

АННОТАЦИЯ ПРОГРАММЫ МАГИСТРАТУРЫ «Центры обнаружения и предотвращения компьютерных атак»

Направление подготовки: 10.04.01 «Информационная безопасность».

Язык обучения: русский.

Срок обучения: 2 года.

Форма обучения: очная, с применением электронного обучения и дистанционных образовательных технологий.

Цели программы: подготовка магистров, способных успешно работать в сфере деятельности, связанной с проектированием, внедрением и эксплуатацией центров обнаружения и предотвращения компьютерных атак (ЦОПКА), обеспечивающих сетевую безопасность информационно-телекоммуникационных сетей (ИТКС) организаций высокотехнологических областей, с обеспечением киберустойчивости таких объектов в условиях существования угроз в информационной сфере, анализом и оценкой уровня информационной безопасности, а также реагированием на компьютерные инциденты и их предотвращением. В результате освоения программы выпускник получает набор универсальных, общепрофессиональных и профессиональных компетенций для решения проектных, научно-исследовательских и организационно-управленческих задач профессиональной деятельности.

Выпускающая кафедра: «Информационная безопасность банковских систем» (№ 44)

Объекты профессиональной деятельности: ИТКС организаций, являющиеся объектами критической информационной структуры (КИИ) Российской Федерации и осуществляющие непрерывную обработку потоков данных, требующую обеспечения сетевой безопасности и реагирования на компьютерные инциденты в них.

Особенности учебного плана: программа позволяет обучающимся приобрести актуальные, востребованные на современном рынке труда знания и практические навыки, и овладеть методами стратегического управления и анализа на основе уверенного владения информационными технологиями и аналитическими методами, развивает у них деловые качества, умение мыслить логически и стратегически, принимать эффективные управленческие решения, что способствует карьерному росту и необходимо для занятия лидирующих позиций в сфере обеспечения информационной безопасности объектов КИИ.

Для этого в обучении применяются такие образовательные технологии как вебинары, электронные образовательные курсы, моделирование реальных ситуаций и решение бизнес-задач от партнеров.

В процессе освоения программы студенты изучают авторские дисциплины, впервые разработанные и опробованные в НИЯУ МИФИ, ориентированные на неудовлетворенный спрос работодателей. Это обязательные дисциплины «Методология обеспечения информационной безопасности», «Управление информационной безопасностью», «Современные информационные технологии и аналитические методы», «Защищенные информационные системы», «Безопасность вычислительных сетей», «Технологии обеспечения информационной безопасности объектов», «Управление уязвимостями», «Управления рисками информационной безопасности», «Проверка и оценка деятельности по управлению информационной безопасностью», «Поиск информации по открытым источникам», «Предотвращение утечки конфиденциальной информации» и дисциплины по выбору: 1) «Управление компьютерными инцидентами» (по выбору в финансовой сфере); 2) «Управление функциональной устойчивостью объектов» / «Управление операционной надежностью объектов»; 3) «Построение центров обнаружения и предотвращения компьютерных атак» (по выбору в финансовой сфере).

Практические занятия по специальным дисциплинам реализуются на современном лабораторном оборудовании и программном обеспечении.

Выпускники могут продолжить образование в аспирантуре.

Перечень предприятий для прохождения практики и трудоустройства выпускников: НИЯУ МИФИ, ФСТЭК России, НКЦКИ, ПАО «Ростелеком», Банк России, ПАО Сбербанк, Банк ГПБ (АО), АО «Российский сельскохозяйственный банк», Тинькофф, АО «Позитив Технолоджис», F.A.C.C.T., UserGate, R-Vision, ООО «Интеллектуальная безопасность», VI.ZONE, Angara SOC, IZ:SOC и т.п.

Наши партнеры: АО «Позитив Технолоджис», ООО «Интеллектуальная безопасность», ООО «СерчИнформ».

Руководитель программы: профессор кафедры 44 НИЯУ МИФИ Милославская Наталья Георгиевна, д.т.н., PhD in Cyber Security (Plymouth University, UK), доцент.