ЕЛЕЦКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ им. И.А. БУНИНА

«УТВЕРЖДАЮ»
Директор института математики, естествознания и техники
_____/Н.В.Черноусова/

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.01.06 Обеспечение безопасности веб-приложений

Направление подготовки: *09.03.01 Информатика и вычислительная техника*
Направленность (профиль): *Компьютерные прикладные технологии*
Квалификация (степень): *бакалавр*
Форма обучения: *очная*

Институт: математики, естествознания и техники
Кафедра: математического моделирования, компьютерных технологий и информационной безопасности

	очная форма	**очно-заочная форма**	**заочная форма**
Курс	**4**		
Семестр	**7**		

Лекции	**36**		
Лабораторные занятия	**36**		
Практические (семинарские) занятия	**-**		
в т. ч. практическая подготовка	**-**		
Форма(ы) промежуточной аттестации	**Зачет с оценкой 0,2 (7 семестр)**		
Контроль	**-**		
Консультация	**2**		
Иные формы работы			
Самостоятельная работа	**69,8**		

Всего часов: 144
Трудоемкость: 4 зачетные единицы.
Разработчик(и) рабочей программы:
кандидат педагогических наук, доцент Таров Д.А

I. ОРГАНИЗАЦИОННО-МЕТОДИЧЕСКИЙ РАЗДЕЛ

Цель изучения дисциплины:

формирование у обучающихся знаний и умений по защите web-приложений применением современных программно-аппаратных средств.

Задачи изучения дисциплины:

- формирование у обучающихся знаний о методах и средствах обеспечения защиты web-приложений;
- ознакомление обучающихся с технологиями межсетевого экранирования;
- обучение обучающихся вопросам уровня защищенности информационных систем.

Место дисциплины в структуре ОПОП: реализуется в вариативной части (части, формируемой участниками образовательных отношений) блока Б1. Дисциплины (модули).

Планируемые результаты обучения по дисциплине:

Код компетенции	Индикаторы достижения компетенции	Планируемые результаты обучения по дисциплине
УК-1	**Знать:** – методы поиска информации и работы с ней; – сущность системного подхода;	**Знает:** – об основных механизмах и методиках поиска, синтеза информации; – примеры применения системного подхода при поиске и обработке информации;
	Уметь: – анализировать задачу, выделять этапы ее решения, осуществлять действия по решению; – находить различные варианты решения задачи, оценивать их преимущества и риски;	**Умеет:** – разрабатывать этапы решения поставленной задачи, выделяя ее основные составляющие; – производить разбор задачи с указанием этапов и конечных целей; – анализировать пути решения задачи с их оценкой и критическим анализом недостатков и достоинств; – разрабатывать наиболее оптимальные пути решения задачи;
	Владеть: – навыками оценивания практических последствий возможных вариантов решения задачи; – навыками грамотного, логичного, аргументированного формулирования собственных суждений и оценок.	**Владеет:** – навыками установления причинно-следственных связей и определения наиболее значимых среди них; – навыками осуществления поиска информации с применением современных технологий.
ПКС-1	**Знать:** – возможности существующей программно-технической архитектуры; – методологию разработки программного обеспечения и технологию программирова-	**Знает:** – методологии разработки и эксплуатации операционных систем; – языки формализации функциональных спецификаций – методы и приемы формализации задач; – методы и средства проектирования опера-

	ния; – методы и средства проектирования программного обеспечения; – типовые решения, библиотеки программных модулей, шаблоны, классы объектов, используемые при разработке программного обеспечения.	ционных систем; – принципы построения и виды архитектуры операционных систем; – типовые решения, библиотеки программных модулей, шаблоны, классы объектов, используемые при разработке операционных систем;
	Уметь: – проводить оценку и обоснование рекомендуемых решений; – вырабатывать варианты реализации программного обеспечения; – применять методы и средства проектирования программного обеспечения, структур данных, программных интерфейсов.	**Умее**т: – использовать существующие типовые решения и шаблоны проектирования операционных систем; – применять методы и средства проектирования операционных систем; – осуществлять коммуникации с заинтересованными сторонами; – выбирать средства реализации требований к операционным системам; – вырабатывать варианты реализации операционной системы и требований к ней; – проводить анализ исполнения требований;
	Владеть: – анализом возможностей реализации требований к программному обеспечению; – навыками распределения заданий между программистами в соответствии с техническими спецификациями; – методами проектирования структур данных; – методами проектирования программных интерфейсов; – навыками осуществления обучения и наставничества.	**Владеет:** – методологией и технологиями проектирования операционных систем; – действиями по разработке и согласованию технических спецификаций на компоненты операционной системы; – действиями по согласованию требований к операционной системе с заинтересованными сторонами, распределению заданий между программистами в соответствии с техническими спецификациями, осуществлению контроля выполнения заданий, формированию отчетности в соответствии с установленными регламентами.

