студента. Конспект является полезным тогда, когда записано самое существенное и сделано это самим обучающимся. Не надо стремиться записать дословно всю лекцию. Такое «конспектирование» приносит больше вреда, чем пользы. Целесообразно вначале понять основную мысль, излагаемую лектором, а затем записать ее. Желательно запись осуществлять на одной странице листа или оставляя поля, на которых позднее, при самостоятельной работе с конспектом, можно сделать дополнительные записи, отметить непонятные места.

Конспект лекции лучше подразделять на пункты, соблюдая красную строку. Этому в большой степени будут способствовать вопросы плана лекции, предложенные преподавателям. Следует обращать внимание на акценты, выводы, которые делает лектор, отмечая наиболее важные моменты в лекционном материале замечаниями «важно», «хорошо запомнить» и т.п. Можно делать это и с помощью разноцветных маркеров или ручек, подчеркивая термины и определения.

Целесообразно разработать собственную систему сокращений, аббревиатур и символов. Однако при дальнейшей работе с конспектом символы лучше заменить обычными словами для быстрого зрительного восприятия текста. Работая над конспектом лекций, всегда необходимо использовать не только учебник, но и ту литературу, которую дополнительно рекомендовал лектор. Именно такая серьезная, кропотливая работа с лекционным материалом позволит глубоко овладеть теоретическим материалом.

16.3. Подготовка к практическим занятиям

Тщательное продумывание и изучение вопросов плана основывается на проработке пройденного материала (материала лекций, практических занятий), а затем изучения обязательной и дополнительной литературы, рекомендованной к данной теме.

Результат такой работы должен проявиться в способности студента свободно ответить на теоретические вопросы практикума, его выступлении и участии в коллективном обсуждении вопросов изучаемой темы, правильном выполнении практических заданий и контрольных работ.

Необходимо понимать, что невозможно во время аудиторных занятий изложить весь материал из-за лимита аудиторных часов, и при изучении дисциплины недостаточно конспектов занятий. Поэтому самостоятельная работа с учебниками, учебными пособиями, научной, справочной литературой, материалами периодических изданий и интернета является наиболее эффективным методом получения дополнительных знаний, позволяет значительно активизировать процесс овладения информацией, способствует более глубокому усвоению изучаемого материала, формирует у студентов свое отношение к конкретной проблеме.

16.4. Рекомендации по работе с литературой

Работу с литературой целесообразно начать с изучения общих работ по теме, а также учебников и учебных пособий. Далее рекомендуется перейти к анализу монографий и статей, рассматривающих отдельные аспекты проблем, изучаемых в рамках курса, а также официальных материалов и неопубликованных документов (научно-исследовательские работы, диссертации), в которых могут содержаться основные вопросы изучаемой проблемы.

Работу с источниками надо начинать с ознакомительного чтения, т.е. просмотреть текст, выделяя его структурные единицы. При ознакомительном чтении закладками отмечаются те страницы, которые требуют более внимательного изучения. В зависимости от результатов ознакомительного чтения выбирается дальнейший способ работы с источником. Если для разрешения поставленной задачи требуется изучение некоторых фрагментов текста, то используется метод выборочного чтения. Если в книге нет подробного оглавления, следует обратить внимание обучающегося на предметные и именные указатели.

Избранные фрагменты или весь текст (если он целиком имеет отношение к теме) требуют вдумчивого, неторопливого чтения с «мысленной проработкой» материала. Такое чтение предполагает выделение: 1) главного в тексте; 2) основных аргументов; 3) выводов. Особое внимание следует обратить на то, вытекает тезис из аргументов или нет. Необходимо также проанализировать, какие из утверждений

автора носят проблематичный, гипотетический характер, и уловить скрытые вопросы.

Понятно, что умение таким образом работать с текстом приходит далеко не сразу. Наилучший способ научиться выделять главное в тексте, улавливать проблематичный характер утверждений, давать оценку авторской позиции – это сравнительное чтение, в ходе которого студент знакомится с различными мнениями по одному и тому же вопросу, сравнивает весомость и доказательность аргументов сторон и делает вывод о наибольшей убедительности той или иной позиции.

Если в литературе встречаются разные точки зрения по тому или иному вопросу из-за сложности прошедших событий и правовых явлений, нельзя их отвергать, не разобравшись. При наличии расхождений между авторами необходимо найти рациональное зерно у каждого из них, что позволит глубже усвоить предмет изучения и более критично оценивать изучаемые вопросы. Знакомясь с особыми позициями авторов, нужно определять их схожие суждения, аргументы, выводы, а затем сравнивать их между собой и применять из них ту, которая более убедительна.

Следующим этапом работы с литературными источниками является создание конспектов, фиксирующих основные тезисы и аргументы. Можно делать записи на отдельных листах, которые потом легко систематизировать по отдельным темам изучаемого курса. Другой способ – это ведение тематических тетрадей-конспектов по одной какой-либо теме. Большие специальные работы монографического характера целесообразно конспектировать в отдельных тетрадях. Здесь важно вспомнить, что конспекты пишутся на одной стороне листа, с полями и достаточным для исправления и ремарок межстрочным расстоянием (эти правила соблюдаются для удобства редактирования). Если в конспектах приводятся цитаты, то непременно должно быть дано указание на источник (автор, название, выходные данные, № страницы). Впоследствии эта информация может быть использована при написании текста реферата или другого задания.

Таким образом, при работе с источниками и литературой важно уметь:

- сопоставлять, сравнивать, классифицировать, группировать, систематизировать информацию в соответствии с определенной учебной задачей;
- обобщать полученную информацию, оценивать прослушанное и прочитанное;
- фиксировать основное содержание сообщений; формулировать, устно и письменно, основную идею сообщения; составлять план, формулировать тезисы;
- готовить и презентовать развернутые сообщения типа доклада;
- работать в разных режимах (индивидуально, в паре, в группе), взаимодействуя друг с другом;
- пользоваться реферативными и справочными материалами;
- контролировать свои действия и действия своих товарищей, объективно оценивать свои действия;
- обращаться за помощью, дополнительными разъяснениями к преподавателю, другим студентам;
- пользоваться лингвистической или контекстуальной догадкой, словарями различного характера, различного рода подсказками, опорами в тексте (ключевые слова, структура текста, предваряющая информация и др.);
- использовать при говорении и письме перифраз, синонимичные средства, слова-

описания общих понятий, разъяснения, примеры, толкования, «словотворчество»
- повторять или перефразировать реплику собеседника в подтверждение понимания его высказывания или вопроса;
- обратиться за помощью к собеседнику (уточнить вопрос, переспросить и др.);
- использовать мимику, жесты (вообще и в тех случаях, когда языковых средств не хватает для выражения тех или иных коммуникативных намерений).

16.5. Подготовка к промежуточной аттестации

При подготовке к промежуточной аттестации целесообразно:
- внимательно изучить перечень вопросов и определить, в каких источниках находятся сведения, необходимые для ответа на них;
- внимательно прочитать рекомендованную литературу;
- составить краткие конспекты ответов (планы ответов).

17. Материально-техническое обеспечение дисциплины

Таблица 15

№ п/п	Наименование специализированных аудиторий и лабораторий	Наименование оборудования
1	Лекционная аудитория	Аудио-видео комплекс
2	Аудитории для проведения групповых и практических занятий	Аудио-видео комплекс
3	Компьютерный класс	Персональные компьютеры
4	Аудитория для курсового и дипломного проектирования	Персональные компьютеры
5	Аудитория для самостоятельной работы	Компьютерная техника
6	Читальный зал	Персональные компьютеры