

МИНОБРНАУКИ РОССИИ



Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Российский государственный гуманитарный университет»
(ФГБОУ ВО «РГГУ»)

ИНСТИТУТ ИНФОРМАЦИОННЫХ НАУК И ТЕХНОЛОГИЙ БЕЗОПАСНОСТИ
ФАКУЛЬТЕТ ИНФОРМАЦИОННЫХ СИСТЕМ И БЕЗОПАСНОСТИ
Кафедра комплексной защиты информации

**ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ
АВТОМАТИЗИРОВАННЫХ СИСТЕМ**

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

10.03.01 Информационная безопасность

Код и наименование направления подготовки/специальности

«Организация и технологии защиты информации»
(по отрасли или в сфере профессиональной деятельности)»

Наименование направленности (профиля)/ специализации

Уровень высшего образования: *бакалавриат*

Форма обучения: *очная*

РПД адаптирована для лиц
с ограниченными возможностями
здоровья и инвалидов

Москва 2023

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ АВТОМАТИЗИРОВАННЫХ СИСТЕМ
Рабочая программа дисциплины

Составитель:

Кандидат технических наук, доцент кафедры КЗИ А.С. Моляков

Ответственный редактор

Кандидат технических наук, и.о. зав. кафедрой КЗИ Д.А. Митюшин

УТВЕРЖДЕНО

Протокол заседания кафедры
комплексной защиты информации
№ 8 от 23.03.2023

Оглавление

1. Пояснительная записка.....	4
1.1. Цель и задачи дисциплины	4
1.2. Формируемые компетенции, соотнесённые с планируемыми результатами обучения по дисциплине:.....	4
1.3. Место дисциплины в структуре образовательной программы	5
2. Структура дисциплины.....	5
3. Содержание дисциплины	5
4. Образовательные технологии	7
5. Оценка планируемых результатов обучения.....	8
5.1. Система оценивания	8
5.2. Критерии выставления оценки по дисциплине	9
5.3. Оценочные средства (материалы) для текущего контроля успеваемости, промежуточной аттестации обучающихся по дисциплине	10
6. Учебно-методическое и информационное обеспечение дисциплины.....	11
6.1. Список источников и литературы	11
6.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет». ..	12
6.3. Профессиональные базы данных и информационно-справочные системы	13
7. Материально-техническое обеспечение дисциплины	13
8. Обеспечение образовательного процесса для лиц с ограниченными возможностями здоровья.....	13
9. Методические материалы.....	15
9.1. Планы практических занятий	15
<i>Приложение 1. Аннотация рабочей программы дисциплины.....</i>	<i>17</i>

1. Пояснительная записка

1.1. Цель и задачи дисциплины

Цель дисциплины – формирование знаний и умений по обеспечению информационной безопасности компьютерных систем и информационных процессов, и навыков по их определению для конкретных условий.

Задачи дисциплины:

- овладение методами мониторинга и аудита, выявления угроз информационной безопасности информационных систем;
- формирование навыков анализа информационной инфраструктуры информационных систем и ее безопасности.

1.2. Формируемые компетенции, соотнесённые с планируемыми результатами обучения по дисциплине:

Компетенция (код и наименование)	Индикаторы компетенций (код и наименование)	Результаты обучения
ПК-11 Способен проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов	ПК-11.1 Знает методики проведения теоретических исследований уровней защищенности информационной безопасности объектов и систем	Знать: основные методики управления защитой информации, информационные ресурсы и базовой модели нарушителя ФСТЭК России
	ПК-11.2 Умеет составлять и оформлять аналитический отчет по проведенным испытаниям, делать выводы по оценке защищенности на основании аналитического отчета	Уметь: составлять и оформлять аналитический отчет по совершенствованию системы управления защиты информации автоматизированных систем, проводить аудит с целью оценки рисков
	ПК-11.3 Владеет навыками использования профиля защиты и задания по безопасности, формулирования выводов по оценке защищенности	Владеть: навыками по использованию профиля защиты в соответствии с требованиями задания по безопасности
ПК-13 Способен принимать участие в формировании, организации и поддержания выполнения комплекса мер по обеспечению информационной безопасности, управлении процессом их реализации	ПК-13.1 Знает процедуру организации установки и настройки технических, программных (программно-технических) средств защиты информации, входящих в состав системы защиты информации организации, в соответствии с техническим проектом и инструкциями по эксплуатации	Знать: процедуру организации установки и настройки технических, программных (программно-технических) средств защиты в соответствии с требованиями технического проекта и инструкциями по эксплуатации
	ПК-13.2 Владеет навыками организации и сопровождения аттестации	Владеть: навыками организации и сопровождения аттестации объектов вычислительной тех-

