Белорусский государственный университет

УТВЕРЖДАЮ
Проректор по учебной работе и образовательным инновациям
_____ О.И. Чуприс
«___» _____ 2019 г.

Регистрационный № УД-7074/уч.

Научный семинар «Актуальные проблемы обеспечения защиты информации»

Учебная программа учреждения высшего образования по учебной дисциплине для специальности:

1-31 80 07 Радиофизика

Профилизации:
Компьютерная безопасность

2019 г.

Учебная программа составлена на основе ОСВО 1-31 80 07 – 2019 и учебного плана G31-044/ уч. от 11.04.2019 г.

СОСТАВИТЕЛИ:

Василий Сергеевич САДОВ, профессор кафедры интеллектуальных систем, факультет радиофизики и компьютерных технологий, Белорусский государственный университет, кандидат технических наук, доцент;

Екатерина Александровна ГОЛОВАТАЯ, старший преподаватель кафедры интеллектуальных систем, факультет радиофизики и компьютерных технологий, Белорусский государственный университет;

Николай Николаевич ЩЕТЬКО, старший преподаватель кафедры интеллектуальных, факультет радиофизики и компьютерных технологий, Белорусский государственный университет;

РЕЦЕНЗЕНТ:

Анатолий Владимирович ГУЛАЙ, заведующий кафедрой интеллектуальных и мехатронных систем, Белорусский национальный технический университет, кандидат технических наук, доцент

РЕКОМЕНДОВАНА К УТВЕРЖДЕНИЮ:

Кафедрой интеллектуальных систем факультета радиофизики и компьютерных технологий Белорусского государственного университета (протокол № 17 от 04.06.2019);

Научно-методическим Советом БГУ

(протокол № 5 от 28.06.2019)

Зав.кафедрой _____ Козлова Е.И.

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Цели и задачи учебной дисциплины

Цель учебной дисциплины – систематизация и углубление знаний в области обеспечения информационной безопасности в различных прикладных аспектах аппаратной, программной и сетевой составляющей информационных систем.

Задачи учебной дисциплины:

1. Сформировать представление о современных прикладных задачах информационной безопасности.
2. Предоставить актуальные сведения о различных видах угроз и атак.
3. Рассмотреть прикладные аспекты обеспечения безопасности в сложных информационных системах.

Место учебной дисциплины в системе подготовки специалиста с высшим образованием (магистра).

Учебная дисциплина относится к модулю «Научно-исследовательская работа» компонента учреждения высшего образования.

Связи с другими учебными дисциплинами, включая учебные дисциплины компонента учреждения высшего образования, дисциплины специализации и др.

Для успешного усвоения данной учебной дисциплины необходимы знания по дисциплинам «Компьютерные сети», «Архитектура компьютеров», «Операционные системы», «Основы информационной безопасности».

Требования к компетенциям

Освоение учебной дисциплины «Научный семинар «Актуальные проблемы обеспечения защиты информации»» должно обеспечить формирование следующих академических, социально-личностных и профессиональных компетенций:

- УК-1. Быть способным применять методы научного познания (анализ, сопоставление, систематизация, абстрагирование, моделирование, проверка достоверности данных, принятие решений и др.) в самостоятельной исследовательской деятельности, генерировать и реализовывать инновационные идеи;
- УК-2. Владеть навыками планирования и проведения экспериментальных исследований, быть способным проводить исследования с использованием современного научно-технического оборудования и приборов.

В результате освоения учебной дисциплины студент должен:

знать:

- основные задачи обеспечения информационной безопасности;
- теоретические основы работы методов обеспечения аппаратной, программной и сетевой информационной безопасности;
- особенности проектирования информационных систем с учетом возможных угроз информационной безопасности;

уметь:

- проводить комплексный анализ информационных систем для выявления потенциальных угроз информационной безопасности;
- корректно выбирать политику безопасности в рамках информационной системы в соответствии с возможными направлениями атак;
- оперативно устранять типовые угрозы информационной безопасности в случае их обнаружения;

владеть:

- методами поиска типовых уязвимостей в информационных системах;
- аппаратными, программными и сетевыми средствами аудита и обеспечения информационной безопасности.

Структура учебной дисциплины

Дисциплина изучается в 1 и 2 семестрах. Всего на изучение учебной дисциплины «Научный семинар «Актуальные проблемы обеспечения защиты информации»» отведено:

– для очной формы получения высшего образования – 216 часов, в том числе 72 аудиторных часа, из них: семинарские занятия – 72 часа.

Трудоемкость учебной дисциплины составляет 6 зачетных единиц.

