

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*

**ОЦЕНКА БЕЗОПАСНОСТИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ
АВТОМАТИЗИРОВАННЫХ СИСТЕМ**
РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
*Направление подготовки 10.03.01 Информационная безопасность
Направленность (профиль) подготовки:
Безопасность автоматизированных систем
Уровень квалификации выпускника – бакалавр*

Форма обучения – очная

РПД адаптирована для лиц
с ограниченными возможностями
здоровья и инвалидов

Москва 2021

Оценка безопасности программного обеспечения 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

№ 10 от 20.05.2021 г.

ОГЛАВЛЕНИЕ

1. Пояснительная записка

1.1 Цель и задачи дисциплины

1.2. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесённых с индикаторами достижения компетенций

1.3. Место дисциплины в структуре образовательной программы

2. Структура дисциплины

3. Содержание дисциплины

4. Образовательные технологии

5. Оценка планируемых результатов обучения

5.1. Система оценивания

5.2. Критерии выставления оценок

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

6. Учебно-методическое и информационное обеспечение дисциплины

6.1. Список источников и литературы

6.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

7. Материально-техническое обеспечение дисциплины

8. Обеспечение образовательного процесса для лиц с ограниченными возможностями здоровья

9. Методические материалы

9.1. Планы практических занятий

Приложения

Приложение 1. Аннотация дисциплины

Приложение 2. Лист изменений

1. Пояснительная записка

1.1. Цель и задачи дисциплины

Цель дисциплины – формирование систематизированных знаний о процессах разработки и оценки безопасности ПО АС на примере DLP-систем, применяемых при этом подходах, методиках и механизмах защиты информации, а также формирование у обучающихся умений и навыков, необходимых при непосредственном участии в указанных процессах.

Задачи дисциплины:

- сформировать знания о моделях и этапах жизненного цикла защищенных объектов информатизации и систем защиты информации, применяемых подходах и методах по обеспечению безопасности на каждом из этапов;
- сформировать представления об уязвимостях, присущих объектам информатизации, связанных с ними угрозами, а также навыки формирования моделей угроз безопасности и моделей потенциальных нарушителей;
- сформировать и развить компетенции, знания и практические навыки обеспечения технологической и эксплуатационной безопасности объектов информатизации.

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

Компетенция (код и наименование)	Индикаторы компетенций (код и наименование)	Результаты обучения
<i>ПК-4</i> <i>Способен обеспечивать работоспособность систем защиты информации при возникновении нештатных ситуаций</i>	<i>ПК-4.1</i> <i>Знает методы и способы обеспечения отказоустойчивости автоматизированных систем, содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и подсистем безопасности автоматизированных систем</i>	<i>Знать: архитектуру подсистем безопасности, смысл базовых понятий, таких как идентификация и аутентификация, разграничение доступа и т.д.; методы и способы отказоустойчивости работы автоматизированных систем</i>
	<i>ПК-4.2</i> <i>Умеет применять типовые программные средства резервирования и восстановления информации, средства обеспечения отказоустойчивости в автоматизированных системах</i>	<i>Уметь: осуществлять настройку политики ученой записей, выполнения резервирования и архивирования, отказоустойчивости DLP-систем</i>

	<p><i>ПК-4.3</i> <i>Владеет навыками обнаружения, устранения неисправностей в работе системы защиты информации автоматизированной системы, резервирования программного обеспечения, технических средств, каналов передачи данных автоматизированной системы управления на случай возникновения нештатных ситуаций</i></p>	<p><i>Владеть: навыками обнаружения, устранения неисправностей в работе DLP-систем</i></p>
<p><i>ПК-6</i> <i>Способен принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации</i></p>	<p><i>ПК-6.1</i> <i>Знает оценки работоспособности применяемых средств защиты информации с использованием штатных средств и методик</i></p>	<p><i>Знать основные принципы оценки работоспособности и тестирования оборудования обработки и передачи данных, критерии и меры надежности, возможности и особенности организационных, аппаратных и программных средств безопасности и защиты информации.</i> <i>Уметь составлять и реализовывать планы тестирующих мероприятий,</i></p>
	<p><i>ПК-6.2</i> <i>Умеет оценить эффективность применяемых средств защиты информации с использованием штатных средств и методик</i></p>	<p><i>Уметь: составлять и реализовывать планы тестирующих мероприятий, моделировать и оценивать эффективность применяемых средств защиты</i></p>
	<p><i>ПК-6.3</i> <i>Владеет навыками определения уровня защищенности и доверия средств защиты информации</i></p>	<p><i>Владеть: навыками эксплуатации и Тестирования DLP-систем, определение профиля защиты.</i></p>

1.3. Место дисциплины в структуре образовательной программы

Дисциплина «Оценка безопасности программного обеспечения автоматизированных систем» относится к дисциплинам по выбору части, формируемой участниками образовательных отношений блока дисциплин учебного плана.

