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

АКТУАЛЬНЫЕ ТЕНДЕНЦИИ В ОБЛАСТИ ЗАЩИТЫ ИНФОРМАЦИИ

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

Актуальные тенденции в области защиты информации
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: является ознакомление студентов с современными тенденциями в области защиты информации, новейшими подходами к построению подсистем информационной безопасности и актуальными изменениями в нормативно-методической базе в этой сфере.

Задачи: рассмотрение следующих актуальных тенденций в области защиты информации: интегрированные решения по защите информации, управление безопасностью информации и событий (SIEM-системы); управление учетными записями (IdAM-системы), унифицированный доступ к приложениям на примере Единой системы идентификации и аутентификации (ЕСИА), обеспечение безопасного взаимодействия с внешними информационными системами на примере Системы межведомственного электронного взаимодействия (СМЭВ),тенденции в применении средств криптографической защиты информации (средств легковесной криптографии), в том числе в системах электронного документооборота, использование «облачных» технологий при реализации механизмов безопасности; многоагентные системы в сфере информационной безопасности; безопасность Интернета вещей (Internet of Things, IoT).

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

Коды компетенции	***Содержание компетенций***	***Перечень планируемых результатов обучения по дисциплине***
ПК-9	способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности	Знать: перспективные направления развития информационной безопасности; наиболее актуальные решения в области криптографической, инженерно-технической и программно-аппаратной защиты информации; наиболее актуальные документы, создаваемые регуляторами в области информационной безопасности; особенности применения современных СЗИ для защиты персональных данных и информации, обрабатывающейся в государственных информационных системах. Уметь: ориентироваться на рынке современных средств защиты информации; выбирать оптимальное решение при проектировании и модернизации подсистемы информационной безопасности, выдвигать обоснованные предложения по применению таковых решений. Владеть: навыками интеграции и эксплуатации наиболее актуальных средств защиты информации, использования современных средств

		криптографической защиты информации и систем контроля и управления доступом
ПК-14	должен обладать способностью способностью организовывать работу малого коллектива исполнителей в профессиональной деятельности	Знать: методологические и технологические основы работы малого коллектива исполнителей. Уметь: разрабатывать модели и политику безопасности, используя известные подходы, методы, средства и их теоретические основы. Владеть: навыками работы с системами защищенного документооборота; навыками работы с документацией.

1.3. Место дисциплины в структуре образовательной программы

Дисциплина «Актуальные тенденции в области защиты информации» относится к вариативной части блока дисциплин учебного плана.
Для освоения дисциплины необходимы компетенции, формируемые в ходе изучения дисциплин: "Безопасность операционных систем", "Математические основы защиты информации", "Вычислительные сети".
В результате освоения дисциплины формируются компетенции, необходимые для изучения следующих дисциплин: "Безопасность программного обеспечения", "Аттестация 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 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	*Тенденции в развитии современных средств защиты информации*	**8**	**4**		**4**			**12**	Опрос. Оценка выполнения практических заданий
2	*Нормативно-методическая база в области применения криптографической, инженерно-технической и про-*	**8**	**4**		**4**			**14**	Опрос. Оценка выполнения практических заданий

	граммно-аппаратной защиты информации								
3	*Интегрированные решения по защите информации*	**8**	**6**		**8**			**20**	Опрос. Оценка выполнения практических заданий Тест
4	*Использование «облачных» технологий при реализации механизмов безопасности и многоагентные системы*	**8**	**6**		**4**			**20**	Опрос. Оценка выполнения практических заданий
	Зачет с оценкой	**8**							*Зачет с оценкой по билетам*
	итого:		**20**		**22**			**66**	