Форма текущей аттестации в 1 семестре – зачет. Форма текущей аттестации в 2 семестре – зачет.

СОДЕРЖАНИЕ УЧЕБНОГО МАТЕРИАЛА

Раздел 1. Безопасность и устойчивость информационных систем

Тема 1.1. Оценка устойчивости информационных систем к атакам. Методы превентивного взлома. Модели политик безопасности и аудита. Социальная инженерия.

Тема 1.2. Поиск уязвимостей в локальных сетях. Типовые атаки на фаерволы в межсетевом взаимодействии. Атаки распределенного отказа от обслуживания с использованием сетей ботов.

Тема 1.3. Безопасность распределенных систем на базе блокчейна, одноранговых и туманных технологий. Проблемы доступа к данным в распределенных системах.

Раздел 2. Информационная безопасность облачных систем

Тема 2.1. Архитектура типовой облачной системы. Безопасность и аудит систем администрирования. Вектора атаки на информационные системы и провайдеров в облаке.

Тема 2.2. Хранение данных в облачных системах. Безопасность доступа к хранилищам данных с шардингом и репликацией. Работа с персональными данными в облаке.

Тема 2.3. Виртуализация как средство изоляции исполняемого кода в облачной среде. Атаки «выхода из песочницы».

Тема 2.4. Информационная безопасность при использовании средств облачной контейнеризации и оркестрации на примере Docker и Kubernetes.

Тема 2.5. Клиент-серверная безопасность веб-приложений. Протокол HTTPS и центральная сертификация. Типовые атаки на веб-приложения.

Раздел 3. Безопасность мобильных устройств и интернета вещей

Тема 3.1. Архитектура систем на базе мобильных устройств. Изоляция приложений. Безопасность передачи данных в сотовых сетях.

Тема 3.2. Безопасность распределенного взаимодействия на базе физических каналов связи. Атаки на каналы цифровой передачи данных в радиочастотном диапазоне.

Тема 3.3. Архитектуры и вектора атаки в системах интернета вещей. Атаки на аппаратные средства поддержки криптографии. Атаки имперсонации.

Раздел 4. Безопасность аппаратных и программных алгоритмов обеспечения информационной безопасности

Тема 4.1. Шифрование и хеширование в каналах передачи данных на базе программных средств. Принцип Керкгоффса. Атаки дней рождения.

Тема 4.2. Генераторы случайных и псевдослучайных чисел и их криптографическая устойчивость. Программная и аппаратная реализация. Вектора атак на генераторы. Динамический хаос.

Тема 4.3. Атаки на методы шифрования и хеширования. Типичные уязвимости в симметричных и ассиметричных системах шифрования. Квантовые алгоритмы для атак на хеш-функции и алгоритмы шифрования.

УЧЕБНО-МЕТОДИЧЕСКАЯ КАРТА УЧЕБНОЙ ДИСЦИПЛИНЫ

Дневная форма получения образования с применением дистанционных образовательных технологий

Номер раздела, темы	Название раздела, темы	Количество аудиторных часов					Количество часов УСР	Форма контроля знаний
		Лекции	Практические занятия	Семинарские занятия	Лабораторные занятия	Иное		
1	2	3	4	5	6	7	8	9
1	**Безопасность и устойчивость информационных систем**			**16**				
1.1	Оценка устойчивости информационных систем к атакам. Методы превентивного взлома. Модели политик безопасности и аудита. Социальная инженерия.			4				отчет
1.2	Поиск уязвимостей в локальных сетях. Типовые атаки на фаерволы в межсетевом взаимодействии. Атаки распределенного отказа от обслуживания с использованием сетей ботов.			6				презентация
1.3	Безопасность распределенных систем на базе блокчейна, одноранговых и туманных технологий. Проблемы доступа к данным в распределенных системах.			6				реферат
2	**Информационная безопасность облачных систем**			**26**				
2.1	Архитектура типовой облачной системы. Безопасность и аудит систем администрирования. Вектора атаки на информационные системы и провайдеров в облаке.			4				проект
2.2	Хранение данных в облачных системах. Безопасность доступа к хранилищам данных с шардингом и репликацией. Работа с персональными данными в облаке.			4				тест

