

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

**ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ
ИНФОРМАЦИИ. ОСНОВНАЯ ЧАСТЬ**

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

Форма обучения – очная

РПД адаптирована для лиц
с ограниченными возможностями
здоровья и инвалидов

Москва 2017

*Программно-аппаратные средства защиты информации. Основная часть
Рабочая программа дисциплины*

Составитель:

Кандидат технических наук, доцент кафедры КЗИ А.С. Моляков

Ответственный редактор

Кандидат технических наук, и.о. зав. кафедрой КЗИ Д.А. Митюшин

УТВЕРЖДЕНО

Протокол заседания кафедры
комплексной защиты информации

№ 6 от 24.01.2017 г. _____

ОГЛАВЛЕНИЕ

1. Пояснительная записка

1.1 Цель и задачи дисциплины

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

1.3. Место дисциплины в структуре образовательной программы

2. Структура дисциплины

3. Содержание дисциплины

4. Образовательные технологии

5. Оценка планируемых результатов обучения

5.1. Система оценивания

5.2. Критерии выставления оценок

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

6. Учебно-методическое и информационное обеспечение дисциплины

6.1. Список источников и литературы

6.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

7. Материально-техническое обеспечение дисциплины

8. Обеспечение образовательного процесса для лиц с ограниченными возможностями здоровья и инвалидов

9. Методические материалы

9.1. Планы лабораторных занятий

Приложения

Приложение 1. Аннотация дисциплины

Приложение 2. Лист изменений

1. Пояснительная записка

1.1. Цель и задачи дисциплины

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

Задачи: изучение основ построения подсистем информационной безопасности, освоение принципов использования программно-аппаратных средств защиты информации, выработка умений проведения оценки защищенности информационных систем.

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

Коды компетенции	Содержание компетенций	Перечень планируемых результатов обучения по дисциплине
<i>ОПК-3</i>	должен обладать способностью применять положения электротехники, электроники и схемотехники для решения профессиональных задач	Знать: архитектуру подсистем безопасности, смысл базовых понятий, таких как идентификация и аутентификация, разграничение доступа и т.д.; протоколы локальной и сетевой аутентификации. Уметь: осуществлять настройку политики учтенных записей, выполнять администрирование учетных записей пользователей на платформах Windows и Linux, идентифицировать слабые места и уязвимости подсистемы идентификации и аутентификации; разрабатывать матрицу разграничения доступа, реализовывать дискреционное разграничение доступа к объектам файловой системы и системного реестра. Владеть навыками администрирования подсистем безопасности, настройки системы управления учетными записями.
<i>ОПК-4</i>	должен обладать способностью понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации	Знать: линейку программно-аппаратных средств защиты информации. Уметь: осуществлять выбор программно-аппаратных средств защиты информации адекватных решаемым задачам. Владеть навыками установки, настройки и эксплуатации средств защиты информации.
<i>ОПК-7</i>	должен обладать способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации	Знать: подходы к тестированию программно-аппаратных средств защиты информации. Уметь: составлять методики

	и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	испытаний средств защиты информации. Владеть: навыками проверки работоспособности программно-аппаратных средств защиты информации, проведения функционального тестирования средств защиты информации, навыками организовать мероприятия по охране труда и технике безопасности.
--	---	--

1.3. Место дисциплины в структуре образовательной программы

«Программно-аппаратные средства защиты информации. Основная часть» является обязательной дисциплиной вариативной части блока Б1 учебного плана по направлению подготовки «Информационная безопасность».

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: "Администрирования подсистем защиты информации", "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., 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 (<i>по семестрам</i>)
			контактная					Самостоятельна я работа	
			Лекции	Семинар	Практические занятия	Лабораторные занятия	Промежуточная я аттестация		
1	Общие представления о программно-аппаратных средствах защиты информации	5	2					5	Опрос.
2	Средства идентификации и аутентификации	5	4			6		15	Опрос. Защита лабораторных работ.
3	Разграничение доступа	5	6			8		10	Опрос. Защита

	3.1. Дискреционное разграничение доступа 3.2. Полномочное разграничение доступа								лабораторных работ.
4	Регистрация событий безопасности	5	4			4		10	Опрос. Защита лабораторных работ.
5	Контроль целостности	5	4			4		8	Опрос. Защита лабораторных работ.
	экзамен						18		экзамен по билетам
	ИТОГО:		20			22	18	48	