3. Содержание дисциплины

№	Наименование раздела дисциплины	Содержание
1	**Тенденции в развитии современных средств защиты информации**	*Анализатор* - автономный инструмент, который поддерживает порождение и управление зондами. Анализатор состоит из базы фактов, база данных сценариев вторжения, основанных на состоянии системы, блока анализа и диспетчера программы конфигурации. Анализатор определяет, для которого события должны быть проверены данные, где они должны быть проверены, какая сетевая информация о топологии требуется, и др. Для выполнения этих действий используется информация об использовании сетевых ресурсов, которая располагается вместе с базой данных сценария. Эта информация затем передается составителю программы конфигурации, который в свою очередь генерирует конфигурацию зондов.
2	**Нормативно-методическая база в области применения криптографической, инженерно-технической и программно-аппаратной защиты информации**	Изучение нормативно-правовых документов ФСТЭК и ФСБ, ГОСТ Р ИСО/МЭК 15408-1-2013. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. 3. ГОСТ Р ИСО/МЭК 15408-2-2013. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности. 4. ГОСТ Р ИСО/МЭК 15408-3-2013. Информационная технология. Методы и средства обеспе-

		чения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности. 5. ГОСТ Р ИСО/МЭК 15408-2013. Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий. 6. ГОСТ Р МЭК 61508-3-2012. Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 3. Требования к программному обеспечению. 7. ГОСТ Р ИСО/МЭК 12207-2010. Информационная технология. Системная и программная инженерия. Процессы жизненного цикла программных средств. 8. Руководящий документ ФСТЭК России. Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля недекларированных возможностей. 9. Руководящий документ ФСТЭК России. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий (Часть 1, Часть 2, Часть 3). 10. Руководящий документ ФСТЭК России. Безопасность информационных технологий. Руководство по разработке профилей защиты и заданий по безопасности. 11. Руководящий документ ФСТЭК России. Безопасность информационных технологий. Руководство по формированию семейств профилей защиты. 12. Руководящий документ ФСТЭК России. Безопасность информационных технологий. Руководство по регистрации профилей защиты.
3	**Интегрированные решения по защите информации**	*Мобильные агенты* являются одной из передовых тем исследований в области информационных технологий в течение ряда лет. Однако результаты этих исследований, главным образом, оставались в пределах лабораторий и не были широко использованы. Вместе с тем, интенсификация работ по созданию Web-приложений имела ключевое значение для взрывного роста заинтересованности к области исследований свойств мобильных агентов, что связано с возможностью создания на их основе распределенных приложений для работы в Интернет. Стала широко применяться процедура запуска на выполнение мобильных агентов через Web-браузеры для

		сбора информации и взаимодействия с любым узлом в сети (технология «ноуботов»). Фирмы IBM и General Magic являются инициаторами работ в этом направлении интерактивных систем.
4	**Использование «облачных» технологий при реализации механизмов безопасности и многоагентные системы**	Современные многоагентные системы ИБ включает набор зондов, которые отвечают за обнаружение и оценку вторжений в тех подсетях, в которых они функционируют. Каждый зонд обеспечен фильтром данных с перестраиваемой конфигурацией, блоком вывода и решателем. Зонды могут действовать автономно. Если обнаружены компоненты вторжения, то информация о событии может быть отправлена другим заинтересованным зондам, которые подпишутся на информацию о подобных событиях, это позволит получать более полное понимание схемы вторжения. Этим способом могут быть идентифицированы разные подсети, которые участвуют в осуществлении вторжения. Зонды связаны с анализаторами *Интернет вещей* (*Internet of Things*, *IoT*) — концепция физических предметов вычислительной сети (*«вещей»*), оснащённых встроенными технологиями для взаимодействия друг с другом или с внешней средой, рассматривающая организацию таких сетей как явление, способное перестроить экономические и общественные процессы, исключающее из части действий и операций необходимость участия человека. Модель безопасного функционирования IoT состоит из следующих уровней: • *«Умные» объекты/встроенные системы:* этот уровень включает в себя сенсорные/исполнительные устройства и другие встроенные системы на границе сети. Эта часть IoT наиболее уязвима. Устройства могут находиться в среде, не защищенной физически, и от них может требоваться функционирование в течение нескольких лет. Доступность тоже является важной проблемой. Кроме того, менеджерам сети необходимо заботиться об аутентичности и целостности данных, генерируемых сенсорами, и о защите исполнительных устройств и других «умных» устройств от несанкционированного использования. Также могут присутствовать такие требования, как конфиденциальность и защита от подслушивания.

