

МИНОБРНАУКИ РОССИИ

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

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

БЕЗОПАСНОСТЬ ОПЕРАЦИОННЫХ СИСТЕМ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
*Направление подготовки 10.03.01 Информационная безопасность
Направленность (профиль) подготовки
№ 3 Комплексная защита объектов информатизации
Уровень квалификации выпускника – бакалавр*

Форма обучения – очная

РПД адаптирована для лиц
с ограниченными возможностями
здоровья и инвалидов

Москва 2017

Безопасность операционных 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

№ 6 от 24.01.2017 г.

ОГЛАВЛЕНИЕ

1. Пояснительная записка

1.1 Цель и задачи дисциплины

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

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 и инвалидов

9. Методические материалы

9.1. Планы лабораторных занятий

Приложения

Приложение 1. Аннотация дисциплины

Приложение 2. Лист изменений

1. Пояснительная записка

1.1. Цель и задачи дисциплины

Цель дисциплины: развить у слушателей подход к решению технических задач программно-аппаратной защиты информации.

Задачи: изучение встроенных механизмов безопасности ОС, освоение принципов использования программно-аппаратных средств защиты информации, выработка умений проведения оценки защищенности информационных систем .

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

Коды компетенции	Содержание компетенций	Перечень планируемых результатов обучения по дисциплине
ПК-3	должен обладать способностью администрировать подсистемы информационной безопасности объекта защиты	<p>Знать место средств защиты информации в современных ОС, принципы реализации механизмов идентификации и аутентификации субъектов доступа в ОС, принципы разграничения доступа к объектам в ОС, принципы организации регистрации событий безопасности в ОС.</p> <p>Уметь определять источники и угрозы информационной безопасности в ОС, разрабатывать меры по защите от идентифицированных угроз;</p> <p>выбирать, устанавливать и настраивать средства защиты информации ОС, принимать участие в разработке политики безопасности.</p> <p>Владеть профессиональной терминологией, навыками настройки и эксплуатации встроенных средств защиты информации ОС.</p>
ПК-6	должен обладать способностью принимать участие в проведении проверок работоспособности и эффективности средств защиты информации	<p>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.</p> <p>Уметь составлять и реализовывать планы тестирующих мероприятий, имитировать внешние и внутренние атаки нарушения системы безопасности.</p> <p>Владеть навыками эксплуатации и тестирования программно-аппаратных, криптографических и технических средств защиты информации.</p>

1.3. Место дисциплины в структуре образовательной программы

Дисциплина «Безопасность операционных систем» относится к вариативной части блока дисциплин учебного плана.

Для освоения дисциплины необходимы компетенции, сформированные в ходе изучения следующих дисциплин: «Теория вероятностей и математическая статистика», «Дискретная математика», «Технология и методы программирования», «Информационные технологии».

В результате освоения дисциплины формируются компетенции, необходимые для изучения следующих и прохождения практик: «Комплексное обеспечение безопасности объекта информатизации», «Безопасность критически важных систем», «Проектирование систем защиты объектов информатизации»

2. Структура дисциплины

Структура дисциплины для очной формы обучения

Общая трудоёмкость дисциплины составляет 3 з.е., 108 ч., в том числе контактная работа обучающихся с преподавателем 42 ч., промежуточная аттестация 18 ч., самостоятельная работа обучающихся 48 ч.

№ п/п	Раздел дисциплины/темы	Семестр	Виды учебной работы (в часах)						Формы текущего контроля успеваемости, форма промежуточной аттестации (по семестрам)
			контактная					Самостоятельная работа	
			Лекции	Семинар	Практические занятия	Лабораторные занятия	Промежуточная аттестация		
1	Общая архитектура ОС	4	2					10	Опрос.
2	Место сервисов безопасности в ОС	4	4			4		10	Опрос. Защита лабораторных работ.
3	Управление учетными записями, идентификация и аутентификация в ОС	4	4			6		10	Опрос. Защита лабораторных работ.
4	Управление доступом к объектам файловой системы	4	6			4		10	Опрос. Защита лабораторных работ.
5	Работа с терминалом	4	6			6		8	Опрос. Защита лабораторных работ.
	Экзамен	4					18		Экзамен по билетам
	ИТОГО:		22			20	18	48	