	объектов вычислительной техники и выделенных (защищаемых) помещений на соответствие требованиям по защите информации	ники и выделенных (защищаемых) помещений на соответствие требованиям ФСТЭК и ФСБ, Минцифры.
	ПК-13.3 Умеет разрабатывать и реализовывать организационные меры, обеспечивающие эффективность системы защиты информации	Уметь: разрабатывать и реализовывать эффективные организационные меры в соответствии с нормативно-правовыми документами

1.3. Место дисциплины в структуре образовательной программы

Дисциплина «Информационная безопасность телекоммуникационных систем» относится к части, формируемой участниками образовательных отношений блока дисциплин учебного плана.

Для освоения дисциплины необходимы знания, умения и владения, сформированные в ходе изучения следующих дисциплин прохождения практик: «Аппаратные средства вычислительной техники», «Безопасность операционных систем», «Сети и системы передачи информации», «Информационные технологии. Администрирование подсистем защиты информации», «Программно-аппаратные средства защиты информации».

В результате освоения дисциплины формируются знания, умения и владения, необходимые для изучения следующих дисциплин и прохождения практик: «Преддипломная практика».

2. Структура дисциплины

Общая трудоемкость дисциплины составляет 3 зачетные единицы, 108 академических часа

Структура дисциплины для очной формы обучения

Объем дисциплины в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении учебных занятий:

Семестр	Тип учебных занятий	Количество часов
7	Лекции	26
7	Практические работы	28
Всего:		54

Объем дисциплины в форме самостоятельной работы обучающихся составляет 54 академических часа.

3. Содержание дисциплины

№	Наименование раздела дисциплины	Содержание
1	Основные понятия, концепции и принципы информационной	Идентификация, аутентификация и авторизация. Модели информационной безопасности. Триада

	безопасности	«конфиденциальность, доступность, целостность». Гексада Паркера и модель STRIDE. Уязвимость, угроза, атака. Ущерб и риск. Управление рисками. Типы и примеры атак. Пассивные и активные атаки. Отказ в обслуживании. Внедрение вредоносных программ. Кража личности, фишинг. Иерархия средств защиты от информационных угроз. Средства безопасности законодательного уровня. Административный уровень. Политика безопасности. Средства безопасности процедурного уровня. Средства безопасности технического уровня. Принципы защиты информационной системы. Подход сверху вниз. Защита как процесс. Эшелонированная защита. Сбалансированная защита. Компромиссы системы безопасности. Шифрование — базовая технология безопасности. Основные понятия и определения. Симметричное шифрование. Проблема распределения ключей. Метод Диффи-Хелмана передачи секретного ключа по незащищенному каналу. Концепция асимметричного шифрования. Алгоритм асимметричного шифрования RSA. Хеш-функции. Односторонние функции шифрования. Проверка целостности.
2	Технологии аутентификации, авторизации и управления доступом	Технологии аутентификации. Факторы аутентификации человека. Аутентификация на основе паролей. Аутентификация на основе аппаратных аутентификаторов. Аутентификация информации. Электронная подпись. Аутентификация на основе цифровых сертификатов. Аутентификация программных кодов. Технологии управления доступом и авторизации. Формы представления ограничений доступа. Системы аутентификации и управления доступом операционных систем. Аутентификации пользователей ОС. Аутентификация в ОС семейства Unix. Протокол SSH. Управление доступом в операционных системах. Централизованные системы аутентификации и авторизации. Концепция единого логического входа. Система Kerberos.
3	Технологии безопасности на основе фильтрации и мониторинга трафика	Фильтрация. Виды фильтрации. Стандартные и дополнительные правила фильтрации маршрутизаторов Cisco. Файерволы. Функциональное назначение файервола. Типы файерволов. Прокси-серверы. Функции прокси-сервера. «Проксификация» приложений. Файерволы с функцией NAT. Традиционная технология NAT. Базовая трансляция сетевых адресов. Трансляция сетевых адресов и портов. Программные файерволы хоста. Типовые архитектуры сетей, защищаемых