		• *Туманная/периферийная сеть:* этот уровень представляет проводные и беспроводные соединения устройств IoT. Кроме того, на этом уровне может осуществляться определенный объем обработки и консолидации данных. Ключевой проблемой является большая вариативность сетевых технологий и протоколов, используемых различными устройствами IoT, и необходимость выработки и воплощения единой политики безопасности. • *Ядро сети:* уровень ядра сети предоставляет пути для передачи данных между платформами в центре сети и устройствами IoT. Здесь проблемы безопасности те же, что в традиционных сетях. Однако огромное количество оконечных узлов, с которыми надо взаимодействовать и управлять ими, создает значительную проблему для безопасности.

4. Образовательные технологии

№ п/п	**Наименование раздела**	**Виды учебных занятий**	**Образовательные технологии**
1	**2**	**3**	**4**
1.	*Тенденции в развитии современных средств защиты информации*	*Лекция 1.1* *Лекция 1.2* *Практическое занятие 1.* *Самостоятельная работа*	*Традиционная с использованием презентаций* *Изучение материалов лекций*
2	*Нормативно-методическая база в области применения криптографической, инженерно-технической и программно-аппаратной защиты информации*	*Лекция 2.1* *Лекция 2.2* *Практическое занятие 2.* *Самостоятельная работа*	*Традиционная с использованием презентаций* *Изучение материалов лекций*
3	*Интегрированные решения по защите информации*	*Лекция 3.1* *Лекция 3.2* *Лекция 3.3* *Практическое занятие 3.* *Самостоятельная работа*	*Традиционная с использованием презентаций* *Выполнение задания* *Изучение материалов лекций*
4	*Использование «облачных» технологий при реализации механизмов безопасности и многоагентные системы*	*Лекция 4.1* *Лекция 4.2* *Лекция 4.3* *Практическое занятие 4.*	*Традиционная с использованием презентаций* *Выполнение задания* *Изучение материалов лекций*

		Самостоятельная работа	

5. Оценка планируемых результатов обучения

5.1. Система оценивания

Форма контроля	**Макс. количество баллов**	
	За одну работу	**Всего**
Текущий контроль: *– опрос (темы 1-4)* *– практическое задание (темы 1-2)* *– практическое задание (темы 3-4)*	 *5 баллов* *6 баллов* *7 баллов*	 *30 баллов* *12 баллов* *14 баллов*
Промежуточная аттестация *Экзамен*		*40 баллов*
Итого за дисциплину *Экзамен*		*100 баллов*

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

100-балльная 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, сформи-

Баллы/ Шкала ECTS	Оценка по дисциплине	Критерии оценки результатов обучения по дисциплине
		рованы 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 (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

Баллы/ Шкала ECTS	Оценка по дисциплине	Критерии оценки результатов обучения по дисциплине
		за дисциплиной, не сформированы.

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

Примерные контрольные вопросы для аттестации - проверка сформированности компетенций ПК-9, ПК-14

1. Организационная структура современных АСОД.
2. Федеральные органы по аттестации и их функции.
3. Механизмы регистрации и аудита в современных ЕИАС.
4. Деятельность ЕИАС.
5. Права, обязанности и ответственность органов по обработке конфиденциальной информации в крупных информационных системах.
6. Аккредитация испытательных лабораторий и органов по сертификации средств защиты информации по требованию безопасности информации. Порядок аккредитации.
7. Контроль и надзор за деятельностью аккредитованных испытательных лабораторий и органов по сертификации.
8. Заявители и их функции. Заявка на проведение аттестации ОИ.
9. Порядок проведения аттестации объектов информатизации. Содержание заявок.
10. Порядок взаимодействия заявителя и органа по проведению аттестации.
11. Основные тенденции в области защиты информации.
12. TSIEM в современном мире.
13. Единая система идентификации и аутентификации.
14. Использование «облачных» технологий при реализации механизмов безопасности и многоагентные системы.
15. Интегрированные решения по защите информации на с Интернет вещей.
16. Направление исследований на примере проектов DARPA и АНБ.
17. Мобильные агенты и их использование.
18. Интеллектуальные системы предупреждения вторжений.
19. Понятие Интернет вещей.
20. Современные СЗИ. Примеры использования.
21. Антивирусы как средство защиты от вредоносного ПО.
22. Средства обнаружения атак на примере Snort и Surricata.
23. Система Enstein. Ее функционал и назначение.
24. Интеграция разных компонентов СЗИ ЕИАС.
25. Криптография в ЕИАС.
26. Аттестация объектов ЕИАС.
27. Регламент работы ЕИАС.
28. Методы перехвата информации и технология противодействия ССИВ.
29. Перспективные направления развития высокоскоростных сетей и их защиты.
30. Этичный хакинг.
31. Основные разработчики пакетов для квантовых вычислений.
32. Правила корреляции событий безопасности.
33. DLP-системы.
34. Технология ноуботов.