3. Содержание дисциплины

№	Наименование раздела дисциплины	Содержание
1	Общая архитектура ОС	Проблема защиты программного обеспечения автоматизированных систем. Объекты защиты. Защита программного обеспечения как система научных дисциплин. Модели угроз безопасности программного обеспечения и ОС. Основные принципы обеспечения безопасности программного обеспечения и ОС.
2	Место сервисов безопасности в ОС	Базовые научные положения и основания теории защиты программ. Понятие Сервиса безопасности.
3	Управление учетными записями, идентификация и аутентификация в ОС	Управление учетными записями и механизмы аутентификации в ОС. Идентификация и аутентификация в домене Active Directory. Процедуры идентичны простой локальной идентификации и аутентификации, но в данном случае, при регистрации в домене, обмен данными между рабочей станцией и сервером происходит по протоколу Kerberos v5 rev6 (более надежный за счет обоюдной аутентификации, более быстрое соединение и др.).
4	Управление доступом к объектам файловой системы	Система контроля доступа состоит из участника безопасности (пользователи, группы пользователей, службы, компьютеры), маркера доступа, объектов доступа, дескрипторов безопасности и алгоритма проверки прав. Дескрипторы безопасности - это список запретов и разрешений (Discretionary Access Control List, DACL), установленных для данного объекта, список назначений аудита (System Access Control List, SACL) и назначение прав для каждого конкретного SID (Access Control Entry, ACE, при этом список назначений аудита объекта Active Directory может содержать строки ACE, назначенные отдельным атрибутам). Регистрация событий и журналы безопасности.
5	Работа с терминалом	Эффективная профессиональная работа в Linux немислима без использования командной строки. Пользователям, привыкшим работать в системах с графическим интерфейсом, работа с командной строкой может показаться неудобной: то, что можно сделать одним перетаскиванием мышью в командной строке потребует ввода с клавиатуры нескольких слов: команды с ар-

		<p>гументами. Однако в Linux этот вид интерфейса всегда был основным, а поэтому и хорошо развитым. В командных оболочках, используемых в Linux, есть масса способов экономии усилий (нажатий на клавиши) при выполнении наиболее распространённых действий: автоматическое дополнение длинных названий команд или имён файлов, поиск и повторное выполнение команды, уже когда-то исполнявшейся раньше, подстановка списков имён файлов по некоторому шаблону и многое другое. Преимущества командной строки становятся особенно очевидны, когда требуется выполнять однотипные операции над множеством объектов. В системе с графическим интерфейсом потребуется столько перетаскиваний мышью, сколько есть объектов, в командной строке будет достаточно одной команды.</p>
--	--	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

4. Образовательные технологии

№ п/п	Наименование раздела	Виды учебных занятий	Образовательные технологии
1	2	3	4
1.	Общая архитектура ОС	Лекция 1.1 Самостоятельная работа	Традиционная с использованием презентаций Изучение материалов лекций
2	Место сервисов безопасности в ОС	Лекция 2.1 Лекция 2.2 Лабораторное занятие 1. Самостоятельная работа	Традиционная с использованием презентаций Изучение материалов лекций
3	Управление учетными записями, идентификация и аутентификация в ОС	Лекция 3.1 Лекция 3.2 Лабораторное занятие 2. Самостоятельная работа	Традиционная с использованием презентаций Изучение материалов лекций
4	Управление доступом к объектам файловой системы	Лекция 4.1 Лекция 4.2 Лекция 4.3 Лабораторное занятие 3. Самостоятельная работа	Традиционная с использованием презентаций Выполнение задания Изучение материалов лекций
5	Работа с терминалом	Лекция 5.1 Лекция 5.2 Лекция 5.3	Традиционная с использованием презентаций

