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 ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

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 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.

Задачи дисциплины: рассмотрение следующих вопросов: основные понятия теории алгоритмов и теории сложности вычислений; методы анализа ПО; методы защиты разрабатываемых программ от автоматической генерации инструментальными средствами программных средств скрытого воздействия; методы идентификации программ и их характеристик; методы защиты программ от компьютерных вирусов; методы защиты программ от исследования; методы обфускации программ; методы защиты программ от несанкционированного копирования; средства и системы тестирования программного обеспечения при испытаниях его на безопасность; операционные системы в защищённом исполнении.

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

Коды компетенции	**Содержание компетенций**	**Перечень планируемых результатов обучения по дисциплине**
ПК-2	способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач	Знать принципы работы программных средств системного, прикладного и специального назначения, инструментальных средств. Уметь выбирать, устанавливать и настраивать средства средства системного, прикладного и специального назначения. Владеть навыками настройки и эксплуатации инструментальные средства, языки и системы программирования для решения профессиональных задач.
ПК-15	способность организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами ФСБ России, ФСТЭК России	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. Уметь: решать типовые задачи с помощью методов защиты информации от несанкционированного доступа; 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 средств защиты ПО; навыками эксплуатации защищенных программных средств, получивших широкое применение в современных автоматизированных системах.

1.3. Место дисциплины в структуре основной образовательной программы

Дисциплина «Безопасность программного обеспечения» относится к дисциплинам по выбору вариативной части частью блока дисциплин учебного плана по направлению подготовки 10.03.01 «Информационная безопасность», профиля КЗОИ. Дисциплина реализуется на факультете информационных систем и безопасности кафедрой комплексной защиты информации.

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 дисциплин и прохождения практик: «Безопасность критически важных систем», «Проектирование систем защиты объектов информатизации», «Преддипломная практика».

2. Структура дисциплины

Структура дисциплины для очной формы обучения

Общая трудоемкость дисциплины «Безопасность программного обеспечения» – 3 зачетные единицы, 108 часов, 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	5	2					4	Опрос
2	Основные положения, понятия и определения, используемые при защите программного обеспечения	5	2					4	Опрос
3	Методы обеспечения технологической	5	4			8		4	Оценка выполнения практиче-

	и эксплуатационной безопасности программного обеспечения								ских и внеаудиторных заданий
4	Средства и системы защиты программного обеспечения	5	4			8		8	Оценка выполнения практических и внеаудиторных заданий
5	Исследование программного обеспечения на предмет отсутствия недекларированных возможностей	5	4			4		16	Оценка выполнения практических и внеаудиторных заданий
6	Отечественные нормативные акты, регламентирующие деятельность в области защиты программного обеспечения	5	4			2		20	Опрос
7	*Зачет с оценкой*	5						10	Зачет по билетам
	Итого:		**20**			**22**		**66**	

3. Содержание дисциплины

№	Наименование раздела дисциплины	Содержание
1	**Введение в теорию и практику защиты программного обеспечения**	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. Основные принципы обеспечения безопасности программного обеспечения
2	**Основные положения, понятия и определения, используемые при защите программного обеспечения**	Базовые научные положения и основания теории защиты программ. Основы теории алгоритмов. Элементы теории сложности вычислений. Элементы криптологии. Конфиденциальные вычисления
3	**Методы обеспечения технологической и эксплуатационной безопасности программного**	Методы анализа безопасности программного обеспечения. Методы идентификации программ и их характеристик. Методы защиты программ

