ПЕРВОЕ ВЫСШЕЕ ТЕХНИЧЕСКОЕ УЧЕБНОЕ ЗАВЕДЕНИЕ РОССИИ

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
САНКТ-ПЕТЕРБУРГСКИЙ ГОРНЫЙ УНИВЕРСИТЕТ

СОГЛАСОВАНО

Руководитель ОПОП ВО
профессор Д.А. Первухин

УТВЕРЖДАЮ

Проректор по образовательной
деятельности Д.Г. Петраков

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ

Уровень высшего образования:	Магистратура
Направление подготовки	27.04.03 «Системный анализ и управление»
Направленность (профиль)	Теория и математические методы системного анализа и управления в технических и социально-экономических системах
Квалификация выпускника:	Магистр
Форма обучения:	очная
Составитель:	доц. Афанасьева О.В.

Санкт-Петербург

Рабочая программа дисциплины «Информационная безопасность и защита информации» разработана:

- в соответствии с требованиями ФГОС ВО - магистратура по направлению подготовки 27.04.03 «Системный анализ и управление», утвержденного приказом Минобрнауки России № 837 от 29.07.2020 г.;

- на основании учебного плана магистратуры по направлению подготовки 27.04.03 «Системный анализ и управление» направленность (профиль) «Теория и математические методы системного анализа и управления в технических и социально-экономических системах».

Составитель_____к.т.н., доц. Афанасьева О.В.

Рабочая программа рассмотрена и одобрена на заседании кафедры системного анализа и управления от «01» февраля 2023 г., протокол № 10.

Заведующий кафедрой САиУ,
д.т.н., проф.

Д.А. Первухин

1.ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ

Цель изучения дисциплины «Информационная безопасность и защита информации»: формирование у студентов знаний в области теоретических основ информационной безопасности; освоение методов решения задач в области развития науки, техники и технологии, применяя методы системного анализа и управления с учетом нормативно-правового регулирования в сфере интеллектуальной собственности.

Основными задачами дисциплины являются:

- приобретение и развитие компетентности, умения применять методы системного анализа и управления с учетом нормативно-правового регулирования в сфере интеллектуальной собственности для решения задач в области развития науки, техники и технологии;
- сформировать у магистров представление о существующих угрозах безопасности информации;
- ознакомление студентов с основными нормативными документами России, по данному вопросу;
- изучение принципов и методов подбора и применения современных методов и способов защиты информации;
- формирование навыков по защите информации.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО

Дисциплина «Информационная безопасность и защита информации» относится к обязательной части Блока 1 «Дисциплины (модули)» основной профессиональной образовательной программы по направлению подготовки 27.04.03 «Системный анализ и управление направленность (профиль) «Теория и математические методы системного анализа и управления в технических и социально-экономических системах» и изучается во 2 семестре.

Дисциплина «Информационная безопасность и защита информации» является основополагающей для изучения следующих дисциплин: «Современные компьютерные технологии в науке», «Основы экспертизы систем на основе анализа данных», «Современные информационно-поисковые системы», «Программное обеспечение теории моделирования и принятия решений», «Системы обработки больших объемов данных».

Особенностью преподавания дисциплины «Информационная безопасность и защита информации» в рамках основной профессиональной образовательной программы по направлению подготовки 27.04.03 «Системный анализ и управление», направленность (профиль) «Теория и математические методы системного анализа и управления в технических и социально-экономических системах» **в Горном университете** является более глубокое рассмотрение вопросов, касающихся исследования развития науки, техники и технологии, с применением теории и математических методов системного анализа и управления организационно-управленческой деятельности в больших системах с учетом нормативно-правового регулирования в сфере интеллектуальной собственности для объектов минерально-сырьевого комплекса.

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ, СООТНЕСЕННЫЕ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Процесс изучения дисциплины «Информационная безопасность и защита информации» направлен на формирование следующих компетенций:

Формируемые компетенции		**Код и наименование индикатора достижения компетенции**
Содержание компетенции	**Код компетенции**	
Способен решать задачи в области развития науки, техники и технологии, применяя современные методы системного анализа и управления с учетом нормативно-правового регулирования в сфере интеллектуальной собственности	ОПК-5	ОПК-5.1. Знать: современные методы системного анализа и управления и нормы правового регулирования в сфере интеллектуальной собственности; ОПК-5.2. Уметь: решать задачи в области развития науки, техники и технологии на основе применения современных методов системного анализа и управления с учетом нормативно-правового регулирования в сфере интеллектуальной собственности; ОПК-5.3. Владеть: навыками использования современных методов системного анализа и управления с учетом нормативно-правового регулирования в сфере интеллектуальной собственности для решения задач в области развития науки, техники и технологии.

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1. Объем дисциплины и виды учебной работы

Общая трудоёмкость учебной дисциплины составляет *3* зачётных единицы, 108 ак. часа.

Вид учебной работы	**Всего ак. часов**	**Ак. часы по семестрам**
		2
Аудиторная работа, в том числе:	**48**	***48***
Лекции (Л)	12	*12*
Практические занятия (ПЗ)	36	*36*
Самостоятельная работа студентов (СРС), в том числе:	**24**	***24***
Подготовка к практическим занятиям	24	*24*
Промежуточная аттестация - экзамен (Э)	**36**	**Э (36)**
Общая трудоемкость дисциплины		
ак. час.	**108**	**108**
зач.ед.	**3**	**3**

4.2. Содержание дисциплины

Учебным планом предусмотрены: лекции, практические занятия, лабораторные работы и самостоятельная работа.