		Лабораторное занятие 4. Самостоятельная работа	Выполнение задания Изучение материалов лекций
--	--	---------------------------------------------------	--------------------------------------------------

5. Оценка планируемых результатов обучения

5.1. Система оценивания

Форма контроля	Макс. количество баллов	
	За одну работу	Всего
Текущий контроль:		
– опрос (темы 1-6)	5 баллов	30 баллов
– лабораторные задания (темы 3)	6 баллов	6 баллов
– лабораторные задания (темы 4-6)	7 баллов	24 балла
Промежуточная аттестация экзамен		40 баллов
Итого за дисциплину экзамен		100 баллов

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 шка- ла	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 дис- циплине	Критерии оценки результатов обучения по дисци- плине
100-83/ A,B	«отлично»/ «зачтено (отлич- но)»/ «зачтено»	Выставляется обучающемуся, если он глубоко и проч- но усвоил теоретический и практический материал, может продемонстрировать это на занятиях и в ходе промежуточной аттестации. Обучающийся исчерпывающе и логически стройно из- лагает учебный материал, умеет увязывать теорию с практикой, справляется с решением задач профессио- нальной направленности высокого уровня сложности, правильно обосновывает принятые решения. Свободно ориентируется в учебной и профессиональ- ной литературе.

Баллы/ Шкала ECTS	Оценка по дисциплине	Критерии оценки результатов обучения по дисциплине
		<p>Оценка по дисциплине выставляются 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 выставляются 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 выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации.</p> <p>Компетенции, закреплённые за дисциплиной, сформированы на уровне – «достаточный».</p>
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 выставляются обучающемуся с</p>

Баллы/ Шкала ECTS	Оценка по дисциплине	Критерии оценки результатов обучения по дисциплине
		учёт результатов текущей и промежуточной аттестации. Компетенции на уровне «достаточный», закреплённые за дисциплиной, не сформированы.

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

Примерные контрольные вопросы для экзамена - проверка сформированности компетенций ПК-3, ПК-6

1. Тактика действия злоумышленника и обманные системы защиты.
2. Администрирование ОС.
3. Аудит безопасности.
4. Защита от НСД в современных ОС.
5. Виды политик безопасности.
6. Аккредитация испытательных лабораторий и органов по сертификации средств защиты информации по требованию безопасности информации. Порядок аккредитации.
7. Контроль целостности исполняемой среды.
8. Заявители и их функции. Заявка на проведение аттестации ОИ.
9. Порядок проведения аттестации объектов информатизации. Содержание заявок.
10. Порядок взаимодействия заявителя и органа по проведению аттестации.
11. Основные тенденции в области защиты информации.
12. Анализаторы трафика в современном мире.
13. Понятия идентификации и аутентификации.
14. Использование «облачных» технологий при реализации механизмов безопасности и многоагентные системы.
15. Защита виртуальной среды ОС с использованием гипервизора.
16. Преимущества аппаратной виртуализации.
17. Мобильные агенты и их использование.
18. Интеллектуальные системы предупреждения вторжений.
19. Штатные средства защиты ОС Windows.
20. Современные СЗИ. Примеры использования.
21. Антивирусы как средство защиты от вредоносного ПО.
22. Средства шифрования дисков.
23. Вредоносное ПО и методы противодействия.
24. Понятие скрытый канал.
25. Виды шифрования в современных ОС.
26. Аттестация СВТ.
27. Парольная защита и хэш-функции.
28. Методы перехвата информации и технология противодействия ССИБ.
29. Перспективные направления развития высокоскоростных сетей и их защиты.
30. Виды атак при реализации эксклюзивных алгоритмов атак.
31. Основные разработчики пакетов для квантовых вычислений.
32. Проблема защиты программного обеспечения автоматизированных систем.
33. Защита программного обеспечения как система научных дисциплин.
34. Угрозы безопасности программного обеспечения.
34. Технологическая и эксплуатационная безопасность программного обеспечения.
35. Модели угроз безопасности программного обеспечения.
36. Основные принципы обеспечения безопасности программного обеспечения.