		файерволами. Мониторинг трафика. Анализаторы протоколов. Анализаторы протоколов. Система мониторинга NetFlow. Системы обнаружения вторжений. Архитектура сети с защитой периметра и разделением внутренних зон. Аудит событий безопасности.
4	Атаки на транспортную инфраструктуру сети	TCP-атаки. ICMP-атаки. UDP-атаки. IP-атаки. Сетевая разведка. Задачи и разновидности сетевой разведки. Сканирование сети. Сканирование портов. Атаки на DNS. Технологии защищенного канала. Способы образования защищенного канала. Иерархия технологий защищенного канала. Распределение функций между протоколами IPSec. Безопасная ассоциация. Транспортный и туннельный режимы. VPN на основе шифрования.
5	Уязвимость программного кода.	Уязвимости программного кода и вредоносные программы. Уязвимости, связанные с нарушением защиты оперативной памяти. Уязвимости контроля вводимых данных.
6	Безопасность программного кода.	Внедрение в компьютеры вредоносных программ. Троянские программы. Сетевые черви. Вирусы. Программные закладки. Антивирусные программы. Ботнет.
7	Безопасность сетевых служб	Безопасность веб-сервиса. Безопасность веб-браузера. Приватность и куки. Протокол HTTPS. Безопасность средств создания динамических страниц. Безопасность электронной почты. Угрозы приватности почтового сервиса. Аутентификация отправителя. Шифрование содержимого письма. Защита метаданных пользователя. Спам. Атаки почтовых приложений. Облачные сервисы и их безопасность. Концепция облачных вычислений. Определение облачных вычислений. Модели сервисов облачных сервисов. Облачные вычисления как источник угрозы. Облачные сервисы как средство повышения сетевой безопасности.

4. Образовательные технологии

Образовательные технологии

№ п/п	Наименование раздела	Виды учебных занятий	Образовательные технологии
1	2	3	4
1	Основные понятия, концепции и принципы информационной безопасности	Лекция 1	Традиционная лекция с использованием презентаций Работа с литературой
2	Технологии аутентификации	Лекция 2	Традиционная лекция с ис-

	ции, авторизации и управления доступом	Практическая работа 1	пользованием презентаций Выполнение заданий Работа с литературой
3	Технологии безопасности на основе фильтрации и мониторинга трафика	Лекция 3 Практическая работа 2	Традиционная лекция с использованием презентаций Выполнение заданий Работа с литературой
4	Атаки на транспортную инфраструктуру сети	Лекция 4.1 Лекция 4.2 Практическая работа 3	Традиционная лекция с использованием презентаций Выполнение заданий Работа с литературой
5	Уязвимость программного кода.	Лекция 5 Практическая работа 4	Традиционная лекция с использованием презентаций Выполнение заданий Работа с литературой
6	Безопасность программного кода.	Лекция 6 Практическая работа 5	Традиционная лекция с использованием презентаций Выполнение заданий Работа с литературой
7	Безопасность сетевых служб	Лекция 7 Практическая работа 6	Традиционная лекция с использованием презентаций Выполнение заданий Работа с литературой