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

В результате освоения дисциплины формируются знания, умения и владения, необходимые для изучения следующих дисциплин и прохождения практик: «Безопасность критически важных систем», «Безопасность программного обеспечения автоматизированных систем», «Преддипломная практика».

2. Структура дисциплины

Структура дисциплины для очной формы обучения

Общая трудоёмкость дисциплины составляет 2 з.е., 76 ч., в том числе контактная работа обучающихся с преподавателем 40 ч., самостоятельная работа обучающихся 36 ч.

№ п/п	Раздел дисциплины/темы	Семестр	Виды учебной работы (в часах)					Самостоятельная работа	Формы текущего контроля успеваемости, форма промежуточной аттестации
			контактная						
			Лекции	Семинар	Практические занятия	Лабораторные занятия	Промежуточная аттестация		
1	<i>Понятие DLP-системы. Базовые знания по защите объектов информатизации</i>	7	2		2			10	Опрос.
2	<i>Проектирование системы защиты конфиденциальной информации на примере DLP-систем</i>	7	4		8			10	Опрос. Оценка выполнения практических заданий
3	<i>Архитектура DLP-систем</i>	7	6		6			10	Опрос. Оценка выполнения практических заданий
4	<i>Нормативно-правовые требования по сертификации DLP-систем</i>	7	4		6			6	Опрос. Оценка выполнения практических заданий
	<i>Зачет с оценкой</i>				2				<i>Зачет по билетам</i>
	Итого:		16		24			36	

3. Содержание дисциплины

№	Наименование раздела дисциплины	Содержание
1	Понятие DLP-системы. Базовые знания по защите объектов информатизации	Понятие, структура и состав DLP-систем. Классификация объектов информатизации с точки зрения безопасности. Принципы обеспечения информационной безопасности.
2	Проектирование системы защиты конфиденциальной информации на примере DLP-систем	Формирование требований к объекту информатизации. Моделирование угроз безопасности. Методы обеспечения защищенности объектов информатизации на этапе внедрения и эксплуатации
3	Архитектура DLP-систем	Структура и назначение системы защиты информации. Этапы построения системы защиты информации. Порядок разработки системы защиты конфиденциальной информации.
4	Нормативно-правовые требования по сертификации DLP-систем	Противоречия между необходимостью применения программно—технических средств защиты информации и требований по осуществлению контрольных мероприятий на основе подобных средств. В данном случае процедуры контрольных мероприятий могут осуществляться с использованием персональных данных работника, подвергающегося проверке. Комплекс нормативно — правовых документов, определяющих как категории и виды конфиденциальной информации, требования по обеспечения информационной безопасности подобных информационных ресурсов, так и перечень рекомендуемых для использования способов и средств защиты информации

4. Образовательные технологии¹

Образовательные технологии

№ п/п	Наименование раздела	Виды учебных занятий	Образовательные технологии
1	2	3	4
1	<i>Понятие DLP-системы. Базовые знания по защите объектов информатизации</i>	<i>Лекция 1 Практическое занятие 1 Самостоятельная работа</i>	<i>Традиционная лекция с использованием презентаций Выполнение заданий Работа с литературой</i>
2	<i>Проектирование системы защиты конфиденциальной информации на примере DLP-систем</i>	<i>Лекция 2.1 Лекция 2.2 Практическое занятие 2 Самостоятельная работа</i>	<i>Традиционная лекция с использованием презентаций Выполнение заданий Работа с литературой</i>
3	<i>Архитектура DLP-систем</i>	<i>Лекция 3.1 Лекция 3.2 Лекция 3.3 Практическое занятие 3 Самостоятельная работа</i>	<i>Традиционная лекция с использованием презентаций Выполнение заданий Работа с литературой</i>
4	<i>Нормативно-правовые требования по сертификации DLP-систем</i>	<i>Лекция 4.1 Лекция 4.2 Практическое занятие 4 Самостоятельная работа</i>	<i>Традиционная лекция с использованием презентаций Выполнение заданий Работа с литературой</i>