II. СОДЕРЖАНИЕ И ОБЪЕМ ДИСЦИПЛИНЫ

с указанием количества часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу

Очная форма обучения

№	Наименование разделов и тем	Всего часов	Аудиторные занятия			Сам. Раб.
			ЛК	ПЗ	ЛБ	
Раздел 1. «Обнаружение компьютерных атак»		**37**	**8**		**8**	**21**
1	Тема 1. Понятие и классификация атак на компьютерные сети. Основные типы сетевых атак. Средства реализации атак. Механизмы типовых атак, основанных на уязвимо-	11	2		2	7

	стях сетевых протоколов. Атаки на сетевые службы. Атаки с использованием промежуточных узлов и территорий					
2	Тема 2. Технологии обнаружения компьютерных атак и их возможности. Прямые и косвенные признаки атак. Методы обнаружения атак. Сигнатурный анализ и обнаружение аномалий. Классификация систем обнаружения атак (СОА). Сетевые и узловые СОА. Требования, предъявляемые к СОА. Стандартизация в области обнаружения атак.	11	2		2	7
3	Тема 3. Архитектура СОА. Типовая архитектура СОА в составе сенсора, модуля управления, анализатора, набора протоколов взаимодействия и средства реагирования. Эксплуатация СОА. Варианты размещения СОА. Размещение сенсоров СОА. Реагирование на инциденты. Проблемы, связанные с СОА.	15	4		4	7
Раздел 2. «Технология межсетевого экранирования»		**45**	**12**		**12**	**21**
4	Тема 4. Стратегии и средства межсетевого экранирования. Создание защищенных сегментов при работе в сети Интернет с использованием межсетевых экранов. Требования руководящих документов ФСТЭК России к межсетевым экранам. Обзор документов RFC, регламентирующих использование межсетевых экранов. Типы межсетевых экранов. Схемы межсетевого экранирования.	15	4		4	7
5	Тема 5. Фильтрация пакетов. Критерии и правила фильтрации. Реализация пакетных фильтров. Понятие демилитаризованной зоны. Укрепленный компьютер бастионного типа. Организация узлов для отвлечения внимания злоумышленника. Особенности фильтрации различных типов трафика. Пакетный фильтр на базе ОС Windows. Служба RRAS. Программа управления службой RRAS.	15	4		4	7
6	Тема 6. Шлюзы прикладного уровня. Сервер SQUID, принципы работы, варианты конфигурации. Контроль HTTP-трафика и электронной почты. Написание правил фильтрации, возможности по анализу содержимого.	15	4		4	7
Раздел 3. «Организация виртуальных частных сетей»		**30**	**8**		**8**	**14**
7	Тема 7. Задачи, решаемые VPN. Туннелирование в VPN. Уровни защищенных каналов. Защита данных на канальном уровне. Организация VPN средствами протокола PPTP. Установка и настройка VPN. Анализ защищенности передаваемой информации. Защита данных на сетевом уровне. Протокол SKIP. Протокол IPSec. Организация VPN средствами СЗИ «VipNet». Использование протокола IPSec для защиты сетей. Шифрование трафика с использованием протокола IPSec. Настройка политики межсетевого экранирования с использованием протокола IPSec.	15	4		4	7
8	Тема 8. Организация VPN средствами СЗИ «StrongNet». Описание системы. Генерация и распространение ключе-	15	4		4	7

