МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Воронежский государственный университет»

«Утверждаю»
Заведующий кафедрой ТО и ЗИ

«05» июля 2018 г.  А.А. Сирота

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Б1.В.01 Информационная безопасность облачных систем

1. Шифр и наименование направления подготовки/специальности:
02.04.01 Математика и компьютерные науки

2. Профиль подготовки/специализации: компьютерное моделирование и искусственный интеллект

3. Квалификация (степень) выпускника: магистр

4. Форма образования: очная

5. Кафедра, отвечающая за реализацию дисциплины:
Кафедра технологий обработки и защиты информации

6. Составители программы:
Дрюченко Михаил Анатольевич, к.т.н., доцент

7. **Рекомендована:**
Научно-методическим советом ФКН, протокол № 6 от 25.06.2018 г.

(отметки о продлении вносятся вручную)

8. Учебный год: 2018/2019 **Семестр(-ы):** 1

9. Цели и задачи учебной дисциплины: изучение современных технологий построения архитектур информационных и вычислительных систем, технологий виртуализации, тенденций развития облачных вычислений, основных моделей предоставления услуг облачных вычислений, вопросов обеспечения конфиденциальности и целостности информации в системах, использующих облачные вычисления; получение профессиональных компетенций в области современных технологий защиты информации.

Основные задачи дисциплины:

- формирование у студентов основополагающих представлений о тенденциях развития современных инфраструктурных решений, технологиях виртуализации;
- ознакомление студентов с общими понятиями облачных вычислений, моделями облачных вычислений, спецификой современных угроз в «Облаке», традиционными атаками на программное обеспечение, функциональными атаками на элементы облака, атаками на клиента, угрозами виртуализации;
- ознакомление студентов с практическими аспектами обеспечения безопасности облачных инфраструктур;
- овладение практическими навыками применения на практике теоретических знаний для создания защищенных приложений и предоставления их в виде «облачных» сервисов.

10. Место учебной дисциплины в структуре ООП: учебная дисциплина относится к блоку обязательных дисциплин вариативной части.

Для успешного освоения дисциплины необходимы входные знания в области устройства ЭВМ и операционных систем, принципах их работы, сетевых технологий, криптографии, информатики.

11. Планируемые результаты обучения по дисциплине/модулю (знания, умения, навыки), соотнесенные с планируемыми результатами освоения образовательной программы (компетенциями выпускников):

Компетенция		Планируемые результаты обучения
Код	Название	
ОПК-3	готовность самостоятельно создавать прикладные программные средства на основе современных информационных технологий и сетевых ресурсов	**знать:** современные методы и средства разработки приложений; **уметь:** использовать стандартные инструменты и среды программирования для разработки, отладки и тестирования прикладных программ; **владеть:** практическими навыками использования современных программных средств для разработки, отладки и тестирования программ
ПК-1	способность к интенсивной научно-исследовательской работе	**знать:** тенденции развития современных инфраструктурных решений, особенности технологий виртуализации и виртуальных машин, модели облачных вычислений, основные риски информационной безопасности облачных вычислений и классы угроз в облаке, основные классы уязвимостей в сетях TCP/IP, разновидности сетевых атак, типы межсетевых экранов, протоколы для обеспечения безопасности сетевого соединения (IPsec, SSL/TLS, SSH), средства обеспечения целостности, репликации, защиты от сбоев; **уметь**: находить, анализировать, систематизировать профессиональную информацию, применять на практике идеи обеспечения безопасности «облачной» ИТ-инфраструктуры; **владеть**: практическими навыками анализа и систематизации информации, навыками работы со специализированными инструментальными средствами и средами разработки

12. Объем дисциплины в зачетных единицах/час — 3/108.

Форма промежуточной аттестации: *зачет*.

13. Виды учебной работы:

Вид учебной работы	Трудоемкость (часы)			
	Всего	По семестрам		
		№ сем.2	№ сем.	Итого
Аудиторные занятия	54	54		54
в том числе: лекции	18	18		18
практические	-	-		-
лабораторные	36	36		36
Самостоятельная работа	54	54		54
Форма промежуточной аттестации *(зачет – __ час. / экзамен – 0 час.)*	-	-		-
Итого:	108	108		108

13.1 Содержание дисциплины:

№ п/п	Наименование раздела дисциплины	Содержание раздела дисциплины
1. Лекции		
1.1	Современные тенденций развития инфраструктурных решений, которые привели к появлению концепции облачных вычислений	Этапы развития аппаратного обеспечения. Blade-системы, системы хранения данных, сети хранения данных. Консолидация ИТ-инфраструктуры. Концепция виртуальной среды. Типы виртуализации. Программная и аппаратная виртуализация, паравиртуализация и бинарная трансляция, виртуализация уровня ОС, виртуализация серверов, приложений, хранилища, данных, СУБД.
1.2	Общее понятие о технологии облачных вычислений (Cloud Computing)	Модели облачных вычислений (инфраструктура как сервис IaaS, платформа как сервис PaaS, программное обеспечение как сервис SaaS, безопасность как сервис SecaaS). Категории «облаков». Обзор существующих сервисов и платформ. Обзор решений ведущих вендоров (Microsoft, Amazon, Google). Облочные технологии с открытим кодом (CloudStack, OpenStack, CloudFoundry, OpenNebula, Eucalyptus).
1.3	Безопасность облачных технологий	Классы угроз в «Облаке». Атаки на программное обеспечение (уязвимости сетевых протоколов, операционных систем). Функциональные атаки на элементы облака (DoS-, EDos-атаки, SQL-инъекции). Атаки на клиента (уязвимость подключения к «облаку» через браузер, атаки межсайтингового выполнения сценариев XSS, перехваты web-сессий, атаки типа «человек посредине»). Угрозы виртуализации (атаки на виртуальные машины, гипервизор, системы управления). Руткиты Blue Pill и SubVirt. Комплексные угрозы, связанные с управляемостью «облаком» как единой информационной системой. Протоколы для обеспечения безопасности сетевого соединения (IPsec, SSL/TLS, SSH). Сертификаты. Межсетевые экраны. Технические и организационные меры для обеспечения безопасности виртуальной инфраструктуры. Средства обеспечения целостности, репликации, защиты от сбоев. «Облачные» антивирусы. Принципы обеспечения безопасности известных платформ «облачных сервисов» Windows Azure, Amazon Web Services (средства аутентификации и управления личностью, шифрования, обеспечения целостности, изолированности, доступности данных, безопасности БД, средства сертификации).
2. Практические занятия		
2.1	нет	
3. Лабораторные работы		
3.1	Безопасность облачных технологий	1. Изучение принципов работы атак типа SQL- injection. 2. Исследование средств идентификации и эксплуатации уязвимостей web-приложений к атакам межсайтингового выполнения сценариев (XSS).

		3. Изучение принципов действия атаки типа «человек посредине». 4. Изучение принципов действия атак типа отказ в обслуживании (DoS-атак). 5. Изучение методов и средств идентификации уязвимостей web-приложений (на примере сканеров безопасности общего назначения).

13.2. Темы (разделы) дисциплины и виды занятий

№ п/п	Наименование раздела дисциплины	Виды занятий (часов)			
		Лекции	Лабораторные	Сам. работа	Всего
1	Современные тенденций развития инфраструктурных решений, которые привели к появлению концепции облачных вычислений	4	-	16	20
2	Общее понятие о технологии облачных вычислений	8	10	28	46
3	Безопасность облачных технологий	6	8	28	42
	Итого:	18	18	72	108

14. Методические указания для обучающихся по освоению дисциплины

(рекомендации обучающимся по освоению дисциплины: работа с конспектами лекций, презентационным материалом, выполнение практических заданий, тестов, заданий текущей аттестации и т.д.)

1) При изучении дисциплины рекомендуется использовать следующие средства**:**

- рекомендуемую основную и дополнительную литературу;
- методические указания и пособия;
- контрольные задания для закрепления теоретического материала;
- электронные версии учебников и методических указаний для выполнения лабораторно - практических работ (при необходимости материалы рассылаются по электронной почте).

2) Для максимального усвоения дисциплины рекомендуется проведение письменного опроса (тестирование, решение задач) студентов по материалам лекций и практических работ. Подборка вопросов для тестирования осуществляется на основе изученного теоретического материала. Такой подход позволяет повысить мотивацию студентов при конспектировании лекционного материала.

3) При проведении практических работ обеспечивается максимальная степень соответствия с материалом лекционных занятий и осуществляется экспериментальная проверка методов, алгоритмов и технологий обработки информации, излагаемых в рамках лекций.