¹ В разделе указываются образовательные технологии, используемые при реализации различных видов учебных занятий для наиболее эффективного освоения дисциплины. При проведении учебных занятий обеспечивается развитие у обучающихся навыков командной работы, межличностной коммуникации, принятия решений, лидерских качеств (включая при необходимости проведение интерактивных лекций, групповых дискуссий, ролевых игр, тренингов, анализ ситуаций и имитационных моделей, преподавание дисциплин (*модулей*) в форме курсов, составленных на основе результатов научных исследований, в том числе с учётом региональных особенностей профессиональной деятельности выпускников и потребностей работодателей (п.34. Приказ №301).

5. Оценка планируемых результатов обучения

5.1. Система оценивания

Форма контроля	Макс. количество баллов	
	За одну ра- боту	Всего
Текущий контроль: - практическое занятие № 1	10 баллов	10 баллов
- практическое занятие № 2	25 баллов	25 баллов
- практическое занятие № 3	25 баллов	25 баллов
- практическое занятие № 4	25 баллов	25 баллов
Промежуточная аттестация зачёт с оценкой		40 баллов
Итого за дисциплину Зачёт с оценкой		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 – 4	ПК-4.1, ПК-4.2, ПК-4.3, ПК-6.1, ПК-6.2, ПК-6.3	Опрос
2.	Практические занятия 1 – 4	ПК-4.1, ПК-4.2, ПК-4.3, ПК-6.1, ПК-6.2, ПК-6.3	План практического занятия

Полученный совокупный результат конвертируется в традиционную шкалу оценок и в шкалу оценок Европейской системы переноса и накопления кредитов (European Credit Transfer System; далее – ECTS) в соответствии с таблицей:

100-балльная шкала	Традиционная шкала		Шкала ECTS
95 – 100	отлично	зачтено	A
83 – 94			B
68 – 82	хорошо		C
56 – 67	удовлетворительно		D
50 – 55			E
20 – 49	неудовлетворительно	не зачтено	FX
0 – 19			F

5.2. Критерии выставления оценки по дисциплине

Баллы/ Шкала ECTS	Оценка по дисциплине	Критерии оценки результатов обучения по дисциплине
100-83/ А,В	«отлично»/ «зачтено (отлично)»/ «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	«хорошо»/ «зачтено (хорошо)»/ «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	«удовлетворительно»/ «зачтено (удовлетворительно)»/ «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>

Баллы/ Шкала ECTS	Оценка по дисциплине	Критерии оценки результатов обучения по дисциплине
		Компетенции, закреплённые за дисциплиной, сформированы на уровне – «достаточный».
49-0/ F,FX	«неудовлетворительно»/ 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 сформированы.</p>

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

Вопросы к зачету - проверка сформированности компетенций ПК-4, ПК-6

Контрольные вопросы	Реализуемые компетенции
1. Понятие, структура и состав DLP-систем.	ПК-4.1, ПК-4.2, ПК-4.3
2. Классификация DLP-систем.	ПК-4.1, ПК-4.2, ПК-4.3
3. Принципы обеспечения информационной безопасности.	ПК-4.1, ПК-4.2, ПК-4.3, ПК-6.1, ПК-6.2, ПК-6.3
4. Жизненный цикл DLP-систем.	ПК-4.1, ПК-4.2, ПК-4.3, ПК-6.1, ПК-6.2, ПК-6.3
5. Моделирование угроз безопасности объекта информатизации.	ПК-6.1, ПК-6.2, ПК-6.3
6. Управление проектированием защищенных объектов информатизации.	ПК-4.1, ПК-4.2, ПК-4.3, ПК-6.1, ПК-6.2, ПК-6.3
7. Структура и назначение системы защиты информации на примере DLP-систем.	ПК-4.1, ПК-4.2, ПК-4.3, ПК-6.1, ПК-6.2, ПК-6.3
8. Этапы построения системы защиты информации.	ПК-4.1, ПК-4.2, ПК-4.3, ПК-6.1, ПК-6.2, ПК-6.3
9. Архитектура DLP-систем.	ПК-4.1, ПК-4.2, ПК-4.3
10. Оценка соответствия системы защиты.	ПК-6.1, ПК-6.2, ПК-6.3
11. Методики анализа рисков информационной безопасности.	ПК-6.1, ПК-6.2, ПК-6.3
12. Аттестация объектов информатизации по безопасности.	ПК-4.1, ПК-4.2, ПК-4.3, ПК-6.1, ПК-6.2, ПК-6.3