	вой информации. Настройка СЗИ «StrongNet». Установка защищенного соединения. Организация VPN прикладного уровня средствами протокола S/MIME и СКЗИ Крипто-Про CSP. Защищенный обмен электронной почтой.					
Раздел 4. «Технологии защищенной обработки информации»		**15**	**4**		**4**	**7**
9	Тема 9. Применение технологии терминального доступа. Общие сведения о технологии терминального доступа. Обеспечение безопасности сервера ОС. Настройка сервера MSTS. Настройка протокола RDP. Службы каталогов. Общие сведения о службах каталогов. Структура каталога LDAP. Система единого входа в сеть на основе протокола Kerberos. Создание единого пространства безопасности на базе Active Directory.	15	4		4	7
Раздел 5. «Аудит информационной безопасности в компьютерных сетях»		**14,8**	**4**		**4**	**6,8**
10	Тема 10. Цели и задачи проведения аудита безопасности. Этапы и методы проведения, результаты работ. Нормативно-правовые и организационные основы проведения аудита безопасности компьютерных систем. Международные, государственные и ведомственные стандарты и рекомендации в области информационной безопасности. Определение структуры информационно-телекоммуникационных сетей. Программные средства анализа топологии вычислительной сети. Определение маршрутов прохождения сетевых пакетов. Обнаружение объектов сети. Построение схемы сети. Выявление телекоммуникационного оборудования. Выявление и построение схемы информационных потоков защищаемой информации.	14,8	4		4	6,8
	Форма отчетности	**Зачет с оценкой**				
	Контроль					
	Консультация	**2**				
	Зачет с оценкой	***0,2***				
	Итого за 7 семестр	***144***	***36***		***36***	***69,8***
	в т.ч. практическая подготовка					
ИТОГО		**144**	**36**		**36**	**69,8**

Очно-заочная форма обучения не реализуется
Заочная форма обучения не реализуется

III. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

Текущая аттестация проводится в форме контрольной работы.

Типовой вариант контрольной работы

1. Создание защищенных сегментов при работе в сети Интернет с использованием межсетевых экранов. Применение фильтрующего маршрутизатора WinRoute.

2. Защита сетевого трафика с использованием протокола IPSec в Windows. Организация VPN средствами протокола PPTP.

3. Применение специализированных средств организации VPN на примере «VipNet» и «StrongNET».

4. Применение COA Snort для обнаружения скрытого сканирования, атак, использующих преднамеренное нарушение структуры сетевых пакетов, атак вида «отказ в обслуживании».

5. Применение технологии терминального доступа.

6. Применение программных средств аудита информационной безопасности с целью тестирования состояния защищенности компьютерных систем от несанкционированного доступа и выработки мер защиты от выявленных угроз.

Промежуточная аттестация обучающихся осуществляется в форме экзамена с использованием следующих оценочных материалов: *перечень вопросов к экзамену*.

Вопросы к зачету с оценкой
(7 семестр, очная форма обучения)

Теоретические вопросы

1. Атаки на протоколы и службы Интернет. Методы и средства защиты.

2. Понятие межсетевых экранов. Компоненты межсетевого экрана. Политика сетевой безопасности.

3. Критерии фильтрации пакетов. Основные схемы сетевой защиты на базе межсетевых экранов.

4. Создание защищенных сегментов сетей с использованием межсетевых экранов.

5. Конфигурирование сетевых фильтров на базе настроек безопасности протокола TCP/IP в ОС.

6. Защита рабочих станций с использованием персональных сетевых фильтров.

7. Организация VPN-сетей. Задачи, решаемые VPN. Туннелирование в VPN.

8. Электронные сертификаты. Понятие инфраструктуры открытых ключей.

9. Протоколы и средства организации VPN на сетевом уровне. Назначение, область применения, аутентификация и шифрование данных в протоколах SKIP и IPSec.

10. Протоколы PPTP, SSL. Назначение, область применения, аутентификация и шифрование данных.

11. Преимущества технологии терминального доступа. Обеспечение безопасности.

12. Назначение систем обнаружения атак. Классификация систем обнаружения атак.

13. Службы каталогов. Общие сведения о службах каталогов. Структура каталога LDAP.

14. Система единого входа в сеть на основе протокола Kerberos. Создание единого пространства безопасности на базе Active Directory.

15. Аудит безопасности компьютерных систем. Цели, стандарты, подходы.

16. Инструментальные средства аудита безопасности компьютерных систем, их возможности и недостатки. Применение инструментальных средств аудита безопасности компьютерных систем.