15. Перечень основной и дополнительной литературы, ресурсов интернет, необходимых для освоения дисциплины:

(список литературы оформляется в соответствии с требованиями ГОСТ и используется общая сквозная нумерация для всех видов литературы)

а) основная литература:

№ п/п	Источник
1	Щербаков, Андрей Юрьевич. Современная компьютерная безопасность. Теоретические основы. Практические аспекты : учебное пособие для студ. вузов / А.Ю. Щербаков .— М. : Кн. мир, 2009 .— 351, [1] с. : ил., табл. — (Высшая школа) .— Библиогр.: с.350-351 .— ISBN 978-5-8041-0378-2.
2	Основы управления информационной безопасностью : [учебное пособие для студентов вузов, обучающихся по направлениям подготовки (специальностям) укрупненной группы специальностей 090000 - "Информ. безопасность"] / А.П. Курило [и др.] .— 2-е изд., испр. — Москва : Горячая линия-Телеком, 2014 .— 243 с. : ил., табл. — (Вопросы управления информационной безопасностью ; Кн.1) .— Библиогр.: с.234-239 .— ISBN 978-5-9912-0361-6.

3	Краковский, Ю.М. Информационная безопасность и защита информации : учебное пособие для студ. обуч. по специальности «Информационные системы и технологии» днев. и заоч. форм обучения / Ю.М. Краковский .— М. ; Ростов н/Д : МарТ, 2008 .— 287 с. : ил .— (Учебный курс) .— Библиогр.: с.221 .— ISBN 978-5-241-00925-8.

б) дополнительная литература:

№ п/п	Источник
4	Таненбаум, Эндрю. Архитектура компьютера : пер. с англ. / Э.Таненбаум .— 4-е изд. — СПб. [и др.] : Питер, 2006 .— 698 с. : ил. табл. — (Классика Computer Science) .— Парал. тит. л. англ. — Библиогр. : с.654-664 .— Алф. указ. : с.685-698 .— ISBN 5-318-00298-6.
5	Голуб, В.А. Информационная безопасность электронной почты : учебное пособие для вузов / В.А. Голуб ; Воронеж. гос. ун-т .— Воронеж : ЛОП ВГУ, 2006 .— 39 с. — Библиогр.: с.38 .— <URL:http://www.lib.vsu.ru/elib/texts/method/vsu/may07044.pdf>.
6	Левин М. Безопасность в сетях Internet и Intranet / М. Левин. – М.: Познават. кн. плюс, 2001. – 319 с.
7	Браун С. Виртуальные частные сети / С. Браун. – М.: Лори, 2001. – 508 с.
8	Теоретические основы компьютерной безопасности (учеб. пособие для ВУЗов) / П.Н. Девянин [и др.]. – М.: Радио и связь, 2000 – 192с.

в)информационные электронно-образовательные ресурсы (официальные ресурсы интернет)*:

№ п/п	Источник
9	Электронный каталог Научной библиотеки Воронежского государственного университета. – (http // www.lib.vsu.ru/).
10	Образовательный портал «Электронный университет ВГУ».– (https://edu.vsu.ru/)
11	ЭБС «Издательства «Лань», Договор №3010-06/71-14 от 25.11.2014, *ЭБС «Университетская библиотека online», Договор №3010-06/70-14 от 25.11.14, Национальный цифровой ресурс «РУКОНТ», Договор №ДС-208 от 01.02.2012*

16. Перечень учебно-методического обеспечения для самостоятельной работы

(учебно-методические рекомендации, пособия, задачники, методические указания по выполнению практических (контрольных) работ и др.)

№ п/п	Источник
1	Основы управления информационной безопасностью : [учебное пособие для студентов вузов, обучающихся по направлениям подготовки (специальностям) укрупненной группы специальностей 090000 - "Информ. безопасность"] / А.П. Курило [и др.] .— 2-е изд., испр. — Москва : Горячая линия-Телеком, 2014 .— 243 с. : ил., табл. — (Вопросы управления информационной безопасностью ; Кн.1) .— Библиогр.: с.234-239 .— ISBN 978-5-9912-0361-6.

17. Информационные технологии, используемые для реализации учебной дисциплины, включая программное обеспечение и информационно-справочные системы (при необходимости)

Для реализации учебного процесса используется:

ПО Microsoft в рамках подписок «Imagine»,ежегодные сублицензионные договоры № 56035/ВРН3739 и № 56036/ВРН3739 от 07.10.2016.

18. Материально-техническое обеспечение дисциплины:

(при использовании лабораторного оборудования указывать полный перечень, при большом количестве оборудования можно вынести данный раздел в приложение к рабочей программе)

1) Мультимедийная лекционная аудитория (корп.1а, ауд. № 479), ПК-Intel-i3, рабочее место преподавателя: проектор, видеокоммутатор, микрофон, аудиосистема, специализированная мебель: доски меловые 2 шт., столы 60 шт., лавки 30 шт., стулья 64 шт.; доступ к фондам учебно-методической документации и электронным библиотечным системам, выход в Интернет.