5. Оценка планируемых результатов обучения

5.1. Система оценивания

Форма контроля	Макс. количество баллов	
	За одну работу	Всего
Текущий контроль:		
- практическая работа №1	9 баллов	9 баллов
- практическая работа №2	9 баллов	9 баллов
- практическая работа №3	9 баллов	9 баллов
- практическая работа №4	9 баллов	9 баллов
- практическая работа №5	12 баллов	12 баллов
- практическая работа №6	12 баллов	12 баллов
Промежуточная аттестация – зачет (зачет по билетам)		40 баллов
Итого за семестр		100 баллов

Перечень компетенций с указанием этапов их формирования в процессе освоения дисциплины представляется в виде таблицы:

№ п/п	Контролируемые разделы дисциплины	Код контролируемой компетенции	Наименование оценочного средства
1.	Темы 1 – 7	ПК-13.3, ПК-13.2, ПК-13.1, ПК-11.3, ПК-11.2, ПК-11.1	Опрос
2.	Практические занятия 1 – 6	ПК-13.3, ПК-13.2, ПК-13.1, ПК-11.3, ПК-11.2, ПК-11.1	План практических занятий

5.2. Критерии выставления оценки по дисциплине

Баллы/ Шкала ECTS	Оценка по дисциплине	Критерии оценки результатов обучения по дисциплине
100-83/ А,В	зачтено	<p>Выставляется обучающемуся, если он глубоко и прочно усвоил теоретический и практический материал, может продемонстрировать это на занятиях и в ходе промежуточной аттестации.</p> <p>Обучающийся исчерпывающе и логически стройно излагает учебный материал, умеет увязывать теорию с практикой, справляется с решением задач профессиональной направленности высокого уровня сложности, правильно обосновывает принятые решения.</p> <p>Свободно ориентируется в учебной и профессиональной литературе.</p> <p>Оценка по дисциплине выставляется обучающемуся с учётом результатов текущей и промежуточной аттестации.</p> <p>Компетенции, закреплённые за дисциплиной, сформированы на уровне – «высокий».</p>
82-68/ С	зачтено	<p>Выставляется обучающемуся, если он знает теоретический и практический материал, грамотно и по существу излагает его на занятиях и в ходе промежуточной аттестации, не допуская существенных неточностей.</p> <p>Обучающийся правильно применяет теоретические положения при решении практических задач профессиональной направленности разного уровня сложности, владеет необходимыми для этого навыками и приёмами.</p> <p>Достаточно хорошо ориентируется в учебной и профессиональной литературе.</p> <p>Оценка по дисциплине выставляется обучающемуся с учётом результатов текущей и промежуточной аттестации.</p> <p>Компетенции, закреплённые за дисциплиной, сформированы на уровне – «хороший».</p>
67-50/ D,E	зачтено	<p>Выставляется обучающемуся, если он знает на базовом уровне теоретический и практический материал, допускает отдельные ошибки при его изложении на занятиях и в ходе промежуточной аттестации.</p> <p>Обучающийся испытывает определённые затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, владеет необходимыми для этого базовыми навыками и приёмами.</p> <p>Демонстрирует достаточный уровень знания учебной литературы по дисциплине.</p> <p>Оценка по дисциплине выставляется обучающемуся с учётом результатов текущей и промежуточной аттестации.</p> <p>Компетенции, закреплённые за дисциплиной, сформированы на уровне – «достаточный».</p>
49-0/ F,FX	не зачтено	<p>Выставляется обучающемуся, если он не знает на базовом уровне теоретический и практический материал, допускает грубые ошибки при его изложении на занятиях и в ходе промежуточной аттестации.</p> <p>Обучающийся испытывает серьёзные затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, не владеет необходимыми для этого навыками и приёмами.</p> <p>Демонстрирует фрагментарные знания учебной литературы по дисциплине.</p> <p>Оценка по дисциплине выставляется обучающемуся с учётом результатов текущей и промежуточной аттестации.</p> <p>Компетенции на уровне «достаточный», закреплённые за дисциплиной, не сфор-</p>

Баллы/ Шкала ECTS	Оценка по дисциплине	Критерии оценки результатов обучения по дисциплине
		мированы.