4.2.1. Разделы дисциплины и виды занятий

Наименование разделов	Виды занятий				
	Всего ак. часов	Лекции	Практические занятия	Лабораторные работы	Самостоятельная работа студента, в том числе курсовая работа (проект)
Раздел 1 «Принципы обеспечения защиты информации. Уровни информационной защиты»	12	2	4	-	6
Раздел 2 «Криптографические системы и криптоанализ»	12	2	4	-	6
Раздел 3 «Технические аспекты обеспечения защиты информации»	14	2	10	-	2
Раздел 4 «Атаки системы снаружи и изнутри»	12	2	8	-	2
Раздел 5 «Основные направления работ по созданию систем комплексной защиты информационной системы объекта (предприятия).»	10	2	4	-	4
Раздел 6 «Мобильные программы»	12	2	6	-	4
Итого:	**72**	**12**	**36**	**-**	**24**

4.2.2. Содержание разделов дисциплины

№ п/п	Наименование раздела дисциплины	Содержание лекционных занятий	Трудоемкость в ак. часах
1	Раздел 1 «Принципы обеспечения защиты информации Уровни информационной защиты»	Понятие безопасности. Угрозы. Злоумышленники. Случайная потеря данных. Системы безопасности и их дефекты. Знаменитые дефекты системы безопасности UNIX, TENEX, OS/360. Принципы проектирования систем безопасности.	2
2	Раздел 2 «Криптографические системы и крипто-анализ»	Основы криптографии. Шифрование с секретным ключом. Шифрование с открытым ключом. Необратимые функции. Цифровые подписи.	2
3	Раздел 3 «Технические аспекты обеспечения защиты информации»	Аутентификация пользователей. Аутентификация с использованием паролей. Как взломщикам удается проникнуть в систему. Защита паролей в системе UNIX. Совершенствование безопасности паролей. Одноразовые пароли. Схема аутентификации «оклик-отзыв». Аутентификации с использованием физического объекта. Аутентификация с использованием биометрических данных. Контрмеры.	2

4	Раздел 4 «Атаки системы снаружи и изнутри»	Атаки системы снаружи. Сценарии нанесения ущерба «вирусами». Как работает «вирус». Вирусы-компаньоны. Вирусы, заражающие исполняемые файлы. Резидентные вирусы. Вирусы, поражающие загрузочный сектор. «Вирусы» драйверов устройств. Макровирусы. Вирусы, заражающие исходные тексты программ. Как распространяются вирусы. Антивирусные программы и анти-антивирусная технология. Сканеры вирусов. Проверка целостности. Проверка поведения. Предохранение от вирусов. Восстановление после «вирусной» атаки. Интернет-черви. Атаки системы изнутри. Троянские кони. Фальшивая программа регистрации. Логические бомбы. Потайные двери. Переполнение буфера. Атака системы безопасности.	2
5	Раздел 5 «Основные направления работ по созданию систем комплексной защиты информационной системы объекта (предприятия)»	Механизмы защиты. Домены защиты. Списки управления доступом. Перечни возможностей. Надежные системы. Высоконадежная вычислительная база. Формальные модели защищенных систем. Многоуровневая защита. Модель Белла-Ла Падулы. Модель Биба. Оранжевая книга безопасности. Тайные каналы.	2
6	Раздел 6 «Мобильные программы».	Метод «песочниц». Интерпретация. Программы с подписями. Безопасность в системе Java. Несколько примеров политик безопасности пакета JDK 1.2.	2
		Итого:	**12**

4.2.3. Практические занятия

№ п/п	Разделы	Тематика практических занятий	Трудоемкость в ак. часах
1.	Раздел 1.	Международные стандарты в области информационной безопасности	4
2.	Раздел 2.	Шифрование текста как метод защиты информации	4
3.	Раздел 3.	Аутентификация пользователей	2
4.	Раздел 3	Компьютерные вирусы и методы борьбы с ними	4
5.	Раздел 3	Методы защиты компьютера от несанкционированного доступа	4
6.	Раздел 4.	Угрозы информационной безопасности	4
7.	Раздел 4.	Электронная цифровая подпись	4
8.	Раздел 5.	Использование цифровых сертификатов	4
9.	Раздел 6.	Программы с подписями	2
10.	Раздел 6	Настройка безопасности почтового клиента Outlook Express	4
		Итого:	**24**

4.2.4. Лабораторные работы

Лабораторные работы не предусмотрены.

4.2.5. Курсовые работы (проекты)

курсовые работы (проекты) не предусмотрены

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

В ходе обучения применяются:

Лекции, которые являются одним из важнейших видов учебных занятий и составляют основу теоретической подготовки обучающихся. Цели лекционных занятий:

-дать систематизированные научные знания по дисциплине, акцентировать внимание на наиболее сложных вопросах дисциплины;

-стимулировать активную познавательную деятельность обучающихся, способствовать формированию их творческого мышления.

Практические занятия. Цели практических занятий:

-совершенствовать умения и навыки решения практических задач.

Главным содержанием этого вида учебных занятий является работа каждого обучающегося по овладению практическими умениями и навыками профессиональной деятельности.

Консультации (текущая консультация, накануне *экзамена* является одной из форм руководства учебной работой обучающихся и оказания им помощи в самостоятельном изучении материала дисциплины, в ликвидации имеющихся пробелов в знаниях, задолженностей по текущим занятиям, в подготовке письменных работ (проектов).

Текущие консультации проводятся преподавателем, ведущим занятия в учебной группе, научным руководителем и носят как индивидуальный, так и групповой характер.

Самостоятельная работа обучающихся направлена на углубление и закрепление знаний, полученных на лекциях и других занятиях, выработку навыков самостоятельного активного приобретения новых, дополнительных знаний, подготовку к предстоящим учебным занятиям и промежуточному контролю.

6. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ, ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ИТОГАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

6.1. Оценочные средства для самостоятельной работы и текущего контроля успеваемости

Раздел 1. Принципы обеспечения защиты информации. Уровни информационной защиты

1. Что такое информационная безопасность?
2. В чем заключаются национальные интересы РФ в информационной сфере?
3. Какие имеются виды угроз информационной безопасности предприятия (организации)?
4. Какие существуют источники наиболее распространенных угроз информационной безопасности?
5. Какие уровни информационной защиты существуют, их основные составляющие?

