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 И ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Направление подготовки 10.03.01 Информационная безопасность
Направленность (профиль) подготовки
№ 2 Организация и технология защиты информации
Уровень квалификации выпускника – бакалавр

Форма обучения – очная

РПД адаптирована для лиц
с ограниченными возможностями
здоровья и инвалидов

Москва *2017*

Безопасность операционных систем и программного обеспечения
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

Цель дисциплины: приобретение знаний о базовых методах и способах защиты программного обеспечения (ПО) автоматизированных систем и умений применять на практике средства защиты программ, имеющиеся на отечественном рынке продукции и услуг в области защиты информации от несанкционированного доступа, научить студентов использовать для решения профессиональных задач современные средства программно-аппаратной защиты информации ОС.

Задачи дисциплины: приобретение знаний о базовых методах и способах защиты ПО автоматизированных систем и умений применять на практике средства защиты программ, имеющиеся на отечественном рынке продукции и услуг в области защиты информации от несанкционированного доступа, формирование у студентов представлений о механизмах защиты ОС, выработка умений настраивать функций безопасности ОС.

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	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. Владеть профессиональной терминологией; навыками настройки и эксплуатации встроенных средствах защиты информации ОС.
ПК-6	должен обладать способностью принимать участие в проведении проверок работоспособности и эффективности средств защиты информации	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. Уметь составлять и реализовывать планы тестирующих мероприятий, имитировать внешние и внутренние атаки нарушения системы безопасности.

Владеть навыками эксплуатации и тестирования программно-аппаратных, криптографических и технических средств
защиты информации

1.3. Место дисциплины в структуре образовательной программы

Дисциплина «Безопасность операционных систем и операционного обеспечения» 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., самостоятельная работа обучающихся 48 ч., промежуточная аттестация – 18 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	*Введение в теорию и практику защиты программного обеспечения и Общая архитектура ОС*	**6**	**2**					**10**	Опрос
2	*Основные положения, понятия и определения, используемые при защите программного обеспечения и Место сервисов безопасности в ОС*	**6**	**4**			**6**		**10**	Опрос. Защита лабораторных работ.
3	*Методы обеспечения технологической и эксплуатационной*	**6**	**4**			**6**		**20**	Опрос. Защита лабораторных работ.

	безопасности программного обеспечения и Управление учетными записями в ОС								
4	*Средства и системы защиты программного обеспечения. Управление доступом к объектам файловой системы*	**6**	**6**			**6**		**10**	Опрос. Защита лабораторных работ.
5	*Отечественные нормативные акты, регламентирующие деятельность в области защиты программного обеспечения*	**6**	**4**			**4**		**16**	Опрос. Защита лабораторных работ.
	Экзамен	**6**					**18**		*Экзамен по билетам*
	итого:		**20**			**22**	**18**	**48**	

3. Содержание дисциплины

№	Наименование раздела дисциплины	Содержание
1	**Введение в теорию и практику защиты программного обеспечения и Общая архитектура ОС**	Проблема защиты программного обеспечения автоматизированных систем. Объекты защиты. Системное и общесистемное программное обеспечение. Специальное программное обеспечение. Прикладное программное обеспечение. Языки, системы и оболочки программирования, инструментальные средства автоматизации программирования. Защита программного обеспечения как система научных дисциплин. Угрозы безопасности программного обеспечения. Принятая аксиоматика и терминология. Жизненный цикл программного обеспечения автоматизированных систем. Технологическая и эксплуатационная безопасность программного обеспечения. 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	**Методы обеспечения технологической и эксплуатационной безопасности программного обеспечения и Управление учетными записями ОС**	Модели и методы разработки безопасного ПО, принципы верификации. 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	**Средства и системы защиты программного обеспечения. Управление доступом к объектам файловой системы.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.
	Отечественные нормативные акты . Работа с терминалом устройств	Федеральный закон «Об информации, информационных технологиях и о защите информации». ГОСТ Р ИСО/МЭК 12207-2010. ГОСТ Р ИСО/МЭК 15408-2002. ГОСТ Р МЭК 61508-2007. Руководящий документ ФСТЭК России. Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля недекларированных возможностей. Эффективная профессиональная работа в `Linux` немыслима 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 аргументами. В командных оболочках, используемых в `Linux`, есть масса способов экономии усилий (нажатий на клавиши) при выполнении наиболее распространённых действий: 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.