2.3	Виртуализация как средство изоляции исполняемого кода в облачной среде. Атаки «выхода из песочницы».			6				реферат
2.4	Информационная безопасность при использовании средств облачной контейнеризации и оркестрации на примере Docker и Kubernetes.			6				реферат
2.5	Клиент-серверная безопасность веб-приложений. Протокол HTTPS и центральная сертификация. Типовые атаки на веб-приложения.			6				реферат
3	**Безопасность мобильных устройств и интернета вещей**			**14**				
3.1	Архитектура систем на базе мобильных устройств. Изоляция приложений. Безопасность передачи данных в сотовых сетях.			4				презентация
3.2	Безопасность распределенного взаимодействия на базе физических каналов связи. Атаки на каналы цифровой передачи данных в радиочастотном диапазоне.			6				презентация
3.3	Архитектуры и вектора атаки в системах интернета вещей. Атаки на аппаратные средства поддержки криптографии. Атаки имперсонации.			4				тест
4	**Безопасность аппаратных и программных алгоритмов обеспечения информационной безопасности**			**16**				
4.1	Шифрование и хеширование в каналах передачи данных на базе программных средств. Принцип Керкгоффса. Атаки дней рождения.			4				презентация
4.2	Генераторы случайных и псевдослучайных чисел и их криптографическая устойчивость. Программная и аппаратная реализация. Вектора атак на генераторы. Динамический хаос.			6				реферат
4.3	Атаки на методы шифрования и хеширования. Типичные уязвимости в симметричных и ассиметричных системах шифрования. Квантовые алгоритмы для атак на хеш-функции и алгоритмы шифрования.			6				презентация

ИНФОРМАЦИОННО-МЕТОДИЧЕСКАЯ ЧАСТЬ

Перечень основной литературы

1. Andress, J. Building a Practical Information Security Program / J. Andress, M. Leary // Syngress, 1st ed.: ISBN-10: 9780128020425., – 2016, – 202 p.

2. Нестеров, С. А. Основы информационной безопасности. Учебное пособие / С. А. Нестеров // 2-е издание, стереотипное., СПб: Лань, – 2016, – 324 с.

3. Bhunia, S. Hardware Security: A Hands-on Learning Approach / S. Bhunia, T. Mark // Morgan Kaufmann: 1st ed.: ISBN-10: 0128124776., – 2018, – 526 p.

4. Таненбаум, Э. Компьютерные сети / Э. Таненбаум // 5-е издание., СПб: Питер – «Классика Computer Science», – 2019, – 960 с.

5. Бирюков, А. А. Информационная безопасность: защита и нападение / А. А. Бирюков // 2-е издание., М.: ДМК Пресс, – 2017, – 434 с.

Перечень дополнительной литературы

1. Ferguson, N. Cryptography Engineering: Design Principles and Practical Applications / N. Ferguson, B. Schneier, T. Kohno // ISBN: 978-0470474242., John Wiley & Sons, – 2010, – 384 p.

2. White, A. J. Blue Team Field Manual / A. J. White, B. Clark // CreateSpace Independent Publishing Platform, – 2017, – 134 p.

3. Harper, A. Gray Hat Hacking: The Ethical Hacker's Handbook / A. Harper, D. Regalado, R. Linn, et. al. // 5th edition: McGraw-Hill Education, – 2018, – 640 p.

4. Hadnagy, C. Social Engineering: The Art of Human Hacking / C. Hadnagy, P. Wilson // Wiley, – 2014, – 416 p.

5. Rosner, G. Privacy and the Internet of Things / G. Rosner // O'Reilly Media, – 2016.

6. Marsh, N. Nmap 6 Cookbok: The Fat Free Guide to Network Security Scanning / N. Marsh // 6th edition: CreateSpace Independent Publishing Platform, – 2015, – 226 p.

Перечень рекомендуемых средств диагностики и методика формирования итоговой оценки

Оценка за ответы на семинарских занятиях включает в себя полноту ответа, наличие аргументов, примеров из практики и т.д.

При оценивании реферата и презентации обращается внимание на: содержание и полноту раскрытия темы, структуру и последовательность изложения, источники и их интерпретацию, корректность оформления и т.д.

Формой итоговой аттестации по дисциплине «Научный семинар «Актуальные проблемы обеспечения защиты информации»» учебным планом предусмотрен зачет.

При формировании итоговой оценки используется рейтинговая оценка знаний студента, дающая возможность проследить и оценить динамику процесса достижения целей обучения. Рейтинговая оценка предусматривает использование весовых коэффициентов для текущего контроля знаний и текущей аттестации студентов по дисциплине.

Весовые коэффициенты, определяющие вклад текущего контроля знаний и текущей аттестации в рейтинговую оценку:

Формирование оценки за текущую успеваемость:

- ответы на семинарских занятиях – 40%;
- подготовка презентаций и рефератов – 20%;
- выполнение тестов – 40 %.