Примерные задания для тестирования- проверка сформированности компетенций ПК-9, ПК-14

1. IoT - это:
а) Понятие "Интернет-вещей"
б) Мобильное устойство.
в) Интернет-приложение.

2. DLP-системы служат для:
а) защиты от вредоносного ПО.
б) контроля утечки защищаемой информации.
в) доверенной загрузки ОС.

6. Учебно-методическое и информационное обеспечение дисциплины

6.1. Список источников и литературы

Источники
основные

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. Методы и средства защиты программного обеспечения [Электронный ресурс] : учеб.-метод. комплекс : для бакалавриата по направлению подготовки 090900 Информационная безопасность : по профилям: Организация и технология защиты информации, Комплексная защита объектов информатизации / Минобрнауки России, Федер. гос. бюджетное образоват. учреждение высш. проф. образования "Рос. гос. гуманитарный ун-т" (РГГУ), Ин-т информац. наук и технологий безопасности, Фак. информац. систем и безопасности, Каф. компьютерной безопасности ; [сост.: Казарин О. В. ; отв. ред. А. А. Тарасов]. - Электрон. дан. - Москва: РГГУ, 2013. - 30 с. - Режим доступа: http://elib.lib.rsuh.ru/elib/000009341. - Загл. с экрана. - ISBN 978-5-7281-1789-6.
3. 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

Дополнительная

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

1. Официальной сайт IBM, глобальная система сбора данных об инцидентах X-Force [Электронный ресурс]: Режим доступа: https://exchange.xforce.ibmcloud.com/, свободный. – Загл. с экрана.
2. Официальный сайт сообщества по проведению разведки в сети Интернет [Электронный ресурс]: Режим доступа: http://osintframework.com/, свободный. – Загл. с экрана.
3. Официальный сайт компании Ineltechniques [Электронный ресурс]: Режим доступа: https://inteltechniques.com/services.html, свободный. – Загл. с экрана.

7. Материально-техническое обеспечение дисциплины

Для проведения занятий необходимо следующее материально-техническое обеспечение:
1) лекционный класс с видеопроектором и компьютером, на котором должны быть установлены:
– лицензионное ПО MS Windows 7 и старше;
– лицензионное ПО MS Office 2010 (с обязательным наличием MS PowerPoint) и старше

2) компьютерный класс, оборудованный современными персональными компьютерами для каждого студента с выходом в интернет. На компьютере должны быть установлены:
– лицензионное ПО MS Windows 7 и старше;
– лицензионное ПО MS Office 2010 и старше;
– система обнаружения вторжений Snort

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
8	Snort	Snort	Свободное ПО, Режим доступа: https://www.snort.org/downloads

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 практических занятий - проверка сформированности компетенций ПК-9, ПК-14

Темы учебной дисциплины предусматривают проведение практических(семинарских) занятий, 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.

Практическое занятие 1(4 ч.).Нормативно-методическая база использования. Краткий обзор руководящих документов (проверка сформированности компетенций ПК-9)

Вопросы для обсуждения:

1.Перечень основных нормативно-правовых документов.

2. Современные средства обнаружения вторжений.

3. Понятие многоагентной системы.

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.

Практическое занятие 2(4 ч.). Структура ЕИАС. Ознакомления студентов с механизмами аутентификации и идентификации (проверка сформированности компетенций ПК-9)

Вопросы для обсуждения:

1.Понятие ЕИАС.