4. Образовательные технологии

№ п/п	Наименование раздела	Виды учебных занятий	Образовательные технологии
1	**2**	**3**	**4**
1.	*Введение в теорию и практику защиты программного обеспечения и 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	*Методы обеспечения технологической и эксплуатационной безопасности программного обеспечения и Управление учетными записями ОС*	*Лекция 3.1* *Лекция 3.2* *Лабораторное занятие 2.* *Самостоятельная работа*	*Традиционная с использованием презентаций* *Изучение материалов лекций*
4	*Средства и системы защиты программного обеспечения. 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	*Отечественные нормативные акты . Работа с терминалом устройств*	*Лекция 5.1* *Лекция 5.2* *Лабораторное занятие 4.* *Самостоятельная работа*	*Традиционная с использованием презентаций* *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)* *– практическое задание (темы 3)* *– практическое задание (темы 4-6)*	 *5 баллов* *6 баллов* *7 баллов*	 *30 баллов* *6 баллов* *24 балла*
Промежуточная аттестация *зачёт*		*40 баллов*

Итого за дисциплину *зачёт*		*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 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/ A,B	«отлично»/ «зачтено (отлично)»/ «зачтено»	Выставляется обучающемуся, если он глубоко и прочно усвоил теоретический и практический материал, может продемонстрировать это на занятиях и в ходе промежуточной аттестации. 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. Свободно ориентируется в учебной и профессиональной литературе. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «высокий».
82-68/ C	«хорошо»/ «зачтено (хорошо)»/ «зачтено»	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. Обучающийся правильно применяет теоретические положения при решении практических задач профессиональной направленности разного уровня сложности, владеет необходимыми для этого навыками и приёмами. Достаточно хорошо ориентируется в учебной и профессиональной литературе. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной атте-

Баллы/ Шкала ECTS	**Оценка по дисциплине**	**Критерии оценки результатов обучения по дисциплине**
		стации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «хороший».
67-50/ D,E	«удовлетворительно»/ «зачтено (удовлетворительно)»/ «зачтено»	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. 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. Демонстрирует достаточный уровень знания учебной литературы по дисциплине. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «достаточный».
49-0/ F,FX	«неудовлетворительно»/ не зачтено	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. 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. Демонстрирует фрагментарные знания учебной литературы по дисциплине. Оценка по дисциплине выставляются обучающемуся с учётом 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

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

1. Наиболее вероятный объект воздействия в АС? Дайте определения «защищенности ПО АС» и «уровня безопасности ПО». Технологическая и эксплуатационная безопасность ПО.