37. Методы анализа безопасности программного обеспечения.
38. Методы защиты программ от компьютерных вирусов.
39. Аутентификация и идентификация. Протокол LDAP.
40. Системы аудиты.
41. Штатные средства защиты ОС Linux.
42. Понятие кольца защиты ОС.
43. Механизмы доменной защиты.
44. Архитектура ОС.
45. Доверенная загрузка и контроль BIOS.
46. Примеры операционных систем в защищенном исполнении.
47. Мониторинг процессов ОС.
48. Электронные ключи. Принципы работы.
49. Идентификация и аутентификация в домене Active Directory.
50. Протокол LDAP.
51. Принципы работы Kerberos,
52. Мультидоменный гипервизор.
53. ОС 2000. Особенности работы планировщика и принципов защиты.
54. ОС «Феникс». Особенности доменной защиты.
55. UAC – Контроль учетных записей в ОС Windows.
56. IPSec. Описание протокола и применение.

Примерные задания для тестирования- проверка сформированности компетенций ПК-3, ПК-6

1. Что такое ААА:

- а) аутентификация, авторизация, аудит.
- б) аудит безопасности.
- в) расследование инцидентов ИБ.

2. Winlogon – это:

- а) Логотип ОС Windows.
- б) Компонент ОС Windows, ответственный за идентификацию/аутентификацию пользователей.
- в) Сервис печати.

6. Учебно-методическое и информационное обеспечение дисциплины

6.1. Список источников и литературы

Источники

Основные

1. *Федеральный закон* от 27 июля 2006 г. №149-ФЗ «Об информации, информационных технологиях и о защите информации» [Электронный ресурс] : Режим доступа : http://www.consultant.ru/document/cons_doc_LAW_61798/, свободный. – Загл. с экрана.
2. *Федеральный закон* от 27 июля 2006 г. №152-ФЗ «О персональных данных» [Электронный ресурс] : Режим доступа : http://www.consultant.ru/document/cons_doc_LAW_61801/, свободный. – Загл. с экрана.
3. *Федеральный закон* от 6 апреля 2011 г. №63-ФЗ «Об электронной подписи» [Электронный ресурс] : Режим доступа : http://www.consultant.ru/document/cons_doc_LAW_112701/, свободный. – Загл. с экрана.
4. *Федеральный закон* от 27 декабря 2002 г. №184-ФЗ «О техническом регулировании» [Электронный ресурс] : Режим доступа : http://www.consultant.ru/document/cons_doc_LAW_40241/, свободный. – Загл. с экрана.

Литература

Основная

1. *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>
2. *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 Microsoft [Электронный ресурс] : Режим доступа: <http://www.microsoft.com/>, свободный. – Загл. с экрана.
2. Центр разработки Microsoft [Электронный ресурс] : Режим доступа: <http://www.msdn.microsoft.com/>, свободный. – Загл. с экрана.

7. Материально-техническое обеспечение дисциплины

Для проведения занятий необходимо следующее материально-техническое обеспечение:

1) лекционный класс с видеопроектором и компьютером, на котором должны быть установлены:

- лицензионное ПО MS Windows 7 и старше;
- лицензионное ПО MS Office 2010 (с обязательным наличием MS PowerPoint) и старше

2) компьютерный класс, оборудованный современными персональными компьютерами для каждого студента с выходом в интернет. На компьютере должны быть установлены:

- лицензионное ПО MS Windows 7 и старше;
- лицензионное ПО MS Office 2010 и старше;
- программный гипервизор VMware Player;

Перечень 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 + Гостевая ОС CentOS 7	VMWare	Свободное ПО, Режим доступа: https://www.vmware.com/products/ Демо-версия Открытое ПО Режим доступа: https://www.centos.org/download/ Инсталляционный дистрибутив Linux

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

Перечень БД и ИСС

№п /п	Наименование
1	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 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 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 лабораторных занятий - проверка сформированности компетенций ПК-3, ПК-6

Темы учебной дисциплины предусматривают проведение лабораторных работ, которые служат как целям текущего и промежуточного контроля за подготовкой студентов, так и целям получения практических навыков применения методов выработки решений, закрепления изученного материала, развития умений, приобретения опыта решения конкретных проблем, ведения дискуссий, аргументации и защиты выбранного решения. Помощь в этом оказывают задания для лабораторных работ, выдаваемые преподавателем на каждом занятии, задания на самостоятельную подготовку, перечень вопросов для подготовки к экзамену и контрольные домашние задания для самостоятельной работы студентов.