Раздел 2. Криптографические системы и криптоанализ

1. В чем заключаются задачи криптографии?
2. Что включает в себя защита информации от несанкционированного доступа?
3. Зачем нужны ключи?
4. В чем заключаются достоинства и недостатки программно-аппаратных средств защиты информации?
5. Какие требования необходимо выполнять при экранировании помещений, предназначенных для размещения вычислительной техники?

Раздел 3. Технические аспекты обеспечения защиты информации

1. Какой процесс называется аутентификацией пользователя?
2. Какие схемы аутентификации вы знаете?
3. Что такое смарт-карты?
4. Какие требования предъявляются к современным криптографическим системам защиты информации?
5. В чем заключается анализ надежности криптосистем?

Раздел 4. Атаки системы снаружи и изнутри

1. Что является основными характеристиками технических средств защиты информации?
2. Какие атаки изнутри вы знаете?
3. От чего зависит выбор класса защищенности?
4. Какая программа называется вирусом? Какие виды «вирусов» вы знаете?
5. Какие методы обнаружения «вирусов» вы знаете?

Раздел 5. Основные направления работ по созданию систем комплексной защиты информационной системы объекта (предприятия)

1. Какие модели многоуровневой защиты вы знаете?
2. В чем заключается организация работ по защите от несанкционированного доступа интегрированной информационной системы управления предприятием?
3. Какие характеристики положены в основу системы классификации информационных систем управления предприятием?
4. Какие существуют пути защиты информации в локальной сети?
5. Что включает в себя защита информационных систем с помощью планирования?

Раздел 6. Мобильные программы

1. Что такое мобильные программы?
2. Что представляет собой метод «песочниц»?
3. Что такое интерпретация?
4. Что такое программы с подписями?
5. Что представляет собой безопасность в системе Java?

6.2. Оценочные средства для проведения промежуточной аттестации (экзамена)

6.2.1. Примерный перечень вопросов/заданий к экзамену (по дисциплине):

1. Сформулируйте понятия и основные составляющие информационной безопасности.
2. Определите понятия «безопасность информации» и его отличие от понятия «защита информации».
3. Назовите объекты защиты при обеспечении компьютерной безопасности.
4. Какие Вы знаете категории и носители информации.
5. Сформулируйте понятия «доступность», «целостность», «конфиденциальность информации».
6. Обоснуйте важность проблемы компьютерной информационной безопасности.
7. Классификация информации по степени важности.
8. Обоснуйте проблемы защиты информации в интернете.
9. Сформулируйте понятие «ценность информации». Назовите порядковую шкалу ценностей.
10. Сформулируйте актуальность решения проблем защиты информации.
11. Назовите наиболее распространенные угрозы для компьютерной информации.
12. Назовите наиболее распространенные пути и каналы утечки информации.
13. Назовите виды атак и методы взлома информационных сетей злоумышленниками.
14. Сформулируйте виды противников или «нарушителей» информационной безопасности.
15. Назовите виды возможных нарушений информационной системы.
16. Сформулируйте понятие «Вредоносные программы (вирусы)». Классификация компьютерных вирусов.
17. Назовите основные правила защиты от компьютерных вирусов.

18. Назовите современные антивирусные программы

19. Сформулируйте достоинства и недостатки современных антивирусных программ.

20. Назовите признаки заражения компьютера от вредоносных программ.

21. Сформулируйте понятие законодательного уровня информационной безопасности.

22. Объясните важность законодательного уровня информационной безопасности.

23. Назовите критерии безопасности компьютерных систем.

24. Сформулируйте текущее состояние российского законодательства в области информационной безопасности.

25. В каком случае сотрудник учреждения может быть привлечен к ответственности за нарушения правил информационной безопасности?

26. Назовите требования российского законодательства в области лицензирования и сертификации.

27. Сформулируйте основные понятия в области лицензирования.

28. Объясните порядок оформления и получения лицензий в области информационной безопасности.

29. Сформулируйте причины отказа в получении лицензии.

30. Объясните порядок оформления и получения сертификатов в области информационной безопасности.

31. Сформулируйте понятие «утечка данных». Назовите каналы утечки и нарушения безопасности компьютерной информации.

32. Назовите способы защиты информации от утечки по техническим каналам.

33. Какие вы знаете современные технические средства защиты информации.

34. Классификация технических средств защиты информации.

35. Назовите мероприятия по защите информации от несанкционированного доступа.

36. Назовите методы защиты информации.

37. Сформулируйте понятие «Идентификация пользователей». Классификация методов идентификации пользователей.

38. Сформулируйте понятия и дайте характеристику «аутентификация пользователей», «парольная аутентификация».

39. Дайте определение понятиям «Управление доступом, ограничение, разграничение, разделение доступа к информации» и сформулируйте их основные характеристики.

40. Сформулируйте преимущества и недостатки метода криптографического преобразования информации.

6.2.2. Примерные тестовые задания к *экзамену*

Вариант № 1

№ п/п	Вопрос	Варианты ответа
1.	Полное имя, дата рождения, номер паспорта относятся к…	1. Персональным данным 2. Данным аутентификации 3. Данным мобильных устройств/компьютеров 4. Данным банковской или финансовой информации
2.	Какая стратегия заключается в том, чтобы попросту избегать использования определенных социальных сетей, ничего не публикуем, не заполняем анкеты, попросту не регистрируемся, не выдаем о себе никакой информации.	1. Стратегия избегания 2. Фрагментация 3. Стратегия деления получателей информации на группы 4. Стратегия открытости
3.	При какой стратегии происходит разделение	1. Стратегия деления получате-

