РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

1. НАИМЕНОВАНИЕ ДИСЦИПЛИНЫ

Информационная безопасность и компьютерные сети

2. УРОВЕНЬ ВЫСШЕГО ОБРАЗОВАНИЯ

Подготовка научно-педагогических кадров в магистратуре.

3. НАПРАВЛЕНИЕ ПОДГОТОВКИ, НАПРАВЛЕННОСТЬ (ПРОФИЛЬ) ПОДГОТОВКИ

Направление 01.04.02 «Прикладная математика и информатика». Направленность (профиль) «Системное программирование и компьютерные науки». Образовательная программа «Компиляторные технологии».

4. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОСНОВНОЙ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина входит в обязательную часть магистерской образовательной программы «Компиляторные технологии», изучается в 3-м семестре.

5. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ

Дисциплина участвует в формировании следующих компетенций образовательной программы:

Формируемые компетенции	Планируемые результаты обучения
Способность разрабатывать защищенное программное обеспечение, использовать современные методы защиты существующих вычислительных систем и исследовать их защищенность (СПК-32).	З1 (СПК-32) Знать: фундаментальные понятия современных сетей; базовые криптографические примитивы; способы реализации базовых сервисов безопасности в телекоммуникационных сетях — аутентификации, целостности, конфиденциальности; базовые принципы протоколов обеспечения безопасности сетевого и транспортного уровня; методы оценки безопасности защищенных систем. У1 (СПК-32) Уметь: проектировать реализации сервисов безопасности; программировать

	сетевой обмен с использованием средств безопасности транспортного уровня TLS. В1 (СПК-32) Владеть: навыками освоения большого объема информации; навыками самостоятельной работы с документацией по примитивам и сервисам безопасности; культурой разработки и реализации системного программного обеспечения современных компьютеров; навыками разработки и отладки программ, использующих средства безопасности транспортного уровня.

Оценочные средства для промежуточной аттестации приведены в Приложении.

6. ОБЪЕМ ДИСЦИПЛИНЫ

Объем дисциплины составляет 4 зачетные единицы, всего 144 часа.

72 часа составляет контактная работа с преподавателем – 32 часов занятий лекционного типа, 30 часов занятий семинарского типа (семинары, научно-практические занятия, лабораторные работы и т.п.), 0 часов индивидуальных консультаций, 2 часа групповых консультаций, 4 часа мероприятий текущего контроля успеваемости, 4 часа промежуточной аттестации.

72 часа составляет самостоятельная работа учащегося.

7. ВХОДНЫЕ ТРЕБОВАНИЯ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Учащиеся должны владеть знаниями по языкам программировании, программной инженерии и компьютерным сетям в объеме, соответствующем основным образовательным программам бакалавриата по укрупненным группам направлений и специальностей 01.00.00 «Математика и механика», 02.00.00 «Компьютерные и информационные науки».

8. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

В процессе обучения используются открытая консольная реализация протокола SSL openssl, сетевой сканер nmap, анализатор сетевых пакетов Wireshark, средство обнаружения вторжений Snort, прокси-сервер Squid.

В рамках курса предполагается проверку практических заданий выполнять в автоматизированном режиме с приемом решений студентов через сеть Интернет. Лекционный материал будет доступен в электронном виде.

9. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Наименование и краткое содержание разделов и тем дисциплины, форма промежуточной аттестации по дисциплине	**Всего (часы)**	В том числе								
		Контактная работа (работа во взаимодействии с преподавателем), часы из них						**Самостоятельная работа учащегося, часы** из них		
		Занятия лекционного типа	Занятия семинарского типа	Групповые консультации	Индивидуальные консультации	Учебные занятия, направленные на проведение текущего контроля успеваемости: коллоквиумы, практические контрольные занятия и др.	**Всего**	Выполнение домашних заданий	Подготовка рефератов и т.п..	**Всего**
Тема 1. Базовые понятии информационной безопасности. Направления в обеспечении ИБ. Безопасность Web.	**10**	4	2	-	-	-	**6**	4	-	**4**
Тема 2. Безопасная передача данных в недоверенной среде. Защита передаваемых данных.	**10**	4	2	-	-	-	**6**	4	-	**4**
Тема 3. Применение криптографии для задач защиты информации при передаче.	**14**	4	4	-	-	2	**10**	4	-	4