	обеспечения	от компьютерных вирусов. Методы защиты программ от исследования. Обфускация программ. Методы и средства обеспечения целостности и достоверности используемого программного кода. Методы защиты программ от несанкционированного копирования. Создание защищенных операционных систем. Использование программы PGP.
4	**Средства и системы защиты программного обеспечения**	Средства и системы тестирования программного обеспечения при испытаниях его на технологическую безопасность. Средства и комплексы защиты программ от компьютерных вирусов. Обфускаторы программ. Средства обеспечения целостности и достоверности используемого программного кода. Средства защиты программ от несанкционированного копирования. Операционные системы в защищенном исполнении. Использование программы TrueCrypt
5	**Исследование программного обеспечения на предмет отсутствия недекларированных возможностей**	Подготовка к исследованию программного обеспечения на предмет отсутствия недекларированных возможностей. Контроль и фиксация исходного состояния программного обеспечения.
6	**Отечественные нормативные акты, регламентирующие деятельность в области защиты программного обеспечения**	Федеральный закон «Об информации, информационных технологиях и о защите информации». ГОСТ Р ИСО/МЭК 12207-2010. ГОСТ Р ИСО/МЭК 15408-2013. ГОСТ Р МЭК 61508-2012. Руководящий документ ФСТЭК России. Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля недекларированных возможностей.

4. Образовательные технологии

При реализации рабочей программы дисциплины «Безопасность программного обеспечения» используются следующие образовательные технологии.

Образовательные технологии

№ п/п	**Наименование темы**	**Виды учебных занятий**	**Образовательные технологии**
1	Введение в теорию и практику защиты программного обеспечения	Лекция.	Традиционная с использованием презентаций
2	Основные положения, понятия и определения, используемые при защите программного обеспечения	Лекция.	Лекция-дискуссия Традиционная
3	Методы обеспечения технологи-	Лекция.	Лекция-дискуссия

№ п/п	Наименование темы	Виды учебных занятий	Образовательные технологии
	ческой и эксплуатационной безопасности программного обеспечения	Лабораторное занятие 1.	Традиционная
4	Средства и системы защиты программного обеспечения	Лекция. Лабораторное занятие 2.	Проблемная лекция Традиционная с использованием презентаций
5	Исследование программного обеспечения на предмет отсутствия недекларированных возможностей	Лекция. Лабораторное занятие 3.	Лекция с разбором конкретных ситуаций Традиционная
6	Отечественные нормативные акты, регламентирующие деятельность в области защиты программного обеспечения	Лекция.	Лекция-дискуссия

5. Оценка планируемых результатов обучения

5.1. Система оценивания

Форма контроля	**Макс. количество баллов**	
	За одну работу	**Всего**
Текущий контроль: *- опрос* *- участие в дискуссии на семинаре* *- практическая работа (темы 3-4)* *- практическая работа (тема 5)*	 *5 баллов* *5 баллов* *10 баллов* *10 баллов*	 *30 баллов* *10 баллов* *10 баллов* *10 баллов*
Промежуточная аттестация *Зачет*		*40 баллов*
Итого за семестр *Зачет*		*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 аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «хороший».
67-50/ D,E	«удовлетворительно»/ «зачтено (удовлетвори-тельно)»/ «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»/	Выставляется обучающемуся, если он не знает на базовом уровне теоретический и практический материал,

Баллы/ Шкала ECTS	Оценка по дисциплине	Критерии оценки результатов обучения по дисциплине
	не зачтено	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

Примерные вопросы и задания для лабораторных заданий - проверка сформированности компетенции ПК-15,ПК-2

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 хэширования. 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.

Примерные темы докладов, вопросов для тестирования - проверка сформированности компетенции ПК-15, ПК-2

1. Проблема защиты программного обеспечения автоматизированных систем.
2. Защита программного обеспечения как система научных дисциплин.
3. Угрозы безопасности программного обеспечения.
4. Технологическая и эксплуатационная безопасность программного обеспечения.
5. Модели угроз безопасности программного обеспечения.
6. Основные принципы обеспечения безопасности программного обеспечения.
7. Методы анализа безопасности программного обеспечения.
8. Методы защиты разрабатываемых программ от автоматической генерации инструментальными средствами ПССИВ.
9. Методы идентификации программ и их характеристик.
10. Методы защиты программ от компьютерных вирусов.
11. Методы защиты программ от исследования.
12. Обфускация программ.
13. Методы и средства обеспечения целостности и достоверности используемого программного кода.
14. Методы защиты программ от несанкционированного копирования.