Целью лабораторных работ является закрепление теоретического материала и приобретение практических навыков использования методов применения пакетов компьютерной математики в профессиональной деятельности, применять навыки для принятия наиболее эффективных решений в условиях быстро меняющейся реальности, для быстрой адаптации к изменяющимся условиям деятельности.

Тематика лабораторных работ соответствует программе курса.

Лабораторное занятие 1(4ч.). Основные сервисы безопасности ОС (проверка сформированности компетенций ПК-3)

Цель работы: получение практических навыков в эксплуатации штатных средств защиты ОС.

Указания по выполнению задания: обратить внимание на свойства защищенности программ на этапах производства, поставки и эксплуатации программных комплексов.

Выполнение задания:

В ходе лабораторной работы студенты на практике знакомятся с сервисами безопасности, предоставляемые ОС Windows и Linux. Обучаются настраивать профили защиты, добавлять и блокировать учетные записи.

Список литературы:

Приведён в п. 6 данной РПД

Материально-техническое обеспечение лабораторного занятия: аудитория, оснащенная презентационной техникой (проектор, экран, компьютер/ноутбук). Компьютеры по количеству обучающихся с развёрнутой ОС MS Windows, виртуальной машиной VMPlayer с гостевой ОС VMPlayer с гостевой ОС CentOS 7. Занятия проводятся в специально оборудованном компьютерном классе.

Лабораторное занятие 2(6 ч.). Идентификация и аутентификация в ОС (проверка сформированности компетенций ПК-6)

Цель работы: получение практических навыков в эксплуатации подсистем разграничения доступа в современных ОС.

Указания по выполнению задания: обратить внимание на оценку криптостойкости функций хеширования паролей.

Выполнение задания:

В ходе лабораторной работы студенты на практике знакомятся с механизмами идентификации и аутентификации ОС Windows и Linux.

Список литературы:

Приведён в п. 6 данной РПД

Материально-техническое обеспечение лабораторного занятия: аудитория, оснащенная презентационной техникой (проектор, экран, компьютер/ноутбук). Компьютеры по количеству обучающихся с развёрнутой ОС MS Windows, виртуальной машиной VMPlayer с гостевой ОС VMPlayer с гостевой ОС CentOS 7. Занятия проводятся в специально оборудованном компьютерном классе.

Лабораторное занятие 3(4 ч.). Регистрация событий и анализ журналов безопасности (проверка сформированности компетенций ПК-6)

Цель работы: получение практических навыков в исследовании несанкционированного доступа и своевременного предупреждения.

Указания по выполнению задания: обратить внимание на режимы записи информации в журналах безопасности ОС Linux и Windows.

Выполнение задания:

В ходе работы имитируется процесс, осуществляющий несанкционированный доступ к ресурсам ОС. Задача студентам, как будущим администраторам СЗИ, своевременно анализировать и выявлять подобные угрозы.

Список литературы:

Приведён в п. 6 данной РПД

Материально-техническое обеспечение лабораторного занятия: аудитория, оснащенная презентационной техникой (проектор, экран, компьютер/ноутбук). Компьютеры по количеству обучающихся с развёрнутой ОС MS Windows, виртуальной машиной VMPlayer с гостевой ОС CentOS 7. Занятия проводятся в специально оборудованном компьютерном классе.

Лабораторное занятие 4(6 ч.). Работа с командной строкой Linux (проверка сформированности компетенций ПК-3, ПК-6)

Цель работы: получение практических навыков в эксплуатации современных ОС.