2) Компьютерный класс (корп. 1б, ауд. № 316п), ПК-Intel-Core2 30 шт., рабочее место преподавателя: проектор, видеокоммутатор, специализированная мебель: доска маркерная 1 шт., доска интерактивная 1 шт., столы 32 шт., стулья 64 шт.; доступ к фондам учебно-методической документации и электронным изданиям, доступ к электронным библиотечным системам, выход в Интернет.

19. Фонд оценочных средств:

19.1 Перечень компетенций с указанием этапов формирования и планируемых результатов обучения

Код и содержание компетенции	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенции посредством формирования знаний, умений, навыков)	Этапы формирования компетенции (разделы (темы) дисциплины или модуля и их наименование)	ФОС* (средства оценивания)
ОПК-3 готовность самостоятельно создавать прикладные программные средства на основе современных информационных технологий и сетевых ресурсов	**знать:** современные методы и средства разработки приложений	Раздел 3 Безопасность облачных технологий.	Устный опрос, Лабораторные работы 1-5
	уметь: использовать стандартные инструменты и среды программирования для разработки, отладки и тестирования прикладных программ	Разделы 3 Безопасность облачных технологий.	Лабораторные работы 1-5
	владеть: практическими навыками использования современных программных средств для разработки, отладки и тестирования программ	Раздел 3 Безопасность облачных технологий	Лабораторные работы 1-5
ПК-1 способность к интенсивной научно-исследовательской работе	**знать:** тенденции развития современных инфраструктурных решений, особенности технологий виртуализации и виртуальных машин, модели облачных вычислений, основные риски информационной безопасности облачных вычислений и классы угроз в облаке, основные классы уязвимостей в сетях TCP/IP, разновидности сетевых атак, типы межсетевых экранов, протоколы для обеспечения безопасности сетевого соединения (IPsec, SSL/TLS, SSH), средства обеспечения целостности, репликации, защиты от сбоев	Разделы 1-3 Современные тенденций развития инфраструктурных решений, которые привели к появлению концепции облачных вычислений. Общее понятие о технологии облачных вычислений. Безопасность облачных технологий	Контрольная работа по разделам дисциплины
	уметь: находить, анализировать, систематизировать профессиональную информацию, применять на практике идеи обеспечения безопасности «облачной» ИТ-инфраструктуры	Разделы 1-3 Современные тенденций развития инфраструктурных решений, которые привели к появлению концепции облачных вычислений. Общее понятие о технологии облачных вычислений. Безопасность облачных технологий	Устный опрос, Лабораторные работы 1-5
	владеть: практическими навыками анализа и систематизации информации, навыками работы со специализированными инструментальными средствами и средами разработки	Разделы 1-3 Современные тенденций развития инфраструктурных решений, которые привели к появлению концепции облачных вычислений. Общее понятие о технологии облачных вычислений. Безопасность облачных технологий	Устный опрос, Лабораторные работы 1-5

19.2. Описание критериев и шкалы оценивания компетенций (результатов обучения) при промежуточной аттестации

Для оценивания результатов обучения на экзамене используются следующие содержательные показатели (формулируется с учетом конкретных требований дисциплины):

1) знание теоретических основ учебного материала, основных определений, понятий и используемой терминологии;

2) умение связывать теорию с практикой, умение выявлять и анализировать основные закономерности, полученные, в том числе, в ходе выполнения практических заданий;

3) умение обосновывать свои суждения и профессиональную позицию по излагаемому вопросу;

4) владение навыками программирования в рамках выполняемых практических заданий;

5) владение навыками проведения компьютерного эксперимента, тестирования алгоритмов обработки информации.

Различные комбинации перечисленных показателей определяют критерии оценивания результатов обучения (сформированности компетенций) на государственном экзамене:

- высокий (углубленный) уровень сформированности компетенций;
- повышенный (продвинутый) уровень сформированности компетенций;
- пороговый (базовый) уровень сформированности компетенций.

Для оценивания результатов обучения на государственном экзамене используется 4-балльная шкала: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно». Для оценивания результатов обучения на зачете используется – зачтено, не зачтено по результатам тестирования.

Соотношение показателей, критериев и шкалы оценивания результатов обучения представлено в следующей таблице.