3. Содержание дисциплины

№	Наименование раздела дисциплины	Содержание
1	Общие представления о программно-аппаратных средствах защиты информации	Общее понятие программно-аппаратных средств защиты информации. Типы программно-аппаратных средств защиты информации. Средства криптографической защиты информации. Генераторы псевдослучайных чисел. Аппаратные модули доверенной загрузки. Средства контроля внешних носителей. Межсетевое экранирование.
2	Средства идентификации и аутентификации	Понятия идентификации и аутентификации. Локальная аутентификация. Свойства хэш-функций. Алгоритм NTLM. Концепция Pluggable Authentication Module. Сетевой протокол аутентификации Kerberos. Атаки на подсистему аутентификации.
3	Разграничение доступа 3.1. Дискреционное разграничение доступа 3.2. Полномочное разграничение доступа	Дискреционное и мандатное разграничение доступа. Субъекты и объекты доступа. Структуры файловых систем NTFS и UFS, метаданные. Списки контроля доступа. Security Reference Monitor, авторизация.
4	Регистрация событий безопасности	Регистрация событий безопасности. Категории регистрируемых событий. Регистрация доступ к объектам файловой системы. Управление регистрационными журналами.
5	Контроль целостности	Процедура контроля целостности. Алгоритмы расчета контрольных сумм (CRC, MD5, SHA-1). Средства гарантийного удаления информации.

4. Образовательные технологии

№ п/п	Наименование раздела	Виды учебных занятий	Образовательные технологии
1	2	3	4
1.	Общие представления о программно-аппаратных средствах защиты информации	Лекция 1 Самостоятельная работа	Традиционная с использованием презентаций Выполнение задания Изучение материалов лекций
2	Средства идентификации и аутентификации	Лекция 2.1 Лекция 2.2 Лабораторное занятие 1. Самостоятельная работа	Традиционная с использованием презентаций Выполнение задания Изучение материалов лекций
3	Разграничение доступа 3.1. Дискреционное разграничение доступа 3.2. Полномочное разграничение доступа	Лекция 3.1 Лекция 3.2 Лекция 3.3 Лабораторное занятие 2. Самостоятельная работа	Традиционная с использованием презентаций Выполнение задания Изучение материалов лекций
4	Регистрация событий безопасности	Лекция 4.1 Лекция 4.2 Лабораторное занятие 3. Самостоятельная работа	Традиционная с использованием презентаций Выполнение задания Изучение материалов лекций
5	Контроль целостности	Лекция 5.1 Лекция 5.2 Лабораторное занятие 4. Самостоятельная работа	Традиционная с использованием презентаций Выполнение задания Изучение материалов лекций

5. Оценка планируемых результатов обучения

5.1. Система оценивания

Форма контроля	Макс. количество баллов	
	За одну работу	Всего
Текущий контроль:		
– опрос (темы 1-5)	5 баллов	30 баллов
– практическое задание (темы 2-3)	6 баллов	12 баллов
– практическое задание (темы 4-5)	7 баллов	24 балла
Промежуточная аттестация экзамен		40 баллов
Итого за дисциплину экзамен		100 баллов

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

100-балльная 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»	<p>Выставляется обучающемуся, если он глубоко и прочно усвоил теоретический и практический материал, может продемонстрировать это на занятиях и в ходе промежуточной аттестации.</p> <p>Обучающийся исчерпывающе и логически стройно излагает учебный материал, умеет увязывать теорию с практикой, справляется с решением задач профессиональной направленности высокого уровня сложности, правильно обосновывает принятые решения.</p> <p>Свободно ориентируется в учебной и профессиональной литературе.</p> <p>Оценка по дисциплине выставляется обучающемуся с учётом результатов текущей и промежуточной аттестации.</p> <p>Компетенции, закреплённые за дисциплиной, сформированы на уровне – «высокий».</p>
82-68/ C	«хорошо»/ «зачтено (хорошо)»/ «зачтено»	<p>Выставляется обучающемуся, если он знает теоретический и практический материал, грамотно и по существу излагает его на занятиях и в ходе промежуточной аттестации, не допуская существенных неточностей.</p> <p>Обучающийся правильно применяет теоретические положения при решении практических задач профессиональной направленности разного уровня сложности, владеет необходимыми для этого навыками и приёмами.</p> <p>Достаточно хорошо ориентируется в учебной и профессиональной литературе.</p> <p>Оценка по дисциплине выставляется обучающемуся с</p>

Баллы/ Шкала ECTS	Оценка по дисциплине	Критерии оценки результатов обучения по дисциплине
		учёт 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 выставляется 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 выставляется 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 контрольные вопросы для экзамена - проверка сформированности компетенций ОПК-3,ОПК-4,ОПК-7

1. Базовые сервисы безопасности.
2. Назначение и принцип работы утилиты «Ревизор 1».
3. Назначение и принцип работы утилиты «Ревизор 2».