5.3. Оценочные средства (материалы) для текущего контроля успеваемости, промежуточной аттестации обучающихся по дисциплине

Вопросы к зачету - проверка сформированности компетенций ПК-13, ПК-11

Контрольные вопросы
1. Понятие идентификации, аутентификации и авторизации.
2. Модели информационной безопасности.
3. Понятие уязвимости, угрозы, атаки.
4. Ущерб и риск. Управление рисками.
5. Пассивные и активные атаки.
6. Иерархия средств защиты от информационных угроз.
7. Понятие политики безопасности.
8. Принципы защиты информационной системы.
9. Основные понятия и определения криптографии.
10. Симметричное шифрование.
11. Асимметричное шифрование.
12. Проблема распределения ключей.
13. Хеш-функции.
14. Проверка целостности.
15. Технологии аутентификации.
16. Аутентификация на основе паролей.
17. Аутентификация на основе аппаратных аутентификаторов.
18. Аутентификация информации.
19. Электронная подпись.
20. Аутентификация на основе цифровых сертификатов.
21. Аутентификация программных кодов.
22. Технологии управления доступом и авторизации.
23. Системы аутентификации и управления доступом операционных систем.
24. Аутентификации пользователей ОС.
25. Аутентификация в ОС семейства Unix.
26. Протокол SSH.
27. Управление доступом в операционных системах.
28. Централизованные системы аутентификации и авторизации. Концепция единого логического входа.
29. Система Kerberos
30. Фильтрация. Виды фильтрации.
31. Файерволы. Функциональное назначение файервола. Типы файерволов.
32. Прокси-серверы. Функции прокси-сервера. «Проксификация» приложений.
33. Файерволы с функцией NAT. Традиционная технология NAT.
34. Базовая трансляция сетевых адресов. Трансляция сетевых адресов и портов.
35. Программные файерволы хоста.
36. Типовые архитектуры сетей, защищаемых файерволами.
37. Мониторинг трафика. Анализаторы протоколов. Анализаторы протоколов.
38. Системы обнаружения вторжений.

**Примерные задания для тестирования-проверка сформированности компетенций
ПК-13, ПК-11**

1. Криptomаршрутизатор - это:

а) аппаратно-программный комплекс криптографической защиты трафика данных, голоса, видео на основе шифрования пакетов по протоколам IPsec AH и/или IPsec ESP при установлении соединения, соответствующий требованиям к средствам криптографической защиты информации ФСБ России и обеспечивающий базовую функциональность современного VPN-устройства..

б) мобильное средство связи.

в) дисковое устройство.

2. Шлюз безопасности VPN – это:

а) сетевое устройство, подключаемое к двум и более сетям и выполняющее функции шифрования и аутентификации для многочисленных хостов, расположенных за ним.

б) сетевое устройство, подключаемое к двум сетям и выполняющее функции шифрования и аутентификации для многочисленных хостов, расположенных за ним.

в) сетевое устройство, подключаемое к двум и более сетям и выполняющее функции шифрования и авторизации для различных хостов.

6. Учебно-методическое и информационное обеспечение дисциплины

6.1. Список источников и литературы

Источники

Основные

1. *Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения. Утверждено решением председателя Гостехкомиссии России от 30 марта 1992 г. [Электронный ресурс] : Режим доступа : <https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/386-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkommisii-rossii-ot-30-marta-1992-g3>, свободный. – Загл. с экрана.*
2. *Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г. [Электронный ресурс] : Режим доступа : <https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/384-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkommisii-rossii-ot-30-marta-1992-g>, свободный. – Загл. с экрана.*
3. *Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищённости от несанкционированного доступа к информации. Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г. [Электронный ресурс] : Режим доступа : <https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/385-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkommisii-rossii-ot-30-marta-1992-g2>, свободный. – Загл. с экрана.*
4. *Руководящий документ. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищённости от несанкционированного доступа к информации. Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 25*

июля 1997 г. [Электронный ресурс] : Режим доступа : <https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/383-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkommisii-rossii-ot-25-iyulya-1997-g>, свободный. – Загл. с экрана.

