Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего профессионального образования
«Липецкий государственный педагогический университет»

Образовательная программа

Направление: 10.06.01 Информационная безопасность
Профиль: Методы и системы защиты информации, информационная безопасность
Квалификация: Исследователь. Преподаватель-исследователь
Форма обучения: очная
Срок обучения: 4 года

Год начала подготовки: 2014 г.

Аннотация рабочей программы дисциплины
Компьютерные вредоносные программы

1. Цель дисциплины:

Целью изучения курса является овладение обучаемыми целостной системой знаний, необходимых для понимания роли и места информационной безопасности в системе национальной безопасности Российской Федерации, уяснения основных методов и средств обеспечения информационной безопасности государства и его информационной инфраструктуры.

Изучение дисциплины «Компьютерные вредоносные программы» должно развивать творческий подход при решении сложных научно-технических задач, связанных с обеспечением информационной безопасности государства и его информационной инфраструктуры; способствовать развитию профессиональной культуры, формированию научного мировоззрения и развитию системного мышления; прививать стремление к поиску оптимальных, простых и надежных решении; способствовать расширению кругозора.

2.Место дисциплины в структуре ООП

Дисциплина «Компьютерные вредоносные программы» относится к Блоку вариативной части основной образовательной программы (ООП) аспирантуры и является дисциплиной по выбору обучающихся. Одна из основных задач курса – подготовка обучаемых к последующей успешной сдаче кандидатского экзамена по специальности в рамках выбранного направления подготовки.

3. Требования к результатам освоения дисциплины:

Дисциплина «Компьютерные вредоносные программы» обеспечивает овладение следующими компетенциями:

Коды компетенций	**Результаты освоения ООП** *(Содержание компетенций)*	**Перечень планируемых результатов обучения по дисциплине**
ОПК-1	способностью формулировать научные задачи в области обеспечения информационной безопасности, применять для их решения методологии теоретических и	Знать: – методы и средства обеспечения безопасности операционных систем от вредоносных программ; – методы и средства обеспечения сетевой безопасности;

	экспериментальных научных исследований, внедрять полученные результаты в практическую деятельность	– современные подходы к предотвращению НСД вредоносных программ;
		Уметь: – выбирать структурные элементы системы обеспечения защиты от вредоносных программ; – обосновывать принципы организации технического, программного информационного обеспечения защиты;
		Владеть: – навыками настройки подсистем защиты от вредоносного программного обеспечения; – навыками противодействия конкретным вирусным угрозам;
ОПК-3	способностью обоснованно оценивать степень соответствия защищаемых объектов информатизации и информационных систем действующим стандартам в области информационной безопасности	Знать: – действующие стандарты в области информационной безопасности; – методы оценки степени соответствия защищаемых объектов информатизации и информационных систем стандартам в области информационной безопасности.
		Уметь: – оценивать степень соответствия защищаемых объектов информатизации действующим стандартам в области информационной безопасности; – обосновывать оценку соответствия, опираясь на знание действующих стандартов в области информационной безопасности.
		Владеть: – навыками оценивания информационных систем на соответствие стандартам информационной безопасности; – навыками оценивания объектов информатизации на соответствие стандартам информационной безопасности.
ПК-1	способность анализировать фундаментальные и прикладные проблемы информационной безопасности в условиях становления современного информационного общества	Знать: – современные фундаментальные проблемы информационной безопасности; – современные методы анализа проблем информационной безопасности; – современные подходы к решению прикладных проблем информационной безопасности;
		Уметь: – анализировать угрозы информационной безопасности объектов в условиях современного информационного общества; – анализировать направления развития информационно-коммуникационных

		технологий объекта защиты, прогнозировать эффективность функционирования систем информационной безопасности, – оценивать затраты и риски, формировать стратегию создания систем информационной безопасности в соответствии со стратегией становления современного информационного общества.
		Владеть: – навыками анализа эффективности функционирования систем информационной безопасности; – навыками анализа угроз информационной безопасности объектов.
ПК-2	владеть методами и организационными, техническими и аппаратно-программными средствами защиты систем (объектов) информатизации	Знать: – методы защиты систем (объектов) информатизации; – организационные средства обеспечения защиты систем информатизации от вредоносных программ; – технические средства обеспечения защиты объектов информатизации; – программные средства обеспечения защиты систем информатизации.
		Уметь: – обоснованно применять организационные, технические, программные средства обеспечения защиты систем информатизации;
		Владеть: – навыками организации защиты информационных объектов; – навыками использования аппаратно-программных средств защиты; – навыками управления техническими средствами защиты систем информатизации.

4. Общая трудоемкость дисциплины составляет зачетные единицы (часа).
Общая трудоемкость дисциплины составляет 8 зачетных единиц (288 часов).
В том числе контактная работа 80 часов. Из них:
– аудиторная: 72 ч.; самостоятельная работа: 209 ч. КСР: 7,4 ч.

5. Семестры:

Семестр	Трудоемкость	Контроль

	Зач. ед.	Часов всего	Контактная работа	Лекции		Практ. груп. и семинары		Прак.мал.гр. и лаб. занятия		Индивид. занятия		Самостоятельная работа	Контрольные работы	Зачет, зачет с оценкой, экзамен	Курсовые работы
				Ауд.	КСР	Ауд.	КСР	Ауд.	КСР	Ауд.	КСР				
6	4	144	39	18		18	2,7				0,2	105		З	
7	4	144	41	18		18	4,2				0,3	104		Э	

*З – зачет, Э – экзамен

6. Основные разделы дисциплины:

№ п/п	Наименование раздела дисциплины	Содержание раздела (дидактические единицы)
1	Виды и классификация вредоносного программного обеспечения	Виды вредоносного ПО и их классификация. Механизмы защиты операционной системы. Угрозы безопасности операционной системы.
2	Технологии обеспечения информационной безопасности объектов от вредоносного программного обеспечения	Типовые угрозы сетевой безопасности. Сетевые атаки. Стадии проведения сетевой атаки. Классификации сетевых угроз, уязвимостей и атак. Примеры типичных сетевых атак. Механизмы реализации атак в сетях TCP/IP. Удаленное определение версии ОС. Методы сканирования портов. Методы обнаружения пакетных сниферов. Методы перехвата сетевых соединений в сетях TCP/IP. Десинхронизация TCP-соединений. Атаки, направленные на маршрутизаторы. Несанкционированный обмен данными. Технические меры защиты от сетевых атак. Методы и средства обеспечения информационной безопасности в вычислительных сетях. Виртуальные частные сети (VPN). Организация туннелирования на различных уровнях модели ISO/OSI. Достоинства и недостатки применения VPN. Протокол IPSEC. Использование протокола PPTP для организации виртуальных частных сетей. Криптографические протоколы аутентификации. Разработка защищенных сетевых приложений. Средства защиты локальных сетей при подключении к Интернет. Межсетевые экраны (МЭ). Основные возможности и схемы развертывания МЭ. Построение правил фильтрации. Методы сетевой трансляции адресов (NAT). Методы обхода межсетевых экранов. Системы обнаружения вторжений (СОВ). Средства обнаружения

		уязвимостей сетевых служб. Способы противодействия вторжениям. Системы виртуальных ловушек (Honey Pot и Padded Cell).
3	Управление программным комплексом направленного на отражение атак вредоносного ПО	Основные программные комплексы против вредоносного ПО. Спецификация комплексов. Антивирусы и принципы защиты.

7. Автор(ы) (ФИО, должность, ученое звание):
д.т.н., проф. Малыш В.Н, к.ф-м.н., доцент Мицук С.В.