Промежуточная аттестация (контрольные вопросы) - проверка сформированности компетенции ПК-15, ПК-2

Примерные контрольные вопросы по курсу

1. Средства и системы тестирования программного обеспечения при испытаниях его на технологическую безопасность.
2. Обобщенные способы анализа программных средств на предмет наличия (отсутствия) недекларированных возможностей.
3. Построение программно-аппаратных комплексов для контроля технологической безопасности программ.
4. Средства и комплексы защиты программ от компьютерных вирусов.
5. Обфускаторы программ.
6. Средства обеспечения целостности и достоверности используемого программного кода.
7. Средства защиты программ от несанкционированного копирования.
8. Операционные системы в защищенном исполнении.

Примерные задания для тестирования- проверка сформированности компетенции ПК-15, ПК-2

1. ССИВ - это:

а) средства скрытого информационного воздействия

б) средства связи типа “волновод”

в) средство контроля радиоизлучений.

2. Обфускация программ - это:

а) сетевое устройство, подключаемое к двум и более.

б) запутывание кода — приведение исходного текста или исполняемого кода програмы к виду, сохраняющему её функциональность, но затрудняющему анализ, понимание алгоритмов работы и модификацию при декомпиляции..

в) процессорный модуль.

6. Учебно-методическое и информационное обеспечение дисциплины

6.1. Список источников и литературы

Источники

Основные

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

Адреса ресурсов 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.

2. Goldreich O. Foundations of cryptography. [Электронный ресурс]. – Режим доступа: http://www.twirpx.com/file/493751/.

3. Гарант [Электронный ресурс]: информационно-правовой портал. – Электрон. дан. – М.: НПП "ГАРАНТ-СЕРВИС”, cop. 2012. – Режим доступа: www.garant.ru.

4. КонсультантПлюс [Электронный ресурс]. – Электрон. дан. – М.: КонсультантПлюс, cop. 1997-2012. – Режим доступа: www.consultant.ru.

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;
– отладчик OllyDebugger;
– утилита Hashcalc;
– сканер безопасности XSpider

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	VMWare	Свободное ПО, Режим доступа: https://www.vmware.com/products/ Демо-версия
8	OllyDebugger 1.10	OllyDbg	Свободное ПО, Режим доступа: http://www.ollydbg.de/ Демо-версия
9	Hashcalc 2.02	Astro	Свободное ПО, Режим доступа: https://hashcalc.ru.downloadastro.com/ Демо-версия
10	XSpider 7.0	Positive Technologies	Свободное ПО, Режим доступа: https://www.ptsecurity.com/ru-ru/ Демо-версия

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, регулируемыми эргономическими партами СИ-1;
  – компьютерной техникой со специальным программным обеспечением.

9. Методические материалы

9.1. Планы лабораторных занятий. Методические указания по организации и проведению - *проверка сформированности компетенции ПК-15, ПК-2*

Лабораторное занятие № 1 (8 часов). Методы обеспечения технологической и эксплуатационной безопасности программного обеспечения (*проверка сформированности компетенции ПК-15,ПК-2)*

Цель занятия: получение практических навыков в защите программ от ПССИВ и их несанкционированного исследования, копирования и распространения.

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

Вопросы для изучения и обсуждения:

1. Методы анализа безопасности программного обеспечения.
2. Методы защиты разрабатываемых программ от автоматической генерации инструментальными средствами ПССИВ.
3. Методы идентификации программ и их характеристик.
4. Методы защиты программ от компьютерных вирусов.
5. Методы защиты программ от исследования.
6. Методы обфускации программ. Методы и средства обеспечения целостности и достоверности используемого программного кода.
7. Методы защиты программ от несанкционированного копирования.
8. Создание защищенных операционных систем.