5. *Федеральный закон* «Об информации, информационных технологиях и о защите информации» от 27.07.2006 N 149-ФЗ (ред. от 19.07.2018). [Электронный ресурс] : Режим доступа : http://www.consultant.ru/document/cons_doc_LAW_61798/, свободный. – Загл. с экрана.

Литература Основная

1. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для вузов / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2020. — 312 с. — (Высшее образование). — ISBN 978-5-9916-9043-0. — Текст: электронный // ЭБС Юрайт [сайт]. — URL: <https://urait.ru/bcode/452368>
2. Дибров, М. В. Сети и телекоммуникации. Маршрутизация в IP-сетях в 2 ч. Часть 1 : учебник и практикум для вузов / М. В. Дибров. — Москва : Издательство Юрайт, 2020. — 333 с. — (Высшее образование). — ISBN 978-5-9916-9956-3. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: <https://urait.ru/bcode/452430>
3. Дибров, М. В. Сети и телекоммуникации. Маршрутизация в IP-сетях в 2 ч. Часть 2 : учебник и практикум для вузов / М. В. Дибров. — Москва : Издательство Юрайт, 2020. — 351 с. — (Высшее образование). — ISBN 978-5-9916-9958-7. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: <https://urait.ru/bcode/453063>
4. Щеглов, А. Ю. Защита информации: основы теории: учебник для бакалавриата и магистратуры / А. Ю. Щеглов, К. А. Щеглов. — Москва: Издательство Юрайт, 2020. — 309 с. — (Бакалавр и магистр. Академический курс). — ISBN 978-5-534-04732-5. — Текст: электронный // ЭБС Юрайт [сайт]. — URL: <https://urait.ru/bcode/449285>
5. Сети и телекоммуникации : учебник и практикум для вузов / К. Е. Самуйлов [и др.] ; под редакцией К. Е. Самуйлова, И. А. Шалимова, Д. С. Кулябова. — Москва : Издательство Юрайт, 2020. — 363 с. — (Высшее образование). — ISBN 978-5-534-00949-1. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: <https://urait.ru/bcode/450234>
6. *Комплексная защита информации в корпоративных системах* : учеб. пособие / В.Ф. Шаньгин. — М. : ИД «ФОРУМ» : ИНФРА-М, 2017. — 592 с. — (Высшее образование: Бакалавриат). - Режим доступа: <http://znanium.com/catalog/product/546679>
7. *Шаньгин В.Ф.* Защита компьютерной информации. Эффективные методы и средства [Электронный ресурс] / В. Ф. Шаньгин. - М.: ДМК Пресс, 2010. - 544 с.: ил. - ISBN 978-5-94074-518-1. - Режим доступа: <http://znanium.com/catalog/product/408107>

6.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет».

1. Официальный сайт компании Криптопро [Электронный ресурс]: Режим доступа: <http://www.cryptopro.com/>, свободный. – Загл. с экрана.
2. Центр разработки Криптоком [Электронный ресурс]: Режим доступа: <http://www.cryptocom.ru/products/index.html/>, свободный. – Загл. с экрана.

Национальная электронная библиотека (НЭБ) www.rusneb.ru
 ELibrary.ru Научная электронная библиотека www.elibrary.ru
 Электронная библиотека Grebennikon.ru www.grebennikon.ru

6.3. Профессиональные базы данных и информационно-справочные системы

Доступ к профессиональным базам данных: <https://liber.rsuh.ru/ru/bases>

Информационные справочные системы:

1. Консультант Плюс
2. Гарант

7. Материально-техническое обеспечение дисциплины

Для обеспечения дисциплины используется материально-техническая база образовательного учреждения:

для лекционных занятий - учебная аудитория, доска, компьютер или ноутбук, проектор (стационарный или переносной) для демонстрации учебных материалов.