2. Принцип системного подхода в организации ЗИ.

3. Вход в систему по паролю и публичному ключу.

4. Коллизии в функциях хеширования.

Список литературы:

Приведён в п. 6 данной РПД

Практическое занятие 3(8 ч.). Современные СЗИ. Приобретение навыков при работе с системами типа Snort (проверка сформированности компетенций ПК-14)

Вопросы для обсуждения:

1.Модель OSI

2. Snort. Функциональность системы.

3. Использование Barnyard для визуализации информации.

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 операционной системой CentOS 7, средство обнаружения вторжений Snort.

Практическое занятие 4(6 ч.). Обзор современных средств шифрования. Использование мобильных агентов (проверка сформированности компетенций ПК-14)

Вопросы для обсуждения:
1.Понятие мобильный агент.
2.Примеры алгоритмов шифрования.
3. Понятие криптостойкости алгоритмов шифрования.
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.

Приложение 1

АННОТАЦИЯ ДИСЦИПЛИНЫ

Дисциплина «Актуальные тенденции в области защиты информации» реализуется на факультете Информационных систем и безопасности для студентов 4-го курса, обучающихся по программе бакалавриата по направлению подготовки 10.03.01 Информационная безопасность (профили подготовки –№ 3 Комплексная защита объектов информатизации) кафедрой комплексной защиты информации.

Цель дисциплины: является ознакомление студентов с современными тенденциями в области защиты информации, новейшими подходами к построению подсистем информационной безопасности и актуальными изменениями в нормативно-методической базе в этой сфере.
Задачи:

- рассмотрение следующих актуальных тенденций в области защиты информации: интегрированные решения по защите информации, управление безопасностью информации и событий (SIEM-системы);
- управление учетными записями (IdAM-системы), унифицированный доступ к приложениям на примере Единой системы идентификации и аутентификации (ЕСИА),
- обеспечение безопасного взаимодействия с внешними информационными системами на примере Системы межведомственного электронного взаимодействия (СМЭВ),тенденции в применении средств криптографической защиты информации (средств легковесной криптографии), в том числе в системах электронного документооборота, использование «облачных» технологий при реализации механизмов безопасности;
- многоагентные системы в сфере информационной безопасности; безопасность Интернета вещей (Internet of Things, IoT).

Дисциплина направлена на формирование следующих компетенций:

- ПК-9 – способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности;
- ПК-14 – должен обладать способностью организовывать работу малого коллектива исполнителей в профессиональной деятельности.

В результате освоения дисциплины обучающийся должен:

Знать: перспективные направления развития информационной безопасности, наиболее актуальные решения в области криптографической, инженерно-технической и программно-аппаратной защиты информации, наиболее актуальные документы, создаваемые регуляторами в области информационной безопасности; особенности применения современных СЗИ для защиты персональных данных и информации, обрабатывающейся в государственных информационных системах; методологические и технологические основы работы малого коллектива исполнителей.
Уметь: ориентироваться на рынке современных средств защиты информации, выбирать оптимальное решение при проектировании и модернизации подсистемы информационной безопасности, выдвигать обоснованные предложения по применению таковых решений; разрабатывать модели и политику безопасности, используя известные подходы, методы, средства и их теоретические основы.

Владеть: навыками интеграции и эксплуатации наиболее актуальных средств защиты информации, использования современных средств криптографической защиты информации и систем контроля и управления доступом; навыками работы с системами защищенного документооборота; навыками работы с документацией.

По дисциплине предусмотрена промежуточная аттестация в форме зачета с оценкой.