	личного и профессионального окружения путем использования Facebook для друзей и семьи, а LinkedIn для личных связей.	лей информации на группы 2. Стратегия избегания 3. Стратегия открытости 4. Фрагментация
4.	Какая стратегия заключается в использовании данных о вашей реальной личности, где все прозрачно и подлинно.	1. Стратегия открытости 2. Стратегия деления получателей информации на группы 3. Фрагментация 4. Стратегия избегания
5.	В чем заключается стратегия открытости?	1. в использовании данных о вашей реальной личности, где все прозрачно и подлинно 2. в разделении личного и профессионального окружения путем использования Facebook для друзей и семьи, а LinkedIn для личных связей 3. в том, чтобы попросту избегать использования определенных социальных сетей, ничего не публикуя, не заполняя анкеты, не регистрируясь, не выдавая о себе никакой информации 4. нет правильного ответа
6.	В чем заключается стратегия избегания?	1. в том, чтобы попросту избегать использования определенных социальных сетей, ничего не публикуя, не заполняя анкеты, не регистрируясь, не выдавая о себе никакой информации 2. в использовании данных о вашей реальной личности, где все прозрачно и подлинно 3.в разделении личного и профессионального окружения путем использования Facebook для друзей и семьи, а LinkedIn для личных связей 4. нет правильного ответа
7.	Что значит иметь контекстуально-независимые друг от друга личности, отделенные от вашей реальной личности?	1. Фрагментация 2. Стратегия деления получателей информации на группы 3. Стратегия избегания 4. Стратегия открытости
8.	Какие сети можно отнести к децентрализованным социальным сетям?	1. Все ниже перечисленные 2.Diaspora 3.Friendica 4.GNU social
9.	В каком году вышла в свет автономная версия Windows 95?	1. 1995 2. 1994 3. 1996

		4. 1997
10.	Главный разработчик Windows NT (New Technology) - ...	1. Дэвид Катлер 2. Стивен Синофски 3. Майкл Тутонги 4. Крейг Мунди
11.	Первый универсальный 8-разрядный центральный процессор с названием Intel 8080 - компания Intel выпустила в ... году.	1. 1974. 2. 1980 3. 1990 4. 2000
12.	Версия Windows ... была переименована в Windows 2000 в начале 1999 года.	1. Windows NT 5.0. 2. Windows XP 3. Windows 98 4. Windows NT 4.0
13.	Первый настоящий цифровой компьютер изобрёл английский математик ...	1. Чарльз Бэббидж. 2. Конрад Цузе 3. Ада Лавлейс 4. Алан Тьюринг
14.	... - программа, находящаяся в режиме выполнения.	1. Процесс 2. Регулирование 3. Загрузка 4. Обновление
15.	Создатель ОС Linux ...	1. Linus Torvalds 2. Andrew Tanenbaum 3. Patrick Volkerding 4. Richard Stallman
16.	Загрузчик операционный системы MS-DOS служит для .	1. считывания в память модулей io.sys и msdos.sys. 2. загрузки программ в оперативную память ЭВМ 3. обработки команд, введенных пользователем 4. подключения устройств ввода-вывода
17.	Сектор 0 диска называется ...	1. главной загрузочной записью. 2. дорожкой 3. геометрическим сектором 4. кластером
18.	Спулинг - это ...	1. предварительное накопление данных 2. сбор заданий с одинаковым набором ресурсов в пакеты заданий 3. организация реального ввода пакета заданий и вывода результатов на отдельных специализированных ЭВМ 4. организация реального ввода пакета заданий и вывода результатов на том же компьютере, который производит вычисления
19.	BIOS - это ...	1. базовая система ввода-вывода 2. игровая программа

		3. диалоговая оболочка 4. командный язык ОС
20.	Где находится BIOS?	1. в постоянно-запоминающем устройстве 2. в оперативно-запоминающем устройстве 3. на винчестере 4. на CD-ROM

Вариант № 2

№	Вопрос	Варианты ответов
1	Явление, когда никто не видит, что вы делаете, но потенциально знает, кто вы такой.	1. Приватность 2. Анонимность 3. Идентификация 4. Псевдо - анонимность
2	Явление, когда никто не знает, кто вы, но потенциально видит, что выделаете.	1. Анонимность 2. Приватность 3. Идентификация 4. Псевдо - анонимность
3	Явление, когда вы желаете сохранить свою репутацию, а не скрыть личность	1. Псевдо - анонимность 2. Анонимность 3. Идентификация 4. Приватность
4	Уровень устойчивости наших активов поотношению к угрозам, исходящим от злоумышленников.	1. Безопасность 2. Индифферентность 3. Идентификация 4. Интерферентность
5	Риск - это вероятность возникновения угрозы, эксплуатирующей уязвимости в ваших средствах обеспечения безопасности и последствия, к которым все это может привести. Он исчисляется формулой:	1. РИСК = (Уязвимость х Угрозы х Последствия) 2. РИСК = (Уязвимость + Угрозы + Последствия) 3. РИСК = (Уязвимость + Угрозы х Последствия) 4. РИСК = (Уязвимость х Угрозы + Последствия)
6	Угрозы и злоумышленники, которым вы противостоите, называются ...	1. ландшафтом угроз или моделью угроз. 2. планом опасностей 3. стратегией атаки 4. уязвимостями
7	Кому принадлежит следующее высказывание «Приватность состоит не в том, чтобы что-либо спрятать. Приватность состоит в том, чтобы иметь возможность контролировать, какими мы предстаем перед этим миром. Она состоит в том, чтобы вы могли сохранять свое публичное лицо и в то же время имели возможность приватно мыслить и действовать. Приватность состоит в поддержании личного достоинства»	1. Брюс Шнайер 2. Нильс Фергюсон 3. Тадаёси Коно 4. Билл Гейтс
8	Перечислить три слоя защиты принципа "эше-	1. Предотвращение - Обна-

