Федеральное государственное автономное образовательное учреждение высшего профессионального образования

Национальный исследовательский ядерный университет «МИФИ»

Факультет «Кибернетика и информационная безопасность»

Межкафедральный учебно-научный центр информационной безопасности

предлагают Вашему вниманию

программы высшего профессионального образования, профессиональной переподготовки и повышения квалификации по направлению подготовки

«Информационная безопасность»

Уважаемые коллеги! В соответствии с «Положением о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств…», утвержденным Постановлением Правительства РФ № 313 от 16 апреля 2012 г., при осуществлении лицензионной деятельности выдвигаются квалификационные требования к штатному персоналу соискателя лицензии.

Для осуществления деятельности, связанной с разработкой, модернизацией и ремонтом криптографических средств и средств изготовления ключевых документов	*– высшее профессиональное образование или переподготовка с нормативным сроком свыше 1000 ауд. часов по направлению «Информационная безопасность»*
Для осуществления деятельности, связанной с разработкой, производством, монтажом, эксплуатацией информационно-телекоммуникационных систем, защищенных криптографическими средствами, а также с предоставлением потребителям защищенных каналов связи и изготовлением ключевых документов	*– высшее профессиональное образование или переподготовка с нормативным сроком свыше 500 ауд. часов по направлению «Информационная безопасность»*
Для осуществления деятельности, связанной с распространением (продажей, передачей) криптографических средств и средств изготовления ключевых документов	*– высшее профессиональное образование или переподготовка с нормативным сроком свыше 100 ауд. часов по направлению «Информационная безопасность»*

Учебно-научный центр реализует на базе кафедр «Информационная безопасность банковских систем», «Криптология и дискретная математика», «Стратегические информационные исследования» следующие учебные программы, отвечающие требованиям «Положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств…»:

- **программу профессиональной переподготовки по направлению подготовки 090900 – «Информационная безопасность автоматизированных систем» «Криптографические методы и средства защиты информации в информационно-телекоммуникационных системах» объёмом 520 ауд. часов;**
- **комплекс программ длительного повышения квалификации объёмом 104 ауд. часа каждая.**

На обучение по всем программам профессиональной переподготовки и повышения квалификации принимаются лица, имеющие диплом о высшем образовании (квалификация «специалист», «бакалавр» или «магистр»).

По окончании программ переподготовки и курсов повышения квалификации выдаются свидетельства государственного образца.

Неизменно высокое качество обучения на факультете «Кибернетика и информационная безопасность» НИЯУ МИФИ обеспечивается:

- **многолетним (с 1992 г.) опытом преподавания основ информационной безопасности, криптографии, программно-аппаратных методов обеспечения информационной безопасности;**
- **сильным профессорско-преподавательским составом, значительную часть которого составляют доктора, кандидаты наук, преподаватели, имеющие значительный опыт работы в структурах, связанных с разработкой, внедрением и эксплуатацией средств обеспечения информационной безопасности информационно-телекоммуникационных систем;**
- **наличием основательной лабораторной базы: учебно-методического стенда, включающего в себя лаборатории «Виртуальные частные сети», «Защищенные телекоммуникационные системы», «Безопасность вычислительных сетей», лабораторий для изучения средств криптографической защиты электронных документов, технических методов и средств защиты информации;**
- **широким набором учебно-методической литературы, написанной нашими преподавателями, среди которой широко известные учебники, допущенные Министерством образования и науки РФ и учебно-методическим объединением вузов по информационной безопасности.**

Справки об условиях, сроках и стоимости обучения можно получить по телефонам и эл. почте:

тел. (499) 324-97-35, AITolstoj@mephi.ru – Толстой Александр Иванович, зам. заведующего кафедрой «Информационная безопасность банковских систем»;

тел. (495) 788-56-99, доб. 92-16, APDurakovskiy@mephi.ru – Дураковский Анатолий Петрович, руководитель межкафедрального учебно-научного центра информационной безопасности.

Сайт Национального исследовательского ядерного университета «МИФИ»: www.mephi.ru

Сайт кафедры «Информационная безопасность банковских систем» НИЯУ МИФИ:

kaf44.mephi.edu

Программа профессиональной переподготовки
«Криптографические методы и средства защиты информации в информационно-телекоммуникационных системах»
и программы повышения квалификации:

- **Программы построены по модульному принципу и включают в себя пять образовательных модулей объёмом 104 ауд. часа каждый. Вы можете выбрать для изучения все пять модулей общим объёмом 520 ауд. часов в качестве программы профессиональной переподготовки или любой отдельный модуль объёмом 104 ауд. часа в качестве программы повышения квалификации.**
- **Каждый образовательный модуль предусматривает сбалансированную теоретическую, методическую и практическую подготовку обучающихся, при этом широко используются современные технологии дистанционного и заочного обучения, электронные и мультимедийные учебно-методические средства.**
- **Особенностью наших образовательных программ является то, что мы даём не абстрактные теоретические знания, а ставим целью подготовку наших слушателей к реальной практической деятельности в современном мире: мы работаем не по принципу «Преподаём, что знаем», а по принципу «Знаем, что преподаём».**
- **Мы постоянно работаем над совершенствованием наших образовательных программ.**

Образовательный модуль
«Основы информационной безопасности и криптографической защиты информации»