Указания по выполнению задания: обратить внимание на требование комплексного похода для защиты СВТ.

Выполнение задания:

В ходе работы студенты на практике знакомятся с командной строкой Linux.

Список литературы:

Приведён в п. 6 данной РПД

Материально-техническое обеспечение лабораторного занятия: аудитория, оснащенная презентационной техникой (проектор, экран, компьютер/ноутбук). Компьютеры по количеству обучающихся с развёрнутой ОС MS Windows, виртуальной машиной VMPlayer с гостевой ОС CentOS 7. Занятия проводятся в специально оборудованном компьютерном классе.

АННОТАЦИЯ ДИСЦИПЛИНЫ

Дисциплина «Безопасность операционных систем» реализуется на факультете Информационных систем и безопасности для студентов 2-го курса, обучающихся по программе бакалавриата по направлению подготовки 10.03.01 Информационная безопасность (профили подготовки – № 3 Комплексная защита объектов информатизации) кафедрой комплексной защиты информации.

Цель дисциплины: научить студентов использовать для решения профессиональных задач современные средства программно-аппаратной защиты информации.

Задачи: формирование у студентов представлений о механизмах защиты ОС, выработка умений настраивать функций безопасности ОС, научить студентов использовать встроенные средства защиты информации ОС.

Дисциплина направлена на формирование следующих компетенций:

- ПК-3 – должен обладать способностью администрировать подсистемы информационной безопасности объекта защиты
- ПК-6 – должен обладать способностью принимать участие в проведении проверок работоспособности и эффективности средств защиты информации.

В результате освоения дисциплины обучающийся должен:

Знать место средств защиты информации в современных ОС, принципы реализации механизмов идентификации и аутентификации субъектов доступа в ОС, принципы разграничения доступа к объектам в ОС, принципы организации регистрации событий безопасности в ОС.

Уметь определять источники и угрозы информационной безопасности в ОС, разрабатывать меры по защите от идентифицированных угроз, выбирать, устанавливать и настраивать средства защиты информации ОС, принимать участие в разработке политики безопасности; составлять и реализовывать планы тестирующих мероприятий, имитировать внешние и внутренние атаки нарушения системы безопасности.

Владеть профессиональной терминологией, навыками настройки и эксплуатации встроенных средств защиты информации ОС; навыками эксплуатации и тестирования программно-аппаратных, криптографических и технических средств защиты информации. По дисциплине предусмотрена промежуточная аттестация в форме экзамена. Общая трудоёмкость освоения дисциплины составляет 3 зачётные единицы.

ЛИСТ ИЗМЕНЕНИЙ

№	Текст актуализации или прилагаемый к РПД документ, содержащий изменения	Дата	№ протокола
1	<i>Обновлен состав программного обеспечения (ПО), современных профессиональных баз данных (БД) и информационно-справочные систем (ИСС)</i>	29.06.2017г.	10
2	<i>Обновлен состав программного обеспечения (ПО), современных профессиональных баз данных (БД) и информационно-справочные систем (ИСС)</i>	26.06.2018г.	11
3	<i>Обновлен состав программного обеспечения (ПО), современных профессиональных баз данных (БД) и информационно-справочные систем (ИСС)</i>	29.08.2019 г.	1
4	<i>Обновлена структура дисциплины (модуля) для очной формы обучения (2020 г.)</i>	23.06.2020	14
5	<i>Обновлена основная и дополнительная литература</i>	23.06.2020	14
6	<i>Обновлен раздел п.4 Образовательные технологии</i>	23.06.2020	14
7	<i>Обновлен состав программного обеспечения (ПО), современных профессиональных баз данных (БД) и информационно-справочные систем (ИСС)</i>	23.06.2020	14

1. Состав программного обеспечения (ПО), современных профессиональных баз данных (БД) и информационно-справочных систем (ИСС) (2017 г.)**Перечень ПО***Таблица 1*