4. Назначение и принцип работы утилиты ФИКС.
5. Идентификация и аутентификация и управление учетными записями пользователей в СУБД Oracle.
6. Разграничение доступа в СУБД Oracle.
7. Мандатное разграничение доступа в Oracle Label Security.
8. Схема аутентификации Нидхема-Шредера.
9. Протокол аутентификации Kerberos.
10. Назначение и принципы работы Oracle Database Vault.
11. Линейка продуктов ОКБ САПР.
12. Назначение и функциональные возможности АМДЗ Аккорд.
13. Типы СКЗИ и их функциональное назначение.
14. Линейка продуктов на рынке СЗИ.
15. Архитектура и состав СЗИ SecretNet.
16. Разграничение доступа к устройствам в SecretNet.
17. Полномочное управление доступом в SecretNet.
18. Контроль целостности в SecretNet.
19. Концепция замкнутой программной среды, реализация в SecretNet.
20. Средства анализа и поиска уязвимостей XSpider и MaxPatrol.
21. Архитектура и состав SafeNet.
22. Состав и назначение PCI Соболев.
23. Понятие «кольца защиты» ОС.
24. Аппаратные технологии поддержки виртуализации.
25. Принципы доменной защиты.
26. Понятие и особенность ролевой политики безопасности.
27. Транзакционная память и защита информации в Супер-ЭВМ.

Примерные задания для тестирования- проверка сформированности компетенций ОПК-3,ОПК-4,ОПК-7

1. Целью защиты информации являются:

- а) предотвращение утечки, искажения, утраты, блокирования или незаконного тиражирования информации.
- б) внедрение сторонних программных агентов.
- в) предотвращение чтения журналов регистрации.

2. Доверенная загрузка — это:

- а) сетевое устройство, подключаемое к материнской плате компьютера.
- б) загрузка различных операционных систем только с заранее определенных постоянных носителей (например, только с жесткого диска) после успешного завершения специальных процедур: проверки целостности технических и программных средств ПК (с использованием механизма пошагового контроля целостности) и аппаратной идентификации / аутентификации пользователя.
- в) загрузка операционной системы с внешних незарегистрированных носителей без контроля целостности образа операционной системы.

6. Учебно-методическое и информационное обеспечение дисциплины

6.1. Список источников и литературы

Источники основные

1. *Федеральный закон от 27 июля 2006 г. №149-ФЗ «Об информации, информационных технологиях и о защите информации» [Электронный ресурс] : Режим*

доступа : http://www.consultant.ru/document/cons_doc_LAW_61798/, свободный. – Загл. с экрана.

2. *Федеральный закон* от 27 июля 2006 г. №152-ФЗ «О персональных данных» [Электронный ресурс] : Режим доступа : http://www.consultant.ru/document/cons_doc_LAW_61801/, свободный. – Загл. с экрана.

3. *Федеральный закон* от 6 апреля 2011 г. №63-ФЗ «Об электронной подписи» [Электронный ресурс] : Режим доступа : http://www.consultant.ru/document/cons_doc_LAW_112701/, свободный. – Загл. с экрана.

4. *Федеральный закон* от 27 декабря 2002 г. №184-ФЗ «О техническом регулировании» [Электронный ресурс] : Режим доступа : http://www.consultant.ru/document/cons_doc_LAW_40241/, свободный. – Загл. с экрана.

Литература

основная

1. *Комплексная защита информации в корпоративных системах* : учеб. пособие / В.Ф. Шаньгин. — М. : ИД «ФОРУМ» : ИНФРА-М, 2017. — 592 с. — (Высшее образование: Бакалавриат). - Режим доступа: <http://znanium.com/catalog/product/546679>

2. *Шаньгин В.Ф. Защита компьютерной информации. Эффективные методы и средства* [Электронный ресурс] / В. Ф. Шаньгин. - М.: ДМК Пресс, 2010. - 544 с.: ил. - ISBN 978-5-94074-518-1. - Режим доступа: <http://znanium.com/catalog/product/408107>

Дополнительная

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

1. Официальный сайт ФСТЭК РФ [Электронный ресурс] : Режим доступа: <http://www.fstec.ru/>, свободный. – Загл. с экрана.