Контрольные вопросы:

1. В чем состоят недостатки и достоинства контрольно-испытательных и логико-аналитических методов анализа программного обеспечения?
2. Что представляет собой статический и динамический анализ программ. При помощи каких средств проводится такой анализ?
3. Опишите способы внедрения ПССИВ посредством средств автоматизации программирования (трансляторов, компиляторов, интерпретаторов, отладчиков и др.).

4. Как оценивается подобие целевой и исследуемой программ с точки зрения наличия ПССИВ?

5. Признаки классификации компьютерных вирусов. Опишите различные типы вирусов в соответствии с этой классификацией. Приведите примеры компьютерных вирусов, с которыми вы сталкивались в повседневной жизни, К какому типу вирусов вы их отнесете? Опишите средства нейтрализации компьютерных вирусов. Приведите примеры использования антивирусных комплексов.

6. Приведите классификацию методов и средств защиты программ от исследования. В чем суть обфускации программ? Дайте определение эффективному вероятностному обфускатору.

7. Опишите методы и средства обеспечения целостности и достоверности используемого программного кода, в том числе криптографические. Опишите методы и средства защиты программ от копирования, в том числе криптографические.

8. Расскажите об отечественных защищенных операционных системах ос2000 и «Феникс».

9. Использование продукта PGP.Функциональные возможности

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, отладчик OllyDebugger и и утилита hashcalc.

Лабораторное занятие № 2 (8 часов). Средства и системы защиты программного обеспечения(*проверка сформированности компетенции ПК-15)*

Цель 1 занятия: получение практических навыков в разработке и эксплуатации средств и систем защиты программного обеспечения.

Указания по выполнению задания: обратить внимание на прикладные области применения средств защиты программного обеспечения.

Вопросы для изучения и обсуждения:

1. Средства и системы тестирования программного обеспечения при испытаниях его на технологическую безопасность.

2. Опишите показатели качества программного обеспечения. Выбор номенклатуры показателей качества ПО с точки зрения его защищенности.

3. Организационные и методологические вопросы проведения испытаний ПО.

4. Построение программно-аппаратных комплексов для контроля технологической безопасности программ. Состав инструментальных средств контроля безопасности ПО при его разработке.

5. Структура и принципы построения программно-аппаратных средств контрольно-испытательного стенда испытания технологической безопасности ПО.

6. Средства и комплексы защиты программ от компьютерных вирусов. Обфускаторы программ. Средства обеспечения целостности и достоверности используемого программного кода. Средства защиты программ от несанкционированного копирования.

7. Операционные системы в защищенном исполнении. Создание операционных систем с открытым исходным кодом в защищенном исполнении.

Контрольные вопросы:

1. Статистические и динамические способы исследования ПО, в чем их достоинства и недостатки? В чем сущность работы дизассемблеров, дискомпиляторов, трассировщиков, следящих систем при исследовании ПО.

2. Опишите способы проведения испытаний ПО, оценки качества и сертификации программных средств. Состав методического обеспечения проведения испытаний программ. Опишите показатели качества ПО разных уровней. последовательность опера-

ций при выборе номенклатуры показателей качества ПО. Оценка значений показателей качества ПО.

3. Основные этапы проведения испытаний ПО и последовательность действий при этом.

4. Технология создания сложных программных комплексов и действия разработчиков при обеспечения технологической безопасности ПО.

5. Структурно-функциональная схема инструментальных средств поддержки создания безопасного программного обеспечения.

6. Опишите этапы контроля безопасности общего и специального ПО на этапе исследования и испытаний ПО.

7. Требования к контрольно-испытательному стенду испытания технологической безопасности ПО. Принципы его построения. Достоинства и недостатки существующих операционных сред для такого стенда.