Критерии оценивания компетенций и шкала оценок на зачет

Критерии оценивания компетенций	Уровень сформированности компетенций	Шкала оценок
Обучающийся демонстрирует полное соответствие знаний, умений, навыков по приведенным критериям оперирует понятийным аппаратом и приобретенными знаниями, умениями, применяет их при решении практических задач.	Базовый уровень	Зачтено
Ошибочное изложение двух вопросов контрольно-измерительного материала, непонимание существа постановки задачи. Обучающийся демонстрирует отрывочные, фрагментарные знания, допускает грубые ошибки	–	Не зачтено

19.3. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующие этапы формирования компетенций в процессе освоения образовательной программы

19.3.1 Примерный перечень применяемых оценочных средств

№ п/п	Наименование оценочного средства	Представление оценочного средства в фонде	Критерии оценки
1	2	3	4
1	Устный опрос	Вопросы по темам/разделам дисциплины	Правильный ответ – зачтено, неправильный или принципиально неточный ответ - не зачтено
2	Контрольная работа по разделам дисциплины	Теоретические вопросы по темам/разделам дисциплины	Шкала оценивания соответствует приведенной в разделе 19.2

3	Лабораторная работа	Содержит 5 лабораторных заданий	При успешном выполнении работы осуществляется допуск к зачету
4	КИМ промежуточной аттестации	Каждый контрольно-измерительный материал для проведения промежуточной аттестации включает 2 заданий вопросов для контроля знаний, умений и владений в рамках оценки уровня сформированности компетенции.	Шкалы оценивания приведены в разделе 19.2

19.3.2. Примерный перечень вопросов к зачету

№	Содержание
1	История и ключевые факторы развития облачных технологий
2	Системы хранения данных
3	Сети хранения данных
4	Технологии виртуализации
5	Преимущества и недостатки облачных вычислений
6	Модели облачных вычислений (*IaaS*, *PaaS*, *SaaS*)
7	Классы угроз в «облаке»
8	Безопасность виртуальной инфраструктуры и гипервизора
9	Функциональные атаки на элементы облака (SQL-инъекции)
10	Атаки на клиента (межсайтинговое выполнение сценариев XSS)
11	Топология сети для частного «облака»
12	Виды сетевых атак
13	Отказ в обслуживании (DoS, distributed DoS), экономический отказ в обслуживании (EDoS)
14	Атаки и инциденты в виртуальных средах
15	Средства синхронизации, репликации, защиты от сбоев
16	Руткиты
17	«Облачные» антивирусы
18	Принципы обеспечения безопасности известных платформ «облачных сервисов»

19.3.3. Примеры заданий для выполнения практических работ

Лабораторная работа № 1

«Изучение принципов работы атак типа SQL-injection»

Цель работы

Практическое изучение средств идентификации и эксплуатации уязвимостей в web-приложениях к атакам SQL-injection.

Форма контроля

Опрос в устной форме по результатам реализации SQL-инъекций.

Количество отведённых аудиторных часов - 8

Содержание работы

Для тестового web-приложения сформировать и ввести SQL-запросы, позволяющие выявить уязвимые параметры и получить данные из БД. Проанализировать полученные результаты и сформулировать выводы по проделанной работе.

Примеры контрольных вопросов:

1. Чем опасны атаки типа SQL-injection?
2. Как предотвратить атаку типа SQL-injection?

19.3.4. Пример контрольно-измерительного материала

УТВЕРЖДАЮ
Заведующий кафедрой технологий обработки и защиты информации

_____ А.А. Сирота
__.__.2018

Направление подготовки / специальность 02.04.01 Математика и компьютерные науки

Дисциплина Б1.В.01 Дополнительные главы информационной безопасности

Форма обучения Очное

Вид контроля Зачет

Вид аттестации Промежуточная

Контрольно-измерительный материал № 1

1. История и ключевые факторы развития облачных технологий
2. Функциональные атаки на элементы облака (SQL-инъекции)

Преподаватель _____ М.А. Дрюченко

19.4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Оценка знаний, умений и навыков, характеризующая этапы формирования компетенций в рамках изучения дисциплины осуществляется в ходе текущей и промежуточной аттестаций.

Текущая аттестация проводится в соответствии с Положением о текущей аттестации обучающихся по программам высшего образования Воронежского государственного университета. Текущая аттестация проводится в формах устного опроса (индивидуальный опрос, фронтальная беседа) и письменных работ (контрольные, лабораторные работы). При оценивании могут использоваться количественные или качественные шкалы оценок.

Промежуточная аттестация может включать в себя теоретические вопросы, позволяющие оценить уровень полученных знаний и/или практическое (ие) задание(я), позволяющее (ие) оценить степень сформированности умений и навыков.

При оценивании используется количественная шкала. Критерии оценивания приведены выше в таблице раздела 19.2.