2. Сайт компании ОКБ САПР [Электронный ресурс] : Режим доступа: <http://www.okbsapr.ru/>, свободный. – Загл. с экрана.

6.3. Перечень БД и ИСС

№п/п	Наименование
1	Международные реферативные наукометрические БД, доступные в рамках национальной подписки в 2017 г. Web of Science Scopus
2	Профессиональные полнотекстовые БД, доступные в рамках национальной подписки в 2017 г. Журналы Oxford University Press ProQuest Dissertation & Theses Global SAGE Journals Журналы Taylor and Francis
3	Компьютерные справочные правовые системы Консультант Плюс, Гарант

7. Материально-техническое обеспечение дисциплины

Для проведения занятий необходимо следующее материально-техническое обеспечение:

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

– лицензионное ПО MS Windows 7 и старше;

– лицензионное ПО MS Office 2010 (с обязательным наличием MS PowerPoint) и старше

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

– лицензионное ПО MS Windows 7 и старше;

– лицензионное ПО MS Office 2010 и старше;

- программный гипервизор Vmware Player;
- система защиты информации SecretNet Studio 8.4, Dallas Lock 8.0;
- средство антивирусной защиты Kaspersky Endpoint Security

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	Secret Net Studio 8.4	Код безопасности	Свободное ПО, Режим доступа: http://securitycode.ru Демо-версия
8	Dallas Lock 8.0	Конфидент	Свободное ПО, Режим доступа: https://dallaslock.ru/ Демо-версия
9	Vmware Player 15.5 + Гостевая ОС CentOS 7	VMWare	Свободное ПО, Режим доступа: https://www.vmware.com/products/ Демо-версия Открытое ПО Режим доступа: https://www.centos.org/download/ Инсталляционный дистрибутив Linux

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

8. Обеспечение образовательного процесса для лиц с ограниченными возможностями здоровья

В ходе реализации дисциплины используются следующие дополнительные методы обучения, текущего контроля успеваемости и промежуточной аттестации обучающихся в зависимости от их индивидуальных особенностей:

- для слепых и слабовидящих:
 - лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением;
 - письменные задания выполняются на компьютере со специализированным программным обеспечением, или могут быть заменены устным ответом;

- обеспечивается индивидуальное равномерное освещение не менее 300 люкс;
- для выполнения задания при необходимости предоставляется увеличивающее устройство; возможно также использование собственных увеличивающих устройств;
- письменные задания оформляются увеличенным шрифтом;
- экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

- для глухих и слабослышащих:
 - лекции оформляются в виде электронного документа, либо предоставляется звукоусиливающая аппаратура индивидуального пользования;
 - письменные задания выполняются на компьютере в письменной форме;
 - экзамен и зачёт проводятся в письменной форме на компьютере; возможно проведение в форме тестирования.

- для лиц с нарушениями опорно-двигательного аппарата:
 - лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением;
 - письменные задания выполняются на компьютере со специализированным программным обеспечением;
 - экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

При необходимости предусматривается увеличение времени для подготовки ответа.

Процедура проведения промежуточной аттестации для обучающихся устанавливается с учётом их индивидуальных психофизических особенностей. Промежуточная аттестация может проводиться в несколько этапов.

При проведении процедуры оценивания результатов обучения предусматривается использование технических средств, необходимых в связи с индивидуальными особенностями обучающихся. Эти средства могут быть предоставлены университетом, или могут использоваться собственные технические средства.

Проведение процедуры оценивания результатов обучения допускается с использованием дистанционных образовательных технологий.

Обеспечивается доступ к информационным и библиографическим ресурсам в сети Интернет для каждого обучающегося в формах, адаптированных к ограничениям их здоровья и восприятия информации:

- для слепых и слабовидящих:
 - в печатной форме увеличенным шрифтом;
 - в форме электронного документа;
 - в форме аудиофайла.
- для глухих и слабослышащих:
 - в печатной форме;
 - в форме электронного документа.
- для обучающихся с нарушениями опорно-двигательного аппарата:
 - в печатной форме;
 - в форме электронного документа;
 - в форме аудиофайла.