8. Приведите примеры существующих на отечественном рынке антивирусных комплексов, их основные достоинства и недостатки. Базовый функционал антивирусных программ.

9. Как обеспечивается функциональная эквивалентность программ до и после их обфускации?

10. Приведите примеры существующих на отечественном рынке средств обеспечения целостности и достоверности используемого программного кода и средств защиты программ от несанкционированного копирования, их основные достоинства и недостатки.

11. Разработка такого дистрибутивов операционной системы с открытыми исходными кодами, который обеспечил бы учет специфики объектов, потенциально уязвимых для кибератак. Основные компоненты такого дистрибутива?

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, отладчик OllyDebugger и и утилита hashcalc.

Лабораторное занятие №3 (4 часа). Исследование программного обеспечения с помощью сканера безопасности и отладчика(*проверка сформированности компетенции ПК-15,ПК-2)*

Цель занятия: получение практических навыков в исследовании конкретных программ при помощи отладчика Ollydebugger и утилиты Hashcalc, сканера XSpider.

Указания по выполнению задания: обратить внимание на обязательность требований РД ФСТЭК России «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля недекларированных возможностей».

Вопросы для изучения и обсуждения:

1. Контроль и фиксация исходного состояния программного обеспечения.
2. Построения стендов для проведения анализа программного обеспечения.
3. Контроль состава и содержания документации на программное обеспечение.
4. Статический анализ исходных текстов программного обеспечения. Контроль полноты и отсутствия избыточности на уровне файлов и функциональных объектов. Проверка соответствия исходных файлов объектному коду. Контроль связей по управлению и информации.
5. Использование сканера XSpider при исследовании ПО.

Выполнение задания:

В ходе практической работы рассматривается пакет документов, необходимый для

сертификации и эксплуатации ПО и собственно сертификат соответствия ПО нормативным документам и/или ТУ.

Контрольные вопросы:

1. В чем заключается контроль полноты и отсутствия избыточности на уровне файлов и функциональных объектов.
2. В чем заключается контроль связей по управлению и информации.
3. В чем заключается контроль выполнения функциональных объектов. Каким образом встраиваются датчики в исходный текст программ.

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, отладчика Ollydebugger и утилита hashcalc, сканер безопасности XSpider.

Приложение 1

АННОТАЦИЯ ДИСЦИПЛИНЫ

Дисциплина «Безопасность программного обеспечения» относится к вариативной части частью блока дисциплин учебного плана по направлению подготовки 10.03.01 «Информационная безопасность», профиля КЗОИ Дисциплина реализуется на факультете информационных систем и безопасности кафедрой комплексной защиты информации.

Цель дисциплины: приобретение знаний о базовых методах и способах защиты программного обеспечения автоматизированных систем и умений применять на практике средства защиты программ, имеющиеся на отечественном рынке продукции и услуг в области защиты информации от несанкционированного доступа.

Задачи: рассмотрение следующих вопросов: основные понятия теории алгоритмов и теории сложности вычислений; методы анализа ПО; методы защиты разрабатываемых программ от автоматической генерации инструментальными средствами программных средств скрытого воздействия; методы идентификации программ и их характеристик; методы защиты программ от компьютерных вирусов; методы защиты программ от исследования; методы обфускации программ; методы защиты программ от несанкционированного копирования; средства и системы тестирования программного обеспечения при испытаниях его на безопасность; операционные системы в защищённом исполнении

Дисциплина направлена на формирование следующих компетенций:

ПК-2 – способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач

ПК-15 – способность организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами ФСБ России, ФСТЭК России

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;

принципы работы программных средств системного, прикладного и специального назначения, инструментальных средств;

основные проектные решения, средства и методы защиты информации от несанкционированного доступа.