№п/п	Наименование ПО	Производитель	Способ распространения (лицензионное или свободно распространяемое)
1	MicrosoftOffice 2013	Microsoft	лицензионное
2	Windows XP	Microsoft	лицензионное
3	KasperskyEndpointSecurity	Kaspersky	лицензионное
4	ОС «Альт Образование» 8	ООО «Базальт СПО	лицензионное

Перечень БД и ИСС*Таблица 2*

№п/п	Наименование
	Международные реферативные наукометрические БД, доступные в рамках национальной подписки в 2017 г. Web of Science Scopus
	Профессиональные полнотекстовые БД, доступные в рамках национальной подписки в 2017 г. Журналы Oxford University Press
	Компьютерные справочные правовые системы Консультант Плюс, Гарант

Составитель: К.т.н, доцент, А.С. Моляков

2. Состав программного обеспечения (ПО), современных профессиональных баз данных (БД) и информационно-справочных систем (ИСС) (2018 г.)**Перечень ПО**

Таблица 1

№п/п	Наименование ПО	Производитель	Способ распространения (лицензионное или свободно- распространяемое)
1	Adobe Master Collection CS4	Adobe	лицензионное
2	Microsoft Office 2010	Microsoft	лицензионное
3	Windows 7 Pro	Microsoft	лицензионное
4	AutoCAD 2010 Student	Autodesk	свободно распространяемое
5	Archicad 21 Rus Student	Graphisoft	свободно распространяемое
6	SPSS Statistics 22	IBM	лицензионное
7	Microsoft Share Point 2010	Microsoft	лицензионное
8	SPSS Statistics 25	IBM	лицензионное
9	Microsoft Office 2013	Microsoft	лицензионное
10	ОС «Альт Образование» 8	ООО «Базальт СПО	лицензионное
11	Microsoft Office 2013	Microsoft	лицензионное
12	Windows 10 Pro	Microsoft	лицензионное
13	Kaspersky Endpoint Security	Kaspersky	лицензионное

Перечень БД и ИСС

Таблица 2

№п/п	Наименование
	Международные реферативные наукометрические БД, доступные в рамках национальной подписки в 2018 г. Web of Science Scopus
	Профессиональные полнотекстовые БД, доступные в рамках национальной подписки в 2018 г. Журналы Cambridge University Press ProQuest Dissertation & Theses Global SAGE Journals Журналы Taylor and Francis Электронные издания издательства Springer
	Профессиональные полнотекстовые БД JSTOR Издания по общественным и гуманитарным наукам
	Компьютерные справочные правовые системы Консультант Плюс, Гарант

Составитель: К.т.н, доцент, А.С. Моляков

3. Состав программного обеспечения (ПО), современных профессиональных баз данных (БД) и информационно-справочных систем (ИСС) (2019 г.)

Перечень ПО

№п /п	Наименование ПО	Производитель	Способ распространения (лицензионное или свободно распространяемое)
1	Adobe Master Collection CS4	Adobe	лицензионное
2	Microsoft Office 2010	Microsoft	лицензионное
3	Windows 7 Pro	Microsoft	лицензионное
4	AutoCAD 2010 Student	Autodesk	свободно распространяемое
5	Archicad 21 Rus Student	Graphisoft	свободно распространяемое
6	SPSS Statistics 22	IBM	лицензионное
7	Microsoft Share Point 2010	Microsoft	лицензионное
8	SPSS Statistics 25	IBM	лицензионное
9	Microsoft Office 2013	Microsoft	лицензионное
10	ОС «Альт Образование» 8	ООО «Базальт СПО	лицензионное
11	Microsoft Office 2013	Microsoft	лицензионное
12	Windows 10 Pro	Microsoft	лицензионное
13	Kaspersky Endpoint Security	Kaspersky	лицензионное
14	Microsoft Office 2016	Microsoft	лицензионное
15	Visual Studio 2019	Microsoft	лицензионное
16	Adobe Creative Cloud	Adobe	лицензионное

Перечень БД и ИСС

№п /п	Наименование
1	Международные реферативные наукометрические БД, доступные в рамках национальной подписки в 2019 г. Web of Science Scopus
2	Профессиональные полнотекстовые БД, доступные в рамках национальной подписки в 2019 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

Составитель: К.т.н, доцент, А.С. Моляков

4. Обновление структуры дисциплины (модуля) для очной формы обучения (2020 г.)**Структура дисциплины (модуля) для очной формы обучения**

Общая трудоемкость дисциплины составляет 3 з. е., 114 ч., в том числе контактная работа обучающихся с преподавателем 42 ч., самостоятельная работа обучающихся 54 ч.