13. Противоречия между необходимостью применения программно—технических средств защиты информации и требований по осуществлению контрольных мероприятий на основе подобных средств.	ПК-4.1, ПК-4.2, ПК-4.3, ПК-6.1, ПК-6.2, ПК-6.3
14. База контентной фильтрации.	ПК-4.1, ПК-4.2, ПК-4.3
15. Два основных способа перехвата — серверный и агентский.	ПК-4.1, ПК-4.2, ПК-4.3, ПК-6.1, ПК-6.2, ПК-6.3
16. DLP-системы для учета рабочего времени сотрудников. Рабочий процесс каждого пользователя можно представить в виде статистики, которая позволяет проанализировать, насколько сотрудник вовлечен в трудовой процесс.	ПК-4.1, ПК-4.2, ПК-4.3, ПК-6.1, ПК-6.2, ПК-6.3
17. Требования, предъявляемые ФСТЭК к усилению мер информационной защиты DLP-систем.	ПК-4.1, ПК-4.2, ПК-4.3, ПК-6.1, ПК-6.2, ПК-6.3
18. Поддержка виртуальных и терминальных сред как расширение функционала подсистемы информационной безопасности при использовании различных решений виртуализации рабочих сред, созданных как в форме локальных виртуальных машин, так и терминальных сессий рабочих столов или опубликованных приложений на гипервизорах.	ПК-4.1, ПК-4.2, ПК-4.3, ПК-6.1, ПК-6.2, ПК-6.3
19. Инспекция содержимого перемещаемых данных в режиме реального времени с возможностью блокировки такой попытки или отправки тревожного оповещения.	ПК-4.1, ПК-4.2, ПК-4.3, ПК-6.1, ПК-6.2, ПК-6.3
20. Лингвистический анализ и статистические методы анализа.	ПК-4.1, ПК-4.2, ПК-4.3, ПК-6.1, ПК-6.2, ПК-6.3

Примерные задания для тестирования- проверка сформированности компетенций ПК-4, ПК-6

1. Проверка подлинности субъекта по предъявленному им идентификатору для принятия решения о предоставлении ему доступа к ресурсам системы — это:
 - a) аудит
 - b) аутентификация
 - c) авторизация
 - d) идентификация
2. Метод управления доступом, при котором каждому объекту системы присваивается метка критичности, определяющая ценность информации, называется:
 - a) избирательным

- b) мандатным
- c) привилегированным

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-predsdatelya-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-predsdatelya-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-predsdatelya-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-predsdatelya-gostekhkommisii-rossii-ot-25-iyulya-1997-g>, 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. Казарин, О. В. Надежность и безопасность программного обеспечения : учебное пособие для вузов / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2020. — 342 с. — (Высшее образование). — ISBN 978-5-534-05142-1. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: <https://urait.ru/bcode/454453>
3. *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>
4. *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>
5. Методы и средства защиты программного обеспечения [Электронный ресурс] : учеб.-метод. комплекс : для бакалавриата по направлению подготовки 090900 Информационная безопасность : по профилям: Организация и технология защиты информации, Комплексная защита объектов информатизации / Минобрнауки России, Федер. гос. бюджетное образоват. учреждение высш. проф. образования "Рос. гос. гуманитарный ун-т" (РГГУ), Ин-т информац. наук и технологий безопасности, Фак. информац. систем и безопасности, Каф. компьютерной безопасности ; [сост.: Казарин О. В. ; отв. ред. А. А. Тарасов]. - Электрон. дан. - Москва: РГГУ, 2013. - 30 с. - Режим доступа: <http://elibr.lib.rsuh.ru/elibr/000009341>. - Загл. с экрана. - ISBN 978-5-7281-1789-6.