	лонированная защита"	ружение - Восстановление 2 Ознакомление - Обнаружение -Восстановление - 3 Обнаружение - Активация -Деактивация - 4 Ознакомление -Активация -Восстановление
9	Какому принципу соответствует следующая идея в том, чтобы обеспечить слои защитыследующим образом: припадении одной защиты другая продолжаетзащищать вас на своейпозиции	1 Эшелонированная защита 2 Активная защита 3 Пассивная защита 4 Линейная защита
10	Защита от компрометации ваших файлов злоумышленникамии их доступа к вашей конфиденциальной информации - это.	1 Предотвращение 2 Обновление антивирусных средств 3 Восстановление данных 4 Симуляция
11	Общее понятие для всех программ, написанных со злым умыслом - это.	1 Вредоносные программы 2 Трояны 3 Руткиты 4 Утилиты
12	Вирусы, которые скрывают производимыеими изменения в системе.	1 Стелс-вирусы 2 Черви 3 Баги 4 Трояны
13	Вирусы, которые создают различные рабочие копии самих себя	1 Полиморфные вирусы 2 Черви 3 Баги 4 Трояны
14	Какой тип вирусов регистрирует нажатия клавиш на клавиатуре или мыши?	1 Кейлоггеры 2 Трояны 3 Черви 4 Руткиты
15	Вредоносные программы для сбора разведывательной информации?	1 Шпионское ПО 2 Сканнеры 3 Утилиты 4 Кейлоггеры
16	Вид атаки, при которой обычно пытаются склонить жертву к переходу по определенной ссылке или запуску вредоносного программного обеспечения	1 Фишинг 2 Спамминг 3 Захват 4 Симуляция
17	Какая самая распространённая техника фишинга?	1 Подмена домена 2 Смена названия сайта 3 Изменение префикса 4 Нет правильного ответа
18	Главная идея фишинга состоит в том, чтобы.	1 Получить доступ к логину и паролю пользователя 2. Заразить компьютер вирусом 3. Исказить правильную информацию

		4. Нет правильного ответа
19	Вирусы, которые при своем размножении тем или иным способом используют файловую систему какой - либо (или каких -либо) операционной системы - это ...	1. Файловые вирусы 2. Трояны 3. Черви 4. Руткиты
20	Задача ... заключается в том, чтобы взять сообщение или файл, называемый открытым текстом, и преобразовать его в зашифрованный текст, таким образом, чтобы только «посвящены» могли преобразовать его обратно в открытый текст.	1. Криптографии. 2. Шифрование 3. Дешифрование 4. Кодирование

Вариант № 3

№ п/п	Вопрос	Варианты ответа
1.	Подобие песочницы, они являются отличным инструментом для реализации изоляции и компартментализации с целью снижения рисков и негативного воздействия, а также для контроля атакующего - это.	1. Виртуальные машины 2. Облачные хранилища 3. Операционные системы 4. Нет правильного ответа
2.	Указать название механизма, который является независимой средой, реализуемой посредством виртуализации на уровне операционной системы, где каждая тюрьма представляет собой виртуальную среду со своими собственными файлами, процессами и учетными записями пользователей, а также привязывается к определенному IP-адресу	1. Jails 2. BSD 3. OpenVZ 4. Whonix
3.	Какая программа в Windows 10 использует технологию безопасности аппаратного оборудования и виртуализацию для изоляции функций принятия решений от остальной части операционной системы, что помогает обеспечить защиту от атакующих и вредоносных программ, которые смогли получить права администратора.	1. Windows 10 Device Guard 2. Windows KM free 3. Windows 10 ESET 4. Windows Avast
4.	Задача первостепенной важности, подчеркивающая необходимость использования отдельного защищенного лэптопа для критических ситуаций, на котором вы можете рассмотреть возможность использования виртуализации в качестве средства обеспечения безопасности при помощи изоляции и компартментализации - это.	1. Поддержание безопасности хостовой операционной системы 2. Обновление браузера 3. Удаление кэша 4. Нет правильного варианта ответа
5.	Были прецеденты, когда вирус мог осуществить побег из виртуальной машины?	1. Да 2. Нет 3. Исследования не проводились 4. Да, но проблема решена навсегда

6.	Какую песочницу имеет Mac OS?	1. Sandbox 2. Xbox 3. Parallel 4. Island
7.	Свободная и открытая операционная система, особое внимание уделяющая анонимности, приватности и безопасности - это…	1. Whonix 2. Symbian 3. KaiOS 4. Puffin OS
8.	Из скольких частей состоит операционная сеть Whonix?	1. 2 2. 1 3. 5 4. 9
9.	Существуют ли сервисы одноразовые учетные записи?	1. Существуют 2. Не существуют 3. Существуют временные 4. Существуют постоянные
10.	Назовите поведенческие меры безопасности	1. Изменение поведения и использование технических средств защиты 2. Использование технических средств защиты 3. Использование антивирусных программ 4. Нет правильного ответа
11.	К угрозам какого типа относятся следующие угрозы: кража личности, спам, фишинг, скам, вишинг, мошенничество и т.д.	1. Социального 2. Технического 3. Экономического 4. Политического
12.	Что относится к техническим средствам защиты?	1. Использование сервиса кредитного мониторинга 2. Проверка вложение 3. Проверка отправителя 4. Проверка ссылок
13.	Выберите технические средства защиты от атак социального типа	1. Все ниже перечисленное 2. Изоляция и компартментализация 3. Использование виртуальных машин 4. Песочницы
14.	Домен безопасности может быть …	1. Физическими 2. Абстрактные 3. Реальный 4. Письменный
15.	Домен безопасности может быть …	1. Виртуальными 2. Абстрактные 3. Реальный 4. Письменный
16.	Что используются для реализации доменов безопасности, путем создания раздельных уровней юзабилити, безопасности и поддержки различных идентификационных данных или псевдонимов для приватности и аноним-	1. Изоляция и компартментализация 2. Домен безопасности 3. Виртуальная машина 4. Песочница