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)*	*29.06.2017г..*	***10***
2	*Обновлена структура дисциплины (модуля) для очной формы обучения (2018 г.)*	*26.06.2018 г.*	***11***
3	*Обновлен состав программного обеспечения (ПО), современных профессиональных баз данных (БД) и информационно-справочные систем (ИСС)*	*26.06.2018 г.*	***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*	***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 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	*Тенденции в развитии современных средств защиты информации*	**8**	**4**		**4**			**16**	Опрос. Оценка выполнения практических заданий
2	*Нормативно-методическая база в области применения криптографической, инженерно-технической и программно-аппаратной защиты информации*	**8**	**4**		**4**			**16**	Опрос. Оценка выполнения практических заданий
3	*Интегрированные решения по защите информации*	**8**	**6**		**8**			**16**	Опрос. Оценка выполнения практических заданий Тест
4	*Использование «облачных» технологий при реализации механизмов безопасности и многоагентные системы*	**8**	**6**		**4**			**18**	Опрос. Оценка выполнения практических заданий
	Зачет	**8**							*Зачет по билетам*
	итого:		**20**		**22**			**66**	

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: К.т.н, доцент, А.С. Моляков

Приложение 3
к листу изменений

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

2. 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., промежуточная аттестация 18 ч., самостоятельная работа обучающихся 48 ч.

№ п/п	Раздел дисциплины/темы	Семестр	Виды учебной работы (в часах)						Формы текущего контроля успеваемости, форма промежуточной аттестации *(по семестрам)*
			контактная					Самостоятельная работа	
			Лекции	Семинар	Практические занятия	Лабораторные занятия	Промежуточная аттестация		
1	*Тенденции в развитии современных средств защиты информации*	**8**	**4**		**4**			**10**	Опрос. Оценка выполнения практических заданий
2	*Нормативно-методическая база в области применения криптографической, инженерно-технической и программно-аппаратной защиты информации*	**8**	**4**		**4**			**10**	Опрос. Оценка выполнения практических заданий
3	*Интегрированные решения по защите информации*	**8**	**6**		**8**			**10**	Опрос. Оценка выполнения практических заданий Тест
4	*Использование «облачных» технологий при реализации механизмов безопасности и многоагентные системы*	**8**	**6**		**4**			**18**	Опрос. Оценка выполнения практических заданий
	Экзамен	**8**					**18**		*Экзамен по билетам*
	итого:		**20**		**22**		**18**	**48**	

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.)

2. 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., промежуточная аттестация – 18 ч., самостоятельная работа обучающихся 54 ч.

№ п/п	Раздел дисциплины/темы	Семестр	Виды учебной работы (в часах)						Формы текущего контроля успеваемости, форма промежуточной аттестации *(по семестрам)*
			контактная					Самостоятельная работа	
			Лекции	Семинар	Практические занятия	Лабораторные занятия	Промежуточная аттестация		
1	*Тенденции в развитии современных средств защиты информации*	**8**	**4**		**4**			**12**	Опрос. Оценка выполнения практических заданий
2	*Нормативно-методическая база в области применения криптографической, инженерно-технической и программно-аппаратной защиты информации*	**8**	**4**		**4**			**12**	Опрос. Оценка выполнения практических заданий
3	*Интегрированные решения по защите информации*	**8**	**6**		**8**			**12**	Опрос. Оценка выполнения практических заданий Тест
4	*Использование «облачных» технологий при реализации механизмов безопасности и многоагентные системы*	**8**	**6**		**4**			**18**	Опрос. Оценка выполнения практических заданий
	Экзамен	**8**					**18**		*Экзамен по билетам*
	итого:		**20**		**22**		**18**	**54**	

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

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

2. Дополнить раздел Основная литература

Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения: учебник и практикум для вузов / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2020. — 312 с. — (Высшее образование). — ISBN 978-5-9916-9043-0. — Текст: электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/452368

Казарин, О. В. Надежность и безопасность программного обеспечения : учебное пособие для вузов / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2020. — 342 с. — (Высшее образование). — ISBN 978-5-534-05142-1. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/454453

2. Дополнить раздел **Дополнительная литература**

Щеглов, А. Ю. Защита информации: основы теории: учебник для бакалавриата и магистратуры / А. Ю. Щеглов, К. А. Щеглов. — Москва: Издательство Юрайт, 2020. — 309 с. — (Бакалавр и магистр. Академический курс). — ISBN 978-5-534-04732-5. — Текст: электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/449285

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

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:

К.т.н, доцент, А.С. Моляков