2. Объекты защиты. Системное и общесистемное ПО. ПО промежуточного слоя. Специальное и прикладное ПО. Языки, системы и оболочки программирования. Защита программного обеспечения как система научных дисциплин.
3. Угрозы и модели угроз безопасности ПО. Основные принципы обеспечения безопасности программного обеспечения.
4. Модели вычислений: Машина Тьюринга, машина Поста, RAM-машина, РАСП-машина и их разновидности. Схемы. Булевы схемы. Процессоры и сети процессоров.
5. Символ О-большое и Омега-большое. Вычислимые функции и разрешимые предикаты. Сложность и классы вычислений. Односторонние функции и функции с секретом. Псевдослучайные генераторы.
6. Криптосистемы с секретным и открытым ключом. Схемы электронной подписи. Схемы хеширования. Схемы построения псевдослучайных генераторов. Схемы вероятностного шифрования. Конфиденциальные вычисления.
7. Методы анализа безопасности программного обеспечения. Контрольно-испытательные методы анализа безопасности программного обеспечения. Логико-аналитические методы контроля безопасности программ. Сравнение логико-аналитических и контрольно-испытательных методов анализа безопасности программ.
8. Методы защиты разрабатываемых программ от автоматической генерации инструментальными средствами ПССИВ. Способы внедрения ПССИВ посредством инструментальных средств. Возможные методы защиты программ от потенциально опасных инструментальных средств.
9. Методы идентификации программ и их характеристик. Идентификация программ по внутренним характеристикам. Способы оценки подобия целевой и исследуемой программ с точки зрения наличия программных дефектов.
10. Методы защиты программ от компьютерных вирусов. Общая характеристика и классификация компьютерных вирусов. Общая характеристика средств нейтрализации компьютерных вирусов. Классификация методов защиты от компьютерных вирусов.
11. Методы защиты программ от исследования. Классификация средств исследования программ. Способы защиты программ от исследования. Способы встраивания защитных механизмов в программное обеспечение. Обфускация программ.
12. Методы и средства обеспечения целостности и достоверности используемого программного кода.
13. Методы защиты программ от несанкционированного копирования. Криптографические методы защиты от копирования. Метод привязки к идентификатору. Методы, основанные на работе с переходами и стеком. Манипуляции с кодом программы. Методы противодействия динамическим способам снятия защиты программ от копирования.
14. Создание защищенных операционных систем.
15. Методы аутентификации и идентификации в современных ОС.
16. Особенности создания защищенных ОС с учетом современных технологий виртуализации.
17. Средства и системы тестирования программного обеспечения при испытаниях его на технологическую безопасность.
18. Обобщенные способы анализа программных средств на предмет наличия (отсутствия) недекларированных возможностей.
19. Построение программно-аппаратных комплексов для контроля технологической безопасности программ.
20. Средства и комплексы защиты программ от компьютерных вирусов.
21. Обфускаторы программ.
22. Средства обеспечения целостности и достоверности используемого программного кода.
23. Изучение дампинга программ.
24. Виды атак при реализации эксклюзивных алгоритмов атак.

25. Основные разработчики пакетов для квантовых вычислений.
26. Проблема защиты программного обеспечения автоматизированных систем.
27. Защита программного обеспечения как система научных дисциплин.
28. Угрозы безопасности программного обеспечения.
29. Технологическая и эксплуатационная безопасность программного обеспечения.
30. Модели угроз безопасности программного обеспечения.
31. Основные принципы обеспечения безопасности программного обеспечения.
32. Методы анализа безопасности программного обеспечения.
33. Методы защиты программ от компьютерных вирусов.
34. Аутентификация и идентификация. Протокол LDAP.
35. Системы аудиты.
36. Штатные средства защиты ОС Linux.
37. Понятие кольца защиты ОС.
38. Механизмы доменной защиты.
39. Архитектура ОС.
40. Доверенная загрузка и контроль BIOS.
41. Примеры операционных систем в защищенном исполнении.
42. Мониторинг процессов ОС.
43. Электронные ключи. Принципы работы.
44. Защита байт-кодов в виртуальной среде.
45. Отладчики системного уровня.
46. Сигнатурный анализ. Принципы детектирования.
47. Эвристический анализ.
48. Контроль выполнений контекстно-зависимых операций в средах виртуализации.

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

1. Что такое X-Force:

а) Глобальная система IBM сбора, обработки и реагирования на инциденты ИБ.

б) Сайт компании IBM.

в) Название ПО.

2. Эвристика — это:

а) мера кривизны пространства.

б) совокупность приёмов и методов, облегчающих и упрощающих решение познавательных, конструктивных, практических задач.

в) раздел математики.