	ности	
17.	Что такое идентификатор производителя в MAC-адресе?	1. Первые три байта в MAC-адресе 2. Последние три байта в MAC-адресе 3. Шесть байт в MAC-адресе 4. Нет правильного ответа
18.	Что такое индивидуальное и уникальное значение для сети, для сетевой карты, для адаптера Wi-Fi, для адаптера Ethernet	1. Последние три байта в MAC-адресе 2. Первые три байта в MAC-адресе 3. Шесть байт в MAC-адресе 4. Нет правильного ответа
19.	Изолированная среда для запуска приложений или кода - это	1. Песочница 2. Домен безопасности 3. Виртуальная машина 4. Изоляция и компартментализация
20.	Что из приведенных технологий является технологией песочницы?	1. Все ниже перечисленное 2. Shadow Defender 3. Returnil 4. Bufferzone

6.3. Описание показателей и критериев контроля успеваемости, описание шкал оценивания

6.3.2. Критерии оценок промежуточной аттестации (экзамен)

Оценка			
«2» (неудовлетворительно)	**Пороговый уровень освоения**	**Углубленный уровень освоения**	**Продвинутый уровень освоения**
	«3» (удовлетворительно)	**«4» (хорошо)**	**«5» (отлично)**
Студент не знает значительной части материала, допускает существенные ошибки в ответах на вопросы	Студент поверхностно знает материал основных разделов и тем учебной дисциплины, допускает неточности в ответе на вопрос	Студент хорошо знает материал, грамотно и по существу излагает его, допуская некоторые неточности в ответе на вопрос.	Студент в полном объёме знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос
Не умеет находить решения большинства предусмотренных программой обучения заданий	Иногда находит решения, предусмотренные программой обучения заданий	Уверенно находит решения, предусмотренные программой обучения заданий	Безошибочно находит решения, предусмотренные программой обучения заданий
Большинство предусмотренных программой обучения заданий не выполнено	Предусмотренные программой обучения задания выполнены удовлетворительно	Предусмотренные программой обучения задания успешно выполнены	Предусмотренные программой обучения задания успешно выполнены

Примерная шкала оценивания знаний в тестовой форме:

Количество правильных ответов, %	Оценка
0-49	Неудовлетворительно
50-65	Удовлетворительно
66-85	Хорошо
86-100	Отлично

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

7.1. Рекомендуемая литература

7.1.1. Основная литература

1. Баранова, Е. К. Информационная безопасность и защита информации : учебное пособие / Е.К. Баранова, А.В. Бабаш. — 4-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2021. — 336 с. — (Высшее образование). — DOI: https://doi.org/10.29039/1761-6. https://znanium.com/catalog/document?id=364911

2. Бахаров, Л. Е. Информационная безопасность и защита информации : разделы криптография и стеганография : практикум / Л. Е. Бахаров. - Москва : Изд. Дом НИТУ «МИСиС», 2019. - 59 с. URL: https://znanium.com/catalog/product/1232734

3. Методы и средства комплексной защиты информации в технических системах : учебное пособие / Э. В. Запонов, А. П. Мартынов, И. Г. Машин [и др.]. - Саров : РФЯЦ-ВНИИЭФ, 2019. - 224 с. URL: https://znanium.com/catalog/product/1230827

4. Жук А.П. Защита информации: учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. — 3-е изд. — Москва : РИОР : ИНФРА-М, 2021. — 400 с. — (Высшее образование). — DOI: https://doi.org/10.12737/1759-3. - URL: https://znanium.com/catalog/product/1210523.

5. Степанов, О. А. Противодействие кибертерроризму в цифровую эпоху : монография / О. А. Степанов. — Москва : Издательство Юрайт, 2021. — 103 с. - https://urait.ru/bcode/476768

6. Мартишин, С. А. Основы теории надежности информационных систем : учебное пособие / С. А. Мартишин, В. Л. Симонов, М. В. Храпченко. — Москва : ФОРУМ : ИНФРА-М, 2020. — 255 с. - URL: https://znanium.com/catalog/product/1062374

7. Мартишин, С. А. Основы теории надежности информационных систем : учебное пособие / С. А. Мартишин, В. Л. Симонов, М. В. Храпченко. — Москва : ФОРУМ : ИНФРА-М, 2020. — 255 с.. - URL: https://znanium.com/catalog/product/1062374

8. Скрипник Д.А. Общие вопросы технической защиты информации : учебное пособие / Скрипник Д.А.. — Москва, Саратов : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 424 с. — URL: https://www.iprbookshop.ru/89451.html

9. Сычев, Ю. Н. Защита информации и информационная безопасность : учебное пособие / Ю.Н. Сычев. — Москва : ИНФРА-М, 2021. — 201 с. DOI 10.12737/1013711. -
URL: https://znanium.com/catalog/product/1013711

7.1.2. Дополнительная литература

1. Программно-аппаратные средства защиты информации [Электронный ресурс]: учебное пособие для студентов вузов по направлению подготовки «Информационная безопасность» / Л.Х. Мифтахова [и др.]. — Электрон. текстовые данные. — СПб.: Интермедия, 2018. — 408 с. — Режим доступа: http://www.iprbookshop.ru/73644.html

2. Основы информационной безопасности [Электронный ресурс]: учебник для студентов вузов, обучающихся по направлению подготовки «Правовое обеспечение национальной безопасности» / В.Ю. Рогозин [и др.]. — Электрон. текстовые данные. — М.: ЮНИТИ-ДАНА, 2017. — 287 с. — Режим доступа: http://www.iprbookshop.ru/72444.html

3. Сафонова Л.А. Экономические аспекты информационной безопасности : учебное пособие / Сафонова Л.А.. — Новосибирск : Сибирский государственный университет телекоммуникаций и информатики, 2019. — 97 с. — URL: https://www.iprbookshop.ru/90606.html

4. Клименко, И. С. Информационная безопасность и защита информации: модели и методы управления : монография / И.С. Клименко. — Москва : ИНФРА-М, 2021. — 180 с. — (Научная мысль). — DOI 10.12737/monography_5d412ff13c0b88.75804464. - ISBN 978-5-16-015149-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1137902

5. Черников, Б. В. Информационные технологии управления : учебник / Б.В. Черников. — 2-е изд., перераб. и доп. — Москва : ФОРУМ : ИНФРА-М, 2021. — 368 с. — (Высшее образование: Бакалавриат). - https://znanium .com/catalog/product/1223242.