Учебные аудитории для всех видов контактной и самостоятельной работы, научная библиотека и иные помещения для обучения оснащены специальным оборудованием и учебными местами с техническими средствами обучения:

- для слепых и слабовидящих:
 - устройством для сканирования и чтения с камерой SARA CE;
 - дисплеем Брайля PAC Mate 20;
 - принтером Брайля EmBraille ViewPlus;
- для глухих и слабослышащих:

- автоматизированным рабочим местом для людей с нарушением слуха и слабослышащих;
- акустический усилитель и колонки;
- для обучающихся с нарушениями опорно-двигательного аппарата:
 - передвижными, регулируемые эргономическими партами СИ-1;
 - компьютерной техникой со специальным программным обеспечением.

9. Методические материалы

9.1. Планы лабораторных занятий - проверка сформированности компетенций ОПК-3, ОПК-4, ОПК-7

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

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

Тематика лабораторных работ соответствует программе курса.

Лабораторное занятие 1(6 ч.). Основные сервисы безопасности (проверка сформированности компетенций ОПК-3, ОПК-4)

Цель работы: получение практических навыков о сервисах безопасности современных продуктов.

Указания по выполнению задания: обратить внимание на базовые механизмы реализации защиты.

Выполнение задания:

В ходе практической работы студенты знакомятся с основными подходами в области реализации сервисов безопасности операционной систем на примере CentOS 7.

Контрольные вопросы:

1. Понятие сервис безопасности.
2. Архитектура реализации сервисов безопасности.
3. Функциональность сервисов безопасности.

Список литературы:

Приведён в п. 6 данной РПД

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

Лабораторное занятие 2(8ч.). Средства аутентификации и идентификации ПАСЗИ защиты от НСД (проверка сформированности компетенций ОПК-3,ОПК-4)

Цель работы: получение практических навыков в разработке и эксплуатации средств аутентификации и идентификации .

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

Выполнение задания:

В ходе практической работы студенты знакомятся с штатными средствами аутентификации и идентификации.

Контрольные вопросы:

- 1.Функции хеширования паролей.
2. Политики безопасности и их реализация в современных ОС.
3. Механизмы идентификации пользователей в ПАСЗИ Secret Net Studio.
4. Идентификация пользователей в ПАСЗИ Dallas Lock.

Список литературы:

Приведён в п. 6 данной РПД

1. *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. Должен быть настроен доступ по ssh и rdp с консоли централизованного управления к удаленным клиентам. Занятия проводятся в специально оборудованном компьютерном классе.

Лабораторное занятие 3(4 ч.). Регистрация событий безопасности ПАСЗИ защиты от НСД (проверка сформированности компетенций ОПК-4,ОПК-7)

Цель работы: получение практических навыков в проведении аудита и регистрации событий ИБ.

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 недеklarированных возможностей».

Выполнение задания:

В ходе практической работы проводится аудит и анализируются события ИБ на предмет угроз.

Контрольные вопросы:

1. Понятие аудит безопасности
2. Классификация событий ИБ на предмет угроз.
3. Составление отчета о проведенной аудите.
4. Работа с журналами безопасности. Настройка аудита в ПАСЗИ Dallas Lock и Secret Net Studio.

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, ПАСЗИ Secret Net Studio 8.4, Dallas Lock 8.0. Занятия проводятся в специально оборудованном компьютерном классе.

Лабораторное занятие 4(4 ч.). Средства контроля целостности ПАЗСИ защиты от НСД (проверка сформированности компетенций ОПК-3,ОПК-4,ОПК-7)

Цель работы: получение практических навыков в исследовании средств контроля целостности.

Указания по выполнению задания: обратить внимание на современные программно-аппаратные средства контроля целостности.

Выполнение задания:

В ходе практической работы студенты приобретают навыки работы со средствами гарантированного удаления информации, знакомятся с принципами контроля целостности ПО.

Контрольные вопросы:

1. Средства доверенной загрузки.
2. Понятие BIOS и механизмы контроля целостности ОС на этапе загрузки.
3. Примеры популярных на рынке решений ПО по контролю целостности.

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. Занятия проводятся в специально оборудованном компьютерном классе.

АННОТАЦИЯ ДИСЦИПЛИНЫ

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

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

Задачи: изучение основ построения подсистем информационной безопасности, освоение принципов использования программно-аппаратных средств защиты информации, выработка умений проведения оценки защищенности информационных систем.