Состав программного обеспечения:

1. Windows
2. MicrosoftOffice
3. KasperskyEndpointSecurity

Для проведения занятий лекционного типа предлагаются тематические иллюстрации в формате презентаций PowerPoint.

2) для практических занятий – компьютерный класс или лаборатория, доска, проектор (стационарный или переносной), компьютер или ноутбук для преподавателя, компьютеры для обучающихся.

Состав программного обеспечения:

1. Windows
2. Microsoft Office
3. Kaspersky Endpoint Security
4. Mozilla Firefox
5. Microsoft Share Point 2010
6. Secret Net Studio 8.4
7. Vmware Player 15.5
8. XSpider 7.0
9. Nmap 7.8
10. Open VPN
11. SoftEther VPN
12. Windscribe VPN
13. TinyFEC VPN

8. Обеспечение образовательного процесса для лиц с ограниченными возможностями здоровья

В ходе реализации дисциплины используются следующие дополнительные методы обучения, текущего контроля успеваемости и промежуточной аттестации обучающихся в зависимости от их индивидуальных особенностей:

- для слепых и слабовидящих:
 - лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением;

- письменные задания выполняются на компьютере со специализированным программным обеспечением, или могут быть заменены устным ответом;
- обеспечивается индивидуальное равномерное освещение не менее 300 люкс;
- для выполнения задания при необходимости предоставляется увеличивающее устройство; возможно также использование собственных увеличивающих устройств;
- письменные задания оформляются увеличенным шрифтом;
- экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

- для глухих и слабослышащих:
 - лекции оформляются в виде электронного документа, либо предоставляется звукоусиливающая аппаратура индивидуального пользования;
 - письменные задания выполняются на компьютере в письменной форме;
 - экзамен и зачёт проводятся в письменной форме на компьютере; возможно проведение в форме тестирования.

- для лиц с нарушениями опорно-двигательного аппарата:
 - лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением;
 - письменные задания выполняются на компьютере со специализированным программным обеспечением;
 - экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

При необходимости предусматривается увеличение времени для подготовки ответа.

Процедура проведения промежуточной аттестации для обучающихся устанавливается с учётом их индивидуальных психофизических особенностей. Промежуточная аттестация может проводиться в несколько этапов.

При проведении процедуры оценивания результатов обучения предусматривается использование технических средств, необходимых в связи с индивидуальными особенностями обучающихся. Эти средства могут быть предоставлены университетом, или могут использоваться собственные технические средства.

Проведение процедуры оценивания результатов обучения допускается с использованием дистанционных образовательных технологий.

Обеспечивается доступ к информационным и библиографическим ресурсам в сети Интернет для каждого обучающегося в формах, адаптированных к ограничениям их здоровья и восприятия информации:

- для слепых и слабовидящих:
 - в печатной форме увеличенным шрифтом;
 - в форме электронного документа;
 - в форме аудиофайла.
- для глухих и слабослышащих:
 - в печатной форме;
 - в форме электронного документа.
- для обучающихся с нарушениями опорно-двигательного аппарата:
 - в печатной форме;
 - в форме электронного документа;
 - в форме аудиофайла.

Учебные аудитории для всех видов контактной и самостоятельной работы, научная библиотека и иные помещения для обучения оснащены специальным оборудованием и учебными местами с техническими средствами обучения:

- для слепых и слабовидящих:
 - устройством для сканирования и чтения с камерой SARA CE;
 - дисплеем Брайля PAC Mate 20;
 - принтером Брайля EmBrailleViewPlus;

- для глухих и слабослышащих:
 - автоматизированным рабочим местом для людей с нарушением слуха и слабослышащих;
 - акустический усилитель и колонки;
- для обучающихся с нарушениями опорно-двигательного аппарата:
 - передвижными, регулируемые эргономическими партами СИ-1;
 - компьютерной техникой со специальным программным обеспечением.