6. Шаньгин, В. Ф. Комплексная защита информации в корпоративных системах : учебное пособие / В. Ф. Шаньгин. — Москва : ФОРУМ : ИНФРА-М, 2020. — 592 с.

URL: https://znanium.com/catalog/product/1093695

7. Пелешенко В.С. Менеджмент инцидентов информационной безопасности защищенных автоматизированных систем управления [Электронный ресурс]: учебное пособие / В.С. Пелешенко, С.В. Говорова, М.А. Лапина. — Электрон. текстовые данные. — Ставрополь: Северо-Кавказский федеральный университет, 2017. — 86 с. — Режим доступа: http://www.iprbookshop.ru/69405.html

7.2. Базы данных, электронно-библиотечные системы, информационно-справочные и поисковые системы

1. Европейская цифровая библиотека Europeana: http://www.europeana.eu/portal
2. КонсультантПлюс: справочно-поисковая система [Электронный ресурс]. - www.consultant.ru/
3. Информационно-издательский центр по геологии и недропользованию Министерства природных ресурсов и экологии Российской Федерации - ООО "ГЕОИНФОРММАРК": http://www.geoinform.ru/
4. Информационно-аналитический центр «Минерал»: http://www.mineral.ru/
5. Мировая цифровая библиотека: http://wdl.org/ru
6. Научная электронная библиотека «Scopus»: https://www.scopus.com
7. Научная электронная библиотека ScienceDirect: http://www.sciencedirect.com
8. Научная электронная библиотека «eLIBRARY»: https://elibrary.ru/
9. Портал «Гуманитарное образование» http://www.humanities.edu.ru/
10. Федеральный портал «Российское образование» http://www.edu.ru/
11. Федеральное хранилище «Единая коллекция цифровых образовательных ресурсов» http://school-collection.edu.ru/
12. Поисковые системы Yandex, Rambler, Yahoo и др.
13. Электронно-библиотечная система издательского центра «Лань»: https://elanbook.com/books
14. Электронная библиотека Российской Государственной Библиотеки (РГБ): http://elibrary.rsl.ru/
15. Электронная библиотека учебников: http://studentam.net
16. Электронно-библиотечная система «ЭБС ЮРАИТ»: www.biblio-online.ru.
17. Электронная библиотечная система «Национальный цифровой ресурс «Руконт»»: http://rucont.ru/
18. Электронно-библиотечная система http://www.sciteclibrary.ru/

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

8. 1. Материально-техническое оснащение аудиторий

1. Аудитория для проведения лекционных занятий и практических работ

Оснащенность помещения: 16 посадочных мест. Стол аудиторный - 10 шт., компьютерное кресло - 23 шт., моноблок - 17 шт. (возможность доступа к сети «Интернет»), доска аудиторная под фломастер - 1 шт., лазерный принтер - 1 шт.

Перечень лицензионного программного обеспечения: Microsoft Windows 7 Professional (ГК № 1464-12/10 от 15.12.10) Microsoft Office 2007 Professional Plus (Microsoft Open License 46082032 от

30.10.2009, GPSS World (свободно распространяемое ПО), Arduino Software (IDE) (свободно распространяемое ПО), Microsoft SQL Server Express (свободно распространяемое ПО).

2. Аудитория для проведения лекционных занятий и практических работ

Оснащенность помещения: 16 посадочных мест. Стол аудиторный - 9 шт., компьютерное кресло - 17 шт., моноблок - 17 шт. (возможность доступа к сети «Интернет»), лазерный принтер - 1 шт., доска - 1 шт.

Перечень лицензионного программного обеспечения: Microsoft Windows 7 Professional (ГК № 1464-12/10 от 15.12.10) Microsoft Office 2007 Professional Plus (Microsoft Open License 46082032 от 30.10.2009 MathCad Education (Договор №1134-11/12 от 28.11.2012), GPSS World (свободно распространяемое ПО), Arduino Software (IDE) (свободно распространяемое ПО), Microsoft SQL Server Express (свободно распространяемое ПО).

8.2. Помещения для самостоятельной работы:

1. Оснащенность помещения для самостоятельной работы: 13 посадочных мест. Стул - 25 шт., стол - 2 шт., стол компьютерный - 13 шт., шкаф - 2 шт., доска аудиторная маркерная - 1 шт., АРМ учебное ПК (монитор + системный блок) - 14 шт. Доступ к сети «Интернет», в электронную информационно-образовательную среду Университета.

Перечень лицензионного программного обеспечения: Microsoft Windows 7 Professional^ № 1464-12/10 от 15.12.10 «На поставку компьютерного оборудования» ГК № 959-09/10 от 22.09.10 «На поставку компьютерной техники» ГК № 447-06/11 от 06.06.11 «На поставку оборудования» ГК № 984-12/11 от 14.12.11 «На поставку оборудования" Договор № 1105-12/11 от 28.12.2011 «На поставку компьютерного оборудования», Договор № 1106-12/11 от 28.12.2011 «На поставку компьютерного оборудования» ГК № 671-08/12 от 20.08.2012 «На поставку продукции», Microsoft Open License 60799400 от 20.08.2012, Microsoft Open License 48358058 от 11.04.2011, Microsoft Open License 49487710 от 20.12.2011, Microsoft Open License 49379550 от 29.11.2011,

Microsoft Office 2010 Standard: Microsoft Open License 60799400 от 20.08.2012, Microsoft Open License 60853086 от 31.08.2012 Kaspersky antivirus 6.0.4.142

2. Оснащенность помещения для самостоятельной работы: 17 посадочных мест. Доска для письма маркером - 1 шт., рабочие места студентов, оборудованные ПК с доступом в сеть университета - 17 шт., мультимедийный проектор - 1 шт., АРМ преподавателя для работы с мультимедиа - 1 шт. (системный блок, мониторы - 2 шт.), стол - 18 шт., стул - 18 шт. Доступ к сети «Интернет», в электронную информационно-образовательную среду Университета.