Дисциплина направлена на формирование следующих компетенций:

- ОПК-3 – должен обладать способностью применять положения электротехники, электроники и схемотехники для решения профессиональных задач.
- ОПК-4 – должен обладать способностью понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации.
- ОПК-7 – должен обладать способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты.

В результате освоения дисциплины обучающийся должен:

Знать архитектуру подсистем безопасности, смысл базовых понятий, таких как идентификация и аутентификация, разграничение доступа и т.д.; протоколы локальной и сетевой аутентификации; линейку программно-аппаратных средств защиты информации; подходы к тестированию программно-аппаратных средств защиты информации.

Уметь осуществлять настройку политики учетных записей, выполнять администрирование учетных записей пользователей на платформах Windows и Linux, идентифицировать слабые места и уязвимости подсистемы идентификации и аутентификации; разрабатывать матрицу разграничения доступа, реализовывать дискреционное разграничение доступа к объектам файловой системы и системного реестра; осуществлять выбор программно-аппаратных средств защиты информации адекватных решаемым задачам; составлять методики испытаний средств защиты информации.

Владеть навыками администрирования подсистем безопасности, настройки системы управления учетными записями; навыками установки, настройки и эксплуатации средств защиты информации; навыками проверки работоспособности программно-аппаратных средств защиты информации, проведения функционального тестирования средств защиты информации; навыками организовать мероприятия по охране труда и технике безопасности.

По дисциплине предусмотрена промежуточная аттестация в форме экзамена.

Общая трудоёмкость освоения дисциплины составляет 3 зачётные единицы.

ЛИСТ ИЗМЕНЕНИЙ

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

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

Таблица 1

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

Перечень БД и ИСС

Таблица 2

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

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

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

Перечень ПО

Таблица 1

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

Перечень БД и ИСС

Таблица 2

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

	Гарант
--	--------

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

3. Состав программного обеспечения (ПО), современных профессиональных баз данных (БД) и информационно-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 Statistics 22	IBM	лицензионное
7	Microsoft Share Point 2010	Microsoft	лицензионное
8	SPSS Statistics 25	IBM	лицензионное
9	Microsoft Office 2013	Microsoft	лицензионное
10	ОС «Альт Образование» 8	ООО «Базальт СПО	лицензионное
11	Microsoft Office 2013	Microsoft	лицензионное
12	Windows 10 Pro	Microsoft	лицензионное
13	Kaspersky Endpoint Security	Kaspersky	лицензионное
14	Microsoft Office 2016	Microsoft	лицензионное
15	Visual Studio 2019	Microsoft	лицензионное
16	Adobe Creative Cloud	Adobe	лицензионное

Перечень БД и ИСС

№п /п	Наименование
1	Международные реферативные наукометрические БД, доступные в рамках национальной подписки в 2019 г. Web of Science Scopus
2	Профессиональные полнотекстовые БД, доступные в рамках национальной подписки в 2019 г. Журналы Cambridge University Press ProQuest Dissertation & Theses Global SAGE Journals Журналы Taylor and Francis
3	Профессиональные полнотекстовые БД JSTOR Издания по общественным и гуманитарным наукам Электронная библиотека Grebennikon.ru
4	Компьютерные справочные правовые системы

	Консультант Плюс, Гарант
--	-----------------------------

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

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

Структура дисциплины (модуля) для очной формы обучения

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

№ п/п	Раздел дисциплины/темы	Семестр	Виды учебной работы (в часах)						Формы текущего контроля успеваемости, форма промежуточной аттестации (по семестрам)
			контактная					Самостоятельна я работа	
			Лекции	Семинар	Практические занятия	Лабораторные занятия	Промежуточно я аттестация		
1	Общие представления о программно-аппаратных средствах защиты информации	5	2					9	Опрос.
2	Средства идентификации и аутентификации	5	4			6		10	Опрос. Защита лабораторных работ.
3	Разграничение доступа 3.1. Дискреционное разграничение доступа 3.2. Полномочное разграничение доступа	5	6			8		15	Опрос. Защита лабораторных работ.
4	Регистрация событий безопасности	5	4			4		10	Опрос. Защита лабораторных работ.
5	Контроль целостности	5	4			4		10	Опрос. Защита лабораторных работ.
	Промежуточная аттестация	5					18		экзамен по билетам
	итоги:		20			22	18	54	

5. 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>

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>

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

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

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

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

Перечень БД и ИСС

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

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

Состав программного обеспечения (ПО)

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

Составитель:

К.т.н, доцент, А.С. Моляков