9. Методические материалы

9.1. Планы практических занятий

- проверка сформированности компетенций ПК-3

Практическое занятие 1 (4 ч.) «Технологии аутентификации, авторизации и управления доступом»- проверка сформированности компетенций ПК-13, ПК-11

Задания:

1. Создание новых пользователей и исследование механизмов расширенной аутентификации на примере SecretNetStudio.
2. Управление доступом в операционных системах с помощью встроенных и наложенных средств защиты информации.

Практическое занятие 2 (4 ч.) «Технологии безопасности на основе фильтрации и мониторинга трафика» - проверка сформированности компетенций ПК-13, ПК-11

Задания:

1. Установка и настройка VPN-клиента.
2. Осуществление мониторинга трафика.
3. Осуществление аудита событий безопасности.

Практическое занятие 3 (4 ч.) «Исследования транспортной инфраструктуры сети» - проверка сформированности компетенций ПК-13, ПК-11

Задания:

1. Изучить стек протокола TCP/IP.
2. Получить у преподавателя метрики зондируемых сетей.
3. Сканирование сети. Сканирование портов.
4. Подготовка отчета об уровне защищенности просканированных узлов.

Практическое занятие 4 (4 ч.) «Уязвимости программного кода и вредоносные программы» - проверка сформированности компетенций ПК-13, ПК-11

Задания:

1. Уязвимости программного кода.
2. Исследование механизмов контроля целостности, контроля приложений и т.д..
3. Настройка компонентов защиты.

Практическое занятие 5 (4 ч.) «Программные закладки. Работа с изолированной программной средой» - проверка сформированности компетенций ПК-13, ПК-11

Задания:

1. Исследование методов внедрения программных закладок в виртуальной “песочнице”.
2. Настройка изолированной программной среды.
3. Конфигурирование компонента контроля съемных машинописных носителей информации.

Практическое занятие (4 ч.) «Безопасность веб-сервиса» - проверка сформированности компетенций ПК-13, ПК-11

Задания:

1. Изучить способы проведения тестов на проникновение.
2. Сбор сведений в сети интернет по уязвимостям Web-серверов на примере apache и nginx.
3. Установить сканеры XSpider и Nmap.
4. Произвести сканирование на защищенность Web-сервисов на примере сайтов www.rsuh.ru, www.yandex.ru, www.ict.cn.

Дисциплина «Информационная безопасность автоматизированных систем» реализуется на факультете Информационных систем и безопасности кафедрой комплексной защиты информации.

Цель дисциплины – формирование знаний и умений по обеспечению информационной безопасности компьютерных систем и информационных процессов, и навыков по их определению для конкретных условий.

Задачи дисциплины:

- овладение методами мониторинга и аудита, выявления угроз информационной безопасности информационных систем;
- формирование навыков анализа информационной инфраструктуры информационных систем и ее безопасности.

Дисциплина направлена на формирование следующих компетенций:

- ПК-11 – Способен проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов;
- ПК-13 – Способен принимать участие в формировании, организации и поддержания выполнения комплекса мер по обеспечению информационной безопасности, управлении процессом их реализации

В результате освоения дисциплины обучающийся должен:

- Знать: основные методики управления защитой информации, информационные ресурсы и базовой модели нарушителя ФСТЭК России; процедуру организации установки и настройки технических, программных (программно-технических) средств защиты в соответствии с требованиями технического проекта и инструкциями по эксплуатации;
- Владеть: навыками по использованию профиля защиты в соответствии с требованиями задания по безопасности; навыками организации и сопровождения аттестации объектов вычислительной техники и выделенных (защищаемых) помещений на соответствие требованиям ФСТЭК и ФСБ, Минцифры;
- Уметь: разрабатывать и реализовывать эффективные организационные меры в соответствии с нормативно-правовыми документами; составлять и оформлять аналитический отчет по совершенствованию системы управления защиты информации автоматизированных систем, проводить аудит с целью оценки рисков.

По дисциплине предусмотрена промежуточная аттестация в форме зачета.

Общая трудоёмкость освоения дисциплины составляет 3 зачётные единицы.