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

1. ОХРАНА.ру. Российское СМИ о безопасности. [Электронный ресурс] : Режим доступа : <https://охрана.ру/>, свободный. – Загл. с экрана.
2. Sec.ru. Портал по безопасности. [Электронный ресурс] : Режим доступа : <http://sec.ru/>, необходима регистрация. – Загл. с экрана.
3. *Банк данных угроз безопасности информации*. [Электронный ресурс] / ФСТЭК России, ФАУ «ГНИИИ ПТЗИ ФСТЭК России» – Режим доступа : <http://sec.ru/>, свободный. – Загл. с экрана.

7. Материально-техническое обеспечение дисциплины

Для проведения занятий необходимо следующее материально-техническое обеспечение:

- 1) для лекционных занятий – лекционный класс с видеопроектором и компьютером, на котором должны быть установлены следующее ПО:

№ п/п	Наименование ПО	Производитель	Способ распространения
1	Microsoft Office 2010	Microsoft	лицензионное
2	Windows 10 Pro	Microsoft	лицензионное
3	Kaspersky Endpoint Security	Kaspersky	лицензионное

- 2) для практических занятий – компьютерный класс, оборудованный современными персональными компьютерами для каждого студента. На компьютере должны быть установлено следующее ПО:

№п/п	Наименование ПО	Производитель	Способ распространения (лицензионное или свободно распространяемое)
1	Microsoft Office 2010	Microsoft	лицензионное
2	Windows 7 Pro	Microsoft	лицензионное

3	Microsoft Share Point 2010	Microsoft	лицензионное
4	Microsoft Office 2013	Microsoft	лицензионное
5	Windows 10 Pro	Microsoft	лицензионное
6	Kaspersky Endpoint Security	Kaspersky	Лицензионное
7	Vmware Player 15.5	VMWare	Режим доступа: https://www.vmware.com/products/ Демо-версия

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

Перечень БД и ИСС

№п /п	Наименование
1	Международные реферативные наукометрические БД, доступные в рамках национальной подписки в 2020 г. Web of Science Scopus
2	Профессиональные полнотекстовые БД, доступные в рамках национальной подписки в 2020 г. Журналы Cambridge University Press ProQuest Dissertation & Theses Global SAGE Journals Журналы Taylor and Francis
3	Профессиональные полнотекстовые БД JSTOR Издания по общественным и гуманитарным наукам Электронная библиотека Grebennikon.ru
4	Компьютерные справочные правовые системы Консультант Плюс, Гарант

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 зачет 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 EmBraille ViewPlus;
- 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-4, ПК-6

Практическое занятие 1 (2 ч.) «Общая архитектура DLP-систем» - проверка сформированности компетенций ПК-4, ПК-6

Задания:

1. Обсудить понятие, структуру и состав DLP-систем. Дать классификацию объектов информатизации по заданию преподавателя.

Список литературы:

Приведён в п. 6 данной РПД

Материально-техническое обеспечение занятия: аудитория, оснащенная презентационной техникой (проектор, экран, компьютер/ноутбук). Компьютеры по количеству обучающихся с развёрнутой ОС MS Windows, виртуальной машиной, ППП MS Office v.2007 и выше

Практическое занятие 2 (8 ч.) «Анализ угроз конфиденциальной информации» - проверка сформированности компетенций ПК-4, ПК-6

Задания:

1. Формирование требований по уровню защищенности.
2. Моделирование угроз безопасности .

Список литературы:

Приведён в п. 6 данной РПД

Материально-техническое обеспечение занятия: аудитория, оснащенная презентационной техникой (проектор, экран, компьютер/ноутбук). Компьютеры по количеству обучающихся с развёрнутой ОС MS Windows, виртуальной машиной, ППП MS Office v.2007 и выше

Практическое занятие 3 (6 ч.) «Проектирование DLP-систем» - проверка сформированности компетенций ПК-4, ПК-6

Задания:

1. Порядок разработки системы защиты DLP.
2. Оценка соответствия системы защиты.

Список литературы:

Приведён в п. 6 данной РПД

Материально-техническое обеспечение занятия: аудитория, оснащенная презентационной техникой (проектор, экран, компьютер/ноутбук). Компьютеры по количеству обучающихся с развёрнутой ОС MS Windows, виртуальной машиной, ППП MS Office v.2007 и выше.