6. Учебно-методическое и информационное обеспечение дисциплины

6.1. Список источников и литературы

Источники

Основные

1. *Базовая модель угроз безопасности* персональных данных при их обработке в информационных системах персональных данных. Утверждена Заместителем директора ФСТЭК России 15 февраля 2008 г. [Электронный ресурс] / ФСТЭК России. – Режим доступа : https://fstec.ru/component/attachments/download/289, свободный. – Загл. с экрана.
2. *ГОСТ Р 50922-2006*. Защита информации. Основные термины и определения. [Электронный ресурс] / Режим доступа : https://allgosts.ru/01/040/gost_r_50922-2006.pdf, свободный. – Загл. с экрана

3. *Методика определения актуальных угроз безопасности* персональных данных при их обработке в информационных системах персональных данных. Утверждена Заместителем директора ФСТЭК России 14 февраля 2008 г. [Электронный ресурс] / ФСТЭК России. – Режим доступа : https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/380, свободный. – Загл. с экрана.
4. *Методические рекомендации по разработке* нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности. Утверждены руководством 8 Центра ФСБ России от 31 марта 2015 года № 149/7/2/6-432 [Электронный ресурс] / ФСТЭК России. – Режим доступа : http://docs.cntd.ru/document/420336137, свободный. – Загл. с экрана.
5. *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-gostekhkomissii-rossii-ot-30-marta-1992-g, свободный. – Загл. с экрана.
6. *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-gostekhkomissii-rossii-ot-30-marta-1992-g2, свободный. – Загл. с экрана.
7. *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-gostekhkomissii-rossii-ot-25-iyulya-1997-g, свободный. – Загл. с экрана.

Дополнительные

8. *Приказ ФСТЭК России* от 11.02.2013 № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» [Электронный ресурс] : Режим доступа : https://fstec.ru/normotvorcheskaya/akty/53-prikazy/702, свободный. – Загл. с экрана.
9. *Руководящий докумен*т. 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-gostekhkomissii-rossii-ot-30-marta-1992-g3, свободный. – Загл. с экрана.
10. *Руководящий документ.* Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей. Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 4 июня 1999 г. № 114

11. *Федеральный закон* «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ (ред. от 19.07.2017). [Электронный ресурс] : Режим доступа : http://www.consultant.ru/document/cons_doc_LAW_61798/, свободный. – Загл. с экрана.

Литература

Основная

1. 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. Варновский Н.П. Курс лекций по математической криптографии [Электронный ресурс]. – Режим доступа: http://cryptography.ru/wp-content/uploads/2014/11/varn_lectures_long.pdf (дата обращения: август 2017).
2. Гарант [Электронный ресурс]: информационно-правовой портал. – Электрон. дан. – М.: НПП "ГАРАНТ-СЕРВИС", сор. 2012. – Режим доступа: www.garant.ru.
3. КонсультантПлюс [Электронный ресурс]. – Электрон. дан. – М.: КонсультантПлюс, сор. 1997-2012. – Режим доступа: www.consultant.ru.

6.3. Перечень БД и ИСС

№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 ProQuest Dissertation & Theses Global SAGE Journals Журналы Taylor and Francis
	Компьютерные справочные правовые системы Консультант Плюс, Гарант

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;
– средства обнаружения вредоносного ПО на примере RootkitHunter, Malware Detector;
– антивирусное средство защиты DrWeb;
– Secret Net Studio 8.4

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.

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, регулируемыми 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. По-

мощь 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.

Лабораторное занятие 1(6 ч.). 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 практической 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 практического 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 практической 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 практического 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(6 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 практической 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 практического 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(2 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 практической работы студенты на практике знакомятся с командной строкой Linux.
Список литературы:
Приведён в п. 6 данной РПД

Материально-техническое обеспечение практического 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.

Приложение 1

АННОТАЦИЯ ДИСЦИПЛИНЫ

Дисциплина «Безопасность операционных систем и программного обеспечения» реализуется на факультете Информационных систем и безопасности для студентов 3-го курса, обучающихся по программе бакалавриата по направлению подготовки 10.03.01 Информационная безопасность (профили подготовки – № 2 Организация и технология защиты информации) кафедрой комплексной защиты информации.
Цель дисциплины: приобретение знаний о базовых методах и способах защиты программного обеспечения (ПО) автоматизированных систем и умений применять на практике средства защиты программ, имеющиеся на отечественном рынке продукции и услуг в области защиты информации от несанкционированного доступа, научить студентов использовать для решения профессиональных задач современные средства программно-аппаратной защиты информации ОС.
Задачи: приобретение знаний о базовых методах и способах защиты ПО автоматизированных систем и умений применять на практике средства защиты программ, имеющиеся на отечественном рынке продукции и услуг в области защиты информации от несанкционированного доступа, формирование у студентов представлений о механизмах защиты ОС, выработка умений настраивать функций безопасности ОС.