Уметь:

решать типовые задачи с помощью методов защиты информации от несанкционированного доступа;

применять современные методы и методики защиты программ от программных средств скрытого информационного воздействия;

выбирать, устанавливать и настраивать средства средства системного, прикладного и специального назначения;

применять современные методы и методики защиты программ от несанкционированного исследования, копирования, распространения и использования.

Владеть:

методами разработки и использования средств защиты ПО;

навыками настройки и эксплуатации инструментальные средства, языки и системы программирования для решения профессиональных задач;

навыками эксплуатации защищенных программных средств, получивших широкое применение в современных автоматизированных системах.

Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме опроса, контрольной работы, реферата, тестирования, промежуточная аттестация в форме зачета с оценкой.

Общая трудоемкость освоения дисциплины составляет 3 зачетные единицы, 108 часов.

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)*	*29.06.2017г.*	***10***
2	*Обновлена структура дисциплины (модуля) для очной формы обучения (2018 г.)*	*26.06.2018 г.*	***11***
3	*Обновление раздела 9. Методические материалы*	*26.06.2018 г.*	***11***
4	*Обновлен состав программного обеспечения (ПО), современных профессиональных баз данных (БД) и информационно-справочные систем (ИСС)*	*26.06.2018 г.*	***11***
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*	***14***
7	*Обновлена основная и дополнительная литература*	*23.06.2020*	***14***
8	*Обновлен раздел п.4 Образовательные технологии*	*23.06.2020*	***14***
9	*Обновлен состав программного обеспечения (ПО), современных профессиональных баз данных (БД) и информационно-справочные систем (ИСС)*	*23.06.2020*	***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: К.т.н, доцент, А.С. Моляков

Приложение 2
к листу изменений

2. Обновление структуры дисциплины (модуля) для очной формы обучения (2018 г.)

Структура дисциплины (модуля) для очной формы обучения

Общая трудоемкость дисциплины «Безопасность программного обеспечения» – 3 зачетные единицы, 108 часов, 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	5	2					4	Опрос
2	Основные положения, понятия и определения, используемые при защите программного обеспечения	5	2					4	Опрос
3	Методы обеспечения технологической и эксплуатационной безопасности программного обеспечения	5	4		8			4	Оценка выполнения практических и внеаудиторных заданий
4	Средства и системы защиты программного обеспечения	5	4		8			8	Оценка выполнения практических и внеаудиторных заданий
5	Исследование программного обеспечения на предмет отсутствия недекларированных возможностей	5	4		4			16	Оценка выполнения практических и внеаудиторных заданий
6	Отечественные нормативные акты, регламентирующие деятельность в области защиты программного обеспечения	5	4		2			20	Опрос
7	*Зачет с оценкой*	5						10	Зачет по билетам
	Итого:		**20**		**22**			**66**	

3.Обновление раздела 9. Методические материалы

Обновить раздел 9. Методические материалы

В раздел 9 внести следующие изменения.

Заменить производные слова от слова «лабораторный» на соответствующие производные слова от слова «практический».

4. 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: К.т.н, доцент, А.С. Моляков

Приложение 3
к листу изменений

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: К.т.н, доцент, 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 трудоемкость 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		**2**					**8**	Опрос
2	Основные положения, понятия и определения, используемые при защите программного обеспечения		**2**					**8**	Опрос
3	Методы обеспечения технологической и эксплуатационной безопасности программного обеспечения		**4**		**8**			**10**	Оценка выполнения практических и внеаудиторных заданий
4	Средства и системы защиты программного обеспечения		**4**		**10**			**10**	Оценка выполнения практических и внеаудиторных заданий
5	Исследование программного обеспечения на предмет отсутствия недекларированных возможностей		**4**		**4**			**16**	Оценка выполнения практических и внеаудиторных заданий
6	Отечественные нормативные акты, регламентирующие деятельность в области защиты программного обеспечения		**4**					**20**	Опрос

7	Промежуточная аттестация								Зачет с оценкой
	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

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

Составитель:

К.т.н, доцент, А.С. Моляков