Тема 4. Защита хранимых данных и вычислительных ресурсов.	**14**	6	4	-	-	-	**10**	4	-	4
Тема 5. Особенности беспроводных и мобильных технологий. Их влияние на требования и подходы к безопасности.	**10**	2	2	-	-	2	**6**	4	-	4
Тема 6. Анонимность в сети.	**10**	4	2				**6**	4		4
Тема 7. Задача надёжного и масштабируемого распространения данных в сети	**10**	2	4				**6**	4	-	4
Тема 8. Потоковые данные и требования к качеству связи	**14**	4	6				**10**	4	-	4
Тема 9. Доступность ресурсов как цель для атаки. Атаки на исчерпание возможностей канала.	**10**	2	4				**6**	4	-	4
Промежуточная аттестация – практические задания, индивидуальное собеседование	**42**	-	-	2	-	4	**6**	36	-	**36**
Итого	**144**						**72**			**72**

10. УЧЕБНО-МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ УЧАЩИХСЯ

Самостоятельная работа учащихся состоит в изучении лекционного материала, учебно-методической литературы, подготовки к практическим заданиям текущего контроля и промежуточной аттестации.

11. РЕСУРСНОЕ ОБЕСПЕЧЕНИЕ

Основная учебно-методическая литература

1. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. М.: Триумф, 2003. — 806 с.
2. Таненбаум Э., Уэзеролл Д. Компьютерные сети. 5-е изд. — СПб.: Питер, 2012. — 960 с.
3. Мао В. Современная криптография. Теория и практика. М.: Вильямс, 2005. — 763 с.
4. Бехроуз А. Фороузан. Криптография и безопасность сетей. Бином. Лаборатория знаний, 2010 г. — 784 с.

Дополнительная учебно-методическая литература

1. Джеймс Куроуз, Кит Росс. Компьютерные сети. Нисходящий подход. Эксмо, 2016 г. - 912 с.
2. А. А. Болотов, С. Б. Гашков, А. Б. Фролов, А. А. Часовских. Элементарное введение в эллиптическую криптографию. УРСС, 2006. - 324 с.

Ресурсы информационно-телекоммуникационной сети «Интернет»

??. IETF RFC 4031. Security Architecture for the Internet Protocol. https://tools.ietf.org/html/rfc4031
2. Описание протоколов SSL/TLS. Информационный документ. ООО КриптоПро. https://www.cryptopro.ru/sites/default/files/docs/TLS_description.pdf
3. IETF RFC 5246. The Transport Layer Security (TLS) ProtocolVersion 1.2. https://tools.ietf.org/html/rfc5246

Информационные технологии, используемые в процессе обучения

В процессе обучения используются открытая консольная реализация протокола SSL openssl, сетевой сканер nmap, анализатор сетевых пакетов Wireshark, средство обнаружения вторжений Snort, прокси-сервер Squid.

Материально-техническая база

Для преподавания дисциплины требуется компьютерный класс, оборудованный маркерной или меловой доской, экраном и мультимедийный проектор. Компьютеры должны иметь подключение к сети Интернет.

12. ЯЗЫК ПРЕПОДАВАНИЯ

Русский

13. РАЗРАБОТЧИК ПРОГРАММЫ, ПРЕПОДАВАТЕЛИ

к.т.н. Маркин Юрий Витальевич (ustas@ispras.ru)
к.ф.-м.н. Гетьман Александр Игоревич (thorin@ispras.ru)

Приложение

Оценочные средства для промежуточной аттестации по дисциплине **«Информационная безопасность и компьютерные сети»**

Промежуточная аттестация состоит из нескольких этапов – выполнения трёх практических заданий, проверяющих приобретенные учащимся умения и навыки, и индивидуального собеседования, проверяющего приобретенные знания.