- *предполагает изучение основополагающих понятий в сфере защиты информации в компьютерных системах, важных для проектировщика, разработчика, эксплуатационщика (стратегии и модели защиты, принципы управления доступом и защиты от несанкционированного доступа, принципы аутентификации, оценка уровня доверия к системе, оценка эффективности защиты и др.);*
- *знакомит с современными концепциями обеспечения информационной безопасности, важными для потребителя информационных услуг и ресурсов (риск, анализ и оценка рисков, управление информационной безопасностью, стандарты и «лучшие практики» в области информационной безопасности;*
- *знакомит с основами организационно-правового и нормативно-технического регулирования деятельности в сфере обеспечения информационной безопасности, знакомит с управленческими и экономическими проблемами выполнения проектов в области информационной безопасности;*
- *дает понятие об основных тенденциях в сфере обеспечения информационной безопасности открытых информационных систем, об управлении информационной безопасностью, об обеспечении непрерывности бизнеса;*
- *делает акцент на основах криптографии как краеугольного камня обеспечения информационной безопасности современных информационно-телекоммуникационных систем (основные понятия криптографии, цели и задачи криптографической защиты, классификация методов криптографической защиты и принципы их функционирования, стандартизация криптографических механизмов, примеры реализации методов криптографии в программно-аппаратных средствах и системах защиты информации).*

Образовательный модуль
«Криптографические методы защиты информации»

- *ставит целью фундаментальное изучение всех основных методов криптографической защиты: симметричных и асимметричных, необходимый для понимания принципов их работы математический аппарат, а также всех российских стандартов по криптографической защите информации;*
- *содержит краткий исторический экскурс в классическую криптографию, ознакомление с принципами устройства самых «красивых» исторических шифров, послужившими основой формирования современной научной криптографии;*
- *предполагает изучение устройства блочных и поточных шифров, режимов их работы, способов генерации случайных и псевдослучайных величин, функций хеширования, схем аутентификации сообщений;*
- *предполагает изучение принципа открытого распределения ключей на примере наиболее известных протоколов, принципов функционирования и примеров реализации схем электронной цифровой подписи, открытого шифрования, совместного применение функций хеширования и цифровой подписи;*
- *знакомит с основными концепциями оценки стойкости криптографических механизмов, включая теоретическо-информационный и теоретико-сложностной подход;*
- *дает представление о методах управления криптографическими ключами, моделях ключевых систем, практических правилах обращения с ключевыми документами.*

Образовательный модуль

«Прикладная криптография. Криптографические протоколы»

- *ставит задачу освоения принципов конструирования и анализа криптографических протоколов для решения широкого спектра задач, стоящих перед создателями средств криптографической защиты информации и защищенных информационно-телекоммуникационных систем;*
- *предполагает изучение методов и протоколов аутентификации, включая аутентификацию по фиксированным и одноразовым паролям, аутентификацию методом «запрос-ответ», аутентификацию на основе доказательств с нулевым разглашением знания, рассмотрение стандартов, в которых применяются эти методы, и практических примеров их реализации;*
- *предполагает изучение методов и протоколов распределения криптографических ключей, включая протоколы транспортировки и обмена ключами, гибридные протоколы, протоколы конференц-связи, протоколы на основе эллиптических кривых и парных отображений;*
- *включает в себя изучение протоколов организации каналов защищенной передачи информации, знакомит с содержанием требований к таким каналам (конфиденциальность, аутентичность) и способами выполнения этих требований;*
- *знакомит со специфическими задачами обеспечения равноправного обмена информацией, обеспечения безопасности электронных платежей, контроля и учета использования ресурсов пользователями, защиты авторских прав на цифровой контент и др., и их решением криптографическими методами.*

Образовательный модуль

«Программно-аппаратные средства криптографической защиты информационно-телекоммуникационных систем»

- *предполагает изучение принципов международной и российской стандартизации в области безопасности информационных технологий, при этом особое внимание уделяется системообразующим стандартам в области криптографической защиты: стандартам ИСО/МЭК, документам серии PKCS, рекомендациям серии RFC;*
- *включает изучение принципов программной реализации криптографических модулей в составе программного обеспечения, интерфейсов криптографических модулей и аппаратно-технических средств поддержки криптографических протоколов (смарт-карт, токенов, защищенных носителей информации), а также критериев оценки их защищенности;*
- *обращает внимание слушателей на основные источники уязвимостей средств криптографической защиты информации, связанные с особенностями реализации криптографических алгоритмов, особенностями управления ключами и паролями, особенностями методов аутентификации, и дает практические советы по недопущению ошибок и устранению «слабостей» реализации;*
- *включает лабораторный практикум по освоению российских средств криптографической защиты информации от ведущих производителей, позволяющих решать основной комплекс задач по защите каналов связи, файлов и баз данных в составе информационно-телекоммуникационных систем.*

Образовательный модуль

«Безопасность банковских технологий. Криптография в банковском деле»

- *включает в себя изучение основ организации и функционирования банковской системы РФ, включая организацию деятельности Центрального банка РФ (Банка России), коммерческих банков, небанковских кредитных организаций, участие их в деятельности международных финансовых организаций и финансовых рынков, услуги кредитных организаций юридическим и физическим лицам;*
- *ставит целью достаточно глубокое изучение современных банковских технологий, в том числе технологий безналичных платежей и расчетов, основ депозитной и кредитной работы коммерческого банка, внутрибанковских технологий (управления ликвидностью, управления рисками, банковского маркетинга и др.);*
- *предполагает глубокое изучение принципов организации и функционирования современных банковских информационных технологий: систем межбанковских расчетов, систем дистанционного банковского обслуживания, систем платежей по банковским картам, банковского электронного документооборота, систем «мгновенных» платежей;*
- *предполагает освоение широкого спектра технологий обеспечения информационной безопасности автоматизированных банковских систем, в том числе технологий управления ключами, развёртывания инфраструктуры открытых ключей, построения виртуальных частных сетей.*

Мы будем рады видеть Вас в числе наших слушателей и надеемся, что наши образовательные услуги помогут Вам в достижении профессиональных высот!