Перечень лицензионного программного обеспечения: Операционная система Microsoft Windows XP Professional: Microsoft Open License 16020041 от 23.01.200.

Операционная система Microsoft Windows 7 Professional Microsoft Open License 49379550 от 29.11.2011.

Microsoft Office 2007 Standard Microsoft Open License 42620959 от 20.08.2007

3. Оснащенность помещения для самостоятельной работы: 16 посадочных мест. Стол компьютерный для студентов (тип 4) - 3 шт., стол компьютерный для студентов (тип 6) - 2 шт., стол компьютерный для студентов (тип 7) - 1 шт., кресло преподавателя (сетка, цвет черный) - 17 шт., доска напольная мобильная белая магнитно-маркерная «Magnetoplan» 1800мм*1200мм - 1 шт., моноблок Lenovo M93Z Intel Q87 - 17 шт., плакат - 5 шт. Доступ к сети «Интернет», в электронную информационно-образовательную среду Университета.

Перечень лицензионного программного обеспечения: Microsoft Windows 7 Professional: Microsoft Open License 49379550 от 29.11.2011.

Microsoft Office 2007 Professional Plus: Microsoft Open License 46431107 от 22.01.2010. CorelDRAW Graphics Suite X5 Договор №559-06/10 от 15.06.2010 «На поставку программного обеспечения». Autodesk product: Building Design Suite Ultimate 2016, product Key: 766H1. Cisco Packet Tracer 7.1 (свободно распространяемое ПО), Quantum GIS (свободно распространяемое ПО), Python (свободно распространяемое ПО), R (свободно распространяемое ПО), Rstudio (свободно распространяемое ПО), SMath Studio (свободно распространяемое ПО), GNU Octave (свободно распространяемое ПО), Scilab (свободно распространяемое ПО)

8.3. Помещения для хранения и профилактического обслуживания оборудования:

1. Центр новых информационных технологий и средств обучения:

Оснащенность: персональный компьютер - 2 шт. (доступ к сети «Интернет»), монитор - 4 шт.,сетевой накопитель - 1 шт.,источник бесперебойного питания - 2 шт., телевизор плазменный Panasonic - 1 шт., точка Wi-Fi - 1 шт., паяльная станция - 2 шт., дрель - 5 шт., перфоратор - 3 шт., набор инструмента - 4 шт., тестер компьютерной сети - 3 шт., баллон со сжатым газом - 1 шт., паста теплопроводная - 1 шт., пылесос - 1 шт., радиостанция - 2 шт., стол - 4 шт., тумба на колесиках - 1 шт., подставка на колесиках - 1 шт., шкаф - 5 шт., кресло - 2 шт., лестница Alve - 1 шт.

Перечень лицензионного программного обеспечения: Microsoft Windows 7 Professional (Лицензионное соглашение Microsoft Open License 60799400 от 20.08.2012)

Microsoft Office 2010 Professional Plus (Лицензионное соглашение Microsoft Open License 60799400 от 20.08.2012)

Антивирусное программное обеспечение Kaspersky Endpoint Security (Договор № Д810(223)-12/17 от 11.12.17)

2. Центр новых информационных технологий и средств обучения:

Оснащенность: стол - 5 шт., стул - 2 шт., кресло - 2 шт., шкаф - 2 шт., персональный компьютер - 2 шт. (доступ к сети «Интернет»), монитор - 2 шт., МФУ - 1 шт., тестер компьютерной сети - 1 шт., балон со сжатым газом - 1 шт., шуруповерт - 1 шт.

Перечень лицензионного программного обеспечения: Microsoft Windows 7 Professional (Лицензионное соглашение Microsoft Open License 60799400 от 20.08.2012)

Microsoft Office 2007 Professional Plus (Лицензионное соглашение Microsoft Open License 46431107 от 22.01.2010)

Антивирусное программное обеспечение Kaspersky Endpoint Security (Договор № Д810(223)-12/17 от 11.12.17)

3. Центр новых информационных технологий и средств обучения:

Оснащенность: стол - 2 шт., стуля - 4 шт., кресло - 1 шт., шкаф - 2 шт., персональный компьютер - 1 шт. (доступ к сети «Интернет»), веб-камера Logitech HD C510 - 1 шт., колонки Logitech - 1 шт., тестер компьютерной сети - 1 шт., дрель - 1 шт., телефон - 1 шт., набор ручных инструментов - 1 шт.

Перечень лицензионного программного обеспечения: Microsoft Windows 7 Professional (Лицензионное соглашение Microsoft Open License 48358058 от 11.04.2011)

Microsoft Office 2007 Professional Plus (Лицензионное соглашение Microsoft Open License 46431107 от 22.01.2010)

Антивирусное программное обеспечение Kaspersky Endpoint Security (Договор № Д810(223)-12/17 от 11.12.17)

8.4. Лицензионное программное обеспечение

1. Microsoft Windows 8 Professional (договор бессрочный ГК № 875-09/13 от 30.09.2013 «На поставку компьютерной техники»)
2. Microsoft Office 2007 Standard (договор бессрочный Microsoft Open License 42620959 от 20.08.2007)
3. Microsoft Office 2010 Professional Plus (договор бессрочный Microsoft Open License 60799400 от 20.08.2012, договор бессрочный Microsoft Open License 47665577 от 10.11.2010, договор бессрочный Microsoft Open License 49379550 от 29.11.2011)
4. MathCad Education, Договор №1134-11/12 от 28.11.2012 "На поставку программного обеспечения"
5. LabView Professional, ГК №1142912/09 от 04.12.2009 " На поставку программного обеспечения".