Дисциплина направлена на формирование следующих компетенций:

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

В результате освоения дисциплины обучающийся должен демонстрировать следующие результаты образования:
Знать основные положения теории информационной безопасности и практики защиты информации от несанкционированного доступа, нормативные правовые документы в области защиты информации, математические модели безопасности и формальные модели доступа систем, модели и методы защиты операционных систем основные проектные решения, средства и методы защиты информации от несанкционированного доступа, 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 решать типовые задачи с помощью методов защиты информации от несанкционированного доступа, применять существующие методы защиты информации от несанкционированного доступа без снижения их стойкости за счет принятия неправильных эксплуатационных решений, применять современные методы и методики защиты программ от программных средств скрытого информационного воздействия, применять современные методы и методики защиты программ от несанкционированного исследования, копирования, распространения и использования.
Владеть методами разработки и использования защищенных программных средств, навыками эксплуатации защищенных программных средств, получивших широкое применение в современных автоматизированных системах, 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.

Новизна программы состоит во введении в учебный процесс моделирование компьютерных атак на ПО, в том числе на операционные системы и средства автоматизации программирования. При изучении дисциплины акцент делается на решении современных проблем защиты информации от несанкционированного доступа и противодействия новейшим методам вскрытия защищенного программного обеспечения.
По дисциплине предусмотрена промежуточная аттестация в форме экзамена.
Общая трудоёмкость освоения дисциплины составляет 3 зачётные единицы.

Приложение 2

ЛИСТ ИЗМЕНЕНИЙ

№	Текст актуализации или прилагаемый к РПД документ, содержащий изменения	Дата	№ протокола
1	*Обновлен состав программного обеспечения (ПО), современных профессиональных баз данных (БД) и информационно-справочные систем (ИСС)*	*29.06.2017 г.*	***10***
2	*Обновлена основная и дополнительная литература*	*26.06.2018*	***11***
3	*Обновлен состав программного обеспечения (ПО), современных профессиональных баз данных (БД) и информационно-справочные систем (ИСС)*	*26.06.2018*	***11***
4	*Обновлена структура дисциплины (модуля) для очной формы обучения (2019 г.)*	*29.08.2019 г.*	***1***
5	*Обновлен состав программного обеспечения (ПО), современных профессиональных баз данных (БД) и информационно-справочные систем (ИСС)*	*29.08.2019 г.*	***1***
6	*Обновлена структура дисциплины (модуля) для очной формы обучения (2020 г.)*	*23.06.2020 г*	***14***
7	*Обновлена основная и дополнительная литература*	*23.06.2020 г*	***14***
8	*Обновлен раздел п.4 Образовательные технологии*	*23.06.2020 г*	***14***
9	*Обновлен состав программного обеспечения (ПО), современных профессиональных баз данных (БД) и информационно-справочные систем (ИСС)*	*23.06.2020 г*	***14***

Приложение 1
к листу изменений

1. Состав программного обеспечения (ПО), современных профессиональных баз данных (БД) и информационно-справочные 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:
Кандидат технических наук, доцент кафедры КЗИ А.С. Моляков

Приложение 2
к листу изменений

2.Обновление основной и дополнительной литературы (2018 г.)