№ п/п	Раздел дисциплины/темы	Семестр	Виды учебной работы (в часах)						Формы текущего контроля успеваемости, форма промежуточной аттестации (по семестрам)
			контактная					Самостоятельная работа	
			Лекции	Семинар	Практические занятия	Лабораторные занятия	Промежуточная аттестация		
1	Общая архитектура ОС	4	2			4		10	Опрос. Защита лабораторных работ.
2	Место сервисов безопасности в ОС	4	4			6		10	Опрос. Защита лабораторных работ.
3	Управление учетными записями, идентификация и аутентификация в ОС	4	4			4		15	Опрос. Защита лабораторных работ.
4	Управление доступом к объектам файловой системы	4	6			6		13	Опрос. Защита лабораторных работ.
5	Регистрация событий безопасности	4	6					6	Опрос
	Экзамен	4					18		Экзамен по билетам
	итоги:		22			20	18	54	

5. Обновление основной и дополнительной литературы (2020 г.)

В раздел 6. Учебно-методическое и информационное обеспечение дисциплины вносятся следующие изменения:

2. Дополнить раздел Основная литература

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>

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>

2. Дополнить раздел **Дополнительная литература**

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>

Гостев, И. М. Операционные системы : учебник и практикум для вузов / И. М. Гостев. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2020. — 164 с. — (Высшее образование). — ISBN 978-5-534-04520-8. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: <https://urait.ru/bcode/451231>

6. В элемент рабочей программы **п.4 Образовательные технологии** вносятся следующие изменения:

В период временного приостановления посещения обучающимися помещений и территории РГГУ. для организации учебного процесса с применением электронного обучения и дистанционных образовательных технологий могут быть использованы следующие образовательные технологии:

- видео-лекции;
- онлайн-лекции в режиме реального времени;
- электронные учебники, учебные пособия, научные издания в электронном виде и доступ к иным электронным образовательным ресурсам;
- системы для электронного тестирования;
- консультации с использованием телекоммуникационных средств.

7. В элемент рабочей программы **7. Материально-техническое обеспечение дисциплины/модуля** вносятся следующие изменения:

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

В элемент рабочей программы **7. Материально-техническое обеспечение дисциплины/модуля** вносятся следующие изменения:

Состав программного обеспечения (ПО)

№п /п	Наименование ПО	Производитель	Способ распространения (<i>лицензионное или свободно распространяемое</i>)
1	Adobe Master Collection CS4	Adobe	лицензионное
2	Microsoft Office 2010	Microsoft	лицензионное
3	Windows 7 Pro	Microsoft	лицензионное
4	AutoCAD 2010 Student	Autodesk	свободно распространяемое
5	Archicad 21 Rus Student	Graphisoft	свободно распространяемое
6	SPSS Statistics 22	IBM	лицензионное
7	Microsoft Share Point 2010	Microsoft	лицензионное
8	SPSS Statistics 25	IBM	лицензионное
9	Microsoft Office 2013	Microsoft	лицензионное
10	ОС «Альт Образование» 8	ООО «Базальт СПО	лицензионное
11	Microsoft Office 2013	Microsoft	лицензионное
12	Windows 10 Pro	Microsoft	лицензионное
13	Kaspersky Endpoint Security	Kaspersky	лицензионное
14	Microsoft Office 2016	Microsoft	лицензионное
15	Visual Studio 2019	Microsoft	лицензионное
16	Adobe Creative Cloud	Adobe	лицензионное
17	Zoom	Zoom	лицензионное

Составитель:

К.т.н, доцент, А.С. Моляков