Описание инновационных подходов и методов к преподаванию учебной дисциплины (эвристический, проективный, практико-ориентированный)

При организации образовательного процесса используется практико-ориентированный подход, который предполагает:

- освоение содержания образования через решения практических задач;
- приобретение навыков эффективного выполнения разных видов профессиональной деятельности;
- ориентацию на генерирование идей, реализацию групповых студенческих проектов, развитие предпринимательской культуры;
- использованию процедур, способов оценивания, фиксирующих сформированность профессиональных компетенций.

При проведении опросов на семинарах используется метод учебной дискуссии, который предполагает участие студентов в целенаправленном обмене мнениями, идеями для предъявления и/или согласования существующих позиций по определенной проблеме. Использование метода обеспечивает появление нового уровня понимания изучаемой темы, применение знаний (теорий, концепций) при решении проблем, определение способов их решения.

Методические рекомендации по организации самостоятельной работы обучающихся

При изучении учебной дисциплины рекомендуется использовать следующие формы самостоятельной работы:

– поиск (подбор) и обзор литературы и электронных источников по индивидуально заданной проблеме курса;

– изучение материала, вынесенного на самостоятельную проработку;

– подготовка к практическим семинарским занятиям;

– подготовка к зачету;

– научно-исследовательские работы;

– анализ статистических и фактических материалов по заданной теме;

– подготовка и написание рефератов и презентаций на заданные темы;

– подготовка к участию в конференциях и конкурсах.

Темы реферативных работ

1. Безопасность распределенных вычислений и распределенных хранилищ данных. Массированные атаки на одноранговые информационные системы. Атаки на методы установления консенсуса в распределенных журналах транзакций блокчейн-систем.
2. Основные аспекты обеспечения аппаратной информационной безопасности в облаке. Модели защиты памяти и изоляции процессов. Атаки на защищенную память. Атаки на программное окружение, направленные на выход из «песочницы». Типичные уязвимости систем облачной оркестрации.
3. Атаки на веб-приложения: XSS, повтор запросов, перехват меток авторизации. Безопасность делегирования аутентификации и авторизации при использовании OAuth и OpenID Connect.
4. Криптографические и стеганографические методы защиты информации в каналах передачи данных.

Примерный перечень вопросов к зачету

1. Конфиденциальность, целостность и доступность как составляющие информационной безопасности. Методы анализа и поиска уязвимостей в информационных системах.
2. Обеспечение информационной безопасности локальных сетей. Методы реализации распределенного отказа от обслуживания.
3. Безопасность распределенных систем и хранилищ данных.
4. Архитектура облачной системы. Основные направления атаки.
5. Защита данных в облачных системах.
6. Изоляция исполняемого кода в облачных системах. Виртуализация и контейнеризация. Атаки на хост-машину.
7. Безопасность средств виртуализации, контейнеризации и оркестрации.
8. Безопасность веб-приложений. Типовые методы атак на веб-приложения.
9. Безопасность мобильных устройств.
10. Безопасность радиочастотной цифровой передачи с использованием различных протоколов.
11. Безопасность систем интернета вещей.
12. Основные положения шифрования и хеширования. Криптографические хэш-функции и электронные цифровые подписи в защите информации.
13. Криптографически стойкая генерация случайных и псевдослучайных последовательностей.
14. Квантовые алгоритмы атаки на криптографические примитивы и алгоритмы хеширования и шифрования.

ПРОТОКОЛ СОГЛАСОВАНИЯ УЧЕБНОЙ ПРОГРАММЫ УВО

Название учебной дисциплины, с которой требуется согласование	Название кафедры	Предложения об изменениях в содержании учебной программы учреждения высшего образования по учебной дисциплине	Решение, принятое кафедрой, разработавшей учебную программу (с указанием даты и номера протокола)
Информационная безопасность и системы защиты информации	Телекоммуникаций и информационных технологий	Внести рассмотрение вопросов безопасности канала связи пользователя с облачным хранилищем данных.	Внести дополнения в программу курса (протокол № 17 от 04.06.2019).

ДОПОЛНЕНИЯ И ИЗМЕНЕНИЯ К УЧЕБНОЙ ПРОГРАММЕ ПО ИЗУЧАЕМОЙ УЧЕБНОЙ ДИСЦИПЛИНЕ

на _____/_____ учебный год

№ п/п	Дополнения и изменения	Основание

Учебная программа пересмотрена и одобрена на заседании кафедры
_____ (протокол № ____ от _____ 201_ г.)

Заведующий кафедрой

_____ _____ _____

УТВЕРЖДАЮ
Декан факультета

_____ _____ _____