17. Тестирование состояния защищенности компьютерных систем от несанкционированного доступа с использованием сканеров безопасности. Методика проведения инструментальных проверок.

18. Классификация средств и информационных ресурсов в соответствии со стандартом ISO-17799.

19. Назначение и основные функции программных комплексов «Гриф-специалист» и «Кондор-специалист». Построение модели защиты компьютерной системы с использованием комплексной экспертной системы «АванГард».

20. Виды требований безопасности согласно ГОСТ Р ИСО/МЭК 15408-1-2002. «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий».

21. Назначение систем обнаружения атак. Классификация систем обнаружения атак. Использование системы обнаружения атак «Snort».

Практические вопросы

1. Разработайте политику для пакетного фильтра, разрешающего только получение информации с FTP-серверов. Реализуйте политику средствами сетевых фильтров.

2. Разработайте политику для пакетного фильтра, разрешающего только получение и отправку электронной почты. Реализуйте политику средствами сетевых фильтров.

3. Разработайте и реализуйте политику для пакетного фильтра, запрещающего сканирование внутренней структуры сети. Реализуйте политику средствами сетевых фильтров.

4. Разработайте и реализуйте политику для пакетного фильтра, запрещающего получение извне доступа к ресурсам компьютера за исключением двух доверенных узлов.

Реализуйте политику средствами сетевых фильтров.

5. Разработайте и реализуйте политику для пакетного фильтра, запрещающего получение доступа к Web-ресурсам определенного узла. Реализуйте политику средствами сетевых фильтров.

6. Разработайте и реализуйте политику для пакетного фильтра, разрешающего только получение доступа к Web-ресурсам двух определенных узлов. Реализуйте политику средствами сетевых фильтров.

7. Разработайте и реализуйте политику для пакетного фильтра, разрешающего только просмотр Web-ресурсов. Реализуйте политику средствами сетевых фильтров.

8. Разработайте политику для пакетного фильтра, разрешающего только получение информации с FTP-серверов. Реализуйте политику средствами протокола IPSec.

9. Разработайте политику для пакетного фильтра, разрешающего только получение и отправку электронной почты. Реализуйте политику средствами протокола IPSec.

10. Разработайте и реализуйте политику для пакетного фильтра, разрешающего только просмотр Web-ресурсов. Реализуйте политику средствами протокола IPSec.

11. С использованием программы «Брандмауэр Windows» (Windows Firewall) выполнить настройки, запрещающие использование всех портов защищаемого узла за исключением TCP-порта 3389.

12. Разработайте и реализуйте политику для пакетного фильтра, запрещающего сканирование внутренней структуры сети. Реализуйте политику средствами протокола IPSec.

13. Сгенерируйте и получите в виде файла сертификат открытого ключа с использованием образа OS.

14. Настройте Web-сервер для организации защищенного доступа к Web-странице с использованием протокола SSL. Выполнить с использованием образа ОС. Файл-сертификат открытого ключа прилагается.

15. Настройте входящее подключение VPN с использованием протокола PPTP. Настроить и установить подключение клиентского узла. Выполнить с использованием образа OS.

16. Осуществите криптографическую защиту сетевого трафика средствами протокола

IPSec в ОС. Перехватите в локальной сети пакеты, убедитесь в шифровании трафика.

17. Осуществите криптографическую защиту сетевого трафика средствами СКЗИ

StrongNet. Перехватите в локальной сети пакеты, убедитесь в шифровании трафика.

18. Организовать защищенный обмен почтовой информацией между двумя пользователями. Шифрование почтовых сообщений выполнить с помощью алгоритма ГОСТ 28147-89, реализуемого средствами СКЗИ КриптоПро CSP. Выполнить с использованием образов ОС.

19. Разработайте файл конфигурации и настройте СОА Snort на обнаружение тестирования внутренней структуры сети ICMP-запросами.

20. Разработайте файл конфигурации и настройте СОА Snort на обнаружение ICMP-

пакетов большой длины.

21. Разработайте файл конфигурации и настройте СОА Snort на обнаружение устанавливаемых из внешней сети TCP-соединений.

22. Установить службу терминального доступа. Выполнить настройки службы MSTS, разрешающие доступ к ресурсам терминального сервера только для учетных

записей, зарегистрированных в созданной по умолчанию группе «Remote Desktop Users».

23. Установить службу терминального доступа. Выполнить настройки протокола RDP, запрещающие использование ресурсов рабочей станции, включая буфер обмена, принтеры и накопители.

24. Выявите сетевые узлы в локальном сетевом сегменте с использованием: утилиты fping; утилиты ping и широковещательной ICMP-посылки; утилиты icmpush (тип ICMP-пакетов13 и 17); утилиты ping и многоадресной рассылки; утилиты arping; утилиты hping3 и методов TCP- и UDP-разведки; утилиты Ethereal и метода прослушивания сети.

25. С помощью утилиты nmap проведите сканирование портов сетевого узла. Сформируйте списки открытых TCP- и UDP-портов, идентифицируйте версии ОС и запущенных сервисов. По результатам сделайте вывод о возможности обнаружения открытых портов и идентификации типа и версии ОС, а также сетевых сервисов.

IV. ПЕРЕЧЕНЬ ЛИТЕРАТУРЫ, НЕОБХОДИМОЙ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

4.1. Основная литература

1. Ищейнов, В. Я. Информационная безопасность и защита информации: теория и практика : учебное пособие : / В. Я. Ищейнов. – Москва ; Берлин : Директ-Медиа, 2020. – 271 с. : схем., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=571485 (дата обращения: 01.09.2021). – Библиогр. в кн. – ISBN 978-5-4499-0496-6. – DOI 10.23681/571485. – Текст : электронный.

4.2. Дополнительная литература

1. Гультяева, Т. А. Основы защиты информации : учебное пособие : / Т. А. Гультяева. – Новосибирск : Новосибирский государственный технический университет, 2018. – 83 с. : ил., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=574730 (дата обращения: 01.09.2021). – Библиогр. в кн. – ISBN 978-5-7782-3641-7. – Текст : электронный.

V. ПЕРЕЧЕНЬ РЕСУРСОВ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ «ИНТЕРНЕТ», НЕОБХОДИМЫХ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

№ пп	Ссылка на информационный ресурс	Наименование разработки в электронной форме	Доступность
1.	http://edu.ru/	**Российское образование: Федеральный портал. Включает** ссылки на порталы и сайты образовательных учреждений; государственные образовательные стандарты; нормативные документы; каталог экскурсий и обучающих программ.	Свободный доступ
2.	http://citforum.ru/database/osbd/contents.shtml	Информационно-аналитические материалы	Свободный доступ

VI. СОВРЕМЕННЫЕ ПРОФЕССИОНАЛЬНЫЕ БАЗЫ ДАННЫХ И ИНФОРМАЦИОННЫЕ СПРАВОЧНЫЕ СИСТЕМЫ

1.	http://www.biblioclub.ru	Электронно-библиотечная система (ЭБС) Университетская библиотека онлайн	Регистрация через любой университетский компьютер. В дальнейшем предоставляется неограниченный индивидуальный доступ из любой точки, в которой имеется доступ к сети Интернет
2.	www.garant.ru	Информационно-правовой портал	Свободный доступ
3.	www.elibrary.ru	Российский информационный портал в области науки, технологии, медицины и образования	Свободный доступ
4.	www.consultant.ru	Российская компьютерная справочно-правовая система	Свободный доступ

VII. ЛИЦЕНЗИОННОЕ И СВОБОДНО РАСПРОСТРАНЯЕМОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

При реализации учебной дисциплины применяется следующее лицензионное и свободно распространяемое программное обеспечение:

- Microsoft Windows;
- Microsoft Office;
- Libre Office и др.

VIII. ОБОРУДОВАНИЕ И ТЕХНИЧЕСКИЕ СРЕДСТВА ОБУЧЕНИЯ, НЕОБХОДИМЫЕ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ

Учебные занятия проводятся в аудиториях, укомплектованных специализированной мебелью, в том числе стационарными или переносными техническими средствами обучения (проектор, экран, компьютер/ноутбук).

Лабораторные занятия, групповые и индивидуальные консультации, текущая и промежуточная аттестации проводятся в специализированных компьютерных классах. Перечень основного оборудования: автоматизированные рабочие места с компьютерами, программное обеспечение общего и профессионального назначения.

Самостоятельная работа проводится в кабинетах, оснащенных компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.