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

Дополнить раздел ***Основная литература***

Защита информации : учеб. пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - 2-е изд. - М. : РИОР : ИНФРА-М, 2018. - 392 с. - (Высшее образование: Бакалавриат; Магистратура). — https://doi.org/10.12737/4868. - Режим доступа: http://znanium.com/catalog/product/937469

3.Состав программного обеспечения (ПО), современных профессиональных баз данных (БД) и информационно-справочные 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 Statisctics 22	IBM	лицензионное
7	Microsoft Share Point 2010	Microsoft	лицензионное
8	SPSS Statisctics 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:
Кандидат технических наук, доцент кафедры КЗИ А.С. Моляков

Приложение 3
к листу изменений

4. Обновление структуры дисциплины (модуля) для очной формы обучения (2019 г.)

Структура дисциплины (модуля) для очной формы обучения

Общая трудоёмкость дисциплины составляет 3 з.е., 108 ч., в том числе контактная работа обучающихся с преподавателем 42 ч., самостоятельная работа обучающихся 66 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	*Введение в теорию и практику защиты программного обеспечения и Общая архитектура ОС*	**6**	**2**					**10**	Опрос
2	*Основные положения, понятия и определения, используемые при защите программного обеспечения и Место сервисов безопасности в ОС*	**6**	**4**			**6**		**10**	Опрос. Защита лабораторных работ.
3	*Методы обеспечения технологической и эксплуатационной безопасности программного обеспечения и Управление учетными записями в ОС*	**6**	**4**			**6**		**20**	Опрос. Защита лабораторных работ.
4	*Средства и системы защиты программного обеспечения. Управление доступом к объектам файловой системы*	**6**	**6**			**6**		**10**	Опрос. Защита лабораторных работ.
5	*Отечественные нормативные акты, регламентирующие деятельность в области защиты программного обеспечения*	**6**	**4**			**4**		**16**	Опрос. Защита лабораторных работ.
	Зачёт	**6**							*Зачёт по билетам*
	итого:		**20**			**22**		**66**	

5.Состав программного обеспечения (ПО), современных профессиональных баз данных (БД) и информационно-справочные 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 Statisctics 22	IBM	лицензионное
7	Microsoft Share Point 2010	Microsoft	лицензионное
8	SPSS Statisctics 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: Кандидат технических наук, доцент кафедры КЗИ А.С. Моляков

Приложение 4
к листу изменений

6. Обновление структуры дисциплины (модуля) для очной формы обучения (2020 г.)

Структура дисциплины (модуля) для очной формы обучения

Общая трудоёмкость дисциплины составляет 3 з.е., 114 ч., в том числе контактная работа обучающихся с преподавателем 42 ч., самостоятельная работа обучающихся 72 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	*Введение в теорию и практику защиты программного обеспечения и Общая архитектура ОС*	**6**	**2**					**10**	Опрос
2	*Основные положения, понятия и определения, используемые при защите программного обеспечения и Место сервисов безопасности в ОС*	**6**	**4**			**6**		**10**	Опрос. Защита лабораторных работ.
3	*Методы обеспечения технологической и эксплуатационной безопасности программного обеспечения и Управление учетными записями в ОС*	**6**	**4**			**6**		**20**	Опрос. Защита лабораторных работ.
4	*Средства и системы защиты программного обеспечения. Управление доступом к объектам файловой системы*	**6**	**6**			**6**		**14**	Опрос. Защита лабораторных работ.
5	*Отечественные нормативные акты, регламентирующие деятельность в области защиты программного обеспечения*	**6**	**4**			**4**		**18**	Опрос. Защита лабораторных работ.
	Зачёт	**6**							*Зачёт по билетам*
	итого:		**20**			**22**		**72**	

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

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

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

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

Клименко, И. С. Информационная безопасность и защита информации: модели и методы управления : монография / И.С. Клименко. — Москва: ИНФРА-М, 2020. — 180 с. — (Научная мысль). — DOI 10.12737/monography_5d412ff13c0b88.75804464. - ISBN 978-5-16-015149-6. - Текст: электронный. - URL: https://znanium.com/catalog/product/1018665

8. 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.

9. 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 (*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 Statisctics 22	IBM	лицензионное
7	Microsoft Share Point 2010	Microsoft	лицензионное
8	SPSS Statisctics 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:
Кандидат технических наук, доцент кафедры КЗИ А.С. Моляков