Практическое занятие 4 (6 ч.) «Нормативно-правовые требования в области создания DLP-систем» - проверка сформированности компетенций ПК-4, ПК-6

Задания:

3. Порядок сертификации и процедура ввода в эксплуатацию
4. Умение поддерживать непрерывный цикл анализа защищенности

Список литературы:

Приведён в п. 6 данной РПД

Материально-техническое обеспечение занятия: аудитория, оснащенная презентационной техникой (проектор, экран, компьютер/ноутбук). Компьютеры по количеству обучающихся с развёрнутой ОС MS Windows, виртуальной машиной, ППП MS Office v.2007 и выше.

Приложение 1

АННОТАЦИЯ ДИСЦИПЛИНЫ

Дисциплина «Оценка безопасности программного обеспечения автоматизированных систем» реализуется на факультете Информационных систем и безопасности для студентов 4-го курса, обучающихся по программе бакалавриата по направлению подготовки 10.03.01 Информационная безопасность (профиль подготовки – Безопасность автоматизированных систем) кафедрой комплексной защиты информации.

Цель дисциплины – формирование систематизированных знаний о процессах разработки защищенных объектов информатизации и систем защиты информации на примере DLP-систем, применяемых при этом подходах, методиках и механизмах защиты информации, а также формирование у обучающихся умений и навыков, необходимых при непосредственном участии в указанных процессах.

Задачи дисциплины:

- сформировать знания о моделях и этапах жизненного цикла защищенных объектов информатизации и систем защиты информации, применяемых подходах и методах по обеспечению безопасности на каждом из этапов;
- сформировать представления об уязвимостях, присущих объектам информатизации, связанных с ними угрозами, а также навыки формирования моделей угроз безопасности и моделей потенциальных нарушителей;
- сформировать и развить компетенции, знания и практические навыки обеспечения технологической и эксплуатационной безопасности объектов информатизации.

Дисциплина направлена на формирование следующих компетенций:

- ПК-4 – Способен обеспечивать работоспособность систем защиты информации при возникновении нештатных ситуаций
- ПК-4.1 – Знает методы и способы обеспечения отказоустойчивости автоматизированных систем, содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и подсистем безопасности автоматизированных систем
- ПК-4.2 – Умеет применять типовые программные средства резервирования и восстановления информации, средства обеспечения отказоустойчивости в автоматизированных системах
- ПК-4.3 – Владеть: навыками обнаружения, устранения неисправностей в работе системы защиты информации, резервирования программного обеспечения, технических средств, каналов передачи данных в условиях нештатных ситуаций
- ПК-6 – Способен принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации
- ПК-6.1 – Знает оценки работоспособности применяемых средств защиты информации с использованием штатных средств и методик
- ПК-6.2 – Умеет оценить эффективности применяемых средств защиты информации с использованием штатных средств и методик
- ПК-6.3 – Владеет навыками определения уровня защищенности и доверия средств защиты информации

В результате освоения дисциплины обучающийся должен:

Знать: архитектуру подсистем безопасности, смысл базовых понятий, таких как идентификация и аутентификация, разграничение доступа и т.д.; методы и способы отказоустойчивости работы автоматизированных систем

Уметь: настраивать и эксплуатировать DLP-системы, составлять и реализовывать планы тестирующих мероприятий, моделировать и оценивать эффективность применяемых средств защиты.

Владеть: методами и инструментами анализа защищенности объектов информатизации с помощью DLP-систем.

По дисциплине предусмотрена промежуточная аттестация в форме зачета с оценкой.

Общая трудоёмкость освоения дисциплины составляет 2 зачётных единицы.

УТВЕРЖДЕНО
Протокол заседания кафедры
№ _____ от _____

ЛИСТ ИЗМЕНЕНИЙ

в рабочей программе дисциплины

Оценка безопасности программного обеспечения
автоматизированных систем

по направлению подготовки 10.03.01 Информационная безопасность

на 20__/20__ учебный год

1. В _____ вносятся следующие изменения:

(элемент рабочей программы)

1.1.;

1.2.;

...

1.9.

2. В _____ вносятся следующие изменения:

(элемент рабочей программы)

2.1.;

2.2.;

...

2.9.

3. В _____ вносятся следующие изменения:

(элемент рабочей программы)

3.1.;

3.2.;

...

3.9.

Составитель
дата

подпись

расшифровка подписи