Средства для оценивания планируемых результатов обучения, критерии и показатели оценивания приведены ниже.

РЕЗУЛЬТАТ ОБУЧЕНИЯ	**КРИТЕРИИ и ПОКАЗАТЕЛИ ОЦЕНИВАНИЯ РЕЗУЛЬТАТА ОБУЧЕНИЯ из соответствующих карт компетенций**					**ОЦЕНОЧНЫЕ СРЕДСТВА**
	1	2	3	4	5	
	Неудовлетворительно	**Неудовлетворительно**	**Удовлетворительно**	**Хорошо**	**Отлично**	
З1 (СПК-32) Знать фундаментальные понятия современных сетей; базовые криптографические примитивы; способы реализации базовых сервисов безопасности в телекоммуникационных сетях — аутентификации, целостности, конфиденци-	Отсутствие знаний	Фрагментарные представления о фундаментальных понятиях современных сетей; базовых криптографических примитивах; способах реализации базовых сервисов безопасности в телекоммуникационных сетях — аутентификации, целостности, конфиденциальности; базовых принципах протоколов обеспечения безопасности сетевого и транспортного уровня; методах оценки	В целом сформированные, но неполные знания о фундаментальных понятиях современных сетей; базовых криптографических примитивах; способах реализации базовых сервисов безопасности в телекоммуникационных сетях — аутентификации, целостности, конфиденциальности; базовых принципах протоколов обеспечения безопасности сетевого и транспортного уров-	Сформированные, но содержащие отдельные пробелы знания о фундаментальных понятиях современных сетей; базовых криптографических примитивах; способах реализации базовых сервисов безопасности в телекоммуникационных сетях — аутентификации, целостности, конфиденциальности; базовых принципах протоколов обеспечения безопасности сетево-	Сформированные систематические знания о фундаментальных понятиях современных сетей; базовых криптографических примитивах; способах реализации базовых сервисов безопасности в телекоммуникационных сетях — аутентификации, целостности, конфиденциальности; базовых принципах протоколов обеспечения безопасности	индивидуальное собеседование

альности; базовые принципы протоколов обеспечения безопасности сетевого и транспортного уровня; методы оценки безопасности защищенных систем.		безопасности защищенных систем.	ня; методах оценки безопасности защищенных систем.	го и транспортного уровня; методах оценки безопасности защищенных систем.	сетевого и транспортного уровня; методах оценки безопасности защищенных систем.	
У1 (СПК-32) Уметь проектировать реализации сервисов безопасности; программировать сетевой обмен с использованием средств безопасности транспортного уровня TLS.	Отсутствие умений	Фрагментарные умения в области проектирования реализации сервисов безопасности; программирования сетевого обмена с использованием средств безопасности транспортного уровня TLS.	В целом сформированное, но не систематическое умение проектировать реализации сервисов безопасности; программировать сетевой обмен с использованием средств безопасности транспортного уровня TLS.	Сформированное, но содержащее отдельные пробелы умение проектировать реализации сервисов безопасности; программировать сетевой обмен с использованием средств безопасности транспортного уровня TLS.	Сформированное систематическое умение проектировать реализации сервисов безопасности; программировать сетевой обмен с использованием средств безопасности транспортного уровня TLS.	три практических задания
В1 (СПК-32) Владеть навыками освоения большого объема информации; навыками самостоятельной	Отсутствие навыков	Фрагментарное владение навыками освоения большого объема информации; навыками самостоятельной работы с документацией по примитивам и сервисам	В целом сформированное, но не систематическое владение навыками освоения большого объема информации; навыками самостоятельной работы с документацией	Сформированное, но содержащее отдельные пробелы владение навыками освоения большого объема информации; навыками самостоятельной работы с	Сформированное систематическое владение навыками освоения большого объема информации; навыками самостоятельной работы с документа-	три практических задания

работы с документацией по примитивам и сервисам безопасности; культурой разработки и реализации системного программного обеспечения современных компьютеров; навыками разработки и отладки программ, использующих средства безопасности транспортного уровня.		безопасности; культурой разработки и реализации системного программного обеспечения современных компьютеров; навыками разработки и отладки программ, использующих средства безопасности транспортного уровня.	по примитивам и сервисам безопасности; культурой разработки и реализации системного программного обеспечения современных компьютеров; навыками разработки и отладки программ, использующих средства безопасности транспортного уровня.	документацией по примитивам и сервисам безопасности; культурой разработки и реализации системного программного обеспечения современных компьютеров; навыками разработки и отладки программ, использующих средства безопасности транспортного уровня.	цией по примитивам и сервисам безопасности; культурой разработки и реализации системного программного обеспечения современных компьютеров; навыками разработки и отладки программ, использующих средства безопасности транспортного уровня.	

Фонды оценочных средств

Примерные практические задания для текущего контроля успеваемости.

ПКЗ ТК1. Отправить на почтовый адрес курса «вручную» составленное письмо с составным содержимым:

- Соединение с почтовым ретранслятором устанавливается через openssl
- Формируются подложные заголовки письма
- Строка-сепаратор должна указывать, что ее ввел человек, а не почтовый клиент или библиотечная функция
- Помимо текста письмо включает фотографию студента размером не более 100КБ, закодированную base64.
- После поледеней строки-сепаратора указывается ФИО

ПКЗ ТК2. Написать детектирующие правила Snort (smth.rules) для обнаружения пакетов, отправляемых Nmap при сканировании ОС.

- Описание отправляемых Nmap пакеты для сканирования ОС (IPv4): https://nmap.org/book/osdetect-methods.html
- Правила написание правил для Snort: http://manual-snort-org.s3-website-us-east-1.amazonaws.com/node27.html
- ПКЗ ТКЗ. Произвести необходимые настройки прокси-сервера Squid для решения следующих задач:
  - Подмена заголовка User-Agent на Вашу фамилию латиницей при осуществлении запроса к сайту ispras.ru через браузер. Остальные заголовки, которые добавляет Squid должны остаться.
  - Блокировка доступа к сайту ispras.ru при осуществлении запроса к сайту ispras.ru через браузер.

Результат должен быть представлен в виде одной сетевой трассы формата pcap, содержащей все (и только их) - HTTP пакеты между браузером, прокси-сервером и сайтом ispras.ru. Для получения трассы можно воспользоваться фильтрацией по нескольким потокам и протоколу http, а также инструментом склейки трасс.

Список вопросов для индивидуального собеседования на промежуточной аттестации.

1) Безопасность Web. Модели угроз в системе Web-сервер-Web-клиент. Дефекты, приводящие к инъекциям. SQL-инъекции.
2) Объектная модель DOM. Понятие HTTP-сессии. Инъекции JavaScript. Cross Site Scripting (XSS), варианты XSS. Место криптографии в обеспечении безопасности.
3) Основные понятия безопасности. Шифр Вернама. Симметричная и асимметричная схемы шифрования. Блочные шифры: DES, AES. Протокол Диффи-Хеллмана. Цифровая подпись, схема DSA.
4) Понятие о криптографической стойкости. Схема RSA. Код аутентификации сообщения. HMAC (HMAC-SHA1). Понятие об эллиптических кривых, схема ECDSA.
5) Сертификаты и цепочки доверия. Модели инфраструктуры сертификатов. Организация защищённого канала связи на разных уровнях сетевого стека. End-to-End шифрование.
6) SSL/TLS. Понятие шифронабора. Протоколы, входящие в SSL/TLS. Схема рукопожатия: фазы, согласуемые параметры, вычисление сеансовых ключей. Понятие сессии, соединения и их состояний. Сокращённое и повторное рукопожатие. Особенности TLS 1.3.
7) Причины появления NAT. Типы NAT. Входящие пакеты и различными видами NAPT. Проброс портов. Особенности трансляции с различными транс портными протоколами.
8) Обход NAT. Hole Punching. Требования к совместимому с hole punching NAT. Протоколы обхода NAT. Протоколы управления отображением в сетевых шлюзах. IPv6.
9) Понятие защита сети и периметра. Межсетевой. экран, его задачи и особенности размещения. Уровни обработки данных. Атаки на межсетевой экран.
10) Системы защиты от вторжений. Сценарии вторжения и защиты. Приманки (Honeypot). Системы управления формой трафика.
11) Классификация беспроводных сетей. Bluetooth. Mesh. Основные риски в беспроводных сетях.
12) Шифрование данных в беспроводных сетях: WEP, WPA2. Предотвращение вторжений в беспроводных сетях.

13) Понятие частных, виртуальных и логических сетей (VPN). Туннелирование и инкапсуляция. VPN: условия создания, типы подключений, классификация. Протоколы, использующиеся для организации VPN.
14) Протокол IPSec: решаемые задачи, модель угроз, архитектура, режимы подключения. Основные элементы IPSec. Другие VPN-протоколы (OpenVPN и Wireguard). Коммерческие VPN-сервисы: схема использования, риски. Особенности работы VPN-клиента. Уязвимости VPN-сервисов: IPv6 и DNS-утечки.
15) Понятие анонимности пользователя в сети. Идентификаторы пользователя в сети. Прокси-серверы. VPN. Атаки на анонимные сети и способы защиты от них.
16) Анонимные сети. Mix. Tor. Организация скрытых сервисов Tor. Анонимность ОС. Защита от отслеживания признаков HTTP и цифрового отпечатка браузера.
17) Интернет: средство коммутации и хранилище содержимого. Подходы к доставке содержимого. Особенности Интернет-трафика. Закон Ципфа. Подходы к распространению содержимого. Веб-кеширование и его ограничения. CDN. Функции и подходы к использованию.
18) Задачи, решаемые при создании и использовании CDN. Выбор содержимого для реплицирования. Выбор узла и способы перенаправления клиентов. Частичное и полное перенаправление DNS. Классификация CDN, возможности по ускорению сайта. Ограничения и негативные последствия использования.
19) Архитектура сети: «клиент-сервер», p2p. Виды p2p-сетей. Napster. Gnutella. Протокол BitTorrent.
20) Структурированные и неструктурированные p2p-сети. Подходы к организации поиска данных в p2p-сети. DHT. Chord: таблицы маршрутизации, добавление/удаление узлов. Pastry. Вопросы безопасности p2p-сетй.
21) Модель угроз STRIDE. Классификация DDoS-атак. Атаки на канальном уровне. Ботнет. Организация атак с использованием IoT-устройств.
22) Оценка риска угроз DREAD. Атаки уровня TCP/IP. Атаки уровня приложений. Протокол QUIC. Смягчение DDoS-атак.
23) Типы приложений. Особенности TCP/UDP. Цифровой звук: восприятие, передача, кодирование, сжатие. Теорема Котельникова. Цифровое видео: терминология, виды кадров, особенности передачи, сжатие кадра, сжатие видеоряда.
24) Потоковое вещание. Последовательная загрузка, буферизация, недостатки. Вещание в реальном времени. Потоковый протокол RTSP. HTTP-стриминг. IP-телефония. Протоколы RTP и SIP. Поиск пользователя. Подходы к коррекции ошибок при потере пакетов.

Методические материалы для проведения процедур оценивания результатов обучения

Оценка по курсу состоит из оценки за выполнение совокупности практических работ (40 баллов) - по 16 баллов за первую и последнюю работы и 8 баллов за вторую работу и оценки за итоговый устный экзамен (60 баллов). Итоговая сумма, таким образом, находится в диапазоне от 0 до 100 баллов. Оценка «отлично» выставляется от 81 балла и выше. Оценка «хорошо» выставляется при сумме от 61 до 80 баллов. Оценка «удовлетворительно» выставляется при сумме от 41 до 60 баллов. Итоговая сумма баллов, меньшая или равная 40, соответствует